40 Seiten

Abgeordnetenhaus von Berlin Drucksache 9/2277

9. Wahlperiode 17. 12. 84

Mitteilungen des Präsidenten

- Nr. 232 -

Inhaltsübersicht

	Nr.	Seite
Vorlage zur Kenntnisnahme		
gemäß § 26 Abs. 2 Berliner Datenschutzgesetz über **Bericht des Berliner Datenschutzbeauftragten zum 31. Dezember 1984**	115	2

Druckschluß: 16. November 1984, 12.00 Uhr

Ausgegeben am 17. Dezember 1984

Der Präsident
Peter Rebsch

Die Veröffentlichungen des Abgeordnetenhauses sind beim Kulturbuchverlag Berlin, Passauer Straße 4, 1000 Berlin 30, Telefon 2 13 60 71, zu beziehen.

Vorlage zur Kenntnisnahme

Bericht des Berliner Datenschutzbeauftragten zum 31. Dezember 1984

Inhaltsverzeichnis

Der Berliner Datenschutzbeauftragte geht zu Beginn des Jahresberichts 1984[1] auf die Auswirkungen des Volkszählungsurteils des Bundesverfassungsgerichts ein (1). Schwerpunkte des Berichts sind die Ergebnisse der Datenschutzkontrolle und Beratung (2, 3 und 4), die Darstellung neuer Entwicklungen und fortbestehender Probleme zu Feststellungen aus den Vorjahren (5) und die Zusammenarbeit auf dem Gebiet des Datenschutzes (6). Dabei kommt der Berliner Datenschutzbeauftragte unter 3 auch der in § 3 Abs. 3 Zustimmungsgesetz zum Staatsvertrag über Bildschirmtext[2] und in § 55 Abs. 1 Kabelpilotprojektgesetz[3] geregelten Berichtspflicht nach[4]. Ein Stichwortverzeichnis zu diesem und allen seit 1979 erschienenen Jahresberichten schließt den Bericht ab.

1. Zur Situation nach dem Volkszählungsurteil

2. Brennpunkte des Datenschutzes

2.1 Die wachsende Furcht vor der Manipulierbarkeit von Datenverarbeitungssystemen („Hacking" und Computerkriminalität)

Hacking als eine Form des Computermißbrauchs

Andere Fälle von Computermißbrauch

Ergebnis

2.2 Die Unzufriedenheit der Bürger mit der Änderung der Allgemeinen Geschäftsbedingungen des Kreditgewerbes (AGB) zum 1. Januar 1984

Bankauskünfte

Schufa

2.3 Der Umgang mit Gesundheitsdaten

Neue Datenschutzbestimmungen im Landeskrankenhausgesetz (LKG)

Krankengeschichtenverordnung

Vernichtung einer unzulässigen Sammlung der Duplikate von Krebsnachsorgedaten

Bestimmt der Computer, wer behandelt wird?

Pauschale Übermittlung von Patientendaten

Anonymisierung psychiatrischer Daten für Forschung und Planung

Neues Verfahren bei der Kostenübernahme für psychologische Therapien

Vertraulichkeit bei medizinischen Daten

Übermittlung personenbezogener Daten vom Amtsarzt an die Dienstbehörde

2.4 Öffentliche Sicherheit und Strafverfolgung

Die dringende Notwendigkeit der Verbesserung der Rechtsgrundlage für die polizeiliche Informationsverarbeitung

Erhebung und Verwendung von Informationen

Automatische Datenverarbeitung

Überprüfungen im Einzelfall

3. Beobachtungen beim Betrieb von Bildschirmtext und anderen Neuen Medien

3.1 Erfordernis ergänzender bundesrechtlicher Datenschutzregelungen

3.2 Mängel der technischen Ausgestaltung des Btx-Systems

3.3 Mängel, für die Betreiber mitverantwortlich sind

3.4 Mängel auf Seiten der Anbieter

Veröffentlichung personenbezogener Daten im Angebot

Erhebung personenbezogener Daten durch den Anbieter

Andere Anbieteraktivitäten

3.5 Kabelpilotprojekt

4. Weitere Fragen aus der Kontroll- und Beratungspraxis

4.1 Systematische Überprüfungen

Öffentliche Wirtschaftsunternehmen

Sozialleistungsträger

Bezirksämter

Aspekte der Auftragsdatenverarbeitung

4.2 Stellungnahme zu neuen Verfahren

Automatisches Liegenschaftsbuch (ALB)

Lastschrifteneinzugsverfahren

ADV-Grundsätze und ADV-Testrichtlinien

Verarbeitung dienstlicher Daten in der Privatwohnung

Mikrocomputer für Stellenplanung

4.3 Der Umgang mit Personaldaten

Notwendigkeit einer gesetzlichen Regelung

Personalfragebogen

Inhalt von Personalakten

Sachakten

Hilfsakten

Offenbarung von Personaldaten

4.4 Ordnungsaufgaben

Die Beratung des neuen Landesmeldegesetzes

Informationssystem Einwohnerwesen

Fahrzeugregister (ZEVIS)

Anhörungsbogen in Bußgeldverfahren

4.5 Amtliche Statistik

Volkszählung

Mikrozensus 1984

EG-Arbeitskräftestichprobe

Hochschulstatistik

Personalbezügedateien

4.6 Justiz

Anordnung über Mitteilungen in Strafsachen (MiStra)

Anordnung über Mitteilungen in Zivilsachen (MiZi)

Datenschutz in den Prozeßordnungen

[1] Nach § 26 Abs. 2 Berliner Datenschutzgesetz berichtet der Berliner Datenschutzbeauftragte dem Abgeordnetenhaus und dem Regierenden Bürgermeister jährlich.
[2] GVBl. 83, 871
[3] GVBl. 84, 964
[4] 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."

4.7 Vom Umgang mit Sozialdaten
Führung von Sozialdaten
Offenbarung von Sozialdaten an den Petitionsausschuß
Nutzung des Telebusverkehrs durch Schwerbehinderte
Veröffentlichung säumiger unterhaltspflichtiger Personen
Offenbarung von Ausbildungsförderungsdaten
Offenbarung von Sozialdaten für Zwecke der Strafverfolgung
Nachweis der Berechtigung zum Bezug von Leistungen
4.8 Bau- und Wohnungswesen
Kaufpreissammlung
Mietobergrenzensystem

5. Nachtrag zu Feststellungen aus den Vorjahren
Kriminalpolizeiliche personenbezogene Sammlungen (KpS) (Jahresbericht 1981, S. 12, Jahresbericht 1982, S. 11, Jahresbericht 1983, S. 23)
Auskunftsvordruck (Schuldnerverzeichnis) (Jahresbericht 1981, S. 15)
Datei der Taxifahreranmeldungen (Jahresbericht 1981, S. 16)
Schülerdaten (Jahresbericht 1980, S. 13, Jahresbericht 1981, S. 11 f, Jahresbericht 1982, S. 19 f, Jahresbericht 1983, S. 24)
Unbeschränkte Auskünfte aus dem Bundeszentralregister (Jahresbericht 1980, S. 12, Jahresbericht 1981, S. 10, Jahresbericht 1982, S. 20, Jahresbericht 1983, S. 24)
Datenverarbeitung bei der Amerika-Gedenkbibliothek (Jahresbericht 1982, S. 17)
ADV-Verfahren Amts- und Staatsanwaltschaften (ASTA) (Jahresbericht 1983, S. 19 f)

6. Zusammenarbeit mit anderen Stellen
Datenschutzbeauftragte des Bundes und der Länder
Abgeordnetenhaus
Koordination mit der zuständigen Verwaltungsbehörde für Bildschirmtext
Aufsichtsbehörde für nicht-öffentliche Stellen

7. Aufgaben des Berliner Datenschutzbeauftragten
7.1 Im Berichtsjahr 1984
Anrufungen durch jedermann
Beratung und Kontrolle
Öffentlichkeitsarbeit
7.2 Voraussichtliche Schwerpunkte
7.3 Absehbare Entwicklungen

Anlagen:

Anlage 1 Gesetz zur Änderung des Landeskrankenhausgesetzes

Anlage 2 Berliner Grundsätze für den Datenschutz bei den Neuen Medien

Anlage 3 Datenschutz bei der Mikroverfilmung von Schriftgut

Anlage 4 Vorschläge zur Verbesserung des Datenschutzes im Bereich der Familienfürsorge

Anlage 5 Gemeinsames Rundschreiben bei Anträgen auf Gewährung von Verhaltenstherapie

Stichwortverzeichnis

1. Zur Situation nach dem Volkszählungsurteil

Die Aufregung um die Volkszählung hat sich gelegt und es werden die rechtlichen Auswirkungen des Volkszählungsurteils[1] eingehend diskutiert[2]. Das Ergebnis der Diskussion bestätigt meine gegenüber dem Abgeordnetenhaus vertretene Auffassung[2c], wonach der Landesgesetzgeber aufgefordert ist, insbesondere folgende bereichsspezifische Regelungen für den Umgang mit personenbezogenen Daten zu treffen:

Verabschiedung der eingebrachten Beschlußvorlage zum Landesmeldegesetz

Novellierung des Gesetzes über die allgemeine Sicherheit und Ordnung (ASOG)

Gesetzliche Regelung der Landesstatistik in einem Landesstatistikgesetz

Gesetzliche Regelung des Archivwesens in einem Landesarchivgesetz

Weitere gesetzliche Regelung des Umgangs mit medizinischen Daten (Novellierung des Landeskrankenhausgesetzes)

Gesetzliche Regelung des Umgangs mit Personaldaten der öffentlichen Verwaltung (Novellierung des Landesbeamtengesetzes)

Novellierung des Gesetzes über das Landesamt für Verfassungsschutz

Zur näheren Begründung und wegen der Konsequenzen für die Bundesgesetzgebung verweise ich auf die Stellungnahme der Datenschutzbeauftragten und meine eigene Vorlage an das Abgeordnetenhaus.

Unterschiedlicher wird die Frage bewertet, welche Bedeutung die Entscheidung des Bundesverfassungsgerichts für die rechtliche Einordnung des Datenschutzes überhaupt hat. Zweifellos hat das Bundesverfassungsgericht den Datenschutz als den informationellen Aspekt des Persönlichkeitsrechts verfassungsrechtlich bestätigt, es wird jedoch noch einer eingehenden Diskussion bedürfen, wie weit dieses Recht des Einzelnen reicht und wie Konflikte zu lösen sind, die beim Zusammentreffen des informationellen Selbstbestimmungsrechts mit anderen, auch aus den Grundrechten abzuleitenden Rechten und Pflichten auftreten.

Die Forderungen nach bereichsspezifischen Regelungen und juristische Diskussionen über das informationelle Selbstbestimmungsrecht dürfen aber nicht den Kern der Entscheidung des Bundesverfassungsgerichts verdecken: die Notwendigkeit, den Freiraum der Bürger gegen Informationsakte zu schützen. Dies ist die politische Aufgabe vor allem der Parlamente und Regierungen. Sie haben die Vorteile, die das Sammeln von Informationen über den Bürger für Verwaltungen versprechen mag, gegen die Nachteile abzuwägen, die damit für den informationellen Frei-

[1] BVerfG, Urteil vom 15. Dezember 1983 - 1 BvR 209/83 u. a. -, Entscheidungen des Bundesverfassungsgerichts Bd. 65, S. 1 ff

[2] Folgende Stellungnahmen zum Volkszählungsurteil liegen vor:
a) Auswirkungen des Volkszählungsurteils/Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 27./28. März 1984
b) Stellungnahme zu den Auswirkungen des Urteils des Bundesverfassungsgerichts vom 15. Dezember 1983 zum Volkszählungsgesetz 1983 vom 25. April 1984, Der Bundesbeauftragte für den Datenschutz
c) Stellungnahme des Berliner Datenschutzbeauftragten zum Urteil des Bundesverfassungsgerichts zum Volkszählungsgesetz 1983 vom 15. Dezember 1983, Berlin, 29. März 1984 Mitteilungen des Präsidenten - Nr. 188 - Drucksache 9/1711 vom 4. April 1984
d) Das Volkszählungsgesetz - Urteil des Bundesverfassungsgerichts vom 15. Dezember 1983 - Erste Folgerungen -, Der Bundesminister des Innern, 25. April 1984
e) Stellungnahme des Innenministeriums Baden-Württemberg betr. Konsequenzen aus dem Urteil des Bundesverfassungsgerichts zum Volkszählungsgesetz vom 23. August 1984
f) Mitteilung zur Kenntnisnahme des Senats von Berlin über die Auswirkungen der Entscheidung des Bundesverfassungsgerichts vom 15. Dezember 1983 zum Volkszählungsgesetz 1983. Mitteilungen des Präsidenten - Nr. 220 - Drs 9/2056 vom 17. September 1984
g) Das Recht auf informationelle Selbstbestimmung und innere Sicherheit, in: Informationsgesellschaft oder Überwachungsstaat, Hessendienst der Staatskanzlei, Wiesbaden S. 285 ff
h) Bericht der Niedersächsischen Landesregierung, Pressemitteilung des Niedersächsischen Ministers des Innern Nr. 95/84 vom 15. Mai 1984
i) Stellungnahme der Landesregierung Rheinland-Pfalz vom 10. April 1984, Drs 10/101

raum des Bürgers entstehen. Dabei ist zu beachten, daß nach dem Urteil des Bundesverfassungsgerichts nicht nur zu erwartende Verletzungen des Freiraums der Bürger, sondern auch bereits Ängste vor solchen Verletzungen rechtlich relevant werden.

Ein Beispiel hierfür ist sicher das Verbot eines übergreifenden bundeseinheitlichen Personenkennzeichens, ferner die Aufnahme der Seriennummer in das Landesmeldegesetz. Aber auch das immer noch erörterte Projekt zentraler Krebsregister mit einer gesetzlichen Meldepflicht, der maschinenlesbare Personalausweis und das zentrale Verkehrsinformationssystem beim Kraftfahrt-Bundesamt müssen unter diesem Gesichtspunkt diskutiert werden.

Um bei den Bürgern die Überzeugung zu festigen, der Datenschutz werde gewahrt, sind daher politische Entscheidungen erforderlich, mit denen Parlamente und Regierungen Flagge zeigen, indem sie die Interessen von Fachverwaltungen in bestimmten Fällen auch einmal geringer werten als das informationelle Selbstbestimmungsrecht der Bürger. Nach meiner Beurteilung der Stimmungslage in der Bevölkerung bedarf es derartiger Entscheidungen, um den Bürgern das Gefühl zu nehmen, ihr persönlicher Freiraum werde immer stärker eingeengt.

2. Brennpunkte des Datenschutzes

2.1 Die wachsende Furcht vor der Manipulierbarkeit von Datenverarbeitungssystemen („Hacking" und Computerkriminalität)

Mit dem Ansteigen der Anzahl von Kleincomputern in den Privathaushalten, dem Trend zur stärkeren Vernetzung von Rechnern sowie der wachsenden Vielfalt im Angebot von Wählnetzen zur Datenübertragung wächst das Risiko, daß in fremde Rechner eingedrungen wird, sie unbefugt gebraucht oder gar Daten manipuliert und mißbraucht werden.

So haben sich in diesem Jahr - zunächst in den Vereinigten Staaten, dann aber auch in der Bundesrepublik - Berichte über verschiedene, im folgenden dargelegte Formen des Computermißbrauchs gehäuft. Für mich war es angesichts der zum Teil sehr emotional geführten Debatte wichtig, einen guten Überblick über die tatsächlichen Gefahren zu gewinnen, Lösungskonzepte zu erarbeiten, die diesen Gefahren vorbeugen und auf deren Verwirklichung bei den Rechenstellen des Landes hinzuwirken.

Hacking als eine Form des Computermißbrauchs

Eine Form des Computermißbrauchs ist das sogenannte Hacking. Darunter versteht man die unbefugte Nutzung von ADV-Systemen (Zeitdiebstahl) und Datenübertragungsmedien sowie das unbefugte Operieren mit Dateien von außen. Der Datenschutz ist betroffen, wenn personenbezogene Daten auf diese Weise unbefugt abgerufen, geändert oder gelöscht werden. Die scheinbare Mühelosigkeit, mit der Hacker den Berichten zufolge Erfolg bei diesen Aktivitäten hatten, warf zunehmend auch bei besorgten Bürgern die Frage auf, ob die Datenverarbeitung noch hinlänglich sicher sei.

Meine Überprüfung hat folgendes ergeben:

Ein ADV-System kann nur dann von außen angegriffen werden, wenn es selbsttätig über Einrichtungen der Datenfernverarbeitung und -übertragung angesteuert werden kann. Der Hacker benötigt eine Einrichtung, über welche er das anzugreifende ADV-System erreichen kann, am wirkungsvollsten in Verbindung mit einem eigenen Computer.

Als Datenübertragungsmedium kommen alle Kommunikationsnetze in Frage, die zur Übertragung digitaler Signale geeignet sind (Telefonnetz, Kabelnetz, spezielle Datenübertragungsnetze (z. B. DATEX-Netze)) und in denen im Prinzip alle angeschlossenen Partner miteinander kommunizieren können, indem sie durch Wählinformationen den gewünschten Partner anrufen können.

Die **Vorgehensweise** ist in der Regel recht einfach:

Zunächst wird das fremde System über seinen meist bekannten oder leicht in Erfahrung zu bringenden Wählcode (Ruf-Nr.) angewählt, so daß die Datenübertragungsverbindung hergestellt ist. Dann gilt es, die Speicher- und Benutzerkontrollmaßnahmen zu überwinden, die das System als Ganzes, einzelne Verfahren, einzelne Dateien, bestimmte Transaktionen usw. auf dem System schützen. Die Erfolgsaussicht bzw. der Aufwand für diese Überwindung hängt von der Qualität der Kontrollmaßnahmen ab. In der Regel sind die Kontrollen durch Paßwörter realisiert, die die eindringende Person ebenfalls anwenden muß, um sich der jeweiligen Ressourcen bedienen zu können.

Dazu gibt es zwei gängige Methoden:

1. Diese Paßwörter werden durch Probieren gefunden, wobei häufig die Tatsache hilfreich ist, daß für die Wahl des Paßwortes durch den berechtigten Benutzer wenig Phantasie aufgewendet wird und er Begriffe aus seinem Lebensbereich wählt, die von Dritten ausgeforscht werden können (Vornamen, Nachname, Geburtsdaten, Automarke von Angehörigen, Freundinnen oder Freunden usw.). Das Probieren kann ebenfalls rechnerunterstützt ablaufen.
2. Befugte Benutzer bzw. Mitarbeiter des Systembetreibers werden übertölpelt, so daß sie die vertraulichen Codes preisgeben. Im Hacker-Slang wird dieses Vorgehen als „social engineering" bezeichnet.

Ist ein Zugangscode einmal bekannt geworden, so kann er von Mund zu Mund, über Zeitschriften, ja sogar über Datenbanken, die über Wählleitungen erreichbar sind, schnell verbreitet werden.

Je tiefer ein Hacker in die Paßwort-Hierarchie eindringt, desto mehr kann er mit dem System anfangen, etwa

- Rechenzeit benutzen
- eigene Programme und Dateien aufbauen und benutzen
- fremde Dateien und Programmtexte abrufen
- fremde Programme und Dateien benutzen
- fremde Datenbestände und Programme ändern, löschen und ergänzen
- besonders geschützte Dateien (z. B. Paßwort-Dateien) abrufen
- Manipulationen am Betriebssystem vornehmen

Die meisten Fälle werden aus den USA bekannt, da dort folgende Voraussetzungen den Computermißbrauch begünstigen:

- größere Verbreitung von Kleinrechnern in Privathaushalten
- höherer Vernetzungsgrad der ADV-Systeme
- Vielfalt von verschiedenen Wählnetzen
- geringer Sicherheitsstandard dieser Wählnetze
- im Schnitt geringerer Standard technischer Maßnahmen zur Speicher- und Benutzerkontrolle
- im Schnitt geringerer Stellenwert der Ordnungsmäßigkeit der Datenverarbeitung und der Anwendung moderner Programmiermethoden.

Die **Situation in der Bundesrepublik,** speziell auch in Berlin erschwert den Mißbrauch demgegenüber, auch wenn die Verbreitung von Kleinrechnern in Privathaushalten wächst und zunehmend offene Datenverarbeitungsnetze installiert werden:

- Die Wählnetze sind wegen des Postmonopols einheitlich und haben einen relativ hohen Sicherheitsstandard.
- Durch gesetzliche Auflagen werden technisch-organisatorische Maßnahmen zur Speicher-, Benutzer-, Übermittlungs- und Eingabekontrolle realisiert (Nr. 3, 4, 6 und 7 der Anlage zu §5 Berliner Datenschutzgesetz).
- Wegen gesetzlicher Auflagen ist der Stellenwert der Ordnungsmäßigkeit der Datenverarbeitung höher (etwa §§ 145 bis 147 Abgabenordnung mit den Grundsätzen ordnungsgemäßer Speicherbuchführung, §16 Satz 2 Nr. 2 Berliner Datenschutzgesetz).

Rechtlich gilt im Zusammenhang mit personenbezogenen Daten,

- daß die Datenverarbeiter im angemessenen Verhältnis zum Schutzzweck technische und organisatorische Maßnahmen zur Abwehr von Hackern zu treffen haben (§ 5 Abs. 1 Berliner Datenschutzgesetz nebst Anlage, speziell Nr. 3 (Speicherkontrolle), Nr. 5 (Zugriffskontrolle) und Nr. 6 (Übermittlungskontrolle));
- daß Personen, die unbefugt personenbezogene Daten abrufen, sich einer Straftat nach § 28 Berliner Datenschutzgesetz schuldig machen.

Im öffentlichen Bereich Berlins gibt es vorläufig noch relativ wenige Datenfernübertragungswege, die über Wählleitungen laufen.

Konkrete Fälle von erfolgreichem Hacking im Bereich der öffentlichen Verwaltung Berlins sind mir bisher noch nicht bekannt geworden. Ich muß jedoch plausible Hinweise aus der Presse oder aus anonymen Quellen ernstnehmen, wonach auch im öffentlichen Bereich Berlins bereits entsprechende Fälle vorgekommen sind. Gründe dafür habe ich, weil ich bei Prüfungen Schwachstellen festgestellt habe, die den unbefugten Zugriff auf Datenbestände begünstigen und leicht hätten ausgenutzt werden können, weil die vorhandenen technischen Möglichkeiten zur Abwehr solcher Gefahren bei einigen Systemen nicht oder höchst unzureichend genutzt werden, und weil nach meinen Beobachtungen der Umgang mit geheimen Paßwörtern und Berechtigungsausweisen häufig sehr unbekümmert erfolgt. Soweit außerhalb Berlins Fälle bekannt geworden sind, liegen ihre Ursachen in Leichtsinnsfehlern oder Programmunzulänglichkeiten - insbesondere bei den Sicherungsmaßnahmen -, also bei **vermeidbaren** Fehlern. Ich werde daher bei meinen Prüfungen den Risiken bei besonders gefährdeten Systemen verstärkte Aufmerksamkeit widmen.

Gegenmaßnahmen zur Eingrenzung der Risiken stehen zur Verfügung:

- Isolierung der Rechner, d.h. Abbau von Datenfernübertragungseinrichtungen, die, nach Veranlassung von außen, Daten und Programme übertragen können
  (Nachteil: kein Zugriff von außen ohne billigende Aktivität von innen).
- Soweit dies nicht möglich ist:

  Zieldeterminierung der Datenfernübertragungsanwendungen, d. h. Sicherstellung der Adressaten, zumindest der adressierten technischen Schnittstellen durch Abbau aller Wählleitungen zu Gunsten von Standleitungen
  (Nachteil: Mangelnde Flexibilität des Zugriffs, unwirtschaftliche Nutzung des Netzes).
- Soweit auch dies nicht möglich ist:

  Vorbeugende automatisierte Rückrufkontrolle bei Anwählungen durch den Rechner zur sicheren Identifizierung der anwählenden Schnittstelle
  (Nachteil: anwählberechtigte Stelle muß vorher festgelegt sein, daher mangelnde Flexibilität hinsichtlich der Wahl der technischen Schnittstelle).
- Soweit auch dies nicht möglich ist:

  Einsatz differenzierter und umfangreicher Speicher- und Benutzerkontrollsysteme;

  Übermittlungskontrolle durch Rückrufkontrollen nach Abruf der Telefonnummer des Anfragenden im Eingangsdialog und Protokollierung der Nummer;

  Sorgfalt bei der Anwendung dieser Systeme (häufige Änderung von Paßwörtern, Wahl langer Paßwörter, die nicht durch Plausibilitätsbetrachtungen erratbar sind);

  Anwendung moderner Programmierverfahren, um Transparenz auch bei längerer Lebensdauer von Programmen zu erhalten, um Programmnischen und die Ausnutzung von Programmschwächen zu verhindern oder sofort zu erkennen;

  Sorgfältige Dokumentation der Verfahren, insbesondere der Programme, hier insbesondere der Kontrollprogramme.

Andere Fälle von Computermißbrauch

Bei den Hackern ist eher sportlich-spielerischer Ehrgeiz, gepaart mit mangelndem Rechtsbewußtsein das vorherrschende Motiv ihrer Aktivitäten. Kriminelle Motive, d.h. vorsätzlich auf den Schaden der Datenverarbeiter bzw. auf den eigenen finanziellen Nutzen gerichtete Antriebe lassen sich meist nicht erkennen.

Im Gegensatz dazu stehen Aktivitäten und Manipulationen an Computern und Daten, die mit kriminellen Motiven vollzogen werden. Diese Delikte werden im allgemeinen mit dem Begriff „Computerkriminalität" erfaßt. Dieser Begriff wird hier bewußt nicht verwendet, weil die deutschen Strafgesetze diesen Bereich bisher nur unvollständig erfaßt haben.

In Fachkreisen gilt als sicher, daß nur etwa 5 % aller Fälle von Computerkriminalität ganz ohne vorsätzliche Mitwirkung aus dem internen Bereich der betroffenen Organisationen begangen werden. Demgegenüber wird davon ausgegangen, daß in 95 % aller Fälle von Computerkriminalität Mitarbeiter oder frühere Mitarbeiter der Organisation, die noch über interne Kontakte oder Kenntnisse verfügen, bzw. sonstige zum Zutritt befugte Personen die kriminellen Handlungen verüben oder an ihnen beteiligt sind. Motive können neben der Absicht, sich zu bereichern, auch Rache, Mißgunst unter Kollegen oder Antriebe politischer Art sein. Zur Computerkriminalität zählen dabei vor allem Sabotageakte, vorsätzliche Sachbeschädigung, Diebstahl von Datenträgern mit Daten und Programmen, Manipulationen an Daten und Programmen, unbefugter Abruf oder Kopieren von Daten und Programmen über selbsttätige Einrichtungen, Offenbarung von geschützten Daten, Anzapfen von Datenübertragungseinrichtungen. Der Datenschutz ist unmittelbar berührt, wenn personenbezogene Daten unbefugt abgerufen oder offenbart werden, wenn sie auf Datenträgern entwendet werden oder wenn sie durch Änderungen oder Löschungen verfälscht werden, und so schutzwürdige Belange von den Betroffenen verletzt werden.

Mir sind über die bereits in der Vergangenheit öffentlich diskutierten Fälle hinaus, in denen dienstlich zugängliche Daten unbefugt verwertet wurden, keine meinen Zuständigkeitsbereich berührenden Fälle bekannt geworden. Angesichts der voraussichtlich sehr hohen Dunkelziffer und der großen Zurückhaltung, mit der vermutlich betroffene Organisationen kriminelle Manipulationen zu ihren Ungunsten aus Reputationsgründen behandeln, kann das Fehlen konkreter Fälle nicht zum Anlaß genommen werden, bei den meiner Zuständigkeit unterliegenden datenverarbeitenden Stellen Sicherheit vor kriminellem Zugriff anzunehmen. Bei meinen Prüfungen in Behörden und öffentlichen Unternehmen habe ich vielmehr häufig feststellen müssen, daß präventive Maßnahmen gegen von innen herauskommende unzulässige Eingriffe in die Datenverarbeitung nicht ausreichend getroffen werden. Insbesondere der Schutz vor unbefugter Kenntnisnahme personenbezogener Daten sollte verstärkt werden.

Eine vollständige präventive **Abwehr von Computerkriminalität** mit technischen und organisatorischen Mitteln ist kaum möglich, da den Mitarbeitern intern für ihre Tätigkeit Kompetenzen und Spielräume eingeräumt werden müssen. Abgesehen von den üblichen, gesetzlich vorgeschriebenen technischen und organisatorischen Maßnahmen zum Datenschutz können jedoch zur Abwehr von intern ausgelösten kriminellen Handlungen bei der Datenverarbeitung verschiedene Maßnahmen ergriffen werden:

- Das Personal, welches unmittelbar Zugang zu Datenträgern hat oder Einfluß auf die Datenverarbeitungsprozesse nehmen kann, ist sorgfältig nach dem Gesichtspunkt der Zuverlässigkeit auszuwählen. Hinsichtlich dieser Maßnahme habe ich bisher jedoch noch keinen Grund zu einer Beanstandung gehabt.
- Die internen Abläufe bei der Datenverarbeitung, d.h. der Arbeit im Rechenzentrum, bei der System- und Anwendungsprogrammierung, in Projektplanung und -durchführung müssen in allen Phasen so transparent sein, daß das Risiko, bei unbefugter Handlung rechtzeitig erkannt zu werden, zu groß ist, um solche Wagnisse einzugehen.

Bei meinen Prüfungen in Organisationen mit Rechenzentren achte ich in besonderem Maße auf die Maßnahmen, die der

Transparenz der Abläufe dienen sollen. Dabei bin ich sehr häufig zu nicht befriedigenden Ergebnissen gekommen:

- Die Funktionentrennung zwischen Operating, Datenträgerarchiv, Arbeitsvor- und -nachbereitung, System- und Anwendungsprogrammierung ist in personeller, vor allem aber in baulicher Hinsicht in den seltensten Fällen so realisiert, wie es jeweils für die Größe des Rechenzentrums und der Organisation sowie die Personalstärke im Rechenzentrum angemessen wäre. Die Trennung der Funktionen und der Unterstützung dieser Trennung durch bauliche Verhältnisse sowie durch eindeutige organisatorische Regelungen ist jedoch eine Grundvoraussetzung für die Transparenz der Abläufe.
- Die Nachvollziehbarkeit der ADV-Verfahren durch sachverständige Dritte genügt zwar bei den nach wirtschaftlichen Gesichtspunkten handelnden öffentlich-rechtlich organisierten Unternehmen im allgemeinen den Mindestanforderungen, die sich aus Haushaltsordnung und Datenschutzgesetzen ergeben, im eigenen Interesse der Unternehmen sollte es jedoch geboten sein, die angewandten Dokumentationsmethoden dem Stand der derzeitigen Technik und des derzeitigen Wissens anzupassen, um Abweichungen vom Sollzustand rechtzeitig erkennen zu können. Wo nicht haushaltsrechtliche Zwänge wirken, ist auch bei neueren Verfahrensentwicklungen zu beobachten, daß entgegen den bestehenden Anordnungen Dokumentationen erst lange nach Inbetriebnahme eines Verfahrens fertiggestellt werden. Dies, obwohl in der Fachwelt anerkannt ist, daß die nachträgliche Dokumentation von Programmen und Verfahren nie annähernd die Transparenz und Zuverlässigkeit erreicht, die bei projektbegleitender Dokumentation erreicht werden kann.

Ergebnis

Aus meiner Prüfpraxis ergibt sich zusammengefaßt,

- daß die Manipulierbarkeit von Datenverarbeitungssystemen ein zunehmendes und besorgniserregendes Risiko darstellt, weil die Anpassung der Systeme und der Rechenzentrumsorganisationen an diese Gefahren mit dem Anstieg der Computerkriminalität und der Verbreitung des Hackerunwesens nicht annähernd Schritt hält. Zulange wurde die Notwendigkeit nicht erkannt, auch in Sicherheit zu investieren;
- daß in meinem Zuständigkeitsbereich zwar Einzelfälle von Computermanipulation aufgetreten sind, daß die Delikte in der Praxis der öffentlichen Stellen Berlins - soweit mir bekannt geworden ist - jedoch noch keinen bedeutenden Stellenwert erlangt haben;
- daß die vorbeugenden Maßnahmen gegen Hacking, soweit diese Gefahr aus technischen Gründen überhaupt gegeben ist, sowie gegen kriminelle Computermanipulation häufig noch nicht ausreichend sind;
- daß jedoch technische Mittel und organisatorische Methoden verfügbar sind, um die Anfälligkeit gegen von außen oder von innen erfolgende unbefugte Handlungen am ADV-System einzudämmen. Es kommt darauf an, diese sinnvoll und sorgfältig einzusetzen;
- daß die Hersteller von Datenverarbeitungsanlagen dringend aufgefordert sind, bei ihren Anlagen - vor allem bei kleineren Rechnern - mehr Sicherheitsvorkehrungen sowohl in der hardware als auch in der software konzeptionell vorzusehen.

Trotz der Dringlichkeit, die sich aus dem Entwicklungstempo der Technik und der Ausbreitung der Computerkriminalität ergibt, wurde bislang eher beiläufig diskutiert, in welchem Umfang die oben angesprochenen Gefahren des Computermißbrauchs **strafrechtlich** geregelt werden sollten. Zwar liegt dem Bundestag ein von der vorherigen Regierung übernommener Entwurf eines Zweiten Gesetzes zur Bekämpfung der Wirtschaftskriminalität vor. Aus Gründen, die ich bereits früher angeführt[1] habe, greift dieser Entwurf zu kurz: Er beseitigt im wesentlichen nur Unstimmigkeiten, die sich aus den Eigenarten des Computers bei der Anwendung der herkömmlichen Straftatbestände ergeben. Neue Gefahren, die für den Computer spezifisch sind, werden nicht erfaßt.

Insbesondere ist hier zu nennen die mißbräuchliche Verwendung von Codekarten, Transaktionsnummern und anderen Einrichtungen, die zur Sicherung des ordnungsgemäßen Gebrauchs automatischer Datenverarbeitungsverfahren eingesetzt werden. Strafrechtlich sanktioniert werden müßte hier bereits das unbefugte Sichverschaffen, die unbefugte Aufbewahrung oder die unbefugte Verwendung auch ohne nachweisbaren Schaden. Interessante Aspekte sind hierzu in einem Gesetzentwurf enthalten, den das US-Repräsentantenhaus am 24. Juli 1984 beschlossen hat. Der „Counterfeit Access Device und Computer Fraud and Abuse Act of 1984"[2] stellt gleichermaßen den Mißbrauch des Computers selbst als auch die Herstellung, den Gebrauch und das Inverkehrbringen gefälschter und unbefugt erlangter Zugangsmittel unter Strafe.

2.2 Die Unzufriedenheit der Bürger mit der Änderung der Allgemeinen Geschäftsbedingungen des Kreditgewerbes (AGB) zum 1. Januar 1984

Bankauskünfte

Größte Aufmerksamkeit hat im vergangenen Jahr die Verarbeitung von Kundendaten durch Kreditinstitute erregt. Zwar hatten die Datenschutzkontrollinstanzen schon seit Jahren die Banken und Sparkassen darauf aufmerksam gemacht, daß die gängige Praxis der Bankauskünfte sowie des Datenaustauschs mit der Schutzgemeinschaft für Allgemeine Kreditsicherung (Schufa) mit dem Datenschutzrecht nicht vereinbar ist. Aber erst der Versuch der Institute, die problematische Praxis der Bankauskünfte durch eine Änderung der AGB zum 1. Januar 1984 festzuschreiben, führte nach einem Beschluß der Konferenz der Datenschutzbeauftragten zu einem Einlenken der Banken.

In der den Kunden vorgelegten Neufassung der AGB war vorgesehen, daß Bankauskünfte nicht nur über Geschäftsleute, sondern auch über Privatkunden ohne ausdrückliche Einwilligung des Kunden gegeben werden dürfen. Die Änderung begründeten die Kreditinstitute im wesentlichen damit, daß sie die Geschäftsbedingungen nur der Praxis angepaßt hätten, sich also tatsächlich nichts geändert habe.

Ich hatte bereits in der Vergangenheit für meinen Zuständigkeitsbereich darauf hingewiesen, daß jedenfalls Auskünfte über Privatkunden nur mit deren ausdrücklicher Einwilligung zulässig seien. Eine andere Auffassung würde dem Recht auf Selbstbestimmung des Kunden hinsichtlich seiner Daten bei Banken und Sparkassen widersprechen. Sie würde den Privatkunden benachteiligen und wäre daher nach §9 Abs. 2 Ziff. 1 und 2 Gesetz über Allgemeine Geschäftsbedingungen unwirksam.

Die Datenschutzbeauftragten mußten nach der für sie überraschenden Änderung der Geschäftsbedingungen ausdrücklich darauf hinweisen, daß die Kreditinstitute auch nach der Neuregelung der AGB keine Auskunft erteilen dürften, selbst wenn der Kunde von seinem Widerspruchsrecht gegen die Neufassung keinen Gebrauch machte.

Angesichts dieser Position der Datenschutzbeauftragten sowie der überwiegenden Ablehnung in der Presse und der Vielzahl der von den Kunden eingelegten Widersprüche kam der Zentrale Kreditausschuß im Februar 1984 der Forderung nach einer Aussetzung dieser Bestimmung nach und trat in Verhandlungen mit den Datenschutzbeauftragten und den Aufsichtsbehörden für den Datenschutz ein mit dem Ziel, ein beiden Seiten gerecht werdendes Verfahren für die Bankauskunft zu finden.

Im Oktober 1984 konnte das Ergebnis der Besprechungen bekanntgegeben werden. Das bedeutendste Ergebnis war, daß Auskünfte über Personen, die nicht Kaufleute sind (für die ohnehin nach dem Handelsgesetzbuch besondere Vorschriften gelten), nur noch mit ausdrücklicher Einwilligung erteilt werden.

Im einzelnen wurden folgende Feststellungen getroffen:

1. Das Kreditinstitut ist berechtigt, über Geschäftskunden (juristische Personen und Kaufleute, die im Handelsregister eingetragen sind) Bankauskünfte zu erteilen, sofern ihm keine anderslautende Weisung des Kunden vorliegt.

[1] Jahresbericht 1981, S. 14

[2] Chapter 47 title 18 des US Code

2. Bankauskünfte über Privatkunden (alle sonstigen Personen und Vereinigungen) erteilt das Kreditinstitut nur dann, wenn diese allgemein oder im Einzelfall ausdrücklich zugestimmt haben.
3. Bankauskünfte sind allgemein gehaltene Feststellungen und Bemerkungen über die wirtschaftlichen Verhältnisse des Kunden, sowie seine Kreditwürdigkeit und Zahlungsfähigkeit; betragsmäßige Angaben über Kontostände, Sparguthaben, Depot- oder sonstige dem Kreditinstitut anvertraute Vermögenswerte sowie Kreditinanspruchnahmen werden nicht gemacht.
4. Bankauskünfte erhalten nur eigene Kunden sowie andere Kreditinstitute für deren eigene Zwecke und die ihrer Kunden; sie werden nur dann erteilt, wenn der Anfragende ein berechtigtes Interesse an der gewünschten Auskunft glaubhaft darlegt.

Im übrigen werden unter bestimmten Voraussetzungen auch Daten über Kunden an die Schufa weitergegeben. Über Einzelheiten des Schufa-Verfahrens erteilen die Kreditinstitute auf Wunsch nähere Auskunft.

Für die Durchführung des Bankauskunftsverfahrens wurde ergänzend auf folgendes hingewiesen:

1. Die Auskunftsverweigerung wegen fehlender Einwilligung ist so zu formulieren, daß sie nicht als negative Auskunft verstanden werden kann. Liegt bei Privatkunden eine Einwilligung nicht vor oder hat bei Geschäftskunden der Kunde die Erteilung einer Auskunft untersagt oder hat die angefragte Stelle keinen Einblick in die wirtschaftlichen Verhältnisse des Kunden, ist dies in der Antwort deutlich zum Ausdruck zu bringen.
2. Die Auskunft darf sich nur auf die wirtschaftlichen Verhältnisse des Kunden und sein Verhalten im Geschäftsleben beziehen.
3. Bankauskünfte werden nur aufgrund von Erkenntnissen erteilt, die der auskunftgebenden Stelle vorliegen. Es werden keine Recherchen (etwa mit Hilfe von Wirtschaftsauskunfteien) angestellt.
4. Hat die Bank eine von Anfang an unrichtige Auskunft erteilt, so ist sie zur Richtigstellung gegenüber dem Auskunftsempfänger verpflichtet.
5. Der Kunde, der eine Auskunft erhält, ist ausdrücklich darauf hinzuweisen, daß er empfangene Informationen nur für den angegebenen Zweck verwenden und nicht an Dritte weitergeben darf.
6. Mündlich erteilte Bankauskünfte werden dokumentiert und sollen in der Regel schriftlich bestätigt werden.
7. Auf Verlangen des Betroffenen hat das Kreditinstitut den Inhalt einer erteilten Auskunft mitzuteilen.
8. Wirtschaftsauskunfteien erhalten keine Bankauskünfte.

Schufa

Während der Bankauskunft Bedeutung eher im Einzelfall zukommt, wird das Massengeschäft der Kleinkredite heute vom Datenaustausch zwischen Kreditinstituten und Schufa beherrscht.

Die Banken hatten bisher hierfür bereits bei Kontoeröffnung, aber auch bei anderen Geschäften (z.B. Kreditvergabe, Bürgschaften u.ä.) eine pauschale Einwilligung des Kunden eingeholt.

Ende 1983 hat nunmehr das Oberlandesgericht Hamburg[1] entschieden, daß diese sogenannte „Schufa-Klausel" unwirksam sei, da sie gegen die Grundsätze des Gesetzes über Allgemeine Geschäftsbedingungen verstoße. Die vorformulierte und uneingeschränkte Einwilligung des Kunden zur Datenübermittlung durch das Kreditinstitut an die Schufa sei viel zu umfassend, zumal der Kunde nur unzureichend über die Datenweitergabe informiert werde. Das Gericht hat daher gefordert, daß vom Kunden eine gesonderte Einwilligungserklärung eingeholt werden müsse (§3 Bundesdatenschutzgesetz). Gegen das Urteil ist beim Bundesgerichtshof Revision eingelegt worden, über die noch nicht entschieden worden ist.

Unabhängig vom Ausgang des Verfahrens besteht Einigkeit, daß der Kunde auch über das Schufa-Verfahren ausführlicher und deutlicher unterrichtet werden soll.

Die Datenschutzbehörden wiesen darauf hin, daß eine Datenübermittlung an die Schufa ein Geschäft mit Kreditrisiko voraussetzt. Sie folgerten hieraus, daß für die Eröffnung eines Girokontos, das nur auf Guthabenbasis geführt werden soll, die Unterzeichnung der Schufa-Klausel nicht verlangt werden darf. Sie forderten deshalb die Kreditwirtschaft auf, die Errichtung von Girokonten, die nur auf Guthabenbasis geführt werden sollen, auch ohne Schufa-Klausel zu ermöglichen.

Die Vertreter der Kreditwirtschaft wiesen demgegenüber darauf hin, daß ein ausschließlich auf Guthabenbasis zu haltendes Konto von seiten des Kreditinstituts eine spezielle Beobachtung erfordert, was die organisatorischen Möglichkeiten eines automatisierten Massengeschäfts überschreiten kann. Außerdem machten sie darauf aufmerksam, daß der Kunde auf verschiedene moderne Formen des Zahlungsverkehrs (ec-Scheck, Geldautomatenkarte) verzichten müßte.

Gegenüber der Sparkasse der Stadt Berlin West habe ich demgegenüber weiterhin die Auffassung vertreten, daß die Möglichkeit zur Errichtung eines „schufalosen" Kontos gewährt werden sollte.

Dabei mußte ich auch auf folgendes Problem hinweisen: In den Kreis der Schufakunden werden zunehmend Unternehmen aus Branchen außerhalb der Kreditwirtschaft aufgenommen (z.B. Versandhäuser, Großvermieter). Hierüber wird der Kunde bei Eröffnung des Kontos ebenfalls nicht hinreichend aufgeklärt.

Es stellte sich heraus, daß die Sparkasse selbst nicht vollständig über den Kreis der sogenannten „B-Kunden" informiert ist.

2.3 Der Umgang mit Gesundheitsdaten

Der Datenschutz von Gesundheitsdaten steht nach wie vor im Brennpunkt und gehört zu meinen besonders wichtigen Aufgaben. Probleme ergeben sich nicht nur unmittelbar bei der ärztlichen Behandlung, sondern auch beim Verwaltungsverfahren anderer Stellen im Gesundheitswesen. Meine Aufgabe reicht von der Bearbeitung der Eingaben einzelner Patienten, der Kontrolle und Beratung von Ärzten und der Gesundheitsverwaltung bis hin zu Überprüfungen und Beratungen im Bereich der Forschung und der Beratung des Ausschusses für Gesundheit, Soziales und Familie des Abgeordnetenhauses bei der Erörterung des Landeskrankenhausgesetzes und des Gesetzes über psychisch Kranke. Insgesamt sind bemerkenswerte Fortschritte erzielt worden.

Neue Datenschutzbestimmungen im Landeskrankenhausgesetz (LKG)

In den dem Abgeordnetenhaus vorgelegten Entwürfen zur Novellierung des LKG war die Aufnahme bereichsspezifischer Datenschutzvorschriften nicht vorgesehen. Da für die Verarbeitung personenbezogener Daten im Krankenhausbereich ein erhebliches Regelungsdefizit bestand, welches zu Unsicherheiten sowohl bei den behandelnden Ärzten als auch im Verwaltungsbereich und bei den betroffenen Patienten führte, habe ich dem zuständigen Ausschuß des Abgeordnetenhauses einen Vorschlag für eine Datenschutzregelung unterbreitet. Er betraf

1. die Verwaltungs- und Behandlungsdaten im Krankenhaus
2. den Zugriff auf Patientendaten
3. die Offenbarung von Patientendaten an Stellen außerhalb der Krankenhauses
4. die wissenschaftliche Forschung
5. die Tätigkeit des Krankenhauses im amtlichen oder privaten Auftrag Dritter
6. das Recht der Patienten, in Krankenunterlagen Einsicht zu nehmen
7. die Aufbewahrung der Patientendaten.

[1] Zeitschrift für Wirtschaftsrecht 1983, S. 1435

Aufgrund der Anregung, bestimmte Punkte meines Vorschlages erst zu regeln, nachdem mit den betroffenen Berufsgruppen eine eingehende Diskussion stattgefunden hat, habe ich mich damit einverstanden erklärt, daß über die gesetzliche Regelung der Punkte 1, 5 und 6 meines Vorschlags erst später entschieden wird. Dies wurde durch die Zusage des Senators für Soziales, Gesundheit und Familie erleichtert, daß eine Novellierung alsbald in Angriff genommen werden soll. Vor allem verspreche ich mir durch eine breitere Diskussion mit den betroffenen Berufsgruppen eine bessere Akzeptanz von Datenschutzbestimmungen, die allen Beteiligten zugutekommen.

Im übrigen wurde mein Vorschlag in das Landeskrankenhausgesetz aufgenommen[1]. Die neue Regelung stellt einen erheblichen Fortschritt dar. War die ärztliche Schweigepflicht bisher nur durch die persönliche berufsethische Verpflichtung in der Standesordnung der Ärztekammer und indirekt durch die Sanktionierung in §203 Strafgesetzbuch konkretisiert, stellt die im Landeskrankenhausgesetz gefundene Regelung erstmals eine Schutznorm dar, durch die nicht nur die Ärzte persönlich, sondern alle im Krankenhauswesen tätigen Personen unmittelbar verpflichtet werden.

Krankengeschichtenverordnung

Im Zuge der Neufassung des Landeskrankenhausgesetzes soll auch die von mir seit längerem geforderte Krankengeschichtenverordnung[2] erlassen werden. Gegen den vorgelegten Entwurf habe ich unter folgenden Voraussetzungen keine Bedenken:

- Eine ausdrückliche Regelung der Einsichtsrechte der Betroffenen im Landeskrankenhausgesetz ist in Aussicht genommen und sollte auch in der Krankengeschichtenverordnung ihren Niederschlag finden;
- die in §8 Krankengeschichtenverordnung vorgesehene Mikroverfilmung sollte von den jeweiligen Krankenhäusern selbst vorgenommen werden;
- nach Schließung eines Krankenhauses (§9 Krankengeschichtenverordnung) sind die Unterlagen so aufzubewahren, daß sich der Kreis der zur Einsicht bzw. Offenbarung Befugten (§15 Landeskrankenhausgesetz neue Fassung) nicht erweitert.

Vernichtung einer unzulässigen Sammlung der Duplikate von Krebsnachsorgedaten

Die Sammlung der Duplikate von Daten über die nachgehende Krankenfürsorge der Bezirke, die bei der Senatsverwaltung während der letzten Jahre angelegt worden[3] war , ist vernichtet worden. Ich hatte darauf hingewiesen, daß die Anfertigung der Duplikate und deren dateimäßige Sammlung bei der Senatsverwaltung für Forschungszwecke in dieser Form datenschutzrechtlich nicht zulässig war, und zumindest eine Anonymisierung gefordert. Die Senatsverwaltung hat demgegenüber die Vernichtung der Unterlagen vorgezogen. Das Register hatte für die Forschung in den letzten Jahren offensichtlich keine Bedeutung. In den Forschungseinrichtungen der Universitätsklinika werden demgegenüber wesentlich effektivere Registrierungsmethoden bei der Krebsbekämpfung erprobt, die auch datenschutzrechtlich als weniger problematisch erscheinen.

Bestimmt der Computer, wer behandelt wird?

Die mit dem Computereinsatz verbundene Routinisierung der Datenerhebung bringt eine spezifische Gefahr mit sich, die auch im Bereich der medizinischen Versorgung zu Beeinträchtigungen der Persönlichkeitsrechte geführt hat.

In einer Beschwerde wurde mir von einem Patienten einer Universitätsklinik berichtet, ihm sei bei der Aufnahme in die Klinik eröffnet worden, daß er nicht zur Behandlung angenommen werden könne, wenn er seinen Arbeitgeber nicht angebe. Angeblich hätte sonst der „Computer nicht weiterarbeiten können".

Mit dieser Argumentation wird der technisch bedingten Vereinheitlichung der Datensätze eine normative Wirkung beigemessen: Die mitunter notwendige Frage (z.B. bei einem Arbeitsunfall) wird zur undifferenziert übernommenen Regel. Bereits früher hatte ich Hinweise darauf erhalten, daß in derselben Klinik Patienten, die wegen eines kleinen Eingriffs sich hatten beraten lassen, einer umfänglichen Befragung nach einer Vielzahl irrelevanter Daten hatten unterziehen müssen.

Dieser unerwünschten Auswirkung der Automatisierung muß sowohl durch eine entsprechende Gestaltung der ADV-Verfahren als auch durch eine eingehende Aufklärung der Bediensteten begegnet werden. Dies würde nicht nur helfen, irrationale Befürchtungen der Bürger hinsichtlich der Datenverarbeitung zu beseitigen, sondern auch dem Gebot einer bürgerfreundlichen Verwaltung entsprechen.

Pauschale Übermittlung von Patientendaten

Auch im Rahmen der Abwicklung eines Patientenvertrages muß die Erforderlichkeit der Übermittlung im Einzelfall überprüft werden. Die Herausgabe ganzer Bestände von Patientendaten ist in der Regel nicht zulässig.

So werden etwa bestimmte Laborproben eines Universitätsklinikums regelmässig von einem **externen Labor** untersucht. Um Unklarheiten und Undeutlichkeiten bei den handschriftlich gefertigten Begleitzetteln mit den erforderlichen Patientendaten zu vermeiden, beabsichtigte man, das beauftragte Labor generell mit allen Patientendaten dieser Klinik zu versorgen, einschließlich der Patienten, von denen keine Laborproben dort untersucht werden sollten.

Mit dem Erforderlichkeitsgrundsatz ist diese Form der Vorratsspeicherung nicht vereinbar. Die Übermittlung der Daten unterblieb.

Differenzierter zu beurteilen war die Übertragung der Aufgaben des **Blutspendedienstes** vom Land Berlin auf das Deutsche Rote Kreuz zum 1. Oktober 1983. Mit der Übernahme der Institution als solcher mußte auch die Blutspenderkartei dem Deutschen Roten Kreuz zur Verfügung gestellt werden. Da hier ein vollständiger Aufgabenbereich abgegeben und mit ihm die Trägerschaft auf eine andere Stelle übertragen werden sollte, konnte der datenschutzrechtliche Übermittlungsbegriff keine unmittelbare Anwendung finden.

Gleichwohl werden durch eine derartige Privatisierung einer öffentlichen Einrichtung datenschutzrechtliche Belange der Betroffenen nur dann nicht beeinträchtigt, wenn die Daten der Blutspender nach der Übergabe dem gleichen Schutz unterliegen wie zuvor.

Dies wurde im Ergebnis zugesichert. Die ebenfalls vorgesehene wissenschaftliche Auswertung der Daten durch das Universitätsklinikum Steglitz der Freien Universität erfolgt nur an Hand anonymisierter Daten.

Anonymisierung psychiatrischer Daten für Forschung und Planung

Forschung und Planung im Bereich medizinischer Versorgung setzen die Auswertung von Daten voraus, die in dem jeweiligen Versorgungsbereich angefallen sind. Die schutzwürdigen Belange der Patienten können, wenn nicht (wie beim Krebsregister) ohnehin die Einwilligung der Patienten zu verlangen ist, nur gewahrt werden, wenn die Daten hinreichend anonymisiert sind. Der für die Anonymisierung erforderliche Aufwand muß dabei von der Sensitivität der Daten und der Genauigkeit, mit der die erfaßten Merkmale die Person der Patienten abbilden, abhängen.

Im Bereich der Psychiatrie gaben zwei Projekte Anlaß zu einer eingehenden Beschäftigung mit dieser Problematik: die Erstellung einer Patientendokumentation im Rahmen des „Modellprogramms Psychiatrie" sowie der geplante Beginn der „Basisdokumentation Psychiatrie".

Bei dem **„Modellprogramm Psychiatrie"**, einer Untersuchung über die Reformmöglichkeiten im Bereich der psychiatrischen Versorgung, habe ich eine Überprüfung der Erhebungen zur Patientendokumentation vorgenommen. Weil das damit beauftragte Institut PROGNOS als private Organisation nicht meiner gesetz-

[1] Anlage 1
[2] Vgl. Jahresbericht 1981, S. 6; 1982, S. 20; 1983, S. 24
[3] Vgl. Jahresbericht 1981, S. 5f

lichen Überprüfungskompetenz unterliegt, die erhobenen Daten jedoch teilweise aus Behandlungseinrichtungen stammen, die der Kontrolle der Landesdatenschutzbeauftragten unterliegen, waren sowohl Landesdatenschutzbeauftragte als auch Aufsichtsbehörden frühzeitig eingeschaltet worden, um von vornherein eine datenschutzgerechte Konzeption des Erhebungsprogramms sicherzustellen. Für Berlin hat sich das Forschungsinstitut vertraglich meiner Kontrollbefugnis unterworfen.

Bei der gemeinsam mit der Aufsichtsbehörde für den Datenschutz durchgeführten Überprüfung der Begleitforschungsstelle im Bezirk Kreuzberg habe ich festgestellt, daß das Erhebungsverfahren in der von mir empfohlenen Weise durchgeführt wurde. Die Fragebogen mit den Angaben über Patienten waren so weitgehend anonymisiert, daß eine Gefährdung des Persönlichkeitsschutzes ausgeschlossen werden kann. Hervorzuheben ist, daß innerhalb der behandelnden Einrichtungen die Daten auf Sammelformularen aggregiert werden und die Fragebögen selbst in der Einrichtung verbleiben. Dadurch wird ein zusätzlicher Schutz erreicht.

Erheblich problematischer ist die Beurteilung der **„Basisdokumentation Psychiatrie"**, die zum 1. Januar 1984 in Berlin eingeführt werden sollte:

Die Bundesarbeitsgemeinschaft der Träger psychiatrischer Krankenhäuser hatte bereits 1973 ihren Mitgliedern empfohlen, zur Dokumentation in den psychiatrischen Krankenhäusern einen einheitlichen Datenkatalog zu versenden. Dieser Katalog enthielt zwanzig definierte Merkmale und verfolgte das Ziel, eine überregionale Vergleichbarkeit der Grunddaten herzustellen. Diese Daten sollten als zuverlässige Grundlage für die Weiterentwicklung der psychiatrischen Versorgung dienen. Die Ausarbeitung eines Erhebungsbogens erfolgte in einer Arbeitsgruppe, der u.a. Vertreter der Deutschen Gesellschaft für Psychiatrie und Nervenheilkunde sowie andere Fachleute angehörten.

Zwar war der Erhebungsbogen so ausgestaltet, daß eine Reindividualisierung der Daten nach den üblichen Kriterien auszuschließen war und die Daten daher als anonymisiert gelten konnten. Andererseits bestand sowohl nach Art der Daten als auch wegen der Detailliertheit der Merkmale ein hohes Gefährdungspotential, das viele Ärzte bewog, sich der geplanten Einführung des Erhebungsbogens zu widersetzen.

Sie kritisierten auch, daß einige Daten nicht erforderlich waren, und daß das Statistische Landesamt zur Verarbeitung der Daten eingeschaltet werde.

Nach eingehender Beratung wurde das laufende Erhebungsverfahren vom Senator für Gesundheit, Soziales und Familie ausgesetzt, um das Verfahren und den Erhebungsbogen noch einmal zu überprüfen.

Neues Verfahren bei der Kostenübernahme für psychologische Therapien

Von grundsätzlicher Bedeutung war die Neuordnung des Verfahrens der Kostenübernahme bei psychologischen Therapien als Eingliederungshilfe für Behinderte nach dem Bundessozialhilfegesetz (BSHG) durch die Jugendämter. Hier wurde früher unter extensiver Auslegung des § 126 BSHG von den Antragstellern in der Regel verlangt, daß sie ihr Einverständnis zur Übermittlung des sogenannten „Kosten- und Behandlungsplanes" von Gesundheitsämtern an die Jugendämter erteilten. Als Ergebnis der Beratungen wurde ein gemeinsames Rundschreiben der Senatoren für Gesundheit, Soziales und Familie und Schule, Jugend und Sport verfaßt, welches das Verfahren von Grund auf neu regelt[1].

Dadurch soll der Datenschutz für die Antragsteller der Eingliederungshilfe verbessert werden, indem sie nur noch insoweit in die Übermittlung von medizinischen Daten durch das Gesundheitsamt an das Jugendamt einwilligen müssen, als dies zur Entscheidung für die Hilfegewährung unbedingt erforderlich ist. Die darüber hinaus beim Gesundheitsamt bekanntgewordenen Informationen unterliegen im Gegensatz zur bisherigen Praxis dem Schutz der ärztlichen Schweigepflicht. Es kommt jetzt darauf an, daß dieses Verfahren auch in der Praxis befolgt wird.

[1] Vgl. Anlage 5

Vertraulichkeit bei medizinischen Daten

Durch mehrere Eingaben bin ich darauf hingewiesen worden, daß die Aufbewahrung und Beseitigung von Informationsträgern bei einzelnen Stellen im Gesundheitsbereich Mängel aufweist.

So wurden in der Nähe eines Gesundheitsamtes Listen mit zahlreichen Adressen und Vermerken über die Durchführung von Impfungen gefunden. Sie waren beim Ausleeren der Papierkörbe aus der überfüllten Mülltonne auf die Straße geraten.

Ein Stapel Abrechnungsunterlagen einer Klinik der Freien Universität (ca. 60 Patienten betreffend) wurde von einem Passanten an einem Feldrain gefunden. Die Ermittlungen ergaben, daß eine Mitarbeiterin der Klinik die Unterlagen in ihrem Auto gelassen hatte, und daß sie von dort durch Einbruch entwendet wurden.

Informationsträger (Briefe, Bilder, technische Datenträger) müssen vor der Übergabe zur **Vernichtung** so weit unkenntlich gemacht werden, daß die Daten nicht in unberechtigte Hände fallen können, zumindest muß der Transport bis zur Vernichtung beaufsichtigt werden.

Zu hohe Transportrisiken birgt auch ein Verfahren, in dem ein Universitätsklinikum **offene Postkarten** versandte, um Patienten bei einer Nierenerkrankung zur turnusmäßigen Dialyse an einem bestimmten Tag aufzufordern. Nicht nur der Postzusteller, sondern auch andere Personen konnten dabei unbefugt Informationen über den Gesundheitszustand des Betroffenen erlangen. Das Verfahren wird aufgrund meiner Beanstandung umgestellt.

Vor dem Hintergrund derartiger Offenbarungsrisiken ist auch die Übung zu bewerten, im Bereich der Krankenhausverwaltungen **externe Schreibkräfte** für die Erstellung der Korrespondenz in Behandlungsangelegenheiten einzusetzen. Die Datensicherheit in den Krankenhäusern könnte beeinträchtigt werden, wenn für die Erledigung der Schreibaufträge ohne weiteres Krankengeschichten u.a. hierzu erforderliche Informationen aus dem Bereich eines Krankenhauses heraus in private Haushalte von Schreibkräften, Sekretärinnen etc. gelangen könnten. Die Einhaltung der ärztlichen Schweigepflicht fordert auch in diesem organisatorischen Bereich Maßnahmen, damit die geltenden Sicherheitsstandards erhalten werden können. So wäre es wohl möglich, Einzelaufträge im Schreibdienst durch externe Schreibkräfte im Krankenhausbereich durchführen zu lassen. Nach außen sollten jedoch nur solche Schreibaufträge vergeben werden, bei denen die Gefahr einer Beeinträchtigung des Arztgeheimnisses nicht entstehen kann. Auf personenbezogene Angaben über Behandlungsverhältnisse sollte hier verzichtet werden.

In Krankenhäusern ist es üblich, die Anamnese von Patienten, die in einem **Mehrbettzimmer** untergebracht sind, vor den Augen und Ohren der Mitpatienten durchzuführen. Diese oder auch anwesende Besucher haben dabei die Möglichkeit, das Gespräch mitzuhören. Aufgrund meines Hinweises wurde vom Senator für Gesundheit, Soziales und Familie die Anweisung gegeben, dem Wunsch eines Patienten, die Anamnese nicht in Anwesenheit dritter Personen durchzuführen, generell zu entsprechen.

Übermittlung personenbezogener Daten vom Amtsarzt an die Dienstbehörde

Die Frage, ob und in welchem Umfang Amtsärzte personenbezogene Daten an Dienstbehörden übermitteln dürfen, wirft erhebliche Probleme auf.

Während bei der Einstellungsuntersuchung Einigkeit dahingehend besteht, daß der Amtsarzt an die Dienstbehörde nur die Tatsache der Eignung mitteilt, nicht aber die bei der Einstellungsuntersuchung erstellte Diagnose bzw. die hierzu erhobenen Daten, gibt es hinsichtlich der Feststellung der allgemeinen (§§ 77 ff Landesbeamtengesetz - LBG -) und der Polizeidienstunfähigkeit (§ 107 LBG) erhebliche Meinungsverschiedenheiten.

Kein Zweifel kann daran bestehen, daß auch Amtsärzte der ärztlichen Schweigepflicht unterliegen, und daß auch öffentlichen Bediensteten gegenüber der Dienstbehörde alle Grundrechte in vollem Umfang zustehen, soweit gesetzlich nichts anderes bestimmt ist.

Eine ausdrückliche gesetzliche Regelung der hier zu behandelnden Fragen besteht allerdings nicht.

Nach § 77 Abs. 1 LBG ist ein Beamter bei Zweifeln an seiner Dienstfähigkeit verpflichtet, sich nach Weisung der Dienstbehörde ärztlich untersuchen und ggf. aufgrund ärztlicher Entscheidung beobachten zu lassen. Nach § 78 LBG erklärt der unmittelbare Dienstvorgesetzte aufgrund eines amtsärztlichen Gutachtens, daß er den Beamten nach pflichtgemäßem Ermessen für dauernd dienstunfähig hält. Aus beidem ergibt sich nicht, in welchem Umfang Daten vom Amtsarzt zu übermitteln sind.

Auch § 107 LBG reicht nicht als Rechtsgrundlage für die Übermittlung des Gutachtens an die Dienstbehörde aus. Er regelt nur, daß ein amtsärztliches Gutachten vorliegen muß. Mitteilungspflichten oder -rechte ergeben sich hieraus nicht.

Die Rechtsprechung des Bundesverfassungsgerichts zum informationellen Selbstbestimmungsrecht verlangt eine ausdrückliche Gesetzesvorschrift. Eine Argumentation mit dem Auftrag der Dienstbehörde oder dem Sinn und Zweck des amtsärztlichen Gutachtens reicht nicht aus. Die Rechtmäßigkeit der Übermittlung kann daher nur auf die Einwilligung des Betroffenen gestützt werden.

Eine derartige Einwilligung wird nicht schon mit dem Dienstverhältnis selbst begründet. Zum Wesen der Einwilligung gehört, daß Zweck und Umfang der Offenbarungen, auf die sich die Einwilligung bezieht, absehbar sind. Dies ist bei den hier zu bewertenden Fragen nicht der Fall, da die Notwendigkeit einer Beurteilung der Dienstuntauglichkeit beim Eingehen des Dienstverhältnisses kaum absehbar sein dürfte. An dieser Überlegung würde im übrigen auch der Vorschlag scheitern, vor Eingehen des Dienstverhältnisses dem Betroffenen eine pauschale Einwilligungserklärung abzuverlangen.

Vielmehr muß jede Mitteilung, die über das reine Untersuchungsergebnis hinausgeht, durch eine ausdrückliche Einwilligung des Betroffenen gedeckt sein. Im Hinblick auf die entsprechende Regelung der Datenschutzgesetze (§§ 6 Berliner Datenschutzgesetz, 3 Bundesdatenschutzgesetz), aber auch aus Gründen der Beweissicherung sollte diese Einwilligung schriftlich erteilt werden.

Auch für den Fall, daß die Dienstbehörde eine eigene ärztliche Stelle als Adressat der Daten bestimmen kann (wie etwa beim Polizeipräsidenten), gilt nichts anderes: Dem Recht auf informationelle Selbstbestimmung kommt auch dann Geltung zu, wenn Ärzte untereinander Daten übermitteln. Dies bringt auch die ärztliche Berufsordnung zum Ausdruck, die eine Offenbarungsbefugnis lediglich bei Parallel- oder Nachbehandlung vorsieht[1].

Die Reichweite der gegebenen Einwilligung ist vom Bindungswillen des Betroffenen abhängig. Im Zweifel reicht dieser nur so weit, als die Übermittlung im konkreten Einzelfall für die Entscheidung der Dienstbehörde erforderlich ist. Auch die Einwilligung stellt den Amtsarzt daher nicht von der Verantwortung frei, den Umfang der Übermittlung auf das erforderliche Maß zu reduzieren. Mitteilungen medizinischer Einzelangaben sind daher in jedem Fall unzulässig. Vielmehr werden die medizinischen Angaben, die mit Einwilligung übermittelt werden, auf das für die Entscheidung der Dienstbehörde unerläßliche Ausmaß zu beschränken sein. Es ist einzuräumen, daß der für erforderlich gehaltene Umfang variieren kann: Eine Rolle kann hier z.B. spielen, welche Kenntnisse die Dienstbehörde bereits aufgrund ihrer eigenen Aktenlage besitzt.

Im Ergebnis führen diese Überlegungen zu einem gestuften Verfahren: Auf die Übermittlung des Untersuchungsergebnisses, die keiner ausdrücklichen Einwilligung bedarf, kann die Dienstbehörde dann, wenn sie einen Bedarf an zusätzlichen Daten geltendmachen kann (z.B. bei einer unterschiedlichen Bewertung der Diensttauglichkeit durch Dienstbehörde und Amtsarzt) den Betroffenen um die (ausdrückliche) Einwilligung in die Übermittlung weiterer Daten bitten, der dann vom Amtsarzt im erforderlichen Umfang entsprochen werden kann. Nicht zu klären ist im übrigen im Rahmen datenschutzrechtlicher Überlegungen, in welchem Umfang der Bedienstete dienstrechtlich zur Abgabe einer derartigen Einwilligungserklärung verpflichtet ist mit der Folge, daß die Verweigerung der Einwilligung zu negativen Konsequenzen führen kann.

Die hier dargestellte, mit der Verfassungslage konforme Lösung setzt eingestandenermaßen eine differenzierte Bewertung der einzelnen Fallkonstellationen voraus. Um eine dem Gleichheitsgebot entsprechende Behandlung zu gewährleisten, empfiehlt es sich, ein Verfahren zu entwickeln, das es erlaubt, die Belange des Betroffenen, des Amtsarztes und der Dienstbehörde in Einklang zu bringen.

In vergleichbaren Fällen hat es sich bewährt, daß von Verwaltungen, die für ihre Entscheidungen ärztliche Gutachten benötigen, Kataloge von Anforderungskriterien entwickelt werden.

Liegen diese vor, kann die Dienstbehörde bereits aus der Mitteilung des Untersuchungsergebnisses vom Zutreffen bzw. Nichtzutreffen des Kriterienkataloges ausgehen. Die Erforderlichkeit der Einholung zusätzlicher Einwilligungen wird dann auf die wenigen strittigen Einzelfälle beschränkt werden können.

Mit berücksichtigt werden sollte bei der Entwicklung entsprechender Verfahrensvorschriften, wo und in welcher Form die erhobenen medizinischen Befunde aufbewahrt werden. Auf jeden Fall muß eine Zusammenführung der Befunddaten (auch der mit Einwilligung übermittelten) mit der Personalakte vermieden werden. Vielmehr ist die Einsicht in diese Unterlagen auf den Personenkreis zu beschränken, für dessen Aufgabenerfüllung die Kenntnis der Daten unerläßlich ist.

2.4 Öffentliche Sicherheit und Strafverfolgung

Meine Arbeitsplanung sah für diesen Bereich vor allem die Fortsetzung der Überprüfungen vor. Mit dem Volkszählungsurteil verlagerte sich der vorgesehene Schwerpunkt der Überprüfung des konkreten polizeilichen Informationssystems zwangsläufig hin zu grundsätzlicheren Überlegungen über den gesetzlichen Regelungsbedarf in diesem Bereich. Bereits früher hatte ich bemängelt, daß der Umfang der gesetzlichen Regelung bei der polizeilichen Datenverarbeitung in einem Mißverhältnis zu deren Bedeutung steht. Dabei stand allerdings mehr die Regelung einzelner Verarbeitungsarten im Vordergrund (z. B. Rasterfahndung, Polizeiliche Beobachtung, Amtshilfe gegenüber dritten Stellen). Heute müssen umfassendere Überlegungen angestellt werden.

Die dringende Notwendigkeit der Verbesserung der Rechtsgrundlage für die polizeiliche Informationsverarbeitung

An erster Stelle muß hier die Forderung stehen, daß den Sicherheitsbehörden eine **grundsätzliche Befugnisnorm zur Datenverarbeitung** verschafft wird. Mag man in anderen Verwaltungsbereichen bezweifeln, ob tatsächlich jede Erhebung oder sonstige Verwendung personenbezogener Daten einen Vorgang darstellt, der wegen seiner grundrechtsrelevanten Bedeutung einer Rechtsgrundlage bedarf, so wird man nach den Ausführungen des Bundesverfassungsgerichts bei Sicherheitsbehörden ohne weitere Erörterung hiervon ausgehen können. Weder in der Strafprozeßordnung (StPO) noch im Gesetz über die Allgemeine Sicherheit und Ordnung (ASOG) findet sich eine geeignete Norm; Beide Gesetze weisen der Polizei und anderen Behörden zwar gewisse Aufgaben zu, nennen aber keine entsprechenden Befugnisse. Hilfskonstruktionen, wie sie bisher notgedrungen herangezogen werden mußten[1], sind mangels der vom Bundesverfassungsgericht geforderten Normenklarheit nicht mehr tauglich.

Im Rahmen dieser grundsätzlichen Befugnisnormen ist klar zwischen der Erforderlichkeit für Zwecke der Strafverfolgung und für Zwecke der Gefahrenabwehr zu unterscheiden; hiervon hängt der Umfang und die Dauer der Zulässigkeit von Speicherungen ebenso ab wie die Frage der Zugriffsberechtigung einzelner bei der Strafverfolgung beteiligter Stellen.

So habe ich festgestellt, daß nach einer Dienstanweisung des Polizeipräsidenten den an die Staatsanwaltschaft zu übersendenden Ermittlungsakten jeweils ein kompletter **Ausdruck aus dem Informationssystem Verbrechensbekämpfung** beizufügen ist; dieser Ausdruck ist nur für die Staatsanwaltschaft bestimmt und wird

[1] Vgl. § 2 Abs. 6 Berufsordnung der Ärztekammer Berlin

[1] Z.B. Verweis auf § 163 StPO oder § 14 ASOG, jeweils i.V.m. §§ 9 ff Berliner Datenschutzgesetz

weder dem Gericht ausgehändigt noch den Anwälten der Beklagten zugänglich gemacht. Abgesehen von der Frage, inwieweit dies mit den Bestimmungen des Bundeszentralregistergesetzes oder dem Prinzip der Waffengleichheit vor Gericht zu vereinbaren ist, liegt hier eine problematische Vermengung zweier Aufgabenbereiche vor: Die Speicherung personenbezogener Daten über Vorgänge, die zu abgeschlossenen Strafverfahren geführt haben oder die aus verschiedenen Gründen (insbesondere fehlender Tatnachweis) eingestellt wurden, kann nur noch unter dem Aspekt der Gefahrenabwehr gerechtfertigt werden. Die sogenannte „präventive Strafverfolgung" ist dabei dem Bereich der Gefahrenabwehr zuzurechnen.

Da eine Zuständigkeit der Staatsanwaltschaft zur Gefahrenabwehr nicht gegeben ist, ist die vollständige Offenbarung der von der Polizei vorgehaltenen Daten, die in der Regel nur Verdachtsdaten sind, zur Aufgabenerfüllung nicht erforderlich und damit jedenfalls nach der derzeitigen Rechtslage rechtswidrig. Vielmehr ist die Polizei verpflichtet, im Rahmen der eigenen Bewertung die für die Strafverfolgung erforderlichen Daten auszuwählen. Im Vorgriff auf entsprechende gesetzliche Regelungen habe ich die derzeitige Praxis gegenüber dem Polizeipräsidenten bemängelt.

Erhebung und Verwendung von Informationen

Neben dieser grundsätzlichen Frage besteht ein Regelungsbedarf bei folgenden polizeilichen Maßnahmen. Sie sind dadurch charakterisiert, daß sie durch die Erhebung oder Verwendung personenbezogener Daten in die informationelle Selbstbestimmung eingreifen (Informationseingriff), und daß darüber hinaus mitunter die Erhebung der Daten mit einem physischen Eingriff verbunden ist (Begleiteingriff).

Zwar ist die **Identitätsfeststellung** bereits jetzt im ASOG geregelt (§ 15); hier sind jedoch nur die Situationen angeführt, in denen Identitätsprüfungen vorgenommen werden dürfen, nicht aber die Befugnisse, die die Polizei anläßlich einer solchen Prüfung hat. Insbesondere ist nicht geregelt, welche Abfragen aufgrund der Prüfung vorgenommen werden dürfen. Die Zulässigkeit maschinenlesbarer Personalausweise setzt nach Auffassung der Datenschutzbeauftragten eine angemessene Regelung dieser Frage voraus. Sie muß insbesondere Bestimmungen enthalten, unter welchen Voraussetzungen ohne Vorliegen konkreter Anhaltspunkte routinemäßig Ausweiskontrollen vorgenommen werden dürfen. Zu verbieten ist die Speicherung der Daten, wenn Erkenntnisse über die geprüfte Person nicht vorliegen, um das Entstehen serienmäßiger Bewegungsbilder zu verhindern.

Die sogenannte **Polizeiliche Beobachtung** wird ebenfalls einer ausdrücklichen Regelung bedürfen. Es handelt sich hier um die - mit Hilfe des bundesweiten polizeilichen Informationssystems realisierte - Ausschreibung von Personen, die zwar bestimmter Straftaten verdächtig sind, bei denen aber die Voraussetzung für die Festnahme noch nicht vorliegen. Diese früher unter der Bezeichnung „Beobachtende Fahndung" (BeFa) laufende Maßnahme hat sich zu einem bedeutenden Instrument der Strafverfolgung entwickelt, ohne daß bisher auch nur die einfachste gesetzliche Regelung vorliegt.

Auch die Anfertigung **erkennungsdienstlicher (ed-) Unterlagen** ist bislang nur teilweise geregelt. So müssen die bestehenden Bestimmungen (§§ 81 b StPO, 16 ASOG) ergänzt werden um Regelungen über die Aufbewahrungsdauer, die Aufklärung der Betroffenen und die Verwertung der Unterlagen. Ungeklärt ist, in welchen Fällen eine ed-Behandlung vorgenommen werden darf: Die hierzu bestehenden Verwaltungsvorschriften reichen nicht aus und sind nicht präzise genug.

Die bestehenden Vorschriften über erkennungsdienstliche Unterlagen sind die einzigen, wenn auch untauglichen Regelungen für die **photographische oder videotechnische Aufnahme** von Personen, die an öffentlichen Veranstaltungen teilnehmen. Obwohl derartige Aufnahmen häufig angefertigt werden, ist bislang unklar, ob dies überhaupt zulässig ist. Die Rechtsprechung hat sich bisher lediglich zu dem (seltenen) Fall geäußert, daß mit Hilfe solcher Maßnahmen gezielt nach einem bekannten Straftäter gesucht wird. Hier wird man in der Tat in den Generalklauseln der StPO bzw. des ASOG eine Befugnis sehen können. In den Fällen, in denen aber lediglich prophylaktisch Beweise gesichert werden oder Straftäter überhaupt erst ermittelt werden sollen, reichen diese Bestimmungen nicht aus, da sie sich im wesentlichen an Nichtbeteiligte richten.

Aufgrund mehrerer Beschwerden über die Videographierung friedlicher Demonstrationen habe ich mich über die Arbeit der **Videogruppe** beim Polizeipräsidenten informiert. Ich stellte fest, daß zwar Aufnahmen gefertigt werden, diese aber nicht zu einer routinemäßigen personenbezogenen Auswertung geeignet sind. Die Aufnahmen dienen daher derzeit fast ausschließlich der Dokumentation des polizeilichen Vorgehens. Angesichts der zu erwartenden technischen Entwicklungen, die durchaus eine automatische Erkennung von Personen einschließen (entsprechende Entwicklungsarbeiten sind bekannt), wird aber eine datenschutzrechtliche Regelung unumgänglich sein.

Auch ohne derartige technische Hilfsmittel stellt die Aufzeichnung von **Beobachtungen über den Besuch von Veranstaltungen,** aber auch der Teilnahme am Straßenverkehr zum Zwecke der Strafverfolgung oder der Gefahrenabwehr einen Eingriff in das informationelle Selbstbestimmungsrecht dar, das präziser Regelungen bedarf. Bereits in dem vor einigen Jahren vorgelegten Alternativentwurf einheitlicher Polizeigesetze des Bundes und der Länder waren Regelungen für die „Ausforschung von Veranstaltungen" gefordert worden. Wie relevant derartige Bestimmungen sein können, zeigt eine in diesem Jahr in Rheinland-Pfalz durchgeführte Fahndungsmaßnahme, bei der heimlich sämtliche Autofahrer auf bestimmten Strecken erfaßt und ihre Personalien bei den polizeilichen Informationssystemen abgefragt wurden.

Über den Regelungsbedarf für **Rasterfahndungen** hatte ich mehrfach berichtet[1].

Neben diesen primär die Erhebung betreffenden Maßnahmen müssen die Bestimmungen über die **Verwendung polizeilicher Daten** gesetzlich geregelt werden; sie sind bisher lediglich in Verwaltungsvorschriften (Richtlinien über die Führung kriminalpolizeilicher personenbezogener Sammlungen, KpS-Richtlinien) enthalten, die in Berlin trotz meiner mehrfach geäußerten Empfehlung noch immer nicht veröffentlicht sind. Gesetzlich geregelt werden sollte, an welche Stellen die Polizei Daten aus ihren Sammlungen übermitteln darf, in welchen Fällen die Auskunft aus den Sammlungen an die Betroffenen verweigert werden darf, wann die Daten gelöscht werden müssen und welches formelle Verfahren bei der Errichtung einzelner Dateien oder Aktensammlungen eingehalten werden soll.

Automatische Datenverarbeitung

Diese alle Formen von Datensammlungen betreffenden Regeln müssen ergänzt werden um spezifische Bestimmungen für die Automatische Datenverarbeitung, die die Polizei unterhält. Dies ergibt sich aus den spezifischen Gefahren, die sich aus den schnellen und einfachen Zugriffsmöglichkeiten über Datenfernverarbeitung sowohl innerhalb des Landes als auch im Rahmen des Datenverbundes im Bundesgebiet ergeben.

Kennzeichnend für die automatisierte Datenverarbeitung bei der Polizei ist, daß mit einer Datensammlung **verschiedene Funktionen** erfüllt werden, für die bei manueller Bearbeitung unterschiedliche Dokumentationen erforderlich wären.

Hervorzuheben sind dabei drei typische Funktionen, deren Integration gerade im Berliner Informationssystem Verbrechensbekämpfung zu beobachten ist:

1. Erfassung von Straftätern und Straftaten: Die ursprünglich in Ermittlungsakten geführten Daten werden (nach der Abgabe an die Staatsanwaltschaft) in dem für die weitere polizeiliche Arbeit erforderlichen Umfang in der Kriminalakte zusammengeführt;
2. Erfassung und Auswertung von Hinweisen und Spuren, aber auch einzelner Tätermerkmale zur Aufklärung bestimmter Straftaten oder Tatkomplexe: Zu diesem Zwecke werden traditionellerweise in den einzelnen für die Aufklärung von Straftaten zuständigen Stellen (z. B. Kriminalpolizeiinspektionen) unterschiedliche, jeweils auf die besondere Situation angepaßte Dokumentationen angelegt (z. B. Spurenakten);

[1] Vgl. insbesondere Jahresbericht 1980, S. 8

3. Vorgangsnachweise: Einmal um polizeiliches Handeln nachweisen zu können, aber auch um verschiedene Ermittlungsvorgänge den richtigen Bearbeitungsstellen zuleiten oder dort solche Vorgänge zusammenführen zu können, wurden traditionellerweise Tagebücher geführt, auf die im Bedarfsfalle zurückgegriffen werden könnte.

Mit Hilfe eines automatisierten Datenverarbeitungssystems können diese drei Funktionen prinzipiell mit einer einzigen Datensammlung wahrgenommen werden. Dies führt allerdings dazu, daß im Hinblick auf die einzelnen erfaßten Personen erheblich mehr Daten an einer Stelle zusammengeführt werden, als dies bisher der Fall war.

Insbesondere die Funktion der Vorgangserfassung führt dazu, daß in einer Datei **(Personendatei)** jede Person registriert ist, die mit polizeilichen Maßnahmen in Berührung gekommen ist. Auf diese Weise finden sich in einer Datei gleichermaßen Schwerkriminelle, schuldunfähige Kinder, hilflos aufgefundene Personen, Anzeigeerstatter, Opfer usw..

Eine Differenzierung der einzelnen Personenkreise findet erst auf einer späteren Stufe des Datenzugriffs statt. Es liegt auf der Hand, daß hier ein beachtliches Risiko an Fehleinschätzungen, über das erforderliche Ausmaß hinausgehenden Zugriffsmöglichkeiten, aber auch Mißbrauchsmöglichkeiten zu verzeichnen ist.

Eine gesetzliche Regelung der automatisierten Datenverarbeitung wird hier insbesondere Einschränkungen des Zugriffs für einzelne Funktionsträger vorsehen müssen. Zu erörtern wäre, ob nicht von vornherein eine dateimäßige Trennung zwischen Daten vorgenommen werden muß, die der Registrierung von Straftätern dienen, und solchen, die andere Personen erfassen und lediglich für Zwecke des Vorgangsnachweises gespeichert werden. Die Voraussetzung für eine Zuordnung zur Straftäterdatei wäre in diesem Fall ein hinreichender Tatverdacht bzw. die auf Tatsachen gestützte Annahme, daß die Wiederholung von Straftaten droht.

Auch soweit es um Strafverdächtige geht, bedarf der Umfang der derzeit gespeicherten und abrufbaren Daten einer Durchsicht. Insbesondere die **taktischen Hinweise,** die auf Anruf jedem Polizeibeamten mitgeteilt werden, bedürfen der Revision: Es ist durchaus zweifelhaft, in welchem Umfang Merkmale wie „geisteskrank", „geistesschwach", „Freitodgefahr", „Prostitution" gespeichert und auf jede Anfrage zur Verfügung gestellt werden müssen.

Die automatisierte Speicherung und Verarbeitung von Spuren- und Hinweisdaten in sog. **Spurendokumentations-Systemen** (SPUDOKs) bedarf ebenfalls einer besonderen Regelung. Gerade hier wird es erforderlich sein, eine Vielzahl von Daten über Nichtbeteiligte, über Hinweisgeber, zu Unrecht Verdächtigte u. ä. geben. Die hierin liegenden Risiken müssen durch strenge Zweckbindung und präzise Löschungsregelungen ausgeglichen werden. Besondere Errichtungsanordnungen für jeden Ermittlungskomplex müssen sicherstellen, daß die Beschränkungen, denen Straftäterdateien unterworfen werden, nicht mit Hilfe derartiger Systeme umgangen werden.

Weiterhin ungelöst ist das Problem, daß mangels einer regelmäßigen **Rückmeldung des Ausgangs der Strafverfahren** durch Gerichte und Staatsanwaltschaften weder eine Vervollständigung der Datensätze von Verdächtigen noch die von den KpS-Richtlinien vorgeschriebene Tilgung der Daten von Unschuldigen möglich ist. Das inzwischen eingeführte automatisierte Verfahren der Staatsanwaltschaft[1] würde hierfür zwar geeignete technische Voraussetzungen schaffen, die beteiligten Stellen haben sich aber zu den erforderlichen Maßnahmen noch nicht bereitgefunden. Es ist zu hoffen, daß entsprechende Bemühungen, im Rahmen einer Revision der Anordnung über Mitteilungen in Strafsachen (MiStra) ein bundeseinheitliches Verfahren zu entwickeln, hier zu einer Besserung führen werden.

Der Berliner Landesgesetzgeber ist aufgerufen, sobald wie möglich hinreichende gesetzliche Grundlagen für die polizeiliche Informationsverarbeitung zu schaffen. Dies hat auch der Senat in seinem Bericht über die Auswirkungen der Entscheidung des Bundesverfassungsgerichts vom 15. Dezember 1983 zum Volkszählungsgesetz 1983[2] zum Ausdruck gebracht. Eine Arbeitsgruppe der Konferenz der Datenschutzbeauftragten wird hierfür Formulierungsvorschläge unterbreiten, die ich umgehend dem Senator für Inneres zuleiten werde.

Überprüfungen im Einzelfall

Einzelfallüberprüfungen wurden in allen Fällen vorgenommen, in denen sich Betroffene über ihrer Ansicht nach mangelhafte Datenverarbeitung bei der Polizei beschwert haben. Wesentliche Mängel konnten dabei nicht festgestellt werden.

Insbesondere hat die Umsetzung der **KpS-Richtlinien** weitere Fortschritte gemacht. Eine eigens geschaffene Arbeitsgruppe beim Referat Dienstleistungen der Direktion Verbrechensbekämpfung ist mit der Anlage, Übermittlung und Aussonderung von Kriminalakten befaßt. Ihr obliegt auch die Auswahl derjenigen Datensätze, die an das Bundeskriminalamt zur Einstellung in den bundesweiten Kriminalaktennachweis (KAN) gemeldet werden. Im Gegensatz zu anderen Bundesländern ist der Anteil derjenigen Daten, auf die ein bundesweiter Zugriff besteht, im Hinblick auf die Gesamtzahl der Datensätze im ISVB gering. Zum Zeitpunkt des Informationsgesprächs waren etwa 100 000 Akten gesichtet, von denen 50 000 vernichtet wurden. Aus 2 000 Akten wurden personenbezogene Daten an den KAN gemeldet.

Auch die Überprüfung einzelner **Dienststellen** von Amts wegen ergab keinen Anlaß zu formellen Beanstandungen. U. a. wurden überprüft die Ermittlungsgruppe Illegale Einreise und Beschäftigung beim Referat U/G der Direktion Verbrechensbekämpfung, das Kommissariat Gruppen-/Rohheitstaten, Rocker im Referat Organisiertes Verbrechen in der Direktion Verbrechensbekämpfung sowie drei zufällig ausgewählte Abschnitte. Die dabei zu Tage getretenen Probleme (Zulässigkeit der Führung von Arbeitskarteien, Speicherung Strafunmündiger im ISVB, Protokollierung der ISVB-Aktivitäten, Zugriffsberechtigung auf ISVB-Daten) müssen in größerem Zusammenhang erörtert werden.

Die Durchführung datenschutzrechtlicher Überprüfungen beim Polizeipräsidenten fand jederzeit die erforderliche Unterstützung, wenn auch die Praxis, mich auch bei geringen Anlässen nur auf dem Dienstweg über den Senator für Inneres zu unterrichten, zu Erschwernissen führt - ein Problem, das auch in anderen Geschäftsbereichen besteht.

3. Beobachtungen beim Betrieb von Bildschirmtext und anderen Neuen Medien

Das Gesetz zum Staatsvertrag über Bildschirmtext vom 23. Juni 1983 (Btx-Zustimmungsgesetz) sieht ebenso wie das Gesetz über die Durchführung des Kabelpilotprojekts Berlin vom 17. Juli 1984 (Kabelpilotprojektgesetz - KPPG) vor, daß der Berliner Datenschutzbeauftragte dem Abgeordnetenhaus von Berlin über von ihm festgestellte Mängel und über seine Vorschläge zu ihrer Behebung und zur Verbesserung des Datenschutzes berichtet[1].

3.1 Erfordernis ergänzender bundesrechtlicher Datenschutzregelungen

Mitte des Jahres wurde der Vollbetrieb des Bildschirmtextsystems aufgenommen. Die Datenschutzbeauftragten hatten von Beginn der Erprobungsphase an darauf hingewirkt, daß der Datenschutz bei Bildschirmtext durch hinreichende rechtliche Regelungen im gesamten Nutzungsbereich abgesichert würde. Die Länder haben im Btx-Staatsvertrag und den entsprechenden Zustimmungsgesetzen zufriedenstellende Regelungen getroffen.

Soweit die Deutsche Bundespost als Betreiber des Systems ebenfalls im Nutzungsbereich Daten erheben, speichern und übermitteln muß, hatte sie den Ländern formell mitgeteilt, daß sie nach den in Art. 9 Btx-Staatsvertrag enthaltenen Grundsätzen verfahren und für ihren Bereich entsprechende Vorschriften vorsehen würde.

So wurden zwar mit der 22. Änderungsverordnung zur Fernmeldeordnung vom 6. Mai 1983 verschiedene Bestimmungen über Bildschirmtext erlassen; ein Vergleich mit Art. 9 Btx-Staats-

[1] Vgl. unter 5.
[2] Mitteilungen des Präsidenten - Nr. 220 -, Drs 9/2056

[1] §§ 3 Abs. 3 Satz 3 Btx-Zustimmungsgesetz und 55 Abs. 1 Satz 2 KPPG

vertrag zeigt jedoch, daß zwischen beiden Regelungen eine erhebliche Differenz besteht. Gegenüber dem Staatsvertrag fehlen insbesondere klare Regelungen zur Verarbeitung der Verbindungsdaten (Umfang der Speicherung, Zeitpunkt der Löschung) und zur Übermittlung von Abrechnungsdaten an den Anbieter.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat hierauf in einer Erklärung hingewiesen und betont, daß die Zustimmung der Länder von einer zufriedenstellenden Regelung des Datenschutzes abhängig gewesen sei[1].

Der Bundespostminister hat auf die Erklärung mit dem Hinweis reagiert, daß sich die Deutsche Bundespost lediglich zur Einhaltung der materiellen Anforderungen des Art. 9 Btx-Staatsvertrag, nicht aber zum Erlaß von Rechtsvorschriften verpflichtet habe. Dem traten die Datenschutzbeauftragten der Länder mit einer Entschließung auf der 20. Konferenz am 6. und 7. Juni 1984 entgegen.

Sie betonten, daß sich die Regelung bei Bildschirmtext nicht in einer einseitigen Verpflichtungserklärung der Deutschen Bundespost gegenüber den Ländern, in Verwaltungsanweisungen oder in Vorkehrungen im technisch-betrieblichen System erschöpfen dürften. Auch das Fernmeldegeheimnis, dessen Erstreckung auf Bildschirmtext nicht unbestritten sei, befreie nicht von der Notwendigkeit, zusätzliche grundrechtssichernde gesetzliche Regelungen zu schaffen, die den besonderen Gefahren der Neuen Medien begegneten.

In einem grundsätzlichen Gespräch zwischen Vertretern der Datenschutzbeauftragten des Bundes und der Länder und der Deutschen Bundespost im November 1984 wurde deutlich, daß die Notwendigkeit bereichsspezifischer Rechtsvorschriften auch von seiten der Deutschen Bundespost anerkannt, jedoch die Frage der Dringlichkeit noch unterschiedlich bewertet wurde. Bei der Post wurde allerdings eine Tendenz erkennbar, entgegen der Forderung der Datenschutzbeauftragten nach einer alsbaldigen bereichsspezifischen Regelung die Novellierung des Bundesdatenschutzgesetzes abzuwarten.

Im einzelnen haben die Datenschutzbeauftragten ihre Ansicht wie folgt begründet:

Das Urteil des Bundesverfassungsgerichts zum Volkszählungsgesetz 1983 gebietet, daß wegen der denkbaren Einschränkungen der informationellen Selbstbestimmung eine dem Gebot der Normenklarheit entsprechende gesetzliche Regelung der Erhebung und Verarbeitung der Daten, die beim Betrieb von Bildschirmtext anfallen, vorhanden sein muß.

Die Freiwilligkeit der Teilnahme kann dem nicht entgegengehalten werden. Auch bei freiwilliger Entscheidung geht der Teilnehmer davon aus, daß die Verwendung der Daten, die aus der Teilnahme resultieren, auf das für die Nutzung Unumgängliche beschränkt ist. Die mangelnde Beeinflußbarkeit der Verarbeitung durch die Teilnehmer macht eine gesetzliche Absicherung erforderlich. Hinzu kommt, daß mit zunehmender Verbreitung sozialer Druck zur Nutzung von Bildschirmtext entstehen kann, der die Freiwilligkeit ohnehin in Frage stellt (z. B. Kontoführung, Bestelldienste, Buchungen).

Die zu Bildschirmtext bestehenden, zum Teil konkurrierenden oder sich überschneidenden Regelungen sind für Anbieter, Teilnehmer und Betreiber nur schwer zu durchschauen. Daraus folgt die Notwendigkeit, Bildschirmtext in seiner Gesamtheit so zu regeln, daß die Rechte und Pflichten der Beteiligten und ihre Rechtsbeziehungen untereinander klar und eindeutig festgelegt werden. Hierzu gehört eine Abgrenzung von Netz- und Nutzungsbereich, an die unterschiedliche Rechtsfolgen anknüpfen. Jedenfalls erscheint die Fernmeldeordnung in ihrer aktuellen Ausgestaltung allein von ihrer Konzeption her für eine solche Regelung ungeeignet.

Im übrigen können technische Sicherungen auch deshalb gesetzliche Sicherungen nicht ersetzen, weil sie jederzeit änderbar sind.

Inhaltlich ist die Verarbeitung personenbezogener Daten bisher in der Fernmeldeordnung auf ungenügende Weise geregelt. Bereichsspezifische Bestimmungen für Verbindungsdaten (Art. 9 Abs. 2 Nr. 1 Btx-Staatsvertrag) fehlen völlig, die für Erhebung und Verarbeitung von Abrechnungsdaten (Art. 9 Abs. 2 Nr. 2 Btx-Staatsvertrag) sind unvollständig. Hinzu müssen flankierende Bestimmungen zur Verstärkung der Kooperation bei der Kontrolle des Datenschutzes bei Bildschirmtext kommen.

Im einzelnen sind folgende Regelungen erforderlich:

1. Abschließende aufgabenbezogene Festlegung der für den Betrieb von Bildschirmtext unerläßlichen Datenarten (insbesondere Verbindungsdaten; Abrechnungsdaten = Vergütungsdaten);
2. Verbot der Speicherung der in Art. 9 Abs. 3 Satz 1 Btx-Staatsvertrag genannten Merkmale in Zusammenhang mit Abrechnungsdaten (Vergütungsdaten) unter Berücksichtigung der mit der Zuteilung mehrerer Leitseiten verbundenen Umgehungsmöglichkeiten;
3. Festlegung der Daten, die an Anbieter übermittelt werden dürfen, einschließlich der ausschlaggebenden Bedingungen und Fristen;
4. Festlegung der Termine für die Löschung der Abrechnungsdaten (Vergütungsdaten);
5. Festlegung des Zeitpunkts der Löschung der Verbindungsdaten; Festlegung, welche Merkmale zur statistischen Auswertung und zur Erzeugung des Abrechnungsdatensatzes (Vergütungsdatensatzes) verwertet werden;
6. Regelung der Verarbeitung personenbezogener Betriebsdaten bei Mitteilungsdiensten (Speicherung, Übermittlung und Löschung der Abrechnungsdaten [Vergütungsdaten]), Verwendung der Verbindungsdaten;
7. Verpflichtung der Deutschen Bundespost zur Auskunft, Berichtigung, Sperrung und Löschung;
8. Präzisierung der von der Bundespost über das Bundesdatenschutzgesetz hinaus durchzuführenden Datensicherungsmaßnahmen (vgl. Art. 9 Abs. 9 Btx-Staatsvertrag).

Der Gesetzgeber muß schließlich klarstellen, daß das Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses (G 10-Gesetz) auf Bildschirmtext nicht anwendbar ist.

Die Datenschutzbeauftragten werden weiterhin für die Verwirklichung dieser Punkte nachdrücklich werben.

3.2 Mängel der technischen Ausgestaltung des Btx-Systems

Anfangs kam die Deutsche Bundespost den Wünschen der Datenschutzbeauftragten von Bund und Ländern nur zögernd entgegen, sie über die technische Konzeption des neuen Bildschirmtextsystems so ausführlich zu informieren, daß es möglich war, die technische Umsetzung der Vorschriften des Art. 9 Btx-Staatsvertrag, insbesondere die des Abs. 8, zu beurteilen. Die Deutsche Bundespost sah ausschließlich den Bundesbeauftragten für den Datenschutz als Adressaten ihrer Informationen an, hat jedoch inzwischen in steigendem – jedoch noch immer eingeschränktem Maße – und ohne jede Verpflichtung anzuerkennen, die Landesdatenschutzbeauftragten in mehreren Informationsveranstaltungen unterrichtet. Die Ende September 1983 durchgeführte und in meinem Jahresbericht 1983, S. 5, erwähnte Informationsveranstaltung der Bundespost war weder aufgrund der Darstellungen noch bezüglich des verteilten Materials geeignet, eine widerspruchsfreie und vollständige Bestandsaufnahme zum technischen System Bildschirmtext zu gewährleisten. Ein Prüfgespräch des Bundesbeauftragten für den Datenschutz auf der Basis eines mit den Ländern abgestimmten Fragenkataloges und eine weitere Informationsveranstaltung im Mai 1984 ergab dann einen Informationsstand, der eine vorläufige Bewertung des Systems aus technischer Sicht erlaubt. Da einige verbindliche schriftliche Unterlagen der Deutschen Bundespost noch fehlen, bleiben jedoch Unsicherheiten. Inzwischen hat sich die Bundespost bemüht, die Informationen zu ergänzen und ihre Offenheit für weitere Verbesserungen angedeutet.

Der seit Juni 1984 realisierte Vollbetrieb setzt bisher noch nicht alle Anforderungen der Deutschen Bundespost an den System-

[1] Erklärung der 19. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 27./28. März 1984

hersteller um. Verschiedene Leistungen des Systems, auch solche, die den Datenschutz unmittelbar betreffen, werden erst in weiteren Ausbaustufen des Systems angeboten werden können.

Meine Beschäftigung mit dem Btx-System hat trotz der begrenzten Information durch die Post gezeigt, daß der Datenschutz bei der jetzigen Gestaltung nicht in allen Punkten den Anforderungen des Art. 9 Btx-Staatsvertrag entspricht, an dessen materielle Anforderungen sich auch die Bundespost für gebunden hält. Es haben sich bisher folgende Defizite gezeigt:

Der **Schutz vor unbefugter Verwendung des Systems** (Art. 9 Abs. 8 Btx-Staatsvertrag) entspricht noch nicht dem Standard, der angesichts der Risiken offener Systeme angemessen wäre:

Die Anschlußkennung, die von der allgemein eingesetzten Bildschirmtext-Anschlußbox DBT 03 automatisch bei Beginn des Dialogs an das System gesendet wird, um damit den verwendeten Anschluß eindeutig zu identifizieren, kann mit Hilfe der ebenfalls zugelassenen Modems oder durch unbefugte Eingriffe simuliert werden.

Die Anschlußkennung und das geheime achtstellige Kennwort sind gegen Ausforschung nicht ausreichend geschützt, da

- beide unverschlüsselt übermittelt werden und somit im Telefonnetz abgehört bzw. mitgeschnitten werden können,
- die Anschlußkennung nicht geändert werden kann und somit die Gefahr, daß die Geheimhaltung durchbrochen wird, mit der Zeit wächst,
- Anforderungen an die Gestaltung des Kennwortes in der derzeitigen Ausbaustufe nicht gestellt werden, so daß leicht erratbare Kennwörter benutzt werden können,
- die Sperrung des Anschlusses nach maximal neun vergeblichen Versuchen pro Tag, das Kennwort zu erproben, kann durch einen relativ einfachen Trick so umgangen werden, daß unbegrenzt Versuche durchgeführt werden können,
- der richtige Anschlußinhaber von Fehlversuchen unter seiner Kennung nicht unterrichtet wird, und somit nicht vor ihn betreffenden Ausforschungsversuchen gewarnt wird,
- eine zufällige Einspielung von Elementen aus fremden Teilnehmerdatensätzen nicht auszuschließen war.

Anders als beim Feldversuch ist die Editierfunktion für Anbieter nicht mehr durch ein besonderes Kennwort geschützt. Jemand, der Anschlußkennung und Kennwort erfolgreich ausgeforscht hat, kann somit das Programm des Anbieters ändern oder löschen.

Aus den vorliegenden Datensatzbeschreibungen ergibt sich, daß die Deutsche Bundespost als Betreiber von Bildschirmtext nicht in vollem Umfang den Anforderungen des Art. 9 Abs. 2 und 3 Btx-Staatsvertrag nachkommt.

Der in der Bildschirmtext-Leitzentrale für die Abrechnung kostenpflichtiger Seiten verwendete Gutschriften- und Entgeltsatz enthält die Teilnehmernummern des Anfragenden (Verursacher) im Zusammenhang mit den Daten des Anbieters, insbesondere der Leitseite, über die der Anfragende in das Programm des Anbieters gelangte, sowie den Zeitpunkt des Anfalls der Gebühr (Zeitstempel). Ein Anbieter kann eine sehr große Anzahl unterschiedlicher Leitseiten eingerichtet haben. Auf diese Weise kann er das Angebot inhaltlich aufteilen und so Rückschlüsse auf Zeitangaben und inhaltliche Differenzierung ableiten. Dies steht im Widerspruch zu Art. 9 Abs. 3 Satz 1 Btx-Staatsvertrag.

3.3 Mängel, für die Betreiber mitverantwortlich sind

Unzulässig sind Praktiken, die beobachtet worden sind, bzw. deren Durchführbarkeit demonstriert worden ist:

- Aus einer Eingabe ergab sich, daß ein Anbieter die Zusendung von Antwortseiten erbittet, bei denen er die Möglichkeit vorsieht, daß der Absender die von der Deutschen Bundespost eingeblendete Adresse des Anschlußinhabers löscht oder ändert, daß er jedoch eine weitere Einblendung dieser Daten auf der Antwortseite vornehmen läßt, die er durch die Wahl einer farbgleichen Hintergrundfarbe unsichtbar für den Teilnehmer macht. Die bisherige Kennzeichnung personenbezogener Daten durch „P" reicht nicht aus.
- Im Zusammenhang mit der Anwendung von intelligenten Decodern, die in Kleincomputern oder in Bildschirmtext-Endgeräten integriert sind, lassen sich unter Einsatz von Telesoftware illegale Praktiken ausführen. Eine Reihe von Anbietern bieten Benutzern solcher Decoder spezielle Bildschirmtextprogramme an, die nicht wie üblich aus Bildschirmtextinhalten bestehen, die im Bildschirmtextsystem gespeichert sind, sondern aus Software, welche Bildschirmtextinhalte beim Teilnehmer aufbaut. Das Bildschirmtextsystem fungiert in solchen Fällen quasi als Softwarebibliothek. Der abrufende Teilnehmer lädt sich solche Programme über Bildschirmtext in seinen intelligenten Decoder und läßt sie ausführen. Es ist möglich, daß solche Programme Kommandos enthalten, die mit dem eigentlichen Zweck des Programmes nichts zu tun haben und deren Ausführung für den Teilnehmer unbemerkt bleibt. Mit solchen Kommandos können z. B. Antwortseiten unmerkbar für den Teilnehmer von ihm an den Anbieter gesendet werden. Das gleiche kann für die Benutzung externer Rechner gelten.
- Beim Mitteilungsdienst wird die durch die eingegebenen Buchstaben dargestellte Information, die für den Empfänger bestimmt ist, in der Btx-Vermittlungsstelle gespeichert. Informationen über Formate, Farben, frei definierte Zeichen usw. werden als sogenannte Decoder-Informationen jedoch bei jedem Aufruf der Mitteilung durch den Empfänger beim Absender abgerufen. Da letzterer die Möglichkeit hat, solche Informationen noch zu ändern, nachdem der Empfänger die Mitteilung bereits gelesen, aber noch nicht gelöscht hat, kann der Text von Mitteilungen nach dem Lesen im beschränkten Rahmen geändert werden.

Diese Praktiken bedeuten zwar auch vorsätzliche Verstöße gegen den Btx-Staatsvertrag; die Post ist jedoch als Betreiber technischer Einrichtungen gefordert, durch technische Maßnahmen und durch die Gestaltung von Zulassungsbedingungen solchen Verstößen von vornherein zu begegnen, die Teilnehmer jedenfalls über die bestehenden Risiken aufzuklären.

Die Deutsche Bundespost hat in dem im November 1984 geführten Gespräch nicht alle diese Punkte anerkannt, jedoch konkrete Maßnahmen zur schrittweisen Erhöhung des Sicherheitsstandards eingeleitet und weitere angekündigt. Danach ist zu hoffen, daß wesentliche Punkte erfüllt werden. Dies wird von den Datenschutzbeauftragten weiter kritisch beobachtet werden.

Wegen der Telesoftware-Problematik habe ich Kontakte mit Herstellern des intelligenten Decoders sowie einem Elektrokonzern, der diese Decoder in einem Teil seiner Bildschirmtext-Endgerätemodelle integriert hat, aufgenommen. Eine zufriedenstellende Lösung des Problems, welches im Prinzip alle Telesoftware-Anwendungen bei Bildschirmtext betrifft, ist noch nicht vorgelegt worden.

Neben der Deutschen Bundespost können **weitere Betreiber,** die zur Nutzung von Bildschirmtext technische Einrichtungen für andere bereitstellen, tätig sein.

Dies ist dann der Fall, wenn nicht die Anbieter selbst technische Einrichtungen schaffen, sondern sich eines Dritten bedienen, der bestimmte Dienste auftragsweise über Bildschirmtext vermittelt. Ein Beispiel für eine derartige Konstellation ist das Rechenzentrum Rheinland, das für verschiedene Sparkassen - so auch für die Sparkasse der Stadt Berlin West - einen Btx-Kontoservice (Kontoabruf, Überweisungen, Bestellung von Scheckheften) vermittelt.

Die Betreiberfunktion bedingt auch hier die Anwendung von Art. 9 Abs. 3 Btx-Staatsvertrag mit der Folge, daß eine Protokollierung der Sitzungen einzelner Teilnehmer nur mit deren Einwilligung möglich ist. Die vorliegenden vertraglichen Vereinbarungen sahen entsprechende Klauseln nicht vor, obwohl derartige Protokolle gefertigt wurden.

3.4 Mängel auf Seiten der Anbieter

Veröffentlichung personenbezogener Daten im Angebot

Nach Art. 9 Abs. 5 Btx-Staatsvertrag sind Angebote an den Übermittlungsvorschriften der Datenschutzgesetze zu messen. Für private Anbieter bedeutet dies, daß personenbezogene Daten

in Btx-Seiten nur aufgenommen werden dürfen, wenn die Voraussetzungen des § 24 Bundesdatenschutzgesetz vorliegen, d. h. wenn die Veröffentlichung entweder durch ein entsprechendes Vertragsverhältnis gedeckt ist oder die Veröffentlichung zur Wahrung der berechtigten Interessen des Anbieters (oder eines Dritten oder der Allgemeinheit) erforderlich ist und dadurch schutzwürdige Belange des Betroffenen nicht beeinträchtigt werden.

Ich habe beobachtet, daß insbesondere von kleineren Anbietern gegen diese Bestimmung verstoßen wird.

Ohne Zweifel ist dies der Fall, wenn diskriminierende Tatsachenbehauptungen über einzelne Personen veröffentlicht werden. So wurde in einem Fall darauf hingewiesen, eine bestimmte Person sei ins Schuldnerverzeichnis eingetragen worden, in einem anderen Fall darauf, daß eine Haftanordnung zur Abgabe der eidesstattlichen Versicherung ergangen sei. Die schutzwürdiben Belange der Betroffenen stehen hier **stets** der Veröffentlichung entgegen.

Problematischer ist die Beurteilung dann, wenn nur Bewertungen über andere Personen abgegeben werden. So habe ich mehrfach abfällige Äußerungen eines Btx-Anbieters über andere Anbieter festgestellt. Zwar handelt es sich hier nur bedingt um Angaben über persönliche oder sachliche Verhältnisse Dritter; da aber Tatsachenbehauptungen und Bewertungen kaum voneinander geschieden werden können, zudem auch aus Bewertungen Schlüsse auf Tatsachen gezogen werden können, wäre eine Differenzierung verfehlt. Auch hier ist demnach eine Verletzung schutzwürdiger Belange zu prüfen.

Sehr beliebt ist es bei manchen Anbietern, Briefe über Btx zu veröffentlichen, die den Anbieter erreicht haben. Hier fehlt in der Regel bereits das berechtigte Interesse des Anbieters. Da die Veröffentlichung eines persönlich adressierten Briefes durch den Empfänger per se schutzwürdige Belange des Verfassers beeinträchtigt, dürfte eine Veröffentlichung überhaupt nur mit Einwilligung des Schreibers zulässig sein.

Diese Einwilligung muß ausdrücklich erteilt werden. Eine Ankündigung des Anbieters (z. B. im Impressum), daß alle eingehenden Briefe veröffentlicht würden, reicht für die Einwilligung keinesfalls aus.

Da das Datenschutzrecht nur natürliche Personen schützt, gelten diese Überlegungen nicht unmittelbar für juristische Personen. Die Praktikabilität der Regelung wird aber auch hier eine Gleichbehandlung gebieten.

Erhebung personenbezogener Daten durch den Anbieter

Besonders strenge Anforderungen stellt der Staatsvertrag an das Abfragen und Speichern personenbezogener Daten des Teilnehmers durch den Anbieter; auch die weitere Verarbeitung dieser Daten unterliegt weitgehenden Einschränkungen: Die Abfrage und die Speicherung sind auf das für den Vertrag (unbedingt) Erforderliche begrenzt; auch die weitere Verarbeitung muß vom Vertragszweck gedeckt sein, wenn nicht der Teilnehmer in eine darüber hinausgehende Verarbeitung einwilligt. An diese Einwilligung sind Aufklärungs- und Formvorschriften geknüpft.

Obwohl dies bereits in der Erprobungszeit beanstandet wurde, verstießen Anbieter noch immer gegen diese Bestimmungen, indem sie in Angebotsseiten, die an den Anbieter zurückgesandt werden mußten, den Namen des Teilnehmers durch die Btx-Zentrale eingeben ließen. Hier fehlt es in der Regel an der Erforderlichkeit für die Vertragserfüllung.

Besonders problematisch wird die Abfrage personenbezogener Daten dann, wenn diese vom Anbieter umgehend wiederum ins eigene Programm eingestellt werden: So lud ein Anbieter die Teilnehmer zu Informationsveranstaltungen ein und bat um Anmeldung über Btx; die Personen, die sich angemeldet hatten, wurden unverzüglich auf einer Angebotsseite bekanntgegeben. Dies ist nur mit ausdrücklicher Einwilligung zulässig.

Das gleiche gilt, wenn Mitteilungen an den Anbieter nicht über Briefpost gesendet werden, sondern über den Btx-Mitteilungsdienst selbst. Hier bedarf die Veröffentlichung ebenfalls der (ausdrücklichen) Einwilligung (nunmehr nach Art. 9 Abs. 6 Btx-Staatsvertrag).

In diesem Fall ist auch fraglich, ob über den (eigenen) Mitteilungsdienst ohne weiteres die Systemnummer der Teilnehmer abgefragt werden darf: Diese ist erforderlich nur für den Fall, daß der Anbieter seinerseits dem Teilnehmer über Btx Mitteilungen übersenden will. Daß der Teilnehmer dies wünscht, kann nicht in jedem Fall unterstellt werden, etwa dann, wenn die Mitteilung sich auf einen sensiblen Bereich bezieht (z. B. Darlehensberechnungen einer Bank), da die Vertraulichkeit beim Empfänger dann nicht gewährleistet werden kann, wenn verschiedene Personen (z. B. Familienmitglieder) unter gleicher Kennung auf das System zugreifen dürfen. In diesem Fall wäre die Erhebung mit der Einholung einer entsprechenden Einwilligung zu verbinden.

In der Regel werden derartige Einwilligungen über Btx selbst eingeholt. Hier ist die Formvorschrift des Art. 9 Abs. 6 Satz 6 Btx-Staatsvertrag zu beachten: Die Einwilligung bedarf (außer einer vorherigen Aufklärung) auch der Bestätigung („Dreistufentheorie").

Anbieter, insbesondere werbende Anbieter, haben aus naheliegenden Gründen ein Interesse zu erfahren, wer sich für ihr Programm interessiert. Normalerweise überlassen sie es dem Teilnehmer, aus eigenem Willen Mitteilungen oder Antwortseiten zu übersenden, motivieren gelegentlich auch besonders dazu, wenn sie etwa die Inanspruchnahme besonders attraktiver Programmteile (z. B. Spiele) von der vorhergehenden Absendung einer Antwortseite abhängig machen. Hier wird zweifellos noch in legaler Weise auf die freie Entscheidung des Teilnehmers Einfluß genommen.

Andere Anbieteraktivitäten

Neben diesen materiell-datenschutzrechtlichen Problemen der Anwendung des Btx-Staatsvertrages habe ich auch Feststellungen getroffen, die darüber hinausgehende Aspekte betreffen, aber zur Gesamteinschätzung des Systems beitragen können:

Häufig beschweren sich Teilnehmer darüber, daß sie über den Mitteilungsdienst der Post in großer Menge unaufgefordert Werbemitteilungen erhalten: Hier kehrt das Problem der Belästigung durch entsprechende Briefsendungen wieder; allerdings tritt es hier dadurch verschärft auf, daß die Versendung derartiger Mitteilungen mit Hilfe geeigneter Kleincomputer automatisch vorgenommen werden kann. Wegen der begrenzten Kapazität des „elektronischen Briefkastens" kann hier eine Blockierung des Mitteilungsdienstes eintreten.

In Btx ist es möglich, fremde Angebotsseiten in das eigene Angebot zu übernehmen. Teilnehmer haben sich darüber beschwert, daß dies geschehen ist und darüber hinaus diskriminierende Verfälschungen vorgenommen wurden. Ähnliche Effekte können dadurch erzielt werden, daß der Teilnehmer (nach einem abfälligen Kommentar) mit einem entsprechenden Hinweis zu einem fremden Angebot hingewiesen wird.

Der oben beschriebene Mißbrauch von Telesoftware, der zur unbewußten Absendung von Antwortseiten führt, kann auch benutzt werden, um unbemerkt kostenpflichtige Seiten des Anbieters aufzurufen und den Teilnehmer so finanziell zu schädigen.

3.5 Kabelpilotprojekt

Am 25. Juli 1984 wurde das Kabelpilotprojektgesetz - KPPG - verkündet. Damit ist eine mehrjährige Phase der Diskussion abgeschlossen und die Tür zu einer neuen Form öffentlicher Kommunikation und Information aufgestoßen. Ich habe schon in meinen früheren Berichten darauf hingewiesen, daß die Einführung der Kabelkommunikation auf Breitbandkabeln die Veranstalter und die Benutzer vor noch nicht bekannte datenschutzrechtliche Probleme stellen wird. Für das Erprobungsgesetz ging es daher darum, auf Grund der Erfahrung mit der Erprobung des Bildschirmtextsystems im Vorgriff auf zu erwartende Gefahren und Risiken eine datenschutzrechtliche Regelung zu schaffen, die einen wirksamen Schutz gegen Verletzungen der Persönlichkeitsrechte erzeugen kann.

Hierzu hatte ich bereits im Vorjahr dem Senator für Kulturelle Angelegenheiten Formulierungsvorschläge unterbreitet, die zwar

von den Datenschutzregelungen des Btx-Staatsvertrages ausgehen, aber darüber hinausgehende spezifische Gefährdungen mit einbeziehen.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat auf der Basis meiner Vorschläge einen Musterentwurf für Datenschutzregelungen in Mediengesetzen verabschiedet, der nach Maßgabe der jeweiligen Landesregelungen zur Übernahme empfohlen werden sollte[1]. Zu Fernmeß- und Fernwirkdiensten wurde ein gesonderter Beschluß gefaßt, der sich ebenfalls an den Berliner Vorschlägen orientiert.

Es ist gelungen, die Empfehlungen der Datenschutzbeauftragten im Berliner Gesetz weitestgehend zu berücksichtigen.

Hervorzuheben sind insbesondere folgende Regelungen:

- Klare Zuständigkeitsregelungen für die Träger des Kabelpilotprojektes (Anstalt für Kabelkommunikation, Kabelrat, Projektgesellschaft, Kabelzentrale), die auch eine klare Zuordnung datenschutzrechtlicher Probleme ermöglichen
- Verbot der Weitergabe personenbezogener Nutzungsdaten von der Projektgesellschaft an die Anbieter („nutzungsneutrale Speicherung von Benutzungsdaten")
- Regelung des Datenschutzes bei Fernmeß- und Fernwirkdiensten
- Zuständigkeit des Berliner Datenschutzbeauftragten auch für die Beobachtung und Beratung der Projektgesellschaft.

Der derzeitige Stand der Projektarbeiten läßt eine Beurteilung der Frage, ob die Datenschutzvorschriften beachtet werden, noch nicht zu.

In den ersten Phasen des Kabelpilotprojektes werden reine Verteildienste und das sogenannte Pay-TV als Abonnementsdienst eingeführt. Bei den Verteildiensten werden keine Daten über die Teilnehmer benötigt, beim Pay-TV soll lediglich festgehalten werden, ob jemand daran teilnimmt oder nicht. In beiden Fällen sollen differenzierte Nutzungsdaten nicht erfaßt werden. Dies soll sich erst mit der ab 1987 geplanten Einführung individueller Abrufdienste ändern.

Hinsichtlich des technischen Konzeptes sind die aus datenschutzrechtlicher Sicht bedeutsamen Entscheidungen noch nicht getroffen worden. Aus technischen Gründen wird die Verteilung innerhalb der Häuser nicht mit dem in anderen Bundesländern teilweise eingesetzten FAT-Konverter zu realisieren sein. Dieser Konverter ist in der Fachpresse als problematisch für den Datenschutz dargestellt worden.

Erstmals für die Bundes- oder Ländergesetzgebung regelt das Berliner Kabelpilotprojektgesetz datenschutzrechtliche Aspekte von Fernmeß- und Fernwirkdiensten wie z.B. TEMEX. Während in München und Ludwigshafen Systemversuche mit TEMEX durchgeführt werden, findet in Berlin auch versuchsweise noch kein Einsatz dieses Dienstes statt. Ich werde die Entwicklung dieses Projektes beobachten und über die Realisierung des Datenschutzes sowie festgestellte Mängel berichten.

4. Weitere Fragen aus der Kontroll- und Beratungspraxis

4.1 Systematische Überprüfungen

Wie geplant habe ich die Landesversicherungsanstalt Berlin (LVA), die Allgemeine Ortskrankenkasse Berlin (AOK), die Sparkasse der Stadt Berlin West, die Feuersozietät/Öffentliche Lebensversicherung, die Wohnungsbau-Kreditanstalt Berlin/Berliner Pfandbriefbank und die Bezirksämter Wedding und Steglitz überprüft. Die Ergebnisse der Prüfungen in der WBK/Pfandbrief-Bank und im Bezirksamt Steglitz liegen noch nicht vor. Die Ergebnisse der Prüfung des Bezirksamts Neukölln von Ende 1983 sind im folgenden berücksichtigt.

Öffentliche Wirtschaftsunternehmen

Bei den geprüften öffentlichen Wirtschaftsunternehmen liegt die Besonderheit vor, daß für sie andere datenschutzrechtliche Rahmenbedingungen bestehen als für ihre privaten Mitbewerber. Dies betrifft insbesondere die externe Datenschutzaufsicht, die bei den geprüften Unternehmen durch den Datenschutzbeauftragten von Amts wegen, bei den Mitbewerbern durch die Aufsichtsbehörde für den Datenschutz nur auf Anlaß ausgeübt wird.

Die bei der Sparkasse der Stadt Berlin West durchgeführten Maßnahmen zum Datenschutz entsprechen den hohen Erwartungen, die an ein Kreditinstitut dieser Größe zu stellen sind. In einzelnen Fällen konnte ich Empfehlungen zur weiteren Verbesserung des Datenschutzes geben. U. a. habe ich angeregt, auf die zuständigen Gremien der Kreditwirtschaft einzuwirken, daß gemeinsam Verfahren geprüft werden, die den vorhandenen Manipulationsschutz bei der Datenfernübertragung durch einen verbesserten Schutz vor der unbefugten Kenntnisnahme von Daten - etwa durch Verschlüsselung - ergänzen. Weitere Anregungen betrafen Verbesserungen in der Organisation des Rechenzentrums, die im Rahmen eines geplanten Neubaus realisiert werden sollen.

Die im Vergleich zur Sparkasse wesentlich kleineren öffentlichen Wirtschaftsunternehmen Feuersozietät und Öffentliche Lebensversicherung betreiben ein gemeinsames Rechenzentrum. Die sich daraus ergebenden datenschutzrechtlichen Probleme sind noch nicht abschließend diskutiert. Unabhängig davon habe ich jedoch die Gelegenheit ergriffen, in verschiedenen Fragen der Rechenzentrumsorganisation und der Speicherung von Kunden- und Vertreterdaten Empfehlungen zur Verbesserung des Datenschutzes auszusprechen.

Sozialleistungsträger

Die Prüfungen der LVA und der AOK ergaben, daß beide Sozialleistungsträger besondere Anstrengungen zur Sicherstellung des Datenschutzes machen. Die Datenschutzbeauftragten beider Versicherungen führen in ihrem Hause selbst interne Datenschutzüberprüfungen durch. Bei der LVA war kurz vor meiner Überprüfung eine solche Untersuchung abgeschlossen worden, die in vielerlei Hinsicht meine Ergebnisse bestätigte. Die Prüfergebnisse von AOK und LVA waren in vielen Aspekten ähnlich: Die Feststellungen beziehen sich im wesentlichen auf Probleme, die die Expansion der Datenverarbeitung mit sich gebracht hatte oder die durch Zeitdruck bei der Neu- und Umgestaltung von Verfahren aufgrund geänderter Gesetzeslagen hervorgerufen wurden.

Auf Grund der räumlichen Verhältnisse im Sicherheitsbereich waren in beiden Fällen Probleme bei der Zugangskontrolle und der Funktionentrennung festzustellen. Hinsichtlich der Zu- und Abgangskontrolle sowie der Funktionentrennung hat die LVA die empfohlenen Sofortmaßnahmen getroffen. Im Rahmen einer ins Auge gefaßten Verlegung des Rechenzentrums sollten meine Empfehlungen zur datenschutzgerechten Organisation des Rechenzentrums einbezogen werden. Die AOK hat in ihrer Stellungnahme zum Prüfbericht angekündigt, daß Umbaumaßnahmen des Sicherheitsbereiches erfolgen werden, die meinen Empfehlungen entsprechen, und Pläne dafür vorgelegt.

Die Verwendung von personenbezogenen Echtdaten zu Testzwecken halte ich grundsätzlich nicht für zulässig. Aufgrund meiner Empfehlung verwendet die LVA nunmehr Testdaten, die durch ein spezielles Programm durch Anonymisierung aus Echtdaten gewonnen werden. Die AOK hat zugesagt, daß ihre Praxis, nicht mit Echtdaten zu testen, durch eine entsprechende Anweisung festgelegt werden soll.

Der Raum- und Schrankverschluß reichte bei der LVA zur angemessenen Unterbringung von manuellen Datensammlungen mit überaus schutzwürdigen Daten der Versicherten oder Antragsteller nicht aus. Auch die vorgesehene Isolierung des Besucherbereichs der LVA von den übrigen Diensträumen räumt meine Bedenken nicht aus.

Die LVA hat jedoch meine Empfehlungen zum besseren Verschluß der Unterlagen als unverhältnismäßig abgewiesen und überdies meine Zuständigkeit bestritten.

Bezirksämter

Bei den Prüfungen in den Bezirksämtern bestätigten sich bereits früher getroffene Feststellungen. Zusammengefaßt ergab sich folgendes:

[1] Vgl. Anlage 2

Die bisher strittige Frage, ob ein Bezirksamt insgesamt als speichernde Stelle anzusehen ist und damit die **Weitergabe von Daten innerhalb des Bezirksamts** nicht den Bestimmungen des Datenschutzgesetzes unterliegt, wurde durch das Urteil zum Volkszählungsgesetz 1983 entschieden. Das Gericht hat darin die Forderung nach „informationeller Gewaltenteilung" innerhalb der Verwaltung aufgestellt. Damit wird meine seit jeher vertretene Auffassung bestätigt, daß die Weitergabe personenbezogener Daten innerhalb des Bezirksamtes von einem Verwaltungsbereich in den anderen nur unter den für die Übermittlung gesetzlich festgelegten Voraussetzungen zulässig ist.

Daher habe ich auch seit jeher bemängelt, daß Auskünfte aus dem Einwohnermeldedatensatz an andere Stellen **desselben** Bezirksamts nicht protokolliert worden sind. Das Argument der Bezirksämter, die Protokollierungspflicht beziehe sich nur auf Übermittlungen und Auskünfte an Dritte, eine Datenweitergabe innerhalb eines Bezirksamts sei keine Übermittlung, läßt sich nun nicht mehr aufrechterhalten. Die Bezirksämter sind gehalten, auch in diesen Fällen zu protokollieren.

Die Meldungen der Kirchensteuerstellen an das Bezirkseinwohneramt enthalten eine Reihe von Daten, die im Rahmen der Aufgabenerfüllung nicht benötigt werden. Wegen der Speicherung überflüssiger Daten habe ich Kontakt mit dem Senator für Inneres und den Kirchen aufgenommen mit dem Ziel, daß nur noch die erforderlichen Daten übermittelt werden.

Nach dem Berliner Datenschutzgesetz (§ 16 Satz 2 Nr. 1) haben die speichernden Stellen eine Dateienübersicht zu führen, in der neben den automatisiert erstellten Dateien auch sämtliche manuellen Karteien enthalten sein sollen. Von den geprüften Stellen wurden derartige Dateienübersichten vorgelegt, jedoch war bei einer in dieser Übersicht aufgeführten aber nicht mehr fortgeschriebenen Kartei der Verbleib bzw. die Vernichtung dieser Kartei nicht mehr nachzuweisen. Weiterhin mußte festgestellt werden, daß veraltete Karteien - je nach Erforderlichkeit - nicht als gesperrt gekennzeichnet bzw. vernichtet wurden.

Auch bei der Meldung zum Dateienregister nach der Veröffentlichung im Amtsblatt für Berlin wurden erneut Mängel festgestellt.

Bei beiden Bezirksämtern habe ich in unterschiedlichem Maße Mängel hinsichtlich der sicheren Unterbringung von manuellen Datenträgern mit personenbezogenen Daten festgestellt. Im Gegensatz zu den vorangegangenen Prüfungen ist jedoch insofern eine Verbesserung zu vermerken, als die Datenträger mehr und mehr unter Sicherheitsverschluß verwahrt werden.

Ich werde die Überprüfung der Bezirksämter auch im nächsten Jahr fortsetzen.

Aspekte der Auftragsdatenverarbeitung

Die Wohnungsbau-Rechenzentrum GmbH verarbeitet zur Zeit für den Senator für Bau- und Wohnungswesen Daten über Sozialwohnungen und für Bezirksämter Mietdaten. Daneben führt die Wohnungsbau-Rechenzentrum GmbH auch Arbeiten für private Auftraggeber, insbesondere Wohnungsbaugesellschaften, durch. In einem gemeinsamen Informationsgespräch mit der Aufsichtsbehörde für den Datenschutz, habe ich festgestellt, daß eine Trennung der Zugriffsberechtigung auf öffentliche und private Daten nicht vorgesehen ist.

Eine derartige Trennung erscheint aus mehreren Gründen geboten: Soweit On-line-Verfahren eingesetzt werden, kann nur eine deutliche technische Trennung den Zugriff öffentlicher Auftragnehmer auf private Daten und umgekehrt verhindern. Eine bloße Absicherung über Codes oder speziell zugeordnete Dateibezeichnungen reicht nicht aus. Ungeachtet der Verpflichtung zur Wahrung des Datengeheimnisses ist anzustreben, daß nicht dieselben Mitarbeiter mit der Bearbeitung privater und öffentlicher Datenbestände betraut werden. Durch klare organisatorische Trennung sollte das bestehende Restrisiko vermindert werden. Im Hinblick auf die Datenschutzkontrolle ist es erstrebenswert, die Verarbeitung öffentlicher und privater Daten getrennt zu protokollieren und die dabei entstehenden Datenbestände getrennt aufzubewahren. Das Wohnungsbau-Rechenzentrum GmbH hat die Verfahren entsprechend meiner Empfehlung umgestellt.

Da die für den Senator für Bau- und Wohnungswesen erledigten Aufgaben im kommenden Jahr vom Wohnungsbau-Rechenzentrum an das Landesamt für Elektronische Datenverarbeitung übergehen werden, betreffen meine Empfehlungen beim Wohnungsbau-Rechenzentrum künftig nur die Mietenabrechnung der Bezirksämter. Die datenschutzrechtlichen Anforderungen sind jedoch in allen Fällen einer Verarbeitung von Verwaltungsdaten in privaten Rechenzentren zu beachten.

Nach § 2 Abs. 2 Berliner Datenschutzgesetz ist die Verarbeitung personenbezogener Daten durch Auftragnehmer nur im Rahmen der Weisungen der Auftraggeber zulässig. In mehreren Eingaben bin ich darauf hingewiesen worden, daß das Landesamt für Elektronische Datenverarbeitung in einem Falle auf Bitte der Betriebskrankenkasse (BKK) Berlin durch Verwendung der ADV-Verfahren Besoldung, Lohn und Vergütung Mitteilungen der BKK aufbereitete und versandte. Durch ein Versehen wurden auch Angestellte erfaßt, die nicht Mitglied der BKK sind. Nicht dieses Versehen, sondern die Tatsache, daß das LED diese Aktion ohne Benehmen mit den Abrechnungsstellen als datenschutzrechtlich verantwortliche speichernde Stellen abgewickelt hat, war für mich Anlaß zur Beanstandung eines Verstoßes gegen § 2 Abs. 2 Satz 2 Berliner Datenschutzgesetz beim Senator für Inneres. Der Senator für Inneres hat in seiner Stellungnahme versichert, daß das LED in Zukunft ohne ausdrückliche Erklärung der speichernden Stelle keine Auswertung personenbezogener Daten mehr vornehmen wird.

4.2 Stellungnahme zu neuen Verfahren

Entsprechend dem Rundschreiben des Senators für Inneres vom 17. März 1981[1] wurde ich von mehreren Verwaltungen um Stellungnahme zur Neukonzeption bzw. Erweiterung bestehender ADV-Verfahren gebeten.

Automatisiertes Liegenschaftsbuch (ALB)

Der Senator für Bau- und Wohnungswesen hat das von der Arbeitsgemeinschaft der Vermessungsverwaltungen der Länder der Bundesrepublik Deutschland (AdV) entwickelte bundeseinheitliche Konzept für die Automatisierung des Liegenschaftskatasters als Basis für ein Grundstücksinformationssystem unter weitergehender Integration mit anderen grundstücksbezogenen Bereichen übernommen.

Dabei werden die Aufgaben wie bisher von den Vermessungsämtern der Abt. Bauwesen in den Bezirken wahrgenommen, die Bearbeitung wurde aber nunmehr durch ein ADV-Verfahren unterstützt. Hierbei stellt sich insbesondere das Problem des On-line-Zugriffes der Vermessungsämter auf die Zentrale Datenbank. Da bei einem On-line-Zugriff gem. § 4 Abs. 2 Nr. 2 Berliner Datenschutzgesetz jedoch der gesamte Bestand als übermittelt gilt, muß stets geprüft werden, ob die Zulässigkeitskriterien nach § 10 Berliner Datenschutzgesetz erfüllt werden; anderenfalls ist durch eine programmtechnische Maßnahme im Rahmen der Zugriffskontrolle (Nr. 5 der Anlage zu § 5 Abs. 1 Berliner Datenschutzgesetz) sicherzustellen, daß der Mitarbeiter ausschließlich auf Daten des eigenen Bezirkes zugreifen darf. Diese Forderung bekommt gerade für das geplante Grundstücksinformationssystem Bedeutung, da an ihm verschiedene speichernde Stellen beteiligt werden sollen.

Lastschrifteneinzugsverfahren

Der Senator für Finanzen hat zum 1. April 1984 eine Verfahrenserweiterung bei der Automatisierung des Zahlungsverkehrs vorgenommen. Seither besteht auch die Möglichkeit, am Lastschrifteneinzugsverfahren teilzunehmen. Bisher konnten Zahlungsverpflichtungen gegenüber dem Land Berlin und den Bezirken nur durch Bareinzahlungen oder als Dauerauftrag durchgeführt werden. In dem mir zugeleiteten Entwurf der Verfahrensregelungen wurde darauf hingewiesen, daß die erstellten Lastschriftbelege keine Angaben des Verwendungszweckes enthalten sollten, da andere Kriterien eine ausreichende Bestimmung gewährleisteten. Diese datenschutzfreundliche Handhabung, die

[1] Dienstblatt des Senats von Berlin, Teil I, Jg. 1981, S. 30

ich bereits in meinen früheren Jahresberichten[1] gefordert hatte, war jedoch in der endgültigen Verfahrensbeschreibung nicht mehr enthalten. Nach Auffassung des Senators für Finanzen dient die Angabe des Verwendungszweckes auf dem Lastschriftbeleg letztlich der besseren Überschaubarkeit für den Zahlungspflichtigen. Ich habe in diesem Zusammenhang dem Senator für Finanzen eine bürgerfreundliche und datenschutzgerechte Lösung empfohlen, nach der der Zahlungspflichtige selbst entscheiden soll, ob der Zahlungsgrund ausgedruckt wird oder nicht.

Dieser Empfehlung wollte der Senator für Finanzen bisher aus programmtechnischen Gründen nicht nachkommen.

ADV-Grundsätze und ADV-Testrichtlinien

Die Neuordnung der Organisation für die automatische Datenverarbeitung in der Berliner Verwaltung wurde mit der Veröffentlichung der ADV-Grundsätze abgeschlossen. Mit dieser Verwaltungsvorschrift werden die Grundlinien dieser Organisation, die Steuerung und Koordinierung des ADV-Einsatzes, das Vorgehen bei Planung, Entwicklung und Betrieb von ADV-Verfahren, die Durchführung der Wirtschaftlichkeitsberechnungen und die Aufstellung der ADV-Gesamtkostenübersicht festgelegt.

Ich sehe in dieser Neuregelung einen wesentlichen Fortschritt, da wichtige Aspekte des Datenschutzes berücksichtigt wurden. So wurde insbesondere die rechtzeitige Beteiligung des Datenschutzbeauftragten bei der Planung neuer ADV-Verfahren festgelegt, die bisher nur durch ein Rundschreiben des Senators für Inneres über die rechtzeitige Information und Beteiligung des Berliner Datenschutzbeauftragten vom 17. März 1981 geregelt war.

Ferner habe ich Empfehlungen zum vorgesehenen Geringfügigkeitsbereich abgegeben, in dem ADV-Grundsätze nicht angewendet werden müssen. Die unkoordinierte Verbreitung und Anwendung von Kleinrechnern bietet erhebliche Risiken für die Transparenz und Ordnungsmäßigkeit der Datenverarbeitung.

Neben den ADV-Grundsätzen hat mir der Senator für Inneres einen Entwurf über die Hinweise für die Durchführung des Tests und der Freigabe von Programmen und Verfahren durch automatische Datenverarbeitung (ADV-Test-Hinweise) zugeleitet. Meine Stellungnahme wurde in vollem Umfang berücksichtigt. Ein wesentlicher Punkt war der bereits bei Prüfungen festgestellte Mangel, daß das Testen vielfach mit echten personenbezogenen Daten durchgeführt wird.

Verarbeitung dienstlicher Daten in der Privatwohnung

Ich wurde darauf hingewiesen, daß ein Schulaufsichtsbeamter personenbezogene Dateien über die seiner Aufsicht unterliegenden Lehrkräfte auf einem **privaten Homecomputer** zu Hause führen wollte. An der nach § 9 Abs. 1 Berliner Datenschutzgesetz zu messenden Zulässigkeit der Speicherung gab es keinen Zweifel. Der Beamte war bereit, seine ADV-Anwendung als Präzedenzfall zur Erprobung einer datenschutzgerechten Lösung zur Verfügung zu stellen.

Wegen der allgemeinen Bedeutung habe ich dieses Problem mit den anderen Datenschutzbeauftragten erörtert. Im Ergebnis ist vorläufig festzuhalten, daß Bedienstete der öffentlichen Verwaltung, die Schriftstücke regelmäßig in den Diensträumen zu bearbeiten haben und nur in Ausnahmefällen mit Zustimmung des Vorgesetzten die Bearbeitung zu Hause vornehmen dürfen[2], keine personenbezogenen Daten zu dienstlichen Zwecken auf dem privaten Computer zu Hause verarbeiten dürfen. Anderenfalls würde aus der Ausnahme die Regel.

Da der Schulaufsichtsbeamte über einen eigenen Dienstraum verfügt, ist demnach davon auszugehen, daß die von ihm beabsichtigte Praxis unzulässig ist.

Anders ist der Fall zu bewerten, wenn er Bedienstete betrifft, die nicht über eigene Diensträume verfügen und daher die Arbeit mit personenbezogenen dienstlichen Unterlagen regelmässig zu Hause ausführen müssen. So würde man z. B. Lehrer daran hindern, moderne Bürotechnik zur Arbeit mit Schülerdaten einzusetzen, wenn man den Einsatz von Homecomputern für diese Zwecke verbieten würde. Jedoch setzt das voraus, daß der Datenschutz bei solchen Anwendungen gleichermaßen sichergestellt ist.

Ich begrüße es daher, daß der Senator für Schulwesen, Jugend und Sport im Entwurf von Ausführungsvorschriften über die Führung von Schülerakten auf meinen Vorschlag das Problem aufgegriffen hat und darin für den Einsatz von Kleincomputern zu Hause Rahmenbedingungen formuliert hat, die der Sicherstellung des Datenschutzes in diesem Bereich dienen. So wird bestimmt, daß der Einsatz privater Datenverarbeitungsgeräte nur zulässig ist, wenn über die Bestimmungen für den dienstlichen Computereinsatz hinaus die Verwendung von privaten Computern ausdrücklich in der erforderlichen Anordnung des Schulleiters genehmigt wird und wenn der Betreiber durch eine Erklärung sicherstellt, daß ich meinen Kontrollaufgaben nachgehen kann.

Eine ähnliche aber im Ergebnis ungleich gefährlichere Situation tritt auf, wenn Mitarbeiter der öffentlichen Verwaltung über **Endgeräte in ihrer Privatwohnung** auf den bei ihrer Dienststelle installierten Computer und die dort gespeicherten Daten zugreifen können. Ein derartiger Zugriff auf personenbezogene Daten ist unzulässig. Ich mußte bei den Berliner Stadtreinigungs-Betrieben beanstanden, daß leitenden Mitarbeitern der Organisation und Datenverarbeitung ein uneingeschränkter und zwei Beratungsfirmen ein beschränkter On-line-Zugriff auf personenbezogene Daten von außen ermöglicht worden war.

Mikrocomputereinsatz für Stellenplanung

Weiter bin ich auf ein Projekt des Bezirksamtes Kreuzberg hingewiesen worden, bei dem ein personenbezogenes Lehrerstellenplanverfahren auf einem Mikrocomputer realisiert werden soll. Ich habe empfohlen, den Betrieb des Verfahrens durch eine Dienstanweisung zu regeln, die u.a. die zulässigen Inhalte von Feldern ohne festgelegte Bedeutung (Bemerkungen) betrifft und festlegt, wer eine Zugangsberechtigung zum System haben soll.

4.3. Der Umgang mit Personaldaten

In mehreren Jahresberichten hatte ich Anlaß, auf Mängel beim Umgang mit personenbezogenen Daten öffentlicher Bediensteter (Personaldaten) hinzuweisen. In letzter Zeit häuften sich wieder Eingaben, die nicht nur von den Betroffenen selbst, sondern in zunehmendem Maße auch von Personalräten oder mit der Bearbeitung von Personaldaten betrauten Mitarbeitern vorgebracht wurden.

Notwendigkeit einer gesetzlichen Regelung

In fast allen Fällen waren Unsicherheiten und datenschutzrechtliche Mängel auf das Fehlen geeigneter materiell-rechtlicher Grundlagen zurückzuführen, die eine unmißverständliche Handhabung von Personaldaten, insbesondere die einheitliche Führung von Personalakten, vorschreiben.

Bereits im Jahresbericht 1981 hatte ich in der Anlage 2 Vorstellungen zur Verbesserung des Personaldatenschutzes im **Landesbeamtengesetz (LBG)** entwickelt. Obwohl das LBG inzwischen mehrfach geändert wurde, ist eine gesetzliche Regelung bisher nicht ins Auge gefaßt worden.

Vielmehr hat der Senator für Inneres im August dieses Jahres einen Entwurf von **Verwaltungsvorschriften über die Führung von Personalakten der Dienstkräfte des Landes Berlin** vorgelegt, an dessen Erarbeitung ich nicht beteiligt worden war.

Zwar entsprechen die Verwaltungsvorschriften formell noch nicht den Anforderungen an eine Rechtsgrundlage für derart weitgehende Eingriffe in das informationelle Selbstbestimmungsrecht, da auch im Hinblick auf die Durchsetzbarkeit der subjektiven Ansprüche der Betroffenen hierfür eine **gesetzliche** Grundlage geschaffen werden muß.

Inhaltlich entspricht der Entwurf jedoch weitgehend den von mir bisher vorgetragenen Vorstellungen. Im Hinblick auf die mit

[1] Jahresbericht 1981, S. 12; Jahresbericht 1982, S. 13 und Jahresbericht 1983, S. 24
[2] Vgl. § 77 GGO I

Verwaltungsvorschriften verbundene Selbstbindung der Behörden stellen sie immerhin einen Schritt zur Verbesserung des Datenschutzes dar.

Meine Prüfungen auf Grund der Beschwerden bestätigen die Erforderlichkeit sowohl der in den Verwaltungsvorschriften vorgesehenen Regelungen als auch darüber hinausgehender gesetzlicher Bestimmungen.

Allerdings wird die Durchsetzung datenschutzrechtlicher Erfordernisse bei Personaldaten dadurch erschwert, daß von den verantwortlichen Behörden, insbesondere vom Senator für Inneres, immer wieder meine Kompetenz in diesem Bereich in Frage gestellt wird, da es sich überwiegend um Aktensammlungen handele.

Ungeachtet der Tatsache, daß zumindest die formatierten Teile der Akten (z.B. Aktenvorblätter) wegen ihrer Umsortierbarkeit den Dateibegriff erfüllen, mußte ich immer wieder betonen, daß ich nach § 21 Berliner Datenschutzgesetz neben der Einhaltung der Vorschriften dieses Gesetzes auch die Verpflichtung habe, die Einhaltung „anderer Vorschriften über den Datenschutz" zu kontrollieren. Hierzu zählen die allgemeinen Verfassungsgrundsätze (Erforderlichkeit, Verhältnismäßigkeit) ebenso wie das Recht auf informationelle Selbstbestimmung und die einschlägige höchstrichterliche Rechtsprechung, die insbesondere ein Personaldatengeheimnis anerkennt. Das - verfassungsrechtlich ohnehin bedenkliche - Fehlen spezialgesetzlicher Regelungen kann in derart sensiblen Bereichen kein Grund für die Zurückweisung der gebotenen Datenschutzkontrolle sein. Eine derartige Argumentation würde letztlich darauf hinauslaufen, daß die Datenschutzkontrolle in Bereichen nicht stattfinden sollte, in denen eine verfassungsrechtlich gebotene Regelung nicht erlassen wird. Dies vermag ich nicht anzuerkennen.

Personalfragebogen

Gegenstand vieler Nachfragen war der bislang bei den Einstellungsbehörden verwendete Personalfragebogen. Dabei ging es insbesondere um den Umfang der abgeforderten Daten und die Frage der Notwendigkeit zur Beantwortung aller Teile bereits zu einem Zeitpunkt, zu dem noch nicht feststeht, ob es überhaupt zu einer Einstellung kommen wird.

Folgende datenschutzrechtliche Bedenken bestehen gegen den Inhalt des derzeit verwendeten Fragebogens:

- Ein Personalfragebogen für die **Bewerbung** um Einstellung sollte nur solche Fragen enthalten, die für die Bewerberauswahl erheblich sind, während Fragen, die erst **nach** einer Einstellung für die Abwicklung des Arbeitsverhältnisses Bedeutung gewinnen, später mit einem besonderen Fragebogen abgefragt werden sollten. Auf dem bisher verwendeten Vordruck müßten durch entsprechenden Hinweis die Fragen kenntlich gemacht werden, die zunächst nur für die Bewerberauswahl erforderlich sind.
- Zum Zeitpunkt der Bewerbung sind noch nicht erforderlich Angaben über anhängige Straf-, Ermittlungs- oder Disziplinarverfahren, über alle bisherigen Tätigkeiten und den jeweiligen Grund des Ausscheidens aus dem Arbeitsverhältnis, über Namen und Beruf des Ehegatten, über Schwerbehinderung (mit Nachweis) sowie Sozialversicherungsnummer, Mitgliedschaft einer Krankenkasse und bestehende Versorgungsansprüche.
- Nicht notwendig dürfte die Frage nach einer bestehenden oder evtl. anstehenden Entmündigung sein, da diese in aller Regel normale Bewerber befremden dürfte, anderenfalls ohnehin keine präjudizierende Wirkung hätte.

Selbst nach der Einstellung sind einige Fragen problematisch:

- Zweifelhaft dürfte sein, ob für den Bewerber eine Rechtspflicht besteht, sich zu seinen wirtschaftlichen Verhältnissen zu äußern und ob falsche Aussagen hierüber arbeitsrechtliche Auswirkungen hätten. Unter diesem Aspekt wäre möglicherweise die Grundlage für eine Datenerhebung ohne ausdrücklichen Hinweis auf die Freiwilligkeit nicht gegeben.
- Die Frage nach politischer oder rassischer Verfolgung müßte unbedingt mit einem Hinweis auf die Freiwilligkeit der Angaben versehen werden.

Auch ein überarbeiteter Entwurf eines Fragebogens berücksichtigte diese Bedenken nicht. Ich gehe davon aus, daß noch eine weitere Überarbeitung erfolgt.

Inhalt von Personalakten

Große öffentliche Anteilnahme fand die Frage, ob in die Personalakten von Lehrern Vorgänge über deren Teilnahme an den Friedensaktionen der GEW am 20. Oktober 1983 aufgenommen werden dürfen. Auf Grund mehrerer Beschwerden von Betroffenen bin ich dieser Frage nachgegangen.

Hierbei handelte es sich insbesondere um die Aufforderung, sich zu dem Unterrichtsversäumnis zu erklären sowie die Stellungnahme der Betroffenen. In einem Bezirksamt wurde zusammen mit diesen Unterlagen eine komplette Liste aller bei den Aktionen beobachteten Lehrer einer Schule zur Personalakte genommen.

Die Aufnahme dieser Vorgänge in die Personalakte stellt die Betroffenen schlechter als sie es bei einem Disziplinarverfahren wären. In diesem Falle würden die Vorgänge als Disziplinarvorgang in einer Beiakte zur Personalakte geführt werden und die Tilgungsvorschriften nach der Landesdisziplinarordnung (LDO) greifen, währenddessen die in der Personalakte paginiert abgehefteten Vorgänge die Betroffenen auf Dauer belasten können. Darüber hinaus stellt die Aufnahme der genannten Liste mit Namen anderer Bediensteter eine unverhältnismäßige - weil für das betreffende Dienstverhältnis nicht erforderliche - Speicherung von Fremddaten dar und ist somit rechtswidrig. Die Betroffenen könnten bei einer Einsicht in die Personalakte Kenntnis über weitere Kollegen der Schulen erhalten, die ebenfalls an den beanstandeten Aktionen teilnahmen und vermutlich gleichen dienstrechtlichen Maßnahmen unterzogen wurden bzw. werden sollten. Dadurch würden Personaldaten unbefugt offenbart.

Während die Namen der anderen Lehrer auf den Listen unkenntlich gemacht wurden, konnte die Entnahme der Vorgänge selbst nicht erreicht werden. In einem von mir beanstandeten Fall wurde vom zuständigen Bezirksstadtrat für Volksbildung zugesagt, daß er sich unabhängig der Überlegungen des Senators für Schulwesen, Jugend und Sport vorbehalte, die Vorgänge in Analogie zu den Regelungen nach § 112 LDO nach einem Jahr aus den Personalakten entfernen zu lassen.

Sachakten

Grundsätzlich ist die Personalakte zwar als eine Einheit zu führen. Es gibt jedoch eine Reihe von Vorgängen, die besonderen, von der Person und dem Beamten- oder Arbeitsverhältnis sachlich zu trennenden Zwecken dienen. Diese Vorgänge sind in Sachakten einzuordnen.

Ein Beispiel für derartige Sachakten sind die über die Gewährung von Kindergeld anzulegenden Akten.

Nach § 45 Bundeskindergeldgesetz (BKKG) sind **Kindergeldangelegenheiten** von Angehörigen des Öffentlichen Dienstes jeweils von der Stelle zu bearbeiten, die für die Festsetzung der Bezüge oder des Arbeitsentgelts zuständig ist. Dies bedeutet in der Praxis eine Doppelzuständigkeit insbesondere der Bearbeiter in den Gehalts- und Lohnstellen, die zur Berechnung von Bezügen bzw. Arbeitsentgelten Beiakten zu den Personalakten führen und sowohl Kenntnis von Personaldaten als auch von Kindergelddaten erhalten.

Bereits im Jahre 1983 hatte die Konferenz der Datenschutzbeauftragten des Bundes und der Länder ausdrücklich festgestellt, daß die für die Kindergeldbearbeitung erhobenen Daten Sozialdaten im Sinne des Sozialgesetzbuches sind und somit einer strengen Zweckbindung unterliegen. Diese Zweckbindung verbietet es demjenigen, der im Bereich des öffentlichen Dienstes nach § 45 BKKG mit der Bearbeitung von Kindergeldangelegenheiten betraut ist, Kindergelddaten an die mit der Bearbeitung von Personalsachen Betrauten weiterzugeben bzw. selbst zu

verwenden, sofern er selbst auch mit der Bearbeitung von Personalangelegenheiten betraut ist.

Diesem Grundgedanken folgend hatten sich die zuständigen Obersten Bundes- und Landesbehörden bereiterklärt, durch Rundschreiben in ihrem jeweiligen Zuständigkeitsbereich diesbezügliche Regelungen zu erlassen. Dem ist der Senator für Inneres mit Rundschreiben vom 11. Juli 1984 (II Nr. 41) nachgekommen.

Dabei hat der Senator für Inneres meine Anregungen aufgenommen und klargestellt, daß es sich bei Kindergelddaten nicht um Personaldaten im dienstrechtlichen Sinne, sondern um Sozialdaten handelt, die grundsätzlich nur für kindergeldbezogene Entscheidungen herangezogen werden dürfen.

Meiner Anregung folgend ist auch ein Hinweis aufgenommen worden, daß Kindergeldvorgänge nicht in der Personal(haupt)akte, sondern nur in eigenen Kindergeldakten als Sachakten geführt werden dürfen. Dabei wird aus Praktikabilitätsgründen zugestanden, daß in diese Sachakte auch Vorgänge über Ortszuschlag, Sozialzuschlag und Anwärterverheiratetenzuschlag aufgenommen werden dürfen. Dies bedeutet allerdings, daß vor einer etwa notwendig werdenden Übermittlung der Akten im Zusammenhang mit dienst- oder arbeitsrechtlichen Vorgängen der das Kindergeld betreffende Aktenteil abgetrennt werden muß.

Die Relevanz dieser Frage zeigt die Beschwerde des Bediensteten einer Hochschule, dem auf Grund gewisser Eintragungen im Einkommenssteuerbescheid (der zur Gewährung des Kindergeldes vorgelegt worden war) Vorhaltungen gemacht wurden, er habe sich eine Nebentätigkeit nicht ordnungsgemäß genehmigen lassen. Ich habe der Hochschule mitgeteilt, daß dem Bediensteten aus der unerlaubten Verwendung dieser Information keine Nachteile entstehen dürfen, und den Petenten gleichzeitig darauf hingewiesen, daß hiervon die Verpflichtung nicht berührt wird, Nebentätigkeiten ordnungsgemäß genehmigen zu lassen.

Ein weiteres Beispiel für Sachakten, die allerdings in dem Entwurf von Verwaltungsvorschriften noch nicht berücksichtigt sind, erläutert folgender Sachverhalt:

Eine Grundschullehrerin beschwerte sich darüber, daß ihr Schulleiter eine „private" Personalakte über sie führe, und bat mich um Überprüfung, ob es sich hierbei um die Führung einer „unerlaubten Nebenakte" zu ihrer Personalakte handeln könnte. Sie befürchtete, daß dadurch für sie unkontrollierbar belastende Personaldaten gesammelt werden und jedermann zugänglich gemacht werden könnten.

Ein datenschutzrechtlicher Mangel war in diesem Falle nicht feststellbar. Der Schulleiter führte lediglich eine Sammelakte, in der er Schriftverkehr mit den Kollegen der Schule sowie Durchschriften, Verfügungen usw. zum Nachweis seiner Verwaltungstätigkeit aufbewahrte.

Ich habe der Petentin mitgeteilt, daß die Art der Aufbewahrung nur dann beanstandungswürdig wäre, wenn auf diese Weise negative Bewertungen aufbewahrt würden, die nicht Bestandteil der Personalakte sein dürften, oder Dritten Daten offenbart werden könnten.

Das wesentliche Problem bei der Führung von Sachakten neben den Personalakten ist, daß die Rechte der Betroffenen durch diese Zuordnung nicht eingeschränkt werden. Insbesondere ist dem Betroffenen jedenfalls in dem für die Wahrung seiner Interessen erforderlichen Umfang auch Einsicht in den ihn betreffenden Teil der Sachakte zu gewähren, sofern dem nicht besondere Gründe (z. B. Verschlußsachencharakter) entgegenstehen.

Hilfsakten

Von Sachakten zu unterscheiden sind Vorgänge, die insbesondere bei räumlicher Entfernung zwischen Beschäftigungsstelle und Personalstelle z.B. von örtlich zuständigen Büroleitern geführt werden (Hilfsakten). Sie dürfen nur solche Vorgänge enthalten, die auch Bestandteil der Personalakte sind.

Auf die Anfrage des Personalrats eines Bezirksamtes nach der Zulässigkeit der „Handakte eines Kollegen bei der Büroleitung" habe ich folgendes ausgeführt:

Als unmittelbare Mitarbeiter des Dienstherrn fungieren die Büroleiter in dem ihnen zugewiesenen innerbehördlichen Teilbereich als Dienstvorgesetzte und sind daher berechtigt, solche das Dienst- oder Arbeitsverhältnis betreffende Vorgänge aus den Personalakten zur Kenntnis zu nehmen, die sie zu ihrer ordnungsgemäßen Aufgabenerfüllung benötigen. Im Hinblick auf diese Funktion ist die Aufbewahrung von Kopien oder Abschriften z.B. von Krankmeldungen, Urlaubsanträgen, Dienstbefreiungen aus besonderem Anlaß in einer Hilfsakte nicht zu beanstanden.

Auf keinen Fall zulässig hielte ich allerdings die Aufbewahrung von Unterlagen, die Bewertungen der Bediensteten enthalten und nicht Bestandteil der (Haupt-)Personalakte sind. So habe ich in einem Fall die Aufbewahrung eines Entwurfs eines später zu Gunsten des Bediensteten abgeänderten Dienstleistungsberichts in einer Hilfsakte bemängelt.

Offenbarung von Personaldaten

Auch die Weitergabe von Personalvorgängen einschließlich der Personalakten unterliegt dem Erforderlichkeitsgrundsatz. Das bedeutet, daß nicht in jedem Fall die gesamte Akte anderen Stellen zur Verfügung gestellt werden muß, sondern durchaus einzelne Aktenbestandteile ausreichen können. Folgende Beschwerde erläutert dies:

Ein Beamter der Berliner Feuerwehr war nach einem anerkannten Dienstunfall in den vorzeitigen Ruhestand versetzt worden. Aufgrund einer Anweisung des Senators für Inneres mußte der Ruhestandsbescheid zurückgenommen werden, weil angeblich noch Zweifel an der Dienstunfähigkeit bestanden. Daraufhin war der Beamte aufgefordert worden, sich einer Untersuchung durch den Leitenden Polizeiarzt, also dem Beamten einer anderen Dienstbehörde zu unterziehen.

Bei der Untersuchung stellte der Beamte fest, daß dem Polizeiarzt seine gesamte Personalakte einschließlich der Prozeßunterlagen über einen umfangreichen Rechtsstreit vorlag.

Zwar ist die Dienstbehörde bei Zweifeln über die Dienstunfähigkeit eines Beamten berechtigt, eine ärztliche Untersuchung durch einen außenstehenden Arzt zu veranlassen und diesem die erforderlichen Unterlagen zur Verfügung zu stellen. Der Umfang der weitergegebenen Unterlagen ist jedoch auf solche Teile zu beschränken, die der untersuchende Arzt für die medizinische Beurteilung benötigt.

Hierzu konnte ich auf Ziff. 77.0.3 des Entwurfs einer Verwaltungsvorschrift zu § 77 Landesbeamtengesetz (Stand: März 1984) hinweisen, nach der dem Antrag auf ärztliche Begutachtung neben der Angabe des Ersuchensgrundes lediglich eine Übersicht über die Fehltage wegen Krankheit und - soweit erforderlich - eine Stellungnahme zur Entwicklung der dienstlichen Leistungsfähigkeit des Beamten beizufügen ist.

Der Hinweis des Innensenators, die Vertraulichkeit bezüglich der nicht relevanten Akteninhalte sei dadurch gewährleistet gewesen, daß der Leitende Polizeiarzt nicht nur der ärztlichen Schweigepflicht, sondern auch der allgemeinen Verschwiegenheitspflicht als beamteter, im dienstlichen Interesse tätig werdender Arzt unterliege, ändert nichts an der Tatsache, daß nach datenschutzrechtlichen Erfordernissen personenbezogene Daten und Sachdarstellungen nur in dem für die Aufgabenerfüllung notwendigen Umfang zur Kenntnis gegeben werden dürfen.

Bedienstete fügen ihren **Beihilfeanträgen** die Anlage mit den Liquidationen der behandelnden Ärzte häufig auch offen bei. Damit wird den personalaktenführenden Stellen und Büroleitungen die Möglichkeit eröffnet, ohne dienstliches Erfordernis Kenntnis von medizinischen Daten zu nehmen, die ausschließlich für die Aufgaben der Beihilfestellen benötigt werden. Dies liegt sicher auch daran, daß der Aufklärungshinweis am Schluß der Ausfüllanleitung, die Anlagen könnten in einem verschlossenen Umschlag beigelegt werden, nicht ausreichend Beachtung findet.

Meiner Empfehlung entsprechend wird der Senator für Inneres in das Antragsformular selbst nahe der Unterschriftzeile zukünftig folgenden Hinweis anbringen:

„Der Beihilfeantrag und die Anlagen hierzu können **verschlossen** über die zuständige personalaktenführende Stelle der Beihilfenstelle übersandt werden.

Dabei können die Zusammenstellung der Aufwendungen und die Belege (Arztrechnungen, ärztliche Verordnungen und dgl.) in einem besonderen verschlossenen Umschlag, auf dem „Anlage zum Beihilfeantrag des ... (Name, Dienststelle)" zu vermerken ist, beigefügt werden, den erst die Beihilfenstelle öffnen darf. Damit stellen Sie sicher, daß Ihre Angaben und die Belege ausschließlich der Beihilfenstelle zur Kenntnis gelangen."

Die maschinell erstellten **Gehalts-, Vergütungs- und Lohnnachweise** werden von der personalaktenführenden Stelle bzw. Beschäftigungsstelle dazu benutzt, auf der Rückseite die für die verschiedensten Zwecke erforderliche Einkommensbescheinigung zu erteilen.

Häufig fragten Betroffene nach, wie sie verhindern könnten, daß bei Vorlage dieser Bescheinigung neben den relevanten Einkommensdaten auch die zusätzlich ausgedruckten personenbezogenen Daten zur Kenntnis gegeben werden.

Dieses Problem hat eine datenschutzfreundliche Lösung erfahren: Der Senator für Inneres hat mit Rundschreiben vom 6. April 1984 (VI Nr. 20) angeordnet, daß künftig die Gehalts- und Lohnstellen auf formlosen Antrag besondere Einkommensbescheinigungen ausstellen. Dabei ist von dem Bediensteten anzugeben, welche Daten diese Bescheinigung enthalten soll, ggf. kann dem Antrag ein von der die Einkommensbescheinigung anfordernden Stelle ausgehändigter Vordruck beigefügt werden.

4.4 Ordnungsaufgaben

Die Beratung des neuen Landesmeldegesetzes

Bei Redaktionsschluß lag eine Terminplanung für die Beratung des Landesmeldegesetzes vor, die vorsieht, daß sich das Abgeordnetenhaus in seiner Sitzung am 31. Januar 1985 mit dem im Unterausschuß „Landesmeldegesetz" und im Ausschuß für Inneres, Sicherheit und Ordnung beratenen Landesmeldegesetz abschließend befaßt.

Dabei ist festzustellen, daß zwischenzeitlich ein Schwebezustand eingetreten ist, in dem bereits Gerichte die Frage aufgeworfen haben, ob nicht das Melderechtsrahmengesetz ungeachtet anders lautender Vorschriften des geltenden Melderechts direkt angewandt werden muß. Die damit verbundenen Unsicherheiten würden sich verstärken, falls es nicht gelingt, das Gesetz noch in dieser Legislaturperiode zu verabschieden. Dafür spricht auch folgendes: Im Gegensatz zu anderen Bundesländern, in denen die Meldegesetze vor dem Urteil des Bundesverfassungsgerichts verabschiedet wurden, hat der Berliner Landesgesetzgeber nun allerdings den Vorteil, sich an den Vorgaben des Volkszählungsurteils orientieren und damit - wie es bereits in einigen anderen Bundesländern erwogen wird - eine Novellierung des gerade novellierten Meldegesetzes vermeiden zu können. Die Fassung des Unterausschusses „Landesmeldegesetz", der seine Beratungen im Dezember abgeschlossen und die Vorlage an den Innenausschuß überwiesen hat, trägt folgenden - im Jahresbericht 1982 unter 2.3 dargelegten - Bedenken Rechnung. Dies gilt

- für meine Forderung, daß die Weitergabe personenbezogener Daten durch die Meldebehörde auch an andere Polizeidienststellen eine den Datenschutzgesetzen unterworfene Datenübermittlung darstellt
- für eine bessere Regelung der Speicherung sogenannter „Hinweise", die nunmehr nur noch unter klar definierten Voraussetzungen aufgenommen werden können
- das Verbot der Übermittlung verwendeter interner Ordnungsmerkmale (Personenkennzeichen)
- die Nichtübernahme der im Entwurf enthaltenen Regelung, nach der erkennungsdienstliche Maßnahmen in bestimmten Fällen nach dem Landesmeldegesetz zulässig gewesen wären
- die starke Überarbeitung der sogenannten Nebenmeldepflichten von Krankenanstalten, des Beherbergungsgewerbes und der Wohnungsgeber
- die völlige Neuregelung der Datenübermittlung.

Bei Redaktionsschluß war offen, ob meinen weiteren Forderungen entsprochen wird, insbesondere die Seriennummer der Personalausweise nicht in den Datensatz aufzunehmen. Diese und andere Fragen, etwa hinsichtlich der Zuständigkeit des Polizeipräsidenten als Meldebehörde, werden Gegenstand einer gutachterlichen Stellungnahme zu verfassungsrechtlichen Fragen des Gesetzentwurfs durch Herrn Prof. Dr. Benda am 14. Januar 1985 vor dem Ausschuß für Inneres, Sicherheit und Ordnung sein.

Informationssystem Einwohnerwesen

Fehlspeicherungen im Informationssystem Einwohnerwesen habe ich in den letzten Jahren mehrfach erörtert[1]. Wie bereits im Vorjahr beschwerte sich erneut ein unbescholtener Bürger darüber, ihm sei auf der Meldestelle das Merkmal aus seinem Datensatz vorgehalten worden, daß er sich in Untersuchungshaft befinde. Es konnte nicht sicher aufgeklärt werden, worauf die Fehlspeicherung beruhte. Der Polizeipräsident hat in den letzten Jahren verschiedene Maßnahmen getroffen, um solchen Fehlspeicherungen vorzubeugen. So ist wegen des erneuten Falles veranlaßt worden, daß alle Hafteintragungen von der ADV-Anwendungsrevision des Einwohnermeldeamtes sofort nach der Eingabe geprüft werden. Diese erfolgt zusätzlich zu der bereits im letzten Jahresbericht geschilderten Maßnahme, daß Änderungszugriffe nur noch unter Verwendung von Familiennamen und Geburtsdatum erfolgen dürfen, sowie zu den Maßnahmen, die der Senat in seiner Stellungnahme zu meinem Jahresbericht 1983 dargelegt hat.

In dieser Stellungnahme hat der Senat ferner darauf hingewiesen, daß angesichts der großen Zahl von Änderungen die wenigen von mir problematisierten Fälle von Fehlspeicherungen als verschwindend gering anzusehen sind. Dem ist entgegenzuhalten, daß mir nur diejenigen Fehlspeicherungen bekannt werden, die von dem Betroffenen auch bemerkt werden. Dies erfolgt meist höchst zufällig oder dann, wenn die Betroffenen so gut informiert sind, daß sie bereits erfolgte Beeinträchtigungen ihrer schutzwürdigen Belange auf fehlerhafte Daten in der Einwohnerdatenbank zurückführen. Es ist daher mit einer beachtlichen Dunkelziffer von nicht erkannten Falschdaten in der Einwohnerdatenbank zu rechnen.

Ich erkenne jedoch die Bemühungen an, Risiken für neue Fehlspeicherungen in geeigneter Form auszuschalten, wenngleich der Polizeipräsident noch nicht in allen Fällen meinen Empfehlungen gefolgt ist.

Aufgrund vielfältiger Eingaben konnte ich in den letzten Jahren feststellen, daß es immer wieder zu **Fehlauskünften** aus der Einwohnerdatei des Einwohnermeldeamtes beim Polizeipräsidenten in Berlin (EMA) kam, obwohl § 17 a Meldegesetz verlangt, daß die Person, über die Auskünfte erteilt werden soll, von dem Anfragenden hinreichend bestimmt sein muß.

So müssen auch Fehlauskünfte in Fällen vermieden werden, in denen der Anfragende in seinem Auskunftsersuchen Suchmerkmale zur Person, über die Auskunft gegeben werden soll, nennt, die auf mehrere im EMA-Datensatz gespeicherte Personen zutreffen, oder in denen der Anfragende Angaben zur Person gibt, die nicht in allen Punkten mit den Eintragungen übereinstimmen.

Bis zu den noch im letzten Jahr begonnenen Grundsatzgesprächen über diese Problematik hatte sich das EMA in solchen Fällen damit beholfen, daß es in dem Auskunftsschreiben darauf hinwies, daß Zweifel hinsichtlich der Identität der gesuchten Person bestehen, bzw. daß dieses oder jenes genannte Merkmal nicht mit den vorhandenen Eintragungen übereinstimmt.

Im Zusammenhang mit einzelnen von mir festgestellten Fehlauskünften hat sich jedoch gezeigt, daß Auskunftsersuchende, insbesondere Gläubiger, solchen Hinweisen keine Beachtung schenkten, vielmehr ohne weitere Recherchen die Identität mit der von ihnen gesuchten Person unterstellten.

Deshalb habe ich darauf hingewiesen, daß der Polizeipräsident nur dann Auskunft erteilen dürfe, wenn alle notwendigen Maßnahmen zu einer eindeutigen Identitätsfeststellung ergriffen wurden.

[1] Jahresbericht 1981, S. 8; Jahresbericht 1982, S. 10. Inzwischen hat der Senator für Inneres ein Organisationsgutachten vorgelegt, in dem ebenfalls eine beachtliche Fehlerrate beim Einwohnerdatenbestand festgestellt wird.

Um Fehler zu vermeiden, habe ich empfohlen, folgende Grundsätze zu beachten:

- Allgemein sind drei Suchmerkmale für die Bestimmtheit einer Person erforderlich.
- Eine einzelne gesuchte Person ist dann durch Suchmerkmale des Anfragenden hinreichend bestimmt, wenn nur eine Person im Melderegister gespeichert ist, auf die diese Merkmale voll zutreffen.
- Sofern die vorgegebenen Merkmale bis auf eine geringfügige Ausnahme nur auf eine gespeicherte Person zutreffen, kann Auskunft gegeben werden, wenn auf die betreffende Datenabweichung ausdrücklich hingewiesen wird.
- Stimmen jedoch die Daten mehrerer Personen mit auch nur geringfügigen Abweichungen bei den Suchmerkmalen überein oder wird anhand der vorgegebenen Suchmerkmale nur eine Person aufgefunden, bei der jedoch eines der notwendigen Merkmale erheblich abweicht, ist die Bestimmtheit der Person nicht gewährleistet. Es sind vom Auskunftsersuchenden weitere Unterscheidungs- bzw. Suchmerkmale anzufordern.
- Wenn alle vorgegebenen Merkmale auf mehrere gespeicherte Personen ohne Abweichungen zutreffen, sind vom Antragsteller soviel weitere Suchmerkmale anzufordern, bis die Person, über die Auskunft gegeben werden soll, hinreichend bestimmt ist.

Die Punkte dieses Forderungskatalogs sind in internen Dienstbesprechungen bereits den Mitarbeitern des EMA und den Leitern der Meldestellen zur Kenntnis gegeben worden und sollen demnächst in eine Geschäftsanweisung für diesen Mitarbeiterkreis einfließen.

Erfreulicherweise kann ich feststellen, daß nach eingehender Erörterung dieses Problemkreises seit Anfang des Berichtsjahres keine Hinweise auf mögliche Fehlauskünfte mehr bei mir eingegangen sind.

Der **Zugriff auf gesperrte Daten** in der Einwohnerdatenbank ist im Einwohnermeldeamt, in den Meldestellen und in den Bezirkseinwohnerämtern nur noch besonders dazu berechtigten Dienstkräften möglich. Diese Beschränkung sowie andere nach § 5 Abs. 1 Berliner Datenschutzgesetz erforderliche Kontrollmaßnahmen werden seit der Umrüstung auf neue Terminals durch personenbezogene, maschinenlesbare Berechtigungsausweise realisiert. Bei einer Überprüfung habe ich festgestellt, daß die Ausweisleser der neuen Terminals bei geeigneter Manipulation nicht sicherstellen, daß die Terminals nur so lange den Zugang zur Datenbank gewähren, wie die Ausweise eingelegt sind. Die sich daraus ergebenden Risiken wurden dann dadurch gemildert, daß programmtechnisch sichergestellt wurde, daß unter gleicher Kennung nur ein Terminal zur selben Zeit betrieben werden kann, und daß Versuche, dies zu umgehen, protokolliert werden. Ferner soll die Zugriffsberechtigung auf gesperrte Daten so gesteuert werden, daß nach jedem Dialog ein Abbruch erfolgt und somit der Abruf gesperrter Daten im Rahmen der Manipulation nicht möglich ist.

Die Restrisiken wären nur durch den Austausch der Ausweisleser zu beseitigen, für die es jedoch nach Ansicht des Polizeipräsidenten zur Zeit keine organisatorisch oder wirtschaftlich vertretbare Alternative auf dem Markt gibt.

Fahrzeugregister (ZEVIS)

Die Berliner Polizei ist an das Zentrale Verkehrsinformationssystem (ZEVIS) des Kraftfahrt-Bundesamts angeschlossen. Es ist davon auszugehen, daß zum Zeitpunkt der Herausgabe dieses Jahresberichts der Aufbau von ZEVIS abgeschlossen sein wird und sämtliche Bundesländer darauf zugreifen können. ZEVIS ist ein umfassendes Datenbanksystem, in dem das zentrale Fahrzeugregister mit den registrierten 32 Millionen Fahrzeugen, die Personalien der im Verkehrszentralregister Eingetragenen (Verkehrssünderkartei) und Angaben über entzogene und versagte Führerscheine gespeichert sind.

Aus dieser Datenbank soll die Polizei im Wege des Direktabrufs (on-line), bei dem entweder das Kraftfahrzeug-Kennzeichen (Halter-Abfrage) oder der Name einer Person (P-Abfrage) eingegeben werden, Daten abfragen können.

Obwohl das System in Betrieb ist, liegt als künftige Rechtsgrundlage für ZEVIS bisher nur ein Entwurf eines Gesetzes zur Änderung des Straßenverkehrsgesetzes vor. Unabhängig davon, daß der Gesetzgeber damit vor vollendete Tatsachen gestellt wird, sind aus datenschutzrechtlicher Sicht einige der Regelungen bedenklich:

Nach übereinstimmender Auffassung der Datenschutzbeauftragten dürfen die Fahrzeugregister-Daten grundsätzlich nur zu dem Zweck verwendet werden, zu dem sie erhoben worden sind: Zur Identifizierung von Kraftfahrzeugen und Kraftfahrzeughaltern im Rahmen der Erfüllung gesetzlicher Aufgaben.

Eine Verwendung von Registerdaten zu weitergehenden Zwekken - unabhängig von der Eigenschaft der gespeicherten Person als Kraftfahrzeug-Halter (sogenannte erweiterte Verwertung) - kommt allenfalls in wenigen Ausnahmefällen in Betracht.

Mit der P-Abfrage können beliebige Polizeidienststellen erfahren, welche verschiedenen Kraftfahrzeuge auf eine bestimmte Person zugelassen und welche sonstigen Informationen über eine bestimmte Person im Zentralfahrzeugregister vorhanden sind (z.B. Adresse, Geburtsdatum, Geburtsort). Es besteht die Gefahr, daß das zentrale Fahrzeugregister in weitem Umfang zweckentfremdet und als Bundes-Adreß-Register für einen großen Teil der Bevölkerung genutzt wird. Ein solches Adreß-Register ist im Zusammenhang mit dem Personalausweisgesetz vom Deutschen Bundestag ausdrücklich abgelehnt worden. Der Bundesbeauftragte für den Datenschutz hat unter Zurückstellung dieses und weiterer Kritikpunkte der Durchführung einer dreijährigen Erprobungsphase zugestimmt, die er in Zusammenarbeit mit den Datenschutzbeauftragten der Länder begleiten und auswerten wird.

Anhörungsbogen in Bußgeldverfahren

Zur Verfolgung von Ordnungswidrigkeiten werden regelmäßig von den damit betrauten Ordnungsbehörden Anhörungsbogen an die Betroffenen verschickt. Mit diesen werden die Betroffenen gem. § 55 Ordnungswidrigkeitengesetz (OWiG) aufgefordert, Angaben zu ihrer Person und dem zugrundeliegenden Sachverhalt zu machen.

In mehreren Eingaben bin ich von Bürgern gebeten worden, diese Bogen zu überprüfen.

Ich habe festgestellt, daß bei den Senatsverwaltungen, den nachgeordneten Behörden und den Bezirksämtern eine Vielzahl von Anhörungsbogen existieren, die in Form und Inhalt zum Teil stark voneinander abweichen.

Nach § 111 OWiG sind bestimmte personenbezogene Daten gegenüber der für die Verfolgung der Ordnungswidrigkeit zuständigen Behörde anzugeben. Diese Vorschrift entspricht den vom Bundesverfassungsgericht im Volkszählungsurteil aufgestellten Anforderungen an die Normenklarheit.

Soweit in den Anhörungsbogen Daten abgefragt werden, die von § 111 OWiG nicht gedeckt sind, bedürfte es gem. § 9 Abs. 2 Berliner Datenschutzgesetz entweder einer anderen Ermächtigungsgrundlage oder aber eines Hinweises auf die Freiwilligkeit der Datenabgabe.

Bei meiner Überprüfung habe ich festgestellt, daß eine größere Anzahl von Anhörungsbogen diesen Anforderungen nicht genügte. Häufig wurde § 111 OWiG als Rechtsgrundlage überhaupt nicht erwähnt. Unter Bezugnahme auf den gesetzlichen Verpflichtungstatbestand in § 111 OWiG wurden Daten erhoben, die in dieser Vorschrift überhaupt nicht genannt sind.

Dazu gehören z.B. Fragen zum gesetzlichen Vertreter, zum Führerschein, zu den wirtschaftlichen Verhältnissen, zur Anzahl der Kinder, zur Telefonnummer, zu Sozialhilfebezügen, zum Vor- und Familiennamen des Ehegatten, zum Beruf des Ehegatten und zum Geburtsnamen der Mutter. Die Erhebung dieser personenbezogenen Daten ist nur auf freiwilliger Basis zulässig, worauf der Betroffene gem. § 9 Abs. 2 Berliner Datenschutzgesetz hinzuweisen ist.

Bereits mein Anschreiben hat zu einer ganzen Reihe von Änderungen geführt. Meinen Empfehlungen wurde dabei weitgehend entsprochen.

4.5 Amtliche Statistik

Es liegt auf der Hand, daß das Urteil des Bundesverfassungsgerichts zum Volkszählungsgesetz 1983 von größter Bedeutung für den Geschäftsbereich der Amtlichen Statistik ist. Die Anforderungen des Gerichts an die Erhebung und Bereitstellung von Daten für statistische Zwecke, die Verfahren der statistischen Auswertung und deren gesetzlicher Regelung sind so weitgehend, daß die Durchführung jeder einzelnen Statistik für Bundes- und Landeszwecke einer kritischen Betrachtung unterzogen werden muß.

Zwar ist einzuräumen, daß die Umsetzung dieser Anforderung einige Zeit in Anspruch nimmt und in dieser Zwischenzeit nicht alle Statistiken eingestellt werden können. Trotz eines gewissen „Übergangsbonus" für den Verwaltungsvollzug mußten jedoch aus dem Urteil für einzelne Erhebungen umgehend Konsequenzen gezogen werden. Einzelne Beispiele sollen im folgenden angeführt werden.

Volkszählung

Kaum war der Spruch des Verfassungsgerichts ergangen, begannen bereits auf Referentenebene Beratungen über ein Gesetz, das die Durchführung einer Volkszählung bereits 1985, nach späteren Entwürfen im Frühjahr 1986 ermöglichen soll.

Ungeachtet der breiten Kritik, die die beabsichtigte Form der Volkszählung 1983 gefunden hatte, wurde das verworfene alte Gesetz zum Ausgangspunkt genommen und lediglich an vielen Stellen nachgebessert, an denen das Gericht Anstoß genommen hatte. Fraglich ist, ob nicht im Hinblick auf die grundsätzlichen Aussagen des Gerichts, aber auch das Ziel, bei der Durchführung der nächsten Volkszählung eine möglichst hohe Akzeptanz in der Bevölkerung zu erreichen, eine grundlegende Neukonzeption der Volkszählung angemessener gewesen wäre. Insbesondere wäre eine starke Reduzierung der Erhebungsmerkmale tunlich gewesen.

Innenverwaltungen und statistische Ämter versuchten diesmal, die Datenschutzbeauftragten frühzeitig in die Beratungen einzubeziehen. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder beschäftigte sich daher mehrfach mit den vorgelegten Entwürfen. Angesichts des Standes der Arbeiten, aber auch der grundsätzlichen Skepsis hielten es die Datenschutzbeauftragten nicht für angebracht, bereits zum derzeitigen Zeitpunkt eine formelle Stellungnahme abzugeben.

Nichtsdestoweniger wurde u. a. auf folgende gesetzliche Mängel verwiesen, die den Entwürfen noch immer anhafteten:

Aus dem Grundsatz der Verhältnismäßigkeit folgte die Verpflichtung zu prüfen, ob nicht alternative Methoden zur Totalerhebung und zum Auskunftszwang in Betracht kommen. Die Datenschutzbeauftragten vermißten Darlegungen, ob nicht zu einzelnen Erhebungseinheiten eine Repräsentativerhebung ausreicht, die auch auf freiwilliger Grundlage durchgeführt werden könnte. Zumindest sollte der Gesetzgeber die statistischen Ämter verpflichten, alternative Erhebungsmethoden für die Zukunft zu erproben, die die Bürger weniger belasten.

Die Absicherung des Zweckentfremdungsverbotes für Zähler und Mitarbeiter in den Erhebungsstellen wurde nicht als ausreichend empfunden.

Daten, die zur Durchführung der Volkszählung von den Meldebehörden an die statistischen Ämter bzw. Erhebungsstellen übermittelt wurden, dürfen entgegen dem Entwurf nicht zur Vervollständigung der Angaben der Volkszählung verwendet werden.

Über das Volkszählungsgesetz hinaus empfahlen die Datenschutzbeauftragten, auch das ergänzend geltende Bundesstatistikgesetz, insbesondere die Regelungen über die Geheimhaltung zu überarbeiten und dabei den Begriff der Anonymisierung präziser zu fassen. Das Verfahren für die Festlegung der Erhebungsvordrucke soll geregelt oder aber bestimmt werden, daß dieses Verfahren in dem jeweiligen Einzelstatistikgesetz (z.B. Volkszählungsgesetz) zu regeln ist.

Mikrozensus 1984

Die in größeren Abständen durchgeführten Volkszählungen wurden bisher ergänzt durch jährlich stattfindende Repräsentativerhebungen bei insgesamt ein Prozent der Bevölkerung der Bundesrepublik (Mikrozensus). Nachdem 1983 diese Erhebung aus anderen Gründen ausgefallen war, konnte der Mikrozensus 1984 nicht durchgeführt werden, da die vorhandenen gesetzlichen Grundlagen den Anforderungen des Bundesverfassungsgerichts nicht entsprachen.

Dem auch hier von den Statistikbehörden vorgebrachten „Übergangsbonus" mußten die Datenschutzbeauftragten entgegenhalten, daß ohne eine gesetzliche Anpassung die Erhebung nur dann durchgeführt werden könne, wenn das Gesetzgebungsverfahren so viel Zeit in Anspruch nähme, daß die Funktionsfähigkeit staatlicher Einrichtungen wesentlich beeinträchtigt würde. Diese Voraussetzung konnte nicht nachgewiesen werden.

Für künftige Mikrozensus-Erhebungen hat die Konferenz der Datenschutzbeauftragten des Bundes und der Länder folgende Kriterien aufgestellt:

- Die Bürger sind nur insoweit zu Auskünften zu verpflichten, als freiwillige Erhebungen nicht zum Ziele führen. Der nächste Mikrozensus sollte deshalb wenigstens probeweise für einen Teil der Befragten ohne Auskunftszwang durchgeführt werden.
- Das Gesetz muß präzise Regelungen über die organisatorischen Vorkehrungen vorsehen, die sicherstellen, daß der Betroffene möglichst wenig belastet wird. Danach sind Regelungen z.B. über das Erhebungsverfahren und über die Löschung der personenbezogenen Daten erforderlich.
- Das Gesetz muß die Sachverhalte, über die Daten erhoben werden sollen, präzise umschreiben.

An der Neufassung des Mikrozensus-Gesetzes für die Erhebungen in den Jahren 1985 bis 1992 wird derzeit gearbeitet. Mit dem als Entwurf bereits vorliegenden Gesetz wird allerdings nicht die grundlegende Frage nach der sachlichen Notwendigkeit dieser Erhebung beantwortet. Insoweit sind gegebenenfalls auch grundlegend neue Überlegungen des Gesetzgebers zu fordern, da es für eine erfolgreiche Durchführung einer Erhebung unerläßlich ist, die Betroffenen von der Bedeutung gerade dieser Statistik zu überzeugen.

EG-Arbeitskräftestichprobe

Auch die Durchführung der EG-Arbeitskräftestichprobe, bei der 0,4% der Bevölkerung befragt werden, mußte auf Kritik stoßen.

Als rechtlich problematisch erwies sich das Fehlen einer EG-Regelung hinsichtlich der Auskunftspflicht. Die Frage der Auskunftspflicht wurde vom EG-Verordnungsgeber bewußt offengelassen, um zu ermöglichen, daß die Erhebung in etwa der Hälfte der Mitgliedstaaten auf der Grundlage freiwilliger Angaben durchgeführt werden konnte. Da es auch an einer ausdrücklichen Entscheidung des Bundesgesetzgebers für eine Auskunftspflicht fehlte, wäre die Datenabgabe lediglich auf freiwilliger Basis zulässig gewesen.

Die auf Betreiben der Datenschutzbeauftragten erfolgte Reduzierung des Fragenkatalogs auf das von der EG-Verordnung vorgesehene Maß und die Gewährleistung von Verfahrenssicherungen im Rahmen des Verwaltungsvollzuges (insbesondere die baldige Abtrennung des Namens und der Adresse der befragten Personen vom Fragebogen), ließen im Hinblick auf die europaweite Bedeutung der Befragung die Erhebung hinnehmbar erscheinen.

Positiv ist hervorzuheben, daß die Statistischen Landesämter ein bundeseinheitliches Informationsblatt zur EG-Arbeitskräftestichprobe an die Betroffenen ausgegeben haben, das auf mögliche Vorbehalte und Ängste der Betroffenen ausführlich eingeht, denkbare Fragen beantwortet und die Gründe der Erhebung veranschaulicht. Nicht zuletzt auf dieses gesteigerte bürgerfreund-

liche Informationsverhalten der Statistischen Landesämter dürfte es zurückzuführen sein, daß es kaum zu Beschwerden gekommen ist.

Hochschulstatistik

In den Hochschulen hat die nach der Verkündigung des Volkszählungsurteils durchgeführte Erhebung des wissenschaftlichen und künstlerischen Personals der Hochschulen nach dem Hochschulstatistikgesetz zu einer Vielzahl von Anfragen Betroffener geführt.

Als verfassungsrechtlich problematisch stellten sich die Regelungen dar, nach denen die Hochschulen die von ihnen für die Statistischen Landesämter erhobenen - noch nicht anonymisierten - Daten für ihre eigenen verwaltungsinternen Zwecke verwenden bzw. bei einem Hochschulwechsel des Betroffenen die Daten der neuen Hochschule übermitteln dürfen.

Ich habe mich an den Senator für Wissenschaft und Forschung gewandt und gebeten, die Hochschulen anzuweisen, bis zur endgültigen Klärung der Rechtslage keine Einzelangaben mit Namen und Anschriften zu verwaltungsinternen Zwecken zu verwenden oder weiterzuleiten. Der Senator hat meiner Empfehlung entsprochen; die Hochschulen haben sich mit dieser Verfahrensweise einverstanden erklärt. Die Durchführung der Erhebung ist von mir kontrolliert worden. Beanstandungen hat es nicht gegeben.

Bemerkenswert an der trotz der rechtlichen Bedenken durchgeführten Erhebung war, daß das Statistische Landesamt versuchte, Bediensteten, die wegen ihrer rechtlichen Zweifel an der Erhebung nicht teilnehmen wollten, mit der Androhung eines Bußgeldes zur Abgabe des Erhebungsbogens zu veranlassen. Die Hochschulen sollten zu diesem Zweck die Daten der Verweigerer an das Statistische Landesamt übermitteln. Dies konnte nicht hingenommen werden.

Bußgelder sollen die davon Betroffenen zu einem gesetzestreuen Verhalten bewegen. Ein solches Zwangsmittel ist jedoch dann widersinnig, wenn das geforderte Verhalten auf einer - zumindest in einzelnen Teilen - rechtswidrigen, weil verfassungswidrigen gesetzlichen Grundlage beruht.

Im Ergebnis ist es weder zu Bußgeldverfahren noch zur entsprechenden Übermittlung von Daten gekommen.

Inzwischen liegt ein Referentenentwurf zur Neuregelung der Hochschulstatistik vor, der auch bei den übrigen dort vorgesehenen Erhebungen (insbesondere von Studentendaten) verfassungskonforme Regelungen vorsieht. Der Entwurf sieht vor allem den Wegfall der bisherigen verwaltungsinternen Verwendungsmöglichkeiten der Daten vor. Er verzichtet auf personenbezogene Erhebungen bei den Studenten und beim wissenschaftlichen und künstlerischen Personal der Hochschulen, obwohl diese unmittelbaren Erhebungen bisher für unersetzbar gehalten wurden.

Personalbezügedateien

Da es in Berlin bisher kein Landesstatistikgesetz gibt, die Aufgaben des Statistischen Landesamtes vielmehr in Verwaltungsvorschriften, insbesondere der Statistischen Ordnung vom 9.April 1974, geregelt sind, wirft die Erstellung von Statistiken, die durch die Aufbereitung und Auswertung der in automatisierten Verwaltungsregistern und in sonstigen Informationsquellen enthaltenen Individualdaten entstehen (Registerstatistiken), große datenschutzrechtliche Probleme auf. Hierzu zählt die im Rahmen der Struktur- und Planungsdatenbank vorgenommene Auswertung der Personalbezügedateien.

Auf Grund einer Weisung der einzelnen beteiligten Verwaltungen übermittelt das LED monatlich dem Statistischen Landesamt Abzüge der Personalbezügedateien zur statistischen Auswertung.

Die Datenübermittlung umfaßt mit Ausnahme des Namens, der Kontonummer sowie der Anschrift des Betroffenen sämtliche Daten, die im Zusammenhang mit der Berechnung, Zahlbarmachung, Auszahlung und Abrechnung von Personalbezügen beim LED stehen. Hierzu gehören insbesondere die Personalnummer, das Geburtsdatum, das Geschlecht, der Familienstand, die Staatsangehörigkeit, die Sozialversicherungsnummer, die Kinderzahl, das Geburtsdatum der Kinder, die Haushaltsstelle sowie Titel und Kapitel des Haushaltsplanes.

Die Übermittlung dieses Datenbestandes entspricht hinsichtlich ihres Umfanges und ihrer Periodizität (monatlich) nicht den Vorgaben des Bundesverfassungsgerichts.

Das Gericht fordert, daß die Übermittlung (Weitergabe) weder anonymisierter noch statistisch aufbereiteter, also noch personenbezogener Daten, zum Zwecke der statistischen Aufbereitung durch andere Behörden bzw. die Statistischen Ämter des Bundes und der Länder nur kraft ausdrücklicher gesetzlicher Ermächtigung erfolgen darf[1].

Die vom LED an das Statistische Landesamt übermittelten Einzelangaben sind jedoch nicht hinreichend (faktisch) anonymisiert, da die Vielzahl der Daten ohne größeren Aufwand die Identifizierung einzelner Personen innerhalb einer bestimmten Verwaltung zuläßt. Unerheblich ist es insoweit, daß das LED dem Statistischen Landesamt keine Angaben über den Namen, die Kontonummer sowie den Wohnort und die Straße des Betroffenen übermittelt. Eine spezialgesetzliche Grundlage existiert für die Vielzahl der übermittelten Daten nicht. Lediglich im Finanzstatistikgesetz sind einige wenige der übermittelten Daten aufgeführt. Die in diesem Gesetz festgelegten zeitlichen Abstände für die Datenübermittlung (jährlich, alle drei, bzw. sechs oder neun Jahre) sind jedoch auch hier nicht erfüllt. Eine andere Rechtsgrundlage besteht nicht, so daß diese Erhebung den Anforderungen des Bundesverfassungsgerichts nicht entspricht.

4.6 Justiz

Entscheidungen der Gerichte, aber auch prozeßvorbereitende Maßnahmen (z.B. Anklageerhebung durch die Staatsanwaltschaft) lösen häufig die Pflicht aus, andere beteiligte Behörden oder Personen über die Entscheidung zu unterrichten. Diese Mitteilungspflichten sind bislang in Verwaltungsvorschriften bundeseinheitlich geregelt.

Die Datenschutzbeauftragten hatten schon bald nach Inkrafttreten der Datenschutzgesetze bemängelt, daß weder die Anordnung über Mitteilungen in Strafsachen (MiStra) noch die entsprechende Anordnung in Zivilsachen (MiZi) auf einer hinreichenden Rechtsgrundlage beruhen. Angesichts der Sensitivität vieler Daten kann diese Situation nicht mehr hingenommen werden.

Anordnung über Mitteilungen in Strafsachen (Mistra)

Die Justizminister und -senatoren haben ihre ursprüngliche Auffassung, eine derartige Rechtsgrundlage sei nicht erforderlich, inzwischen aufgegeben. Auf ihrer Konferenz vom 18. bis 20. September 1984 haben sie erklärt, daß die in der MiStra zusammengefaßten Mitteilungen einer gesetzlichen Grundlage bedürften und dem Bundesminister der Justiz Unterstützung bei der Erarbeitung neuer Vorschläge zugesagt.

Ein Unterausschuß soll für die Zwischenzeit prüfen, inwieweit die geltenden Mitteilungspflichten eingeschränkt werden können. Hierzu war im Dezember 1983 bereits ein Entwurf erarbeitet worden, der allerdings entscheidende Fragen offenließ:

- Es mangelt an einer eindeutigen Vorschrift, die die Beachtung der Zweckbindung in allen Mitteilungsfällen sicherstellt.
- Neben den Regelungen für einzelne Mitteilungspflichten sind im Entwurf auch relativ weit gefaßte Bestimmungen enthalten, wodurch die begrenzenden Einzelfallregelungen umgangen werden können. Die Neufassung sollte eine abschließende Regelung der Mitteilungsvorgänge enthalten.
- Ein strafrechtlicher Sachverhalt läßt sich endgültig erst nach Abschluß des Strafverfahrens beurteilen. Damit den von den Mitteilungen Betroffenen nicht unnötige Nachteile entstehen, sollte im Regelfall eine Mitteilung erst nach rechtskräftigem Abschluß des Verfahrens erfolgen. Ausnahmen hinsichtlich einer vorzeitigen Mitteilung müssen auf Fälle beschränkt werden, in denen wegen der Bedeutung des möglicherweise verletzten Rechtsguts die begründete Annahme

[1] BVerfGE 65, 51 ff.

besteht, daß vorzeitige Maßnahmen zu veranlassen sind bzw. die zu benachrichtigende Behörde nur aufgrund umfassender Kenntnisse des dem Strafverfahren zugrundeliegenden Sachverhalts geeignete Maßnahmen treffen kann.

- Der Inhalt der Mitteilungen ist auf das im Einzelfall wirklich erforderliche Mindestmaß zu beschränken. Das bedeutet, daß die Mitteilung sich auf die Tatsache der Verurteilung oder auf den Abdruck des Urteilstenors beschränken sollte.
- Der Betroffene sollte grundsätzlich davon benachrichtigt werden, welchen Stellen Mitteilungen nach der MiStra gemacht wurden. Davon kann ausnahmsweise abgesehen werden, wenn schwerwiegende Bedenken in der Person des Betroffenen entgegenstehen.
- Durch eindeutige Adressierung des Empfängers der Mitteilungen ist sicherzustellen, daß nur diejenigen Behörden Kenntnis erhalten, welche diese Kenntnis zu ihrer Aufgabenerfüllung benötigen.
- Die Mitteilungen sind in jedem Fall verschlossen zu versenden.
- Wegen der geringeren strafrechtlichen Vorwerfbarkeit sollten Mitteilungen bei Fahrlässigkeitstaten grundsätzlich nicht im Rahmen der MiStra erfolgen. Ausnahmen sollten nur im engen Bezug zur beruflichen Tätigkeit des von der Mitteilung Betroffenen oder bei besonderem Gewicht des verletzten Rechtsguts gemacht werden.
- Es muß sichergestellt werden, daß der Vollzug der Mitteilungen gleichmäßig erfolgt.

Anordnung über Mitteilungen in Zivilsachen (MiZi)

Diese Anordnung wirft ähnliche Probleme auf, wenn sich auch hier ein Teil der vorgeschriebenen Mitteilungen auf Rechtsvorschriften zurückführen läßt. Auch hier muß eine Überprüfung der Rechtsgrundlagen mit einer Überprüfung der Erforderlichkeit Hand in Hand gehen. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat hierzu einen entsprechenden Beschluß gefaßt. Kritisiert wurde insbesondere die Generalklausel, daß Mitteilungen im Einzelfall auch dann zu machen sind, wenn sie zwar nicht ausdrücklich vorgeschrieben, aber durch ein besonderes öffentliches Interesse geboten sind, sowie die Vorschrift, daß bisher in der Regel nicht nur der Tenor der Entscheidung, sondern der gesamte Text der Entscheidungsgründe übermittelt wird. Gefordert werden mehr Transparenz für den Bürger, eine Zweckbindung der übermittelten Daten, mehr Datensicherung und eine Begrenzung der Aufbewahrungsdauer der Mitteilungen.

Eine dem Beschluß zur MiStra vergleichbare Entscheidung der Justizminister und -senatoren ist bislang nicht bekannt.

Datenschutz in den Prozeßordnungen

Über Mängel der Prozeßordnungen im Hinblick auf den Schutz der Persönlichkeitsrechte hatte ich bereits 1982 berichtet und im Rahmen des Entwurfs einer Verwaltungsprozeßordnung Regelungen dafür gefordert, daß personenbezogene Daten Prozeßbeteiligten nicht über das verfahrensmäßig erforderliche Ausmaß hinaus offenbart werden.

Die Beschwerde eines älteren Mitbürgers machte mich auf ein weiteres Problem aufmerksam. Der Petent hatte einen Mietprozeß geführt und auch gewonnen. Wegen verschiedener Leiden war er aufgrund eines relativ ausführlichen Gutachtens von einem Facharzt für verhandlungsunfähig erklärt worden. Der unterlegene Prozeßgegner, ein Anwalt, übersandte daraufhin eine Kopie des ärztlichen Gutachtens, die er aus den Prozeßakten gefertigt hatte, an den Polizeipräsidenten, Referat Fahrerlaubnisse, mit der Bitte um Prüfung, ob es angesichts der bescheinigten Leiden noch verantwortet werden könne, daß der Petent weiterhin ein Kraftfahrzeug führt. Der Polizeipräsident bat den Petenten zu einer für diesen (positiv verlaufenen) Untersuchung.

Obwohl dieser Vorgang durchaus geeignet ist, Empörung über die Handlungsweise des Anwalts hervorzurufen, bieten weder das bestehende Datenschutzrecht noch andere Vorschriften über den Datenschutz eine Handhabe, diese Handlungsweise als rechtswidrig zu qualifizieren. Insbesondere greifen weder die Vorschriften über die Verschwiegenheitspflicht des Arztes noch die des Anwalts, da Informationen, die dem Prozeßgegner in einem Prozeß bekannt werden, nicht unter den Geltungsbereich von § 203 Strafgesetzbuch fallen. Auch die Strafvorschriften über den Schutz der persönlichen Ehre greifen nicht.

Gleichwohl stellen Vorgänge wie der vorliegende Fall einen empfindlichen Eingriff in die Persönlichkeitsrechte dar. Wer aus gesundheitlichen Gründen zu bestimmten Prozeßhandlungen nicht in der Lage ist, muß dies zu Recht begründet darlegen. Nicht erforderlich ist hingegen, daß er damit gezwungen wird, die in der Begründung enthaltenen personenbezogenen Daten dem Prozeßgegner oder gar der Öffentlichkeit zu unterbreiten und dabei das Risiko einzugehen, daß die so bekannt gewordenen Angaben zu anderen Zwecken verwertet werden.

Eine Lösung könnte darin bestehen, daß (ähnlich wie dies für die Unterlagen zur Gewährung von Prozeßkostenhilfe zu fordern ist) medizinische Gutachten und andere ähnlich sensible Schriftstücke nicht zum Gegenstand öffentlicher Verhandlungen gemacht und so in der Akte geführt werden, daß sie der Einsichtnahme durch die Prozeßbeteiligten entzogen sind, wenn nicht besondere Gründe die Einsicht rechtfertigen.

Denkbar wäre auch, in Überlegungen darüber einzutreten, ob die Strafvorschriften über den Ehrschutz nicht ergänzt werden sollten um die böswillige Verbreitung besonders sensibler persönlicher Angaben, auch wenn diese der Wahrheit entsprechen.

Dessenungeachtet ist Ärzten und anderen mit Gutachten betrauten Sachverständigen zu empfehlen, sensible Daten in Berichte und Gutachten nur im unbedingt erforderlichen Ausmaß aufzunehmen.

Ungeklärt und im Rahmen anstehender Änderungen der Prozeßordnungen ebenfalls regelungsbedürftig ist die Frage, in welchem Umfang Anwälte Daten, die sie auf Grund des ihnen zustehenden Akteneinsichtsrechts (z.B. § 141 StPO) aus Akten der eigenen Mandanten zur Kenntnis genommen haben, weitergeben dürfen. Problematisch sind dabei insbesondere Daten über Dritte. So erregte ein Fall Aufsehen, in dem bei der Wohnungsdurchsuchung eines mit Haftbefehl gesuchten Verdächtigen eine komplette Kopie der Ermittlungsakte gefunden wurde: In der Akte fanden sich personenbezogene Daten über Belastungszeugen, die mit Repressalien rechnen mußten. Es ist nicht ausgeschlossen, daß der Verdächtige die Kenntnisse über seinen Anwalt erhalten hat.

4.7 Vom Umgang mit Sozialdaten

Führung von Sozialakten

Vom Senator für Schulwesen, Jugend und Sport wurde eine weiterführende Fortbildung zu Problemen des Sozialgeheimnisses in der behördlichen Jugendhilfe angeboten, die sich mit Problemen des Datenschutzes im Bereich der Familienfürsorge befaßte und an der sein zuständiger Mitarbeiter teilgenommen hat. Die Gruppe hat Vorschläge zur Verbesserung des Datenschutzes erarbeitet[1)], die ich den zuständigen Ämtern in den Bezirken mit der Bitte übersandt habe, sie insbesondere bei der Aktenführung zu berücksichtigen.

Zwei Vorgänge verdeutlichen die Bedeutung dieser Regelungen:

Eine Petentin beschwerte sich darüber, daß in ihrer Familienfürsorgeakte der Heimeinweisungsbericht über ein Kind enthalten sei, in dem äußerst private Angelegenheiten erörtert wurden. Ihr sei von dem Zustandekommen des Berichts nichts bekanntgeworden und dieser Bericht sei mit der Familienfürsorgeakte an das Amt für wirtschaftliche Hilfen weitergeleitet und damit einem nicht berechtigten Personenkreis zugänglich geworden. Diese Beschwerde war sachlich begründet. Ihr wurde vom zuständigen Bezirksamt schnell abgeholfen.

In einem anderen Fall wurde mir die Frage vorgelegt, ob ein Sozialamt aus der Sozialakte, die dem Sozialgericht vorzulegen war,

[1)] Vgl. Anlage 4

ein längst veraltetes Führungszeugnis herausnehmen muß. Das Gericht erhält auf diese Weise möglicherweise Kenntnisse, die es nach den Bestimmungen des Bundeszentralregistergesetzes nicht mehr verwerten darf.

Zwar fehlt in diesem Fall die Erforderlichkeit der Offenbarung an das Gericht; andererseits wäre es problematisch, wenn die Behörden Akten, die einem Gericht vorzulegen sind, vor der Herausgabe bereinigen würden. Eine sachgerechte Handhabung wäre hier nur gewährleistet, wenn bereits die Art der Aktenführung so erfolgt, daß Konflikte verhindert werden. Dies bedeutet, daß an die Stelle einer Familienakte nach Aufgaben und Vorgängen differenzierte Akten zu einer Familie geführt werden.

Offenbarung von Sozialdaten an den Petitionsausschuß

Die Zulässigkeit der Offenbarung von Sozialdaten an den Petitionsausschuß des Abgeordnetenhauses ist - wie überhaupt die Offenbarung an öffentliche Stellen mit Kontrollaufgaben - im Sozialgesetzbuch nicht eindeutig geregelt. Ich vertrete hierzu die Auffassung, daß auch ohne besondere Einwilligung des Petenten der Petitionsausschuß in dessen Sozialakten Einsicht nehmen kann, wenn die Akte Gegenstand der Petition ist.

Denn auch die Arbeit der Sozialleistungsträger darf nicht der erforderlichen Überprüfung entzogen werden. Zwar stellt § 35 SGB X nur „aufsichtsberechtigte Behörden" den Sozialleistungsträgern gleich. Ungeachtet der Tendenz der Rechtsprechung, auch parlamentarischen Gremien behördenähnliche Befugnisse einzuräumen, kommt es auf die Behördeneigenschaft des Petitionsausschusses hier nicht an: Die Befugnis, nach § 69 Abs. 1 Ziff. 1 SBG X zur Wahrnehmung von Aufgaben nach dem Sozialgesetzbuch Sozialdaten zu offenbaren, umfaßt auch die Offenbarung zu Zwecken der Verwaltungskontrolle. Die Gewährleistung der Kontrolle ist als Bestandteil der Aufgabenerfüllung zu betrachten. Da § 69 Abs. 1 Ziff. 1 SGB X eine zulässige Durchbrechung des Sozialgeheimnisses darstellt, spielt § 5 Abs. 3 a Petitionsgesetz nur noch insoweit eine Rolle, als die Daten über die allgemeine Verpflichtung zur Wahrung des Datengeheimnisses hinaus einer besonderen Verschwiegenheitspflicht, insbesondere einem Berufs- oder Amtsgeheimnis unterliegen. Medizinische Daten sollten daher nur mit Einwilligung des Betroffenen an den Petitionsausschuß gegeben werden.

Nutzung des Telebusverkehrs durch Schwerbehinderte

Durch die Neuregelung der Freifahrt für Schwerbehinderte seit 1. April 1984 wurde es erforderlich, Telebusbenutzer in unterschiedlicher Höhe an den Kosten zu beteiligen. Die Fahrtberechtigung muß seither durch eine Wertmarke nachgewiesen werden. Um die Telebusbenutzer von dem ständigen und wiederholten Nachweis zu befreien, sollte der Berliner Zentralausschuß für soziale Angelegenheiten vom Landesversorgungsamt darüber informiert werden, welcher Telebusbenutzer eine Wertmarke besitzt.

Eine Datenübermittlung nach § 68 SGB X kam nicht in Frage, weil außer den dort genannten Kategorien auch zusätzlich das Kriterium des Besitzes einer Kostenmarke übermittelt werden sollte. Eine Datenübermittlung nach § 69 SGB X scheiterte daran, daß der Grundsatz der Verhältnismäßigkeit Zweifel an der Erforderlichkeit zur Aufgabenerfüllung aufkommen ließ. Das Prinzip der Verhältnismäßigkeit, welches auch bei der Auslegung des Begriffs der Erforderlichkeit maßgeblich ist, stellt auf die geeignete und am geringsten belastende Qualität eines Eingriffs ab.

Damit war die Datenübermittlung nur auf Grund der Einwilligung der Betroffenen zulässig. Die Senatsverwaltung realisierte daher das „Einwilligungsmodell" und versandte an die derzeitigen Benutzer des Telebusses entsprechende Formulare. Allerdings war der Text des Formulars entgegen meiner Empfehlung so abgefaßt, daß bei den Benutzern Zweifel über den Umfang des Datenabgleichs entstanden. Übermittelt werden sollte lediglich die Tatsache des Besitzes einer Kostenmarke. Das mißverständlich formulierte Formular führte zu zahlreichen Beschwerden durch die Betroffenen.

Veröffentlichung säumiger unterhaltspflichtiger Personen

Im Suchblatt des Deutschen Instituts für Vormundschaftswesen werden unterhaltspflichtige Personen, für deren unterhaltsberechtigte Kinder ein Amtsvormund bestellt wurde, namentlich veröffentlicht, wenn sie sich ihren Unterhaltspflichten entzogen haben. Diese Publikation ist auch in Bibliotheken zugänglich. Obwohl die Vormundschaft im Bürgerlichen Gesetzbuch geregelt ist, sehe ich die Amtsvormundschaft als eine Aufgabe nach dem Sozialgesetzbuch an, da sie gemäß § 4 Ziff. 2 Jugendwohlfahrtsgesetz als Aufgabe den Jugendämtern übertragen wurde. Ich habe der Senatsverwaltung für Schulwesen, Jugend und Sport empfohlen, sich auch bei diesem Verfahren an das Erforderlichkeitsprinzip zu halten. Die Suchlisten dürfen daher nur an einschlägige Stellen übersandt werden, von denen sachdienliche Hinweise zur Auffindung des Unterhaltsverpflichteten zu erwarten sind. Die Offenbarung der Daten an die Öffentlichkeit ist daher unzulässig.

Offenbarung von Ausbildungsförderungsdaten

Die Förderung von Studenten nach dem Bundesausbildungsförderungsgesetz (BAföG) macht einen Datenaustausch zwischen Hochschulen und dem Studentenwerk, dem die Aufgabe des Ausbildungsförderungsamtes übertragen ist, erforderlich. Dies wirft Schwierigkeiten auf: Übermittelt das Studentenwerk Förderungsdaten an die Hochschulen, entstehen dort im Studentendatensatz Sozialdaten, die die Hochschule nicht benötigt. Übermitteln die Hochschulen die Daten aller Studenten an das Studentenwerk, erhält dieses erheblich mehr Daten als es zur Aufgabenerfüllung benötigt.

Da die Datenermittlung auf das erforderliche Ausmaß zu beschränken ist, darf ein genereller Datenabgleich nicht erfolgen. Ich habe deshalb empfohlen, in gewissen Abständen von den Universitäten eine Liste aller Studenten, bei denen die Mitteilungsvoraussetzungen vorliegen (Exmatrikulation, Prüfungsabschluß, Beurlaubung), zu erstellen. Im LED werden diese Daten mit dem BAföG-Bestand abgeglichen. Die aus dem Abgleich entstehende Liste geht an das Studentenwerk, welches daraufhin die Zahlungen einstellen kann. Die entstehenden Zwischendateien sowie die von den Hochschulen übermittelten Listen sind nach der Verarbeitung sofort zu löschen.

Meine Empfehlung wurde allerdings angeblich wegen „Arbeitserschwernissen" nicht realisiert. Stattdessen wurde auf eine Änderung des Berliner Hochschulgesetzes verwiesen, wonach die Hochschulen verpflichtet sind, Beiträge für die Studentenschaft zu erheben und einzuziehen (§ 24 Berliner Hochschulgesetz). Es wird darauf verwiesen, daß es nunmehr für die Aufgabenerfüllung der Freien Universität erforderlich sei, zu wissen, welcher Studierende BAföG-Empfänger sei, da diese eine geringfügige Ermäßigung der AStA-Beiträge erhielten.

Die von mir vorgebrachten Bedenken sind damit nicht entfallen: Das Berliner Hochschulgesetz ist kein Gesetz i.S. des § 69 Abs. 1 SGB X. Die Datenübermittlung vom Studentenwerk an die Hochschule ist somit nicht zur Erfüllung der Vorschriften des Sozialgesetzbuches und der dort genannten weiteren Folgevorschriften erforderlich. Eine endgültige Stellungnahme der beteiligten Stellen steht noch aus.

Offenbarung von Sozialdaten für Zwecke der Strafverfolgung

Nach ausgiebigen Verhandlungen mit Vertretern der Senatsverwaltungen für Inneres, Justiz, Arbeit und Betriebe, Schulwesen, Jugend und Sport, sowie Vertretern der Bezirksämter aus den Abteilungen für Soziales und den Kontaktpersonen für den Datenschutz wurde ein gemeinsames Rundschreiben der Senatoren für Gesundheit, Soziales und Familie, für Schulwesen, Jugend und Sport und für Arbeit und Betriebe[1] entworfen, in dem Empfehlungen zum Verfahren zur Datenoffenbarung nach § 68 SGB X sowie zur Auslegung dieser Vorschrift gegeben wurden.

[1] Rundschreiben über die Offenbarung von Sozialdaten im Rahmen der Amtshilfe nach § 68 SGB X vom 22. März 1984, Dienstblatt IV, S. 58

Der Inhalt entspricht meiner Empfehlung. Im Ergebnis kann auch den Strafverfolgungsbehörden gemäß § 68 SGB X Auskunft im dort genannten Umfang gegeben werden. Soweit zu Zwecken der Strafverfolgung weitergehende Auskünfte benötigt werden, können diese grundsätzlich erteilt werden, jedoch bedarf es zuvor einer richterlichen Anordnung nach § 73 SGB X, die mit dem Auskunftsbegehren vorgelegt werden muß.

Unabhängig von diesem Verfahren kann auch aufgrund einer Einwilligung des Hilfeempfängers Auskunft gegeben werden. Hierzu hatte die Polizei ein Erklärungsformular entwickelt, worin der Unterzeichner auch die Einwilligung für seine Kinder erklären sollte. Eine solche Erklärung kann zunächst nur für den Erklärenden selbst wirken. Eine Einwilligungserklärung für minderjährige Kinder ist nur insoweit zulässig, als die Kinder selbst noch nicht die erforderliche Willensfähigkeit haben.

Nachweis der Berechtigung zum Bezug von Leistungen

In mehreren Eingaben wurde ich von Beziehern von Leistungen der Bundesanstalt für Arbeit darauf aufmerksam gemacht, daß die BVG von ihnen bei der Gewährung von Fahrpreisermäßigungen als Nachweis für den Fortbestand der Arbeitslosigkeit die Vorlage von Bankauszügen verlangt.

Diese Praxis halte ich für bedenklich, da die Leistungsbezieher bei der Inanspruchnahme der Fahrpreisermäßigung über das erforderliche Maß hinaus gezwungen werden, personenbezogene Daten (weitere Abbuchungen, Gutschriften, Kontostände) zu offenbaren.

Ein Unkenntlichmachen kann in diesem Zusammenhang keine befriedigende Lösung darstellen, da dieser Kontoauszug möglicherweise für andere Zwecke - z.B. Vorlage beim Finanzamt - benötigt wird.

Auf meine Anregung hin hat der für die Berliner Arbeitsämter zuständige Bundesbeauftragte für den Datenschutz mit der Bundesanstalt für Arbeit die meiner Meinung nach praktikable Empfehlung ausgesprochen, daß den arbeitslosen Leistungsempfängern auf der Besucherkarte der Arbeitsämter mit Dienststellenstempel und Datum in Intervallen von drei Monaten der Bezug von Leistungen bestätigt wird. Ein ähnliches Problem stellt die Forderung der BVG dar, daß Auszubildende zur Erlangung der Fahrpreisermäßigung ihren Ausbildungsvertrag vorlegen müssen. Auch diese Praxis konnte bisher nicht geändert werden.

Leider wurde dieser Vorschlag weder von der BVG noch vom Landesarbeitsamt Berlin angenommen. Über eine Verbesserung des Verfahrens werden noch weitere Beratungen geführt.

4.8 Bau- und Wohnungswesen

Kaufpreissammlung

Bereits in meinem Jahresbericht 1983 hatte ich auf das Problem des Zugriffs auf die Kaufpreissammlung beim Senator für Bau- und Wohnungswesen hingewiesen und mitgeteilt, daß die Möglichkeit des unbeschränkten Zugangs für die bezirklichen Vermessungsämter mit §§ 136 ff. Bundesbaugesetz unvereinbar sei. Nach diesen Vorschriften steht die Kaufpreissammlung nur dem Gutachterausschuß bzw. dessen Geschäftsstelle und den Finanzämtern zur Verfügung.

Inzwischen hat sich herausgestellt, daß auch die kommunalen Bewertungsstellen in vollem Umfang die Kaufpreissammlung für bezirkliche Grundstücksbewertungen nutzten. Eine Rechtsgrundlage für dieses Verfahren ist nicht ersichtlich. Vielmehr werden die in der Kaufpreissammlung enthaltenen persönlichen und sachlichen Angaben über Grundstücke und deren Eigentümer, Verkaufspreise usw. Stellen zugänglich gemacht, die nach dem Bundesbaugesetz vom Zugriff ausgeschlossen sind.

Ich habe gegenüber dem Senator für Bau- und Wohnungswesen eine Beanstandung ausgesprochen, da ich in der mangelnden Abschottung der Kaufpreissammlung eine Verletzung der datenschutzrechtlichen Vorschriften des Bundesbaugesetzes sehe. Ich habe empfohlen, organisatorische und technische Maßnahmen zu ergreifen, um die Einhaltung der Regelungen des Bundesbaugesetzes sicherzustellen.

Der Senator für Bau- und Wohnungswesen hat daraufhin die Bezirksämter angewiesen, die Kaufpreissammlung ausschließlich zu Zwecken des Gutachterausschusses zu nutzen. Den Belangen der Bewertungsstellen soll künftig durch die Herausgabe anonymisierter Werttabellen Rechnung getragen werden.

Nach wie vor klärungsbedürftig ist, wie sichergestellt werden kann, daß die beim Gutachterausschuß mitwirkenden bezirklichen Vermessungsämter nicht auf mehr Daten zugreifen können, als für ihren regionalen Zuständigkeitsbereich erforderlich sind.

Mietobergrenzensystem

Um die Folgen von Mietsprüngen im sozialen Wohnungsbau aufzufangen, hat der Senat beschlossen, vom nächsten Jahr an bestimmte Mieter besonders zu fördern. Es soll durch ein „Mietobergrenzensystem" sichergestellt werden, daß eine Miethöhe von 25 % des Einkommens nicht überschritten wird. Der Einfachheit halber sollte bei der Berechnung der jeweiligen Miete die beim Senator für Bau-und Wohnungswesen vorliegende Datei zur Fehlbelegungsabgabe verwendet werden; Personen, bei denen aufgrund ihrer Pflicht zur Zahlung einer Fehlbelegungsabgabe festgestellt wurde, daß ihr Einkommen bestimmte Grenzen überstieg, kamen als Förderungsempfänger des Mietobergrenzensystems nicht in Betracht.

Ich habe darauf hingewiesen, daß die für die Zahlung der Fehlbelegungsabgabe erhobenen, z. T. sehr sensiblen Daten über Einkommen und Wohnungssituation, nicht für einen ganz anderen Zweck verwendet werden dürften und es an einer gesetzlichen Grundlage für einen Abgleich fehle.

Im Zusammenwirken mit dem Senator für Bau- und Wohnungswesen ist eine Lösung gefunden worden, welche die Belange der Verwaltung an einer rationellen Verfahrensweise und das Interesse des Bürgers an einer zweckgebundenen Verwendung seiner Angaben gleichermaßen berücksichtigt. Der aufgrund der Fehlbelegungsdatei bekannte Personenkreis wird dabei angeschrieben und kann anhand des Anschreibens feststellen, ob im jeweiligen Fall eine Förderung in Betracht kommt. Der Mieter kann sich dann mit einem Antrag an die Bewilligungsstelle wenden. Dabei wird sein Einverständnis mit der Verwendung von Angaben aus der Fehlbelegungsdatei eingeholt. Bei dieser Verfahrensweise ist der Bürger darüber informiert, welche Daten von ihm verwendet werden.

An diesem Abstimmungsverfahren zwischen dem Senator für Bau- und Wohnungswesen und mir zeigte sich erneut, daß bei einer rechtzeitigen Erörterung anstehender Fragen datenschutzrechtliche Probleme vermieden werden können.

5. Nachtrag zu Feststellungen aus den Vorjahren

Neben den in den bisherigen Abschnitten dargestellten neuen Entwicklungen zu Feststellungen aus den Vorjahren sind folgende Entwicklungen von besonderer Bedeutung:

Kriminalpolizeiliche personenbezogene Sammlungen (KpS) (Jahresbericht 1981, S. 10, Jahresbericht 1982, S. 11, Jahresbericht 1983, S. 23)

Zu Beginn des Jahres wurde damit begonnen, von Berlin aus Daten in den Kriminalaktennachweis (KAN) beim Bundeskriminalamt einzuspeisen. Verfahren wird dabei nach den bundesweit geltenden Richtlinien. Wegen der besonderen Lage Berlins spielt diese Übermittlung jedoch eine geringere Rolle als in anderen Ländern.

Die Aussonderung von Akten, die nach den Richtlinien über die KpS nicht mehr erforderlich sind, wurden vorangetrieben. Vor Ort habe ich mich über die Arbeit der eigens für diesen Zweck beim Polizeipräsidenten eingerichteten Arbeitsgruppe informiert.

Die Sammlungen, die im Zusammenhang mit Hausbesetzungen eingerichtet worden waren, sind inzwischen im gebotenen Umfang vernichtet bzw. bereinigt. Auch die Stellen, an die die Daten übermittelt worden waren, haben entsprechende Bereinigungen ihrer Datenbestände vorgenommen.

Auskunftsvordruck Schuldnerverzeichnis
(Jahresbericht 1981, S. 15)

Bei dem Antrag auf Auskunft über einen Schuldner aus dem Schuldnerverzeichnis wird nunmehr ein neues Formular verwendet. Bei nicht hinreichend sicherer Identität der nachgefragten Person mit einem im Verzeichnis befindlichen Schuldner wird der Antragsteller aufgefordert, zuerst durch eine Anfrage beim Einwohnermeldeamt das Geburtsdatum und die frühere Anschrift ermitteln zu lassen und sodann die Anfrage mit diesen Angaben zu wiederholen. Die Justizverwaltung hat damit meinem Anliegen, unliebsame Verwechslungen - insbesondere bei häufigen Namen - zu verhindern, Rechnung getragen. Eingaben wegen fehlerhafter Auskünfte aus dem Schuldnerverzeichnis hat es seitdem nicht mehr gegeben.

Datei der Taxifahreranmeldungen
(Jahresbericht 1981, S. 16)

Da es nicht gelungen ist, in einer Novelle zum Personenbeförderungsgesetz eine Bestimmung über die Meldung von Taxifahrern unterzubringen, wurde für Berlin in der am 1. September 1983 in Kraft getretenen Taxenordnung eine Verpflichtung zur namentlichen Benennung der Fahrzeugführer geschaffen. Ich bin der Auffassung, daß diese Bestimmung mangels einer entsprechenden Ermächtigung im Personenbeförderungsgesetz nicht wirksam ist. Aufgrund der Klage eines Taxiunternehmers wird das Verwaltungsgericht hierüber zu entscheiden haben.

Schülerdaten
(Jahresbericht 1980, S. 13, Jahresbericht 1981, S. 11 f. Jahresbericht 1982, S. 20, Jahresbericht 1983, S. 24)

Die Einholung unbeschränkter Auskünfte aus dem Bundeszentralregister wurde von mir erneut überprüft. Wiederum ergab sich trotz des Rundschreibens des Senators für Inneres, daß Auskünfte in einem über das Zulässige hinausgehenden Ausmaß eingeholt wurden. In den festgestellten Fällen habe ich Beanstandungen ausgesprochen. In den meisten Fällen hat die Beanstandung zu einer Änderung des Verfahrens geführt.

Unbeschränkte Auskünfte aus dem Bundeszentralregister
(Jahresbericht 1980, S. 12, Jahresbericht 1981, S. 10, Jahresbericht 1982, S. 20, Jahresbericht 1983, S. 24)

Die Einholung unbeschränkter Auskünfte aus dem Bundeszentralregister wurde von mir erneut überprüft. Wiederum ergab sich trotz des Rundschreibens des Senators für Inneres, daß Auskünfte in einem über das Zulässige hinausgehenden Ausmaß eingeholt wurden. In den festgestellten Fällen habe ich Beanstandungen ausgesprochen. In den meisten Fällen hat die Beanstandung zu einer Änderung des Verfahrens geführt.

Datenverarbeitung bei der Amerika-Gedenkbibliothek
(Jahresbericht 1982, S. 17)

Aufgrund meiner Anregungen werden bei der demnächst anlaufenden computergestützten Ausleihverbuchung die variablen Benutzerdaten, die die einzelnen Ausleihvorgänge beschreiben, nach Abschluß des Ausleihvorganges gelöscht. Statistisch relevante Daten werden in computergestützter Form weiterhin gespeichert. Die Ableitung von individuellen Leserprofilen ist mit diesen Daten ausgeschlossen.

ADV-Verfahren Amts- und Staatsanwaltschaften (ASTA)
(Jahresbericht 1983, S. 19 f.)

Das ADV-Verfahren Amts- und Staatsanwaltschaften (ASTA), zu dessen Gestaltung ich schwerwiegende Bedenken geäußert habe, ist nunmehr in den Vollbetrieb übergegangen. Ich habe mich bei einer Vorführung davon unterrichten lassen, daß entsprechend der Stellungnahme des Senats zu meinem Jahresbericht 1983 meinen Empfehlungen nur in geringfügigem Maße Rechnung getragen wurde. Inwieweit die praktische Verwendung des Systems die von mir kritisierten Eigenschaften des Verfahrens zu Verletzungen schutzwürdiger Belange von Betroffenen führen werden oder können, wird Gegenstand weiterer Überprüfungen sein müssen.

6. Zusammenarbeit mit anderen Stellen

Datenschutzbeauftragte des Bundes und der Länder

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat in vier Sitzungen unter dem Vorsitz des Hamburgischen Datenschutzbeauftragten beraten.

Die wichtigsten Ergebnisse lassen sich wie folgt zusammenfassen:

18. Konferenz am 18. Januar 1984:

- Beschluß einer gemeinsamen Erklärung zur Erteilung von Bankauskünften nach der Neufassung der Allgemeinen Geschäftsbedingungen der Banken und Sparkassen
- Beschluß einer gemeinsamen Stellungnahme zur Errichtung des bundesweiten Kriminalaktennachweises (KAN)

19. Konferenz am 27./28. März 1984:

- Beschluß über die Auswirkungen des Bundesverfassungsgerichtsurteils vom 15. Dezember 1983 zum Volkszählungsgesetz 1983
- Beschluß über die gesetzliche Regelung des Datenschutzes bei der Kabelkommunikation

20. Konferenz am 6./7. Juni 1984:

- Beschluß über das Telefonfernwirksystem "TEMEX"

21. Konferenz am 15./16. Oktober 1984:

- Beratung über Planungen zur vorgesehenen Volkszählung
- Beschluß über das Hochschulstatistikgesetz

Der Konferenzvorsitz wird mit dem Jahreswechsel turnusgemäß auf den Hessischen Datenschutzbeauftragten übergehen.

Abgeordnetenhaus

Die aufgrund meiner Hilfsfunktion für das Parlament bestehenden vielfältigen Beziehungen zu den Fraktionen und Abgeordneten konnten weiter ausgebaut werden. So ergab sich insbesondere aus der Beratung des Kabelpilotprojektgesetzes die Notwendigkeit zu Stellungnahmen gegenüber dem federführenden Ausschuß für Kulturelle Angelegenheiten, dem Rechtsausschuß sowie Ausschuß für Bundesangelegenheiten und Gesamtdeutsche Fragen. Bei der Beratung des Krankenhausgesetzes habe ich gegenüber dem Ausschuß für Gesundheit, Soziales und Familie sowohl schriftlich wie auch mündlich Stellung genommen, um die Aufnahme einer Datenschutzvorschrift zu erreichen. Ferner sind die Beratungen des Unterausschusses zum Berliner Meldegesetz des Ausschusses für Inneres, Sicherheit und Ordnung weiter fortgesetzt worden. Schließlich habe ich gegenüber dem Ausschuß für Bundesangelegenheiten und Gesamtdeutsche Fragen über den Zugang zum Berlin Document Center eine Stellungnahme abgegeben.

Die gerade in diesem Jahr erreichten wesentlichen Fortschritte in dem Bereich der Einbeziehung des Datenschutzes in das Gesetzgebungsverfahren sind das Ergebnis der Zusammenarbeit mit allen Fraktionen des Abgeordnetenhauses.

Koordination mit der zuständigen Verwaltungsbehörde für Bildschirmtext

Das Bildschirmtext-Zustimmungsgesetz sieht eine relativ komplizierte Zuständigkeitsverteilung bei der Überprüfung der Einhaltung von Datenschutzbestimmungen bei Bildschirmtext vor. Während mir die Aufgabe zugewiesen ist, die Auswirkungen von Bildschirmtext zu beobachten, nehmen der Senator für Inneres, die jeweiligen Senatsverwaltungen in ihrem Geschäftsbereich (für öffentliche Anbieter) und der Senator für Kulturelle Angelegenheiten Aufgaben der zuständigen Verwaltungsbehörde wahr. Deren Hauptfunktion besteht darin, zu überprüfen, ob bestimmte Anbieter oder bestimmte Angebote von der Nutzung von Bildschirmtext auszuschließen sind.

Um Unstimmigkeiten und Mehrarbeit zu vermeiden, habe ich zunächst mit dem Senator für Inneres eine Vereinbarung darüber getroffen, wie vorgegangen werden soll, wenn Beschwerden von

Bürgern über Bildschirmtext eingehen. Mit dieser Vereinbarung ist einerseits sichergestellt, daß ich in die Lage versetzt werde, entsprechend dem Zustimmungsgesetz Mängel gegenüber dem Senator für Inneres festzustellen und entsprechende Empfehlungen auszusprechen. Andererseits wird eine unverzügliche Bearbeitung durch die zuständige Stelle dann gewährleistet, wenn Beschwerden bei mir eingehen. In der Praxis ist die Zusammenarbeit reibungslos erfolgt.

Aufsichtsbehörde für nicht-öffentliche Stellen

In den turnusmäßigen Sitzungen mit dem Senator für Inneres als Aufsichtsbehörde für den Datenschutz wurden zahlreiche Grundsatz- und Einzelfragen behandelt: Die Auslegung und Auswirkungen des Volkszählungsurteils, die Änderung der Allgemeinen Geschäftsbedingungen der Banken und Sparkassen, die Nutzung privater Computer für dienstliche Zwecke und die private Heimarbeit mit sensiblen Daten.

7. Aufgaben des Berliner Datenschutzbeauftragten

7.1 Im Berichtsjahr 1984

Anrufungen durch jedermann

Die Zahl der schriftlichen Eingaben ist gegenüber dem Vorjahr gleich geblieben, dagegen hat sich die Verteilung der Eingaben auf die einzelnen Verwaltungsgebiete teilweise erheblich geändert. Sie entfallen nach der Häufigkeit geordnet insbesondere auf folgende Gebiete:

1. Öffentliche Ordnung
2. Eingaben zum Bildschirmtext
3. Personalangelegenheiten
4. Öffentliche Sicherheit
5. Gesundheit und Soziales
6. Körperschaften/Anstalten/Eigenbetriebe
7. Bezirke

In gut 60 % (Vorjahr 50 %) aller Eingaben haben sich Mängel herausgestellt. Der gestiegene Anteil an festgestellten Mängeln bestätigt den bereits im vergangenen Jahr beobachteten Trend, daß der Anteil nicht substantiierter Eingaben weiter zurückgegangen ist.

Den Bund, die Kirchen und den Bereich der Privatwirtschaft betreffende Eingaben habe ich an die zuständigen Stellen abgegeben.

Beratung und Kontrolle

Bei den Beratungsersuchen (§ 21 Abs. 1 letzter Satz Berliner Datenschutzgesetz) war wiederum eine ganz erhebliche Zunahme zu beobachten. Dies beruhte nicht zuletzt auf der verstärkten Einbindung des Berliner Datenschutzbeauftragten in die Gesetzgebungstätigkeit.

Öffentlichkeitsarbeit

Der gute Kontakt zur Bevölkerung und zu den Medien hat sich fortgesetzt. Zahlreiche Presseberichte, Rundfunk- und Fernsehsendungen haben sich mit der Arbeit des Berliner Datenschutzbeauftragten befaßt. Anlaß dafür gaben vor allem das Bankauskunftsverfahren, die Konsequenzen des Volkszählungsurteils, Bildschirmtext und das Vorhaben, einen maschinenlesbaren Personalausweis einzuführen. Weiter haben meine Mitarbeiter und ich wiederum an zahlreichen öffentlichen Veranstaltungen und Podiumsdiskussionen teilgenommen. Auch ist die Nachfrage nach Informationsmaterial erheblich gestiegen. Besonderes Interesse bestand an dem Urteil des Bundesverfassungsgerichts, meinen Jahresberichten sowie meiner Stellungnahme zu den Konsequenzen dieses Urteils.

7.2 Voraussichtliche Schwerpunkte

Aufgrund der bisherigen Erfahrungen ergeben sich folgende Schwerpunkte für das Jahr 1985:

a) Erledigung der Anliegen, die die Bürger mit ihren Eingaben verfolgen

b) Werbung für eine zügige Verwirklichung der auf Landesebene erforderlichen bereichsspezifischen Regelungen (vgl. oben unter 1.)

c) Überprüfungen von Amts wegen und Beratungen
   - bei Anwendungen mit offenen Datennetzen
   - im Bereich Öffentliche Sicherheit und Strafverfolgung
   - beim Kabelpilotprojekt/TEMEX/Btx
   - in weiteren Bezirksämtern

Im Rahmen der Internationalen Funkausstellung 1985 ist ein Workshop Datenschutz und Neue Medien mit internationaler Beteiligung geplant.

7.3 Absehbare Entwicklungen

Im Mittelpunkt der Erörterungen um die Weiterentwicklung des Datenschutzes steht naturgemäß die Diskussion der Auswirkungen des Urteils des Bundesverfassungsgerichts zum Volkszählungsgesetz. Über die Konsequenzen, die sich aus meiner Sicht für den Berliner Gesetzgeber ergeben, habe ich in einer besonderen Stellungnahme berichtet. Einen entsprechenden Beschluß hat die Konferenz der Datenschutzbeauftragten gefaßt; der Bundesbeauftragte für den Datenschutz hat dem Bundestag gesondert berichtet. Der Senat hat entsprechend einem Beschluß des Abgeordnetenhauses ebenfalls berichtet und im wesentlichen die Positionen der Datenschutzbeauftragten bestätigt, wenn hier auch gewisse Einschränkungen im Detail vorgenommen werden.

Die einzelnen Rechtsbereiche, die einer Neuregelung bedürfen, habe ich eingangs (1.) geschildert. Ein Teil dieser Aufgaben ist auf Bundes- und Landesebene bereits in Angriff genommen worden. Dabei vertritt die Berliner Verwaltung die Auffassung, daß in Bereichen, die sowohl vom Bund als auch vom Land zu regeln sind, die Gesetzgebung des Bundes abgewartet werden sollte.

In der Tat ist auf Bundesebene die Gesetzgebung in mehreren Rechtsbereichen in Angriff genommen worden. Zu nennen sind insbesondere mehrere Vorhaben zur Novellierung der Statistikgesetzgebung und die Schaffung eines Bundesarchivgesetzes. Auf anderen Gebieten werden bundeseinheitliche Verwaltungsvorschriften (z.B. zur Führung von Personalakten) diskutiert.

Das Abwarten des Berliner Gesetzgebers führt allerdings zu Schwierigkeiten in der Verwaltungspraxis: Legt man z.B. die Kriterien des Bundesverfassungsgerichts an die derzeitigen Verfahren der amtlichen Statistik an, müßte man zu einer weitgehenden Blockierung gelangen. Diese Schwierigkeit kann man nur mühsam mit Hilfe des „Übergangsbonus" überwinden, den das Gericht bisher in vergleichbaren Situationen gewährt hat. Um diese schwierige Lage überwinden zu können, muß auch der Landesgesetzgeber unverzüglich Anstrengungen unternehmen, eine befriedigende Rechtslage zu schaffen.

Da die Datenschutzgesetze ihrer Bestimmung nach Auffanggesetze sind, sollten erst im erforderlichen Umfang die spezialgesetzlichen Regelungen getroffen werden. Erst wenn auf diese Weise absehbar ist, welche Lücken noch regelungsbedürftig sind, sollten die Datenschutzgesetze nach reiflicher Diskussion und unter Berücksichtigung bisher nicht geregelter Aspekte novelliert werden.

Berlin, 17. Dezember 1984

Der Berliner Datenschutzbeauftragte

Dr. Kerkau

Anlage 1

Gesetz
zur Änderung des Landeskrankenhausgesetzes
vom 23. Juli 1984
(GVBl. S. 1008)

Auszug

§ 15 wird wie folgt gefaßt:

„§ 15
Krankengeschichten, Datenschutz

(1) Im Krankenhaus wird vom behandelnden Arzt über jeden Patienten für die Zeit des Krankenhausaufenthaltes eine Krankengeschichte geführt.

(2) Die Krankenhausleitung gewährleistet, daß im Krankenhaus auf Patientendaten nur im erforderlichen Umfang zugegriffen wird. Im Rahmen der Aus-, Fort- und Weiterbildung von Ärzten und Medizinalfachpersonen ist zu gewährleisten, daß auf Patientendaten nur insoweit zugegriffen wird, als dies für die dem Berufsbild entsprechenden Funktionen erforderlich ist.

(3) Eine Offenbarung von Patientendaten an Stellen außerhalb des Krankenhauses ist nur zulässig

1. zur Erfüllung einer gesetzlich vorgeschriebenen Behandlungs- oder Mitteilungspflicht,
2. zur Durchführung des Behandlungsvertrages einschließlich einer Nachbehandlung, soweit nicht der Patient etwas anderes bestimmt hat,
3. zur Abwehr von Gefahren für Leib, Leben, oder persönlicher Freiheit des Patienten oder eines Dritten,
4. zur Durchführung eines mit der Behandlung zusammenhängenden gerichtlichen Verfahrens.

Im übrigen ist eine Offenbarung nur mit Einwilligung des Patienten zulässig.

(4) Zum Zwecke der wissenschaftlichen Forschung dürfen Patientendaten nur offenbart werden, wenn der Patient ausdrücklich der personenbezogenen Offenbarung zugestimmt hat oder wenn die Anonymität des Patienten hinreichend gesichert ist.

(5) Durch Rechtsverordnung werden nähere Regelungen getroffen über die Art der Führung, den Inhalt, die Aufbewahrung und die Aufbewahrungszeit von Krankengeschichten."

Anlage 2

Berliner Grundsätze für den Datenschutz
bei den Neuen Medien
(insbesondere bei Bildschirmtext und Kabelkommunikation)
vom 1. Juli 1984 unter Berücksichtigung der
Beschlüsse der Konferenz der Datenschutzbeauftragten
des Bundes und der Länder

Die Grundsätze berücksichtigen folgende Beschlüsse:

1. Grundsätze für den Datenschutz bei den Neuen Medien (insbesondere bei Bildschirmtext und Kabelfernsehen)
   Beschluß der 7. Konferenz der Datenschutzbeauftragten des Bundes und der Länder in Berlin am 11. Dezember 1980 - in der Fassung vom 21. Januar 1981 -
2. Beschluß der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 27./28. März 1984: Erklärung zur Kabelkommunikation
3. Beschluß der Konferenz der Datenschutzbeauftragten vom 6./7. Juni 1984: Einführung des Telefon-Fernwirksystems „Temex"
4. Beschluß der Internationalen Konferenz der Datenschutzbeauftragten vom 18. Oktober 1983 in Stockholm

Übersicht

Vorbemerkung

1 Informationssammlung über Teilnehmer

2 Bedeutung des Versuchsstadiums (Pilotprojekte)

3 Die Bedeutung der „Einwilligung" bei der Speicherung von Teilnehmerdaten

4 Rückkanal und sonstige technische Vorkehrungen, über die Äußerungen der Teilnehmer dem System gegenüber kundgegeben werden können

5 Medienprivileg

6 Fernmeldegeheimnis und Neue Medien

7 Datenschutzkontrolle und Datensicherung

8 Organisation

9 Formelle Gestaltung

Vorbemerkung

Die Datenschutzbeauftragten des Bundes und der Länder haben die Pilotprojekte zum Bildschirmtext und deren gesetzliche Regelung sowie die Verhandlungen über den Bildschirmtext-Staatsvertrag und die Erörterungen zur gesetzlichen Regelung der geplanten Kabelkommunikationsprojekte kritisch begleitet und sich für eine sachgerechte Regelung des Datenschutzes eingesetzt. So hat die Konferenz der Datenschutzbeauftragten am 11. Dezember 1980 Grundsätze zum Datenschutz beschlossen und diese durch Beschlüsse vom 27./28. März 1984 und vom 6./7. Juni 1984 ergänzt.

Auf der Grundlage dieser Beschlüsse hat der Berliner Datenschutzbeauftragte eine Neuformulierung der Grundsätze erarbeitet. Sie soll dazu beitragen, daß bei Btx und der Kabelkommunikation, aber auch bei ähnlichen Diensten auf schmalbandigen Netzen, die folgenden Vorschriften über den Datenschutz berücksichtigt werden und dieser hinter der Entwicklung der neuen Technologien nicht zurückbleibt.

Die Grundsätze können dem Fortschreiten der technischen Entwicklung entsprechend nicht abschließend sein.

1 Informationssammlung über den Teilnehmer

1.1 Bei der Einführung und Entwicklung von EDV-gestützten öffentlichen Kommunikationssystemen (Neue Medien) ist der Datenschutz von Anfang an sicherzustellen. Dies gilt auch für die Versuchsphase. Gemäß den Grundsätzen aus dem Bundesverfassungsgerichtsurteil vom 15. Dezember 1983 zur Volkszählung sollte dies durch gesetzliche Regelungen geschehen. Die bei Btx bereits getroffenen Regelungen für einen bereichsspezifischen Datenschutz sind kritisch daraufhin zu beobachten, ob sie sich in der Praxis bewähren und ggf. weiterzuentwickeln.

1.2 Personenbezogene Benutzerdaten dürfen nur erhoben, gespeichert oder übermittelt werden, soweit ihre Verarbeitung für den Betrieb unumgänglich ist und ohne sie eine der gesetzlich zugelassenen Kommunikationsformen nicht durchgeführt werden könnte.

1.3 Der Schutz der in den Neuen Medien anfallenden personenbezogenen Teilnehmerdaten ist unabhängig vom Dateibegriff regelungsbedürftig.

1.4 Sofern bei bestimmten Diensten eine unmittelbare Teilnehmer-Anbieter-Kommunikation vorgesehen ist, dürfen Daten nur in dem Umfang festgehalten und übermittelt werden, wie dies zur Durchführung des jeweiligen Dienstes unumgänglich und aufgrund der einschlägigen gesetzlichen Regelungen zulässig ist.

1.5 Gebühren und Entgelte sind in anonymer Form zu berechnen und abzurechnen, soweit eine individualisierbare Registrierung von einzelnen Kommunikationsvorgängen zur Abwicklung von Vertragsverhältnissen nicht erforderlich ist. Sollte eine zusätzliche Kontrolle erforderlich werden, so könnte beim Benutzer eine Zähleinrichtung installiert werden.

2 Datenschutz in der Versuchsphase

2.1 Bereits in der Versuchsphase ist ein möglichst wirksamer Datenschutz sicherzustellen, da diese Phase die spätere Nutzung der Neuen Medien prägt.

2.2 In der Versuchsphase ist zu prüfen, ob weitere Datenschutzregelungen auf dem Gebiet der Neuen Medien nötig sind oder ob vorhandene Vorschriften modifiziert werden müssen.

2.3 Im Rahmen wissenschaftlicher Begleituntersuchungen ist dafür zu sorgen, daß auch die Datenschutzfragen besonders geprüft werden.

2.4 Im Rahmen einer wissenschaftlichen Begleituntersuchung ist der Zugriff auf gespeicherte Datenbestände nur gestattet, sofern diese Daten anonymisiert worden sind. Darüber hinausgehende Daten dürfen nur von den Teilnehmern direkt erfragt werden.

Die Verarbeitung personenbezogener Daten sollte in allen Phasen nur mit Einwilligung des Teilnehmers erfolgen (vgl. dazu Ziff. 3).

3 Die Bedeutung der „Einwilligung" bei der Speicherung von Teilnehmerdaten

3.1 Die Speicherung von Teilnehmerdaten in einer Form, die die Erstellung individueller Persönlichkeitsprofile gestattet, ist zu verbieten. Darüber hinaus kann in einzelnen Diensten die Speicherung besonders sensibler Daten aus dem „unantastbaren Bereich privater Lebensgestaltung" (vgl. BVerfGE 27, 1, 7; s. a. § 27 Abs. 3 Satz 3 BDSG) grundsätzlich verboten werden. Eine Einwilligung des Teilnehmers hebt das Verbot nicht auf.

3.2 Im übrigen ist eine Speicherung von Teilnehmerdaten nur erlaubt,

a) wenn eine gesetzliche Regelung dies zuläßt;

b) wenn der Teilnehmer seine Einwilligung gibt.

Diese Einwilligung ist nur wirksam, wenn der Teilnehmer zuvor sorgfältig über ihre Konsequenzen aufgeklärt worden ist (informed consent). Dies gilt auch für den Abschluß von Verträgen.

4 Rückkanal und sonstige technische Vorkehrungen, über die Äußerungen der Teilnehmer dem System gegenüber kundgegeben werden können:

4.1 Nutzungsmöglichkeiten des Rückkanals und aller sonstigen technischen Vorkehrungen, über die Äußerungen der Teilnehmer dem System gegenüber kundgetan werden können, sollten gesetzlich geregelt werden. Soweit Teilnehmerdaten gespeichert werden können, dürfen sie nur zu dem Zweck verwertet werden, zu dem sie offenbart wurden.

4.2 Persönlichkeitsprofile der Teilnehmer dürfen aus Kommunikationsdaten der Betriebszentralen nicht erstellt werden. Dies gilt für jede Betriebszentrale, unabhängig von der angewendeten Technologie.

4.3 Umfragen mit Angabe personenbezogener Daten sowie Abstimmungen und Wahlen über den Rückkanal dürfen nicht durchgeführt werden.

4.4 Soweit der Anschluß privater Endeinrichtungen bei der Telekommunikation über mikroprozessorgesteuerte Konverter erfolgt, ist das Leistungsprofil der Konverter wesentlicher Ansatzpunkt für Datenschutzüberlegungen. Daher muß eine öffentlich-rechtlich organisierte Kabelzentrale folgende Funktionen wahrnehmen:

- Bereitstellung der Konverter
- Steuerung und Programmierung der Konverter
- Sammlung der abrechnungsrelevanten Daten und Inkasso
- Abrechnung mit Anbietern.

4.5 In Zukunft können die Fernwirkdienste in die Wohnung des Betroffenen hineinreichen. Wegen der durch Art. 13 GG garantierten Unverletzlichkeit der Wohnung dürfen derartige Eingriffe nur unter ganz besonderen Voraussetzungen vorgenommen werden:

- Angebote, die ferngesteuert in der Wohnung von Teilnehmern Messungen vornehmen oder andere Wirkungen auslösen (Fernwirkdienste), dürfen nur mit schriftlicher Einwilligung des Betroffenen eingesetzt werden. Dieser ist zuvor über den Verwendungszweck sowie über Art, Umfang und den Zeitpunkt des Einsatzes der Dienste zu unterrichten. Verweigert ein Betroffener seine Einwilligung, dürfen ihm keine Nachteile entstehen, die über die unmittelbaren Kosten der Verweigerung hinausgehen.

  Der Betroffene kann seine Einwilligung jederzeit widerrufen.

- Soweit im Rahmen von Fernwirkdiensten personenbezogene Daten erhoben werden, dürfen diese nur zu den vereinbarten Zwecken verarbeitet werden. Sie sind zu löschen, wenn sie zur Erfüllung dieser Zwecke nicht mehr erforderlich sind.

- Die Einrichtung von Fernwirkdiensten ist nur zulässig, wenn
  - beim Betroffenen ein Anzeigegerät installiert ist, das jederzeit erkennen läßt, wann ein Dienst in Anspruch genommen wird und welcher Art der Dienst ist,
  - der Betroffene jederzeit den Dienst abstellen kann.

4.6 Zwischenspeicher- und Zwischensteuerungseinrichtungen sind so zu gestalten und zuzuordnen, daß personenbezogene Daten nicht einem erleichterten unberechtigten Zugriff Dritter ausgesetzt sind.

5 Medienprivileg

5.1 Das Verhältnis des Medienprivilegs zu den EDV-gestützten Kommunikationssystemen bedarf einer eingehenden Untersuchung:

- ob die einzelnen Neuen Medien als Presse bzw. Rundfunk anzusehen sind oder ob es sich um Medien sui generis handelt,
- in welchen Fällen nach geltendem Recht personenbezogene Daten ausschließlich zu publizistischen Zwecken verarbeitet werden,
- ob der Geltungsbereich des Medienprivilegs im Hinblick auf die für die Benutzer bestehenden Gefahren sachgerecht geregelt ist,
- falls dies bejaht wird:
  ob der Geltungsbereich zur Klarstellung gesetzlich geregelt werden soll,
- falls dies verneint wird:
  inwieweit der Geltungsbereich neu geregelt werden sollte.

In Medienarchiven gespeicherte, personenbezogene Daten dürfen nicht in die Speicherzentralen eingegeben werden und unter Berufung auf das Medienprivileg (§ 1 Abs. 3 BDSG und entsprechende Regelungen in den Ländergesetzen) frei zugänglich gemacht werden. Unter diesem Gesichtspunkt verdienen auch die im Urteil des Bundesverfassungsgerichts vom 5. Juni 1973 - 1 BvR 536/72 - (BVerfGE 35, S. 202 ff [219 ff] „Lebach") aufgestellten Grundsätze zum Schutze der

Persönlichkeit vor dem Zugriff der Öffentlichkeit besondere Berücksichtigung. Durch Art. 9 Abs. 5 Btx-Staatsvertrag ist bereits eine entsprechende Schutzwirkung erzielt.

6 Fernmeldegeheimnis und Neue Medien

6.1 Im gesamten Netzbereich werden die zentralen Einrichtungen der Neuen Medien ebenso wie die Übertragungswege vom Fernmeldegeheimnis im Sinne von Art. 10 GG umfaßt, sofern es sich dabei um juristische Personen des öffentlichen Rechts handelt.

6.2 Folgt man der Auffassung, daß die zentralen Einrichtungen der Neuen Medien keine Fernmeldeanlagen sind, ist ein dem Fernmeldegeheimnis vergleichbares Amtsgeheimnis für den Nutzungsbereich - unter Umständen in Verfassungsrang - zu schaffen.

6.3 Die Einblicknahme in und die Übermittlung von personenbezogenen Daten aus Speichereinrichtungen einer Bildschirmtext- bzw. Kabelfernsehzentrale ist nur aufgrund gesetzlicher Regelungen unter engen, genau bestimmten Voraussetzungen zulässig. Aus Datenschutzgesichtspunkten ist es bedenklich, die Regelungen des Gesetzes zu Art. 10 GG uneingeschränkt anzuwenden.

6.4 Für die in den zentralen Einrichtungen der Neuen Medien beschäftigten Bediensteten ist ein Zeugnisverweigerungsrecht und für alle dort gespeicherten Daten ein Beschlagnahmeverbot (vgl. § 97 StPO) zu verlangen.

7 Datenschutzkontrolle und Datensicherung

7.1 Die Kontrolle des Datenschutzes bei Neuen Medien sollte Aufgabe der Datenschutzbeauftragten sein.

7.2 Beim Anschluß von EDV-Einrichtungen durch Teilnehmer sind hinreichende technische und organisatorische Maßnahmen zu fordern, sowohl hardware- als auch softwaremäßig z. B. Schlüsselschalter, Paßwortroutinen.

8 Neue Kommunikationssysteme sollten nach Organisation, Trägerschaft und innerer Struktur so ausgelegt werden, daß eindeutige Verantwortlichkeiten ermittelt werden können.

9 Kommunikationsdienste und Kommunikationsstrukturen sollten gesetzlich definiert werden. In Verbindung mit der Gestaltung durchdachter Suchbaumstrukturen könnte sich eine positive datenschutzrechtliche Wirkung ergeben.

Anlage 3

Datenschutz bei der Mikroverfilmung von Schriftgut

Vom Bayerischen Landesbeauftragten für den Datenschutz entwickelte und vom Arbeitskreis „Technik" der Konferenz der Datenschutzbeauftragten beratene Orientierungshilfe (Stand: Januar 1984)

Arbeitsschritte bei der Mikroverfilmung	Risiken bei den einzelnen Arbeitsschritten	Maßnahmen zur Risikominderung
1	2	3
Aufgabe:		
Verfilmung von: - Altaktenbeständen (Passivverfilmung) - Aktuellen Vorgängen (Aktivverfilmung)		
Bildträger: - Rollfilm - Jackets		
Vorbereitung:		
Schriftgut zur Verfilmung aufbereiten: - Entfernung von Metallteilen (Heft-, Büroklammern u. ä.) - Glätten, chronologisches Einordnen, Sortieren, Reduzieren (z. B. Entfernen von Duplikaten), Durchnumerieren der Vorgänge - Abgabe zur Verfilmungsstelle	Unvollständigkeit des Schriftgutes Zusätzlich bei der Verfilmung außer Haus: - Unzulässige Offenbarung - Transportrisiken (Verlust, Diebstahl)	- Stichprobenhafte Prüfung - Zählung der aufbereiteten Vorgänge (Schriftstücke) - Aufbereitung durch eigenes Personal - Sorgfältige Auswahl der Firmen nach Sicherheitsstandard (evtl. Ortsferne) - Vertragsgestaltung (Verpflichtung zur Verschwiegenheit, Auflagen für Transport und Aufbewahrung) - Transportsicherungen - Transport durch eigenes Personal
Verfilmung:		
- Unter Beachtung der geltenden Normen (DIN 19053 und 19059) - Verwendung der Mikrofilm-Bildzeichen - Einzelblattverfilmung: Seitenweise Blattweise Vorder- und Rückseite zugleich Duplikatrollfilmerstellung in einem Arbeitsgang	- Unvollständige Schriftgutverfilmung - Unbefugte Offenbarung von Inhalten - Unberechtigte Nutzung des verfilmten Schriftgutes bis zur Vernichtung	- Vergleich der zur Verfilmung bereitgestellten und tatsächlich verfilmten Akten (durch Zählerstandsnummern) - Einblendung von Bildmarkennummern (Blips) - Verschluß des verfilmten Materials

Arbeitsschritte bei der Mikroverfilmung	Risiken bei den einzelnen Arbeitsschritten	Maßnahmen zur Risikominderung
1	2	3
– Anlage der Verfilmungskartei: Vermerk der Aktenplannummer Sachgebiet Filmrollen-, Zählerstandsnummer Fallidentifizierung		– Anmietung einer Verfilmungsanlage („mobile Kamera"), um Außerhausverfilmung zu vermeiden – Kontrolle der verbrauchten Rollfilme
	Zusätzlich bei Verfilmung außer Haus: – Transportrisiken – Unberechtigte Nutzung des verfilmten Schriftgutes beim Auftragnehmer	bei Außerhausverfilmung: – Unter Aufsicht eigenen Personals – Auswahl örtlich entfernter Auftragnehmer – Eigentransport – Vollzähligkeitskontrolle – Ergänzende Absicherungen durch vertragliche Maßnahmen
– Speicherkontrolle		– z. B. A.B.Dick-Verfahren
Entwickeln des Films und Filmkontrolle:		
Entwickeln der belichteten Rollfilme	– Transportrisiken – Unberechtigte Anfertigung von Filmkopien	Eigenentwicklung
		Beim Entwickeln außer Haus: – Kurierdienst – Höherwertige Versandart auf dem Postweg – Begleitpapiere (z. B. Anzahl der Filme; Längenangaben 35/65 m) – Sorgfältige Auswahl des Auftragnehmers – Ergänzende, vertragliche Absicherungen
Prüfung des Verfilmungsergebnisses: – Lesbarkeit – Wiedergabefähigkeit (Rückvergrößerung) – Verwendung der Bildzeichen – Vollständigkeit der Blattnummern innerhalb eines Falles – Anlegen der Verfilmungskartei: Eintragung der Blip-Nummer Hinweis auf Verbleib von Originalunterlagen Prüfvermerk	Verlust der Verfilmungskartei	– Zugangssicherung – Zugriffssicherung – Verfilmung der Verfilmungskartei in gewissen Zeitabständen
Vernichtung des verfilmten Schriftgutes	Unvollständige und schlechte Entsorgung	– Eigener Reißwolf – Verschließbares Zwischenlager – Transport und Vernichtung unter Aufsicht, auch bei Auftragsvergabe
Verwaltung des Filmgutes: – Rollfilmverwaltung – Jacketverwaltung – Erzeugung von Sicherungsbeständen – Aufbewahrung der Sicherungsbestände – Löschen und Sperren von verfilmten Einzelfällen	– Bestandsverlust – Unberechtigte Vervielfältigung von Rollfilmen und Filmjackets – Unberechtigte Rückvergrößerung – Unberechtigter Zugriff auf Sicherungsbestände	– Kontrolle des Dupliziervorgangs (Zählwerk am Gerät) – Protokoll über Dupliziervorgang (evtl. 4-Augen-Prinzip) – Arbeitsexemplar nicht duplizierbar durch Verwendung entsprechenden Filmmaterials – Trennung von Sicherungskopien und Duplikaten des Filmgutes – Vorgabe des Filmaterials (Schacht mit abgezählten Filmen) – Rückgabe von Fehlverfilmungen – Vernichtung der entsprechenden Verfilmungskarteikarte beim Löschen eines Falles – Hinweis auf Verwendungssperre auf Verfilmungskarteikarte anbringen – Zählen der Rückvergrößerungskopien durch Abgleich mit Aufträgen – Sicherungskopien räumlich oder örtlich getrennt zugriffssicher lagern

Anlage 4

Vorschläge zur Verbesserung des Datenschutzes
im Bereich der Familienfürsorge

- Arbeitsergebnisse einer weiterführenden Fortbildung
zu Problemen des Sozialgeheimnisses
in der behördlichen Jugendhilfe -

Vorbemerkung

Der Gedanke des Datenschutzes im Sinne eines Informationsschutzes ist im Bereich der Sozialverwaltung und insbesondere im Bereich der Familienfürsorge älter als die Gesetze zum Datenschutz. Durch § 35 SGB I i.V.m. § 67 ff SGB X sind jedoch die Wirkungen des Informationsschutzes spezifiziert und auf eine solide Rechtsgrundlage gestellt worden. Die Wirkungen dieser Normen dürfen nicht daran scheitern, daß Verwaltungsstrukturen und Verfahrensweisen gegenläufig ausgestaltet sind.

Die Achtung des Sozialgeheimnisses mit allen damit verbundenen Rechten und Pflichten der Beteiligten ist als integraler Bestandteil der Sozialarbeit zu verstehen. Die Beteiligung und Mitwirkung der Betroffenen ist ein zentrales Erfordernis bei der sozialen personenbezogenen Dienstleistung. Sie soll letztlich die Verantwortungsbereitschaft und Verantwortungsfähigkeit der Leistungsempfänger fördern und entwickeln. Dafür ist das Vertrauen in die Arbeit der Institutionen, die diese Dienstleistungen anbieten, unerläßlich.

Für eine datenschutzgerechte Informationsübermittlung und Akteneinsicht ist die Datenerhebung und die Form der Dokumentation von zentraler Bedeutung. Hier sind Verfahrensweisen zu entwickeln, die sowohl den Erfordernissen der Verwaltungspraxis wie auch den gesetzlich garantierten Rechten der Betroffenen gerecht werden.

Die bisherige Dokumentationsform im Bereich der Bezirksfürsorge mit sozialpädagogischer Zielvorstellung führte oft zu einer über Generationen sich erstreckenden familienbezogenen Bündelung von Einzelvorgängen. Daraus folgte die „Nichtablage" von abgeschlossenen Leistungen oder Vorgängen anderer Art. Hier müssen Verbesserungsmaßnahmen ansetzen.

1. Datenerhebung

1.1 Entsprechend dem in den Sozialgesetzen konkretisierten Verfassungsgrundsatz der Verhältnismäßigkeit dürfen personenbezogene Informationen zur Durchführung von Leistungsverhältnissen im Sinne des Sozialrechts nur insoweit erhoben werden, als dies für eine konkrete Aufgabenerfüllung erforderlich ist. An das Kriterium der Erforderlichkeit sind strenge Maßstäbe anzulegen, d. h. es muß ein direkter Bezug zur jeweiligen konkreten Hilfeleistung gegeben sein.

1.2 Die Datenerhebung sollte im Interesse einer nachvollziehbaren und übersichtlichen Arbeitsweise begrenzt und auf die unterschiedlichen Leistungsformen bezogen werden.

2. Dokumentation

2.1 Eine „Akte" ist eine Sammlung von Geschäftsvorfällen und Schriftverkehr. Jedoch muß nicht alles, was bisher dokumentiert wurde, notwendigerweise Bestandteil einer nach dem „Familienprinzip" geführten Akte sein.

2.2 Tätigkeitsnachweise von Behördenmitarbeitern, die nicht in direktem Zusammenhang mit der Durchführung eines konkreten Leistungsverhältnisses stehen, lassen im Nebeneffekt eine über das Erforderliche hinausgehende Informationssammlung über die beratenen Personen entstehen. Die Dienstaufsicht muß daher andere Wege suchen, um die Effektivität der Tätigkeit von Sozialarbeitern in der Behörde zu überprüfen. Der Nachweis fachlicher Fähigkeiten, der Nachweis des Arbeitsaufwandes sowie die Supervision sollten sich anonymisierter Methoden bedienen.

2.3 Informationen und Meldungen von Dritten (Nachbarn, Schulen, Polizei) sind nicht nach dem Betroffenenprinzip, sondern nach anderen Kategorien wie z.B. nach Meldeeinrichtungen oder nach Arbeitsgruppen abzulegen. Hat sich der gemeldete Tatbestand bei den Betroffenen bestätigt und sind Aktivitäten durch das Jugendamt erfolgt oder in der Zukunft notwendig, kann dies in der pädagogisch erforderlichen Form als Arbeitsergebnis des zuständigen Sozialarbeiters vermerkt werden. Eine Beratungs- oder Leistungsakte für die Person sollte nur angelegt werden, wenn ein konkretes Leistungsverhältnis für die Zukunft entstehen soll oder entstehen wird.

2.4 Bei der Durchführung eines Leistungsverhältnisses sollen nur Informationen mit unmittelbarem Bezug zu einer Leistung dokumentiert werden (Leistungserheblichkeit). Ein enger Begriff der Leistungserheblichkeit soll bei der Dokumentation den subjektiven Aspekt des Sozialarbeiters bezüglich der persönlichen Verhältnisse des Betroffenen zu Gunsten einer Handlungs- und Tatbestandsdokumentation reduzieren. Persönliche Wertungen sollen soweit als möglich zurückgestellt werden. Besteht die Leistung in einer einmaligen in sich abgeschlossenen Beratungstätigkeit, ist die Aufzeichnung von Einzelheiten des Beratungsgesprächs nicht mehr erforderlich.

2.5 Bei freiwilligen Leistungsverhältnissen, die aufgrund eines Antrags entstehen, ist die Dokumentation der gesetzlichen Leistungsvoraussetzungen zulässig, soweit diese vom Antragsteller vorgetragen wurden.

2.6 Bei Leistungsverhältnissen, die mit einem Eingriff in Rechtspositionen (z.B. das Erziehungsrecht der Eltern) verbunden sind, sind die hierfür erheblichen Tatbestandsvoraussetzungen zu dokumentieren. Die Dokumentation kann auch in einer früheren Phase beginnen, wenn sich dafür ausreichende Anhaltspunkte bieten.

2.7 Bei allgemeinen Beratungs- und Betreuungsfunktionen darf eine Datendokumentation nur unter strenger Berücksichtigung des Verhältnismäßigkeitsgrundsatzes erfolgen. Es soll nicht dokumentiert werden, wenn nicht besondere Umstände dies erforderlich erscheinen lassen (z. B. um dem Vorwurf der Dienstpflichtverletzung vorzubeugen).

3. Aktenführung

3.1 Soweit Verwaltungsvorgänge über einzelne Personen angelegt werden müssen, ist innerhalb der Akte nach Leistungsansprüchen, Leistungskategorien und Leistungszeiträumen zu unterscheiden, so daß der Zugriff auf den einzelnen abgrenzbaren Leistungsbereich zum Zwecke der Einsichtnahme oder zu Zwecken der rechtmäßigen Übermittlung möglich ist. Die Bündelung und Vermengung unterschiedlicher Leistungskategorien in einem Aktenvorgang sollte soweit als möglich für die Zukunft vermieden werden. Soweit eine Bündelung nach Personen unvermeidlich ist (Familienakte), sollte die Akte nach Betroffenen und nach Leistungsformen gegliedert aufgeführt werden.

3.2 Sind Vorgänge zu einzelnen Leistungsformen abgeschlossen, sollten sie aus der Akte ausgegliedert und abgelegt werden. Sie sollten unter Beachtung der im übrigen geltenden Verwaltungsvorschriften vernichtet werden, sofern nicht gesetzliche Aufbewahrungsvorschriften dem entgegenstehen.

Anlage 5

Die Senatoren für
Gesundheit, Soziales und Familie
sowie für
Schulwesen, Jugend und Sport

Gemeinsames Rundschreiben

über das Verfahren bei Anträgen auf Gewährung von Verhaltenstherapie/Gesprächstherapie/Spieltherapie als Leistung der Eingliederungshilfe für Behinderte nach dem Bundessozialhilfegesetz durch das Jugendamt (Gem. Rdschr. VV)

vom 24. Mai 1984

Für die Kostenübernahme bei psychologischen Therapien (Verhaltenstherapie/Gesprächstherapie) als Eingliederungshilfe für Behinderte nach dem Bundessozialhilfegesetz (BSHG) wird

- im Verhältnis zu den Leistungen der gesetzlichen Krankenversicherung klargestellt und
- aus Gründen des Schutzes der Sozialdaten (Sozialgeheimnis, § 35 SGB I)

das folgende Verfahren empfohlen:

Abschnitt I: Abgrenzungen

1 - Kassenleistungen

(1) Verhaltens- und zum Teil auch gesprächstherapeutische Behandlungen sind dann Leistungen der gesetzlichen Krankenversicherung, wenn sie der Beseitigung oder Linderung einer Krankheit dienen. Unter Hinweis auf das Urteil des Bundessozialgerichts - 3 RK 43/80 - kommt in derartigen Fällen der Aufklärungspflicht der Krankenkassen und der Pflicht zur Sicherstellung der Versorgung durch die Kassenärztliche Vereinigung eine besondere Bedeutung zu.

(2) Ist nach ärztlicher Diagnose die Verhaltenstherapie/Gesprächstherapie zur Beseitigung oder Linderung einer Krankheit im Sinne der RVO die geeignete Therapieform, weil eine analytisch orientierte oder tiefenpsychologisch fundierte Psychotherapie nicht indiziert ist, dann ist im Falle eines bestehenden Versicherungsverhältnisses die Krankenkasse leistungsverpflichtet.

(3) Verweigert die Krankenkasse trotz Vorliegens der individuellen Voraussetzungen für die Verhaltenstherapie/Gesprächstherapie eines Versicherten die Leistung oder kommt diese nicht in zumutbarer Zeit zustande oder verletzt die Kasse ihre Aufklärungspflicht gegenüber ihrem Versicherten, so besteht nach dem Urteil des BSG ein Anspruch auf Erstattung der Kosten, die für die Behandlung außerhalb des kassenärztlichen Versorgungssystems aufzuwenden waren. In solchen Fällen besteht auch die Möglichkeit des Trägers der Sozialhilfe zur Vorleistung, wobei er in diesen Fällen seinen Ersatzanspruch nach § 102 SGB X geltend machen muß.

2 - Sozialhilfeleistung

Verhaltenstherapie, auch Gesprächstherapie oder Spieltherapie sind aber dann keine Leistung der gesetzlichen Krankenversicherung und gehören nicht zur vertragsärztlichen Versorgung, wenn sie nicht der Heilung oder Besserung einer Krankheit im Sinne der RVO oder der medizinischen Rehabilitation dienen, sondern als präventive Maßnahmen anzusehen sind. Eine Krankheit im Sinne der RVO liegt auch dann nicht vor, wenn es sich ausschließlich um Maßnahmen zur beruflichen oder sozialen Anpassung, zur Berufsförderung sowie für Erziehungsberatung und ähnliche Maßnahmen handelt. Insbesondere Verhaltenstherapien werden auch dann nicht als Leistung der gesetzlichen Krankenkassen gewährt, wenn sie ausschließlich der Behebung z. B. von Erziehungs-, Ehe-, Lebens- oder Sexualproblemen dienen. Gerade aber in diesen Bereichen können Störungen, die im Vorfeld von Krankheit oder Behinderung liegen, aufgefangen werden; in diesen Fällen kann die Therapie das Auftreten von Krankheiten oder Behinderungen vermeiden helfen.

Abschnitt II: Verfahren

3 - Antragstellung

(1) Die Eingliederungshilfe nach §§ 39, 40 BSHG wird vom Jugendamt im Rahmen seiner allgemeinen Beratungs- und Betreuungsaufgaben gegenüber Kindern und Jugendlichen und ihren Erziehungsberechtigten gewährt. Sie wird gewährt, soweit sie über die allgemeine Beratung und Betreuung hinaus das geeignete Mittel zur Erfüllung der Aufgaben nach § 39 Abs. 3 BSHG ist und keine vorrangige Verpflichtung durch einen anderen Leistungsträger besteht. Das Gleiche gilt für volljährige Behinderte bis zum vollendeten 25. Lebensjahr entsprechend der Regelung in Nr. 14 der Gemeinsamen Ausführungsvorschriften zu §§ 30 und 31 AGJWG über die sachliche Zuständigkeit auf dem Gebiet der Sozialhilfe vom 24. Januar 1978 (ABl. S. 402 / DBl. IV S. 2).

(2) Hilfesuchende dieser Personengruppe sind daher an das Jugendamt zur Beratung über die Erfordernisse des Antragsverfahrens und zur Prüfung der Notwendigkeit einer Beteiligung anderer Fachstellen zu verweisen. Das Jugendamt nimmt den Antrag entgegen und veranlaßt die Erstellung eines Kosten- und Behandlungsplanes für das Gesundheitsamt durch den Therapeuten, der die Behandlung des Behinderten übernimmt. Der Hilfesuchende oder sein gesetzlicher Vertreter entbindet den Therapeuten gegenüber dem Gesundheitsamt von der gesetzlichen Schweigepflicht.

(3) Zur Feststellung einer Behinderung ist dem Hilfesuchenden aufzugeben, sich durch den Kinder-, Jugendpsychiatrischen Dienst des Gesundheitsamtes untersuchen zu lassen, soweit dies zur Entscheidung über die vom Träger der Sozialhilfe geforderte Leistung erforderlich ist.

(4) Für die beabsichtigte Untersuchung sind die festzustellenden Tatsachen im Gespräch mit dem Hilfesuchenden hinreichend durch das Jugendamt zu spezifizieren. Der Hilfesuchende oder sein gesetzlicher Vertreter entscheidet, ob er sich einer ärztlichen Untersuchung durch den Kinder-, Jugendpsychiatrischen Dienst unterziehen will. Er ist darauf hinzuweisen, daß in aller Regel die Verweigerung dieser ärztlichen Untersuchung zu einer Ablehnung der beantragten Eingliederungshilfemaßnahme führen muß, da dann die Voraussetzungen für die Hilfegewährung nicht ausreichend nachgewiesen sind. Das Jugendamt meldet den Hilfesuchenden beim Gesundheitsamt schriftlich mit der kurzgefaßten Angabe des Grundes an.

4 - Aufgaben des Gesundheitsamtes

(1) Ein Arzt des Gesundheitsamtes stellt fest, ob eine Krankheit im Sinne der RVO vorliegt. Dazu gehören auch körperliche, geistige oder seelische Behinderungen, die medizinische Rehabilitationsmaßnahmen in Form einer psychologischen Therapie notwendig machen. Bei festgestelltem Krankheitswert ist dem Hilfesuchenden eine ärztliche Mitteilung auszuhändigen, die sowohl die angemessene Therapieart als auch die Notwendigkeit des unverzüglichen Einsetzens der Therapie begründet. Der Hilfesuchende ist mit dieser ärztlichen Mitteilung an seine Krankenkasse wegen der Übernahme der Kosten zu verweisen.

(2) In den Fällen nach Abschnitt I Nr. 2 stellt der Arzt des Kinder-, Jugendpsychiatrischen Dienstes die Diagnose und empfiehlt die erforderliche Art der Behandlungsmaßnahme (Therapie und Umfang). Gleichzeitig stellt er fest, daß es sich nicht um eine Krankheit im Sinne der RVO und eine daraus abzuleitende Therapie handelt. Die ärztliche Stellungnahme muß ferner die Aussage treffen, ob der Hilfesuchende zum Personenkreis nach § 39 Abs. 1 oder Abs. 2 BSHG zählt und

a) nicht nur vorübergehend (länger als sechs Monate) wesentlich behindert und infolgedessen seine Fähigkeit zur Eingliederung in die Gesellschaft in erheblichem Umfang beeinträchtigt ist (§ 39 Abs. 1 Satz 1 BSHG) oder

   von einer solchen Behinderung bedroht ist und der Eintritt der nicht nur vorübergehend wesentlichen Behinderung nach fachlichen Erkenntnissen mit hoher Wahrscheinlichkeit zu erwarten ist (§ 39 Abs. 2 BSHG);

b) eine andere - also eine vorübergehende oder eine nicht wesentliche - Behinderung (§ 39 Abs. 1 Satz 2 BSHG) hat oder

   von einer solchen Behinderung bedroht ist.

Im übrigen nimmt der Arzt zu den Hilfemöglichkeiten nach § 40 BSHG Stellung.

(3) Über die nach Nr. 4 Abs. 2 festgestellten Tatsachen und Empfehlungen händigt er dem Hilfesuchenden oder seinem gesetzlichen Vertreter eine schriftliche Mitteilung als Unterlage für die weitere Antragsbearbeitung beim Träger der Sozialhilfe aus. Die Mitteilung enthält lediglich die für die Entscheidung erforderlichen Angaben.

(4) Diese ärztliche Mitteilung dient dem Träger der Sozialhilfe als Grundlage für seine Entscheidung, wobei er in diesen Fällen

ein Verweisung an die Krankenkassen nicht vorzunehmen braucht.

5 - Bewilligung der Eingliederungshilfe

(1) Ergibt sich aus dem Befund, daß keine Krankheit im Sinne der RVO vorliegt, entscheidet das Jugendamt über die Gewährung der Hilfe, wenn vom Gesundheitsamt die Zugehörigkeit zum Personenkreis des § 39 Abs. 1 oder 2 BSHG festgestellt worden ist und die übrigen sozialhilferechtlichen Voraussetzungen vorliegen.

(2) Der Bewilligungsbescheid (Kostenübernahmeerklärung) wird unter der Auflage erteilt, daß der Hilfesuchende oder sein gesetzlicher Vertreter den für die Behandlung vorgesehenen Therapeuten von der Schweigepflicht entbindet, soweit es zur Gewährleistung des Therapieerfolges und der damit zusammenhängenden Maßnahmen des Jugendamtes bei der Familienbetreuung unbedingt erforderlich ist. Der Erforderlichkeit sind im Zweifel enge Grenzen zu ziehen.

(3) Im Interesse eines schnellen Therapiebeginns wird dem Jugendamt empfohlen, zunächst einen Teilbescheid für den ersten Bewilligungszeitraum mit dem vom Gesundheitsamt vorgeschlagenen wöchentlichen Therapieumfang zu erteilen. Unterschiedliche Beurteilungen der zu gewährenden Maßnahme (z. B. Dauer oder Häufigkeit der Therapie) können von den Beteiligten (Jugendamt und/oder Hilfesuchender oder Therapeut) während des ersten Bewilligungszeitraumes mit dem Gesundheitsamt geklärt werden. Hierbei kann dem Hilfesuchenden aufgegeben werden, sich einer zusätzlichen Untersuchung (z. B. beim Landesarzt) zur Feststellung weiterer entscheidungserheblicher Tatsachen zu unterziehen. Nr. 4 Abs. 3 gilt insoweit entsprechend. Spätestens nach Ablauf des ersten Bewilligungszeitraumes ist ein rechtsmittelfähiger Bescheid zu erteilen.

Stichwortverzeichnis

Angegeben sind die Fundstellen aller Jahresberichte seit 1979. Die Ziffern ohne Jahreszahl beziehen sich auf den Zusammendruck der Jahresberichte in den von mir herausgegebenen Materialien zum Datenschutz, Band 2, Datenschutz in Berlin 1979 bis 1983

Abgangskontrolle 104
Abgeordnetenhaus 14, 121; 1984/28
Abiturienten 118
Ablichtung 42, 55, 87, 113
Abonnentenverwaltung 106
Abruf, unbefugter 76, 107
Adoption 108, 109
Adrema-Platten 115
Adressenmittlung 26
Adreßlisten 58, 115
ADV-Grundsätze 1984/18
Akten 25, 49, 58
Akten, Vollständigkeitsprinzip 56
Akteneinsicht 25, 28, 50, 59
Akteneinsicht, medizinische Daten 100
Akteneinsicht, Sozialgesetzbuch 59
Aktenführung 110; 1984/34
Aktenvernichtung 63
Allgemeine Geschäftsbedingungen 1984/6
Allgemeine Ortskrankenkasse 1984/16
Allgemeines Sicherheits- und Ordnungsgesetz 107; 1984/3, 10
Amerika-Gedenkbibliothek 85; 1984/28
Amtsanwaltschaft, s. Staatsanwaltschaft
Amtsarzt 1984/9
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
Anordnung über Mitteilungen in Zivilsachen 54; 1984/25
Anrufungen 9, 25, 32, 50, 89, 121; 1984/29
Anschriften 115
Anzapfen 77
Archive 46, 88, 106; 1984/3
ASOG, s. Allgemeines Sicherheits- und Ordnungsgesetz
ASTA, s. Staatsanwaltschaft
Aufklärung bei der Erhebung 42
Aufsichtsbehörde für den Datenschutz 27, 45, 61, 64, 88, 120; 1984/29
Auftragsdatenverarbeitung 112; 1984/17
Ausbildungsförderung, s. Bundesausbildungsförderungsgesetz
Auskunft 25, 35, 52, 116
Auskunft, Gebührenpflicht 28
Auskunft, Sicherheitsbehörden 35
Auskunftssperre 108, 109
Auskunftsverweigerung 35
Ausländer 33, 53, 82, 117
Ausländerbehörde 58, 111, 119
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
Beamtenversorgungsgesetz 72
Bebauungsplan 74
BEHALA 105
Beihilfe 1984/20
Belegfluß 54
Benutzerkontrolle 86
Beratung 13, 26, 32, 43, 50, 64, 89, 121; 1984/29
bereichsspezifischer Datenschutz 28, 31, 45; 1984/3, 12
Berichtigungsanspruch 35
Berliner Datenschutzgesetz 24, 121
Berliner Entwässerungswerke 105
Berliner Philharmonisches Orchester 106
Berliner Stadtreinigungsbetriebe 57; 1984/18
Berliner Wasserwerke 105
Beschwerden s. Anrufung
Betriebsdatenbank 85
Betriebskrankenkasse des Landes und der Stadt Berlin 1984/17
BEWAG 36
Bezirksämter 109, 116; 1984/16
Bezirkseinwohneramt 54
Bezirksverordnetenversammlungen 15, 73
Bibliotheken 85, 105
Bildschirmtext 33, 37, 45, 59, 67, 75, 87, 101; 1984/12, 28
Bildschirmtext, Anbieter 1984/14
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
Bundeskindergeldgesetz s. Kindergeld
Bundeskriminalamt 44
Bundessozialhilfegesetz 72
Bundesstatistikgesetz 31
Bundeszentralregister, unbeschränkte Auskunft 40, 56, 88, 120; 1984/28
Bußgeldverfahren 1984/22
BVG 104
Codes 34, 60, 77, 101; 1984/6
Computerkriminalität 1984/5
Computermißbrauch 1984/4
Datei 25, 31, 49, 55, 58
Dateienregister 12, 24, 26, 27, 30, 43, 57, 64, 86, 88, 105, 120, 121
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
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
Einsichtsrecht, Schülerbogen 41
Einwilligung 24, 26, 31, 34, 51, 57, 59, 67
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
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
Fernwirkdienste 101, 102; 1984/16
Feuersozietät 1984/16
Feuerwehr 79
Finanzverwaltung 88
Formulare 26
Forschung 33, 51, 59, 61, 82, 112, 117
Forschung, Sozialgesetzbuch X 82
Forschungsprojekte 50, 61, 87, 118
Fremdfirmen 63, 84, 86
Funk 42
Führungszeugnis 57
Funktionentrennung 86, 101, 114; 1984/6
GASAG 36, 104
Geburtsdaten 41
Gebührenpflicht bei Auskünften 28
Gemeinsame Geschäftsordnung für die Berliner Verwaltung 89, 106
Geschäftsverteilungsplan 115
Gesetz über Abbau der Fehlsubventionierung s. Fehlbelegungsabgabe
Gesetz über psychisch Kranke 121
Gesundheitsdaten, s. medizinische Daten
Gewerbeordnung 62, 87
Gewerberegister 31, 62, 87, 88
GGO, s. Gemeinsame Geschäftsordnung
Glaubwürdigkeit kindlicher Zeugen 36
Grundrecht auf Datenschutz 28
Grundrechte 30
Hacking 1984/4
Hausbesetzungen 80, 120
Haushaltbegleitgesetz 100
Haushaltsstrukturgesetze 72
Herstellerfirmen 63
Hochschulen 25, 32, 50, 57, 63
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
Informationsverarbeitung, Entwicklung 49
INPOL-System 44
Institutionsleihe 44
interner Datenschutzbeauftragter 105, 112, 116
internes Dateienregister 105
Intimbereich 39
isolierte Rechner 63, 114
ISVB, s. Informationssystem Verbrechensbekämpfung
Jugendgerichtshilfe 58, 110
Justizverwaltung 50, 60
Justizvollzugsanstalten 55, 81, 87
Kabelkommunikation 33, 37, 39, 46, 67, 102
Kabelpilotprojekt 101; 1984/15
KAN, s. Kriminalaktennachweis
Kaufpreissammlung 119; 1984/27
Kindergeld 72, 100; 1984/19
Kirchen 24, 27, 32
Kirchensteuerstelle 1984/17
Klassenliste 118
Kleinrechner 84, 114
Klinische Nachsorgeregister 50
Konferenz der Datenschutzbeauftragten 18, 43, 64, 88, 120; 1984/28
Konsolprotokolle 63
Kontrollen von Amts wegen 11, 24, 25, 26, 32, 50, 68
Konverter 102
Kosten- und Behandlungsplan 110; 1984/9, 34
Kostenübernahmescheine 81
KPM 105
KpS-Richtlinien 27, 43, 56, 79, 119; 1984/12, 27
Kraftfahrzeuge 25, 79
Krankenakten, s. medizinische Daten
Krankengeschichtenverordnung 120; 1984/8
Krankenhäuser, s. medizinische Daten
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
Landeskrankenhausgesetz 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
Lastschrifteinzug 1984/17
LED, s. Landesamt für Elektronische Datenverarbeitung
Lehrerindividualdatei 118
Liegenschaftskataster 75; 1984/17
Lohnsteuerkarte 43, 54, 57
Lohnsteuerstellen 119
Löschungsanspruch 35
manuelle Datensammlungen 89, 91, 93, 112, 114, 117
Max-Planck-Gesellschaft 61, 87
Medienprivileg 8, 38, 65, 68
medizinische Daten 25, 27, 31, 40, 49, 63, 100, 112, 120; 1984/3, 7
Meldepflicht, s. Landesmeldegesetz, Melderechtsrahmengesetz
Melderechtsrahmengesetz 27, 31, 44, 55, 100
Melderegister 54, 63, 64, 78, 87, 107; 1984/21
Menschenrechtskonvention 28
Mieterlisten 73
Mietobergrenzen 1984/27
Mietpreisstellen 73
Mikrocomputer 1984/18
Mikroverfilmung 1984/32
Mikrozensus 1984/23
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
Neue Medien 32, 37, 45, 49, 59, 67, 75, 91, 100; 1984/12, 28, 30
Neue Medien, Grundsätze 64, 67; 1984/30
Notare 87
Novellierung des Bundesdatenschutzgesetzes, s. Bundesdatenschutzgesetz
OECD 28, 46
on-line-Anschlüsse 39, 49, 78, 84, 115
Ordnungsmäßigkeit der Datenverarbeitung 114
Ordnungsmerkmal 53, 77
Organleihe 44
Orwell 99
Öffentliche Lebensversicherung 1984/16
öffentliche Wirtschaftsunternehmen 1984/16
Öffentlichkeitsarbeit 33, 50, 89, 121; 1984/29
Paß 126
Pay - TV 102
Personalakten 26, 40, 67; 1984/18
Personalausweis 26, 31, 42, 55, 87, 106, 120, 126
Personalausweisgesetz 44, 100, 106; 1984/4
Personalbezügedatei 1984/24
Personaldaten 25, 32, 40, 45, 49, 56, 66, 67; 1984/9, 18
Personalfragebogen 1984/19
Personalverzeichnis 41
Personenbeförderungsgesetz 62
Personenkennzeichen 53; 1984/4

Persönlichkeitsprofil 39, 67, 68
Persönlichkeitsrecht 59, 73
Petitionsausschuß 1984/26
Pflegschaft 54
Planung 51, 52, 59, 73
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
Postkarte 43
Postzustellungsurkunde 43
private Computernutzung 1984/18
private EDV-Unternehmen 84
Programmdokumentation 106, 114
Programmtests 86, 113
Protokollisten 116
Prozeßordnungen 1984/25
psychiatrische Daten 53, 66; 1984/8
psychiatrische Gutachten 41
Quellabzugsverfahren 57
Rasterfahndung 33, 35, 43; 1984/11
Rechenzentren, Funktionentrennung 114
Rechenzentrum 62, 114
Rechenzentrum, Datenträgerarchiv 86
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 1984/7
Schuldnerverzeichnis 61; 1984/28
Schule 25, 32, 36, 41, 50, 57, 87, 118, 120; 1984/28
Schulfragebogen 36
Schulpsychologischer Dienst 118
Schutzgemeinschaft für allgemeine Kreditsicherung (Schufa) 61
Schweiz 65
Schwerbehinderte 1984/26
Selbsthilfeeinrichtungen 57
Sender Freies Berlin 24, 45
Seriennummer, s. Personalausweis
Sozialbericht 64
Sozialdaten, s. Sozialgesetzbuch X
Sozialgeheimnis, s. Sozialgesetzbuch X
Sozialgesetzbuch I, Mitwirkung (§ 60) 26
Sozialgesetzbuch X 25, 26, 27, 31, 44, 50, 58, 64, 72, 81, 109; 1984/25
Sozialgesetzbuch X, Aktenführung 1984/25, 34
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; 1984/26
Sozialgesetzbuch X, Zweckbindung 83
Sozialgesetzbuch X, 3. Kapitel 83, 100
Sozialhilfe 58, 87
Sozialhilfe, Ausländer 58, 82
Sozialhilfestatistik 64
Sozialleistungsträger 1984/16
Sozialwissenschaftliche Untersuchungen 33
Sparkasse der Stadt Berlin West 1984/16
speichernde Stelle 62, 109
Sperrung 1984/22
Spezialgesetze s. bereichsspezifische Regelungen
Spurendokumentationssysteme 1984/12
Staatsanwaltschaft 60, 64, 115; 1984/28
stand-alone-Rechner 63
Statistik 31, 59, 64, 102, 104; 1984/23
Städtebauförderungsgesetz 74
Steuerfahndung 88
Steuerverwaltung 88
Strafgesetzbuch, § 200 81
Strafprozeßordnung 1984/10
Strafverfolgung 37, 79; 1984/10
Strafvollzug, s. Justizvollzugsanstalten
Studentendaten s.Hochschulen
Taxifahrer 62; 1984/28
Technische Prüfstellen für den Kraftfahrzeugverkehr 64
Telebus 1984/26
Telefon, Benutzung 42
Telefondatenerfassung 63, 87, 120
Teletex 37, 38
Testdaten 86, 113; 1984/18
Textverarbeitung 84, 85
Todesursachenstatistik 104
Transparenz der Datenverarbeitung 30, 86, 104, 114
Transportkontrolle 86
Umwandlung von Mietwohnungen 73
unbeschränkte Auskunft, s. Bundeszentralregister
UNESCO 46
Universitätsklinikum Steglitz 112
Unterhaltsansprüche 58; 1984/26
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
Vernichtung von Datenträgern 63, 115
Veröffentlichung von Verurteilungen 81
Versand von Schriftstücken 54
Vertraulichkeit 111; 1984/9
Verurteilungen, Veröffentlichung 81
Verwaltungsprozeßordnung 90
Verwechslungen 61
Verwertungsverbot 66
Videotext 37
Vieh- und Schlachthof Spandau 105
Volksbegehren 55
Volkszählung 1983 99, 100, 103, 120; 1984/3, 23
Vordrucke 53, 87
Wahlen 54, 55, 59, 68
Warnkartei 40
Wählerliste, s. Wahlen
Werbung 28
Wettbewerbsunternehmen, Krankenhäuser 112
Wirtschaftskriminalität 77; 1984/6
Wohnung 100
Wohnungsbau-Rechenzentrum 85, 120; 1984/17
Zentrale Vormundschaftskasse / Unterhaltsvorschußkasse 85
Zugriffsberechtigung 55
Zugriffskontrolle 86
Zustimmung, s. Einwilligung
Zweckbindung 66

Zusammenstellung der Originalseitenzahlen
in den Mitteilungen des Präsidenten des Abgeordnetenhauses
und den im obigen Stichwortverzeichnis angegebenen
Seitenzahlen

1979		1981		1982		1983	
1	23	1	47	1	69	1	97
2	24	2	48	2	70	2	98
3	25	3	49	3	71	3	99
4	26	4	50	4	72	4	100
5	27	5	51	5	73	5	101
6	28	6	52	6	74	6	102
		7	53	7	75	7	103
		8	54	8	76	8	104
1980		9	55	9	77	9	105
		10	56	10	78	10	106
1	29	11	57	11	79	11	107
2	30	12	58	12	80	12	108
3	31	13	59	13	81	13	109
4	32	14	60	14	82	14	110
5	33	15	61	15	83	15	111
6	34	16	62	16	84	16	112
7	35	17	63	17	85	17	113
8	36	18	64	18	86	18	114
9	37	19	65	19	87	19	115
10	38	20	66	20	88	20	116
11	39	21	67	21	89	21	117
12	40	22	68	22	90	22	118
13	41			23	91	23	119
14	42			24	92	24	120
15	43			25	93	25	121
16	44			26	94	26	122
17	45			27	95	27	123
18	46			28	96	28	124
						29	125
						30	126