Abgeordnetenhaus von Berlin Drucksache 10/ **424**

10. Wahlperiode **18. 12. 85**

Mitteilungen des Präsidenten
- Nr. 40 -

Inhaltsübersicht | Nr. | Seite

Vorlage zur Kenntnisnahme

gemäß § 26 Abs. 2 Berliner Datenschutzgesetz über
Bericht des Berliner Datenschutzbeauftragten zum 31. Dezember 1985 . . . . . 27 2

Druckschluß: 22. November 1985

Ausgegeben am 18. Dezember 1985

Der Präsident
Peter Rebsch

Die Veröffentlichungen des Abgeordnetenhauses sind beim Kulturbuchverlag Berlin, Passauer Straße 4, 1000 Berlin 30, Telefon 2136071, zu beziehen.

Vorlage zur Kenntnisnahme

Bericht des Berliner Datenschutzbeauftragten zum 31. Dezember 1985

Inhaltsverzeichnis

Der Berliner Datenschutzbeauftragte gibt zu Beginn des Jahresberichts 1985[1] einen Überblick über Gesetze, in denen das Abgeordnetenhaus die Grundsätze des Volkszählungsurteils berücksichtigt hat, und über den Stand von Gesetzesvorhaben von erheblicher Bedeutung, die aufgrund der Rechtsprechung des Bundesverfassungsgerichts vordringlich sind (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 den anderen seit 1979 erschienenen Jahresberichten schließt den Bericht ab.

1. Zur Situation
Gesetzgebung als dringliche Aufgabe
Falsch verstandener Datenschutz

2. Brennpunkte des Datenschutzes
2.1 Personalcomputer: Die kleinen großen Brüder
Einzelne Anwendungen
Grundsätze
2.2 Der registrierte Einwohner
Meldegesetz
Stadtadreßbuch
2.3 Das Informationssystem der Sicherheitsbehörden
Suche nach einem neuen Polizeirecht
Die anderen Begleitgesetze
Informationssystem für Verbrechensbekämpfung
2.4 Der Postaustausch der Behörden: Eine Schwachstelle der öffentlichen Informationsverarbeitung
2.5 Der Bürger im Visier von Planung und Statistik
2.6 Archive und Bibliotheken: Schutz für Betroffene und Leser

3. Beobachtungen beim Betrieb von Bildschirmtext und bei der Entwicklung anderer Neuer Medien
3.1 Bildschirmtext
Situation
Fortschritte
Defizite
Ausblick
3.2 Fernwirkdienst TEMEX
3.3 Kabelpilotprojekt Berlin
3.4 Workshop „Datenschutz und Neue Medien"

4. Weitere Fragen aus der Kontroll- und Beratungspraxis
4.1 Systematische Überprüfungen
Berliner Stadtreinigungs-Betriebe
Wohnungsbau-Kreditanstalt und
Berliner Pfandbrief-Bank
Bezirksämter
4.2 Wahlen zum Abgeordnetenhaus 1985
Wahlwerbung mit Einwohnerdaten
Einsatz von Bildschirmtext zur Präsentation der Wahlergebnisse
Die Speicherung der Wählerdaten
Briefwahl im Strafvollzug
Geburtsdaten von Wahlbewerbern
4.3 Der Umgang mit Personaldaten
Personaldaten: eine heilige Kuh?
Ein Prüfergebnis
Veröffentlichung von Personaldaten
Personalrat und Datenschutz
4.4 Gesundheitswesen
Änderung des Landeskrankenhausgesetzes
Gewährleistung des Datenschutzes in Krankenhäusern
Datenschutz im öffentlichen Gesundheitsdienst
Gewährung und Abrechnung von Leistungen
4.5 Sozialverwaltung
Mitwirkungspflicht des Leistungsempfängers
Offenbarung von Sozialdaten
Vertraulichkeit
Besondere Leistungen

5. Nachtrag zu Feststellungen aus den Vorjahren
Nachweis der Berechtigung zum Bezug von Leistungen
Fehlauskünfte aus dem Melderegister
Anordnung über Mitteilungen in Strafsachen
Übermittlung personenbezogener Daten vom Amtsarzt an die Dienstbehörde
Schülerdaten
Betriebsdatenbank

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

7. Aufgaben des Berliner Datenschutzbeauftragten
7.1 Im Berichtsjahr 1985
7.2 Voraussichtliche Schwerpunkte

[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".

Anlagen

1. Übersicht der wesentlichen datenschutzrelevanten Gesetzesvorhaben auf Landesebene
2. Anforderungen an Datenschutzregelungen im Polizeirecht Beschluß der Konferenz der Datenschutzbeauftragten
3. Rundschreiben über die Offenbarung von Sozialdaten im Rahmen der Amtshilfe nach § 68 SGB X
4. Anforderungen an Datenschutzregelungen für den Verfassungsschutz Beschluß der Konferenz der Datenschutzbeauftragten
5. Datenschutz und Neue Medien Beschluß der nationalen Datenschutzbeauftragten
6. Grundsätze für organisatorische und technische Maßnahmen zum Datenschutz beim Einsatz von Personalcomputern (PC) des Berliner Datenschutzbeauftragten
7. Technische und organisatorische Datensicherungsmaßnahmen bei der Wartung und Fernwartung von DV-Anlagen – im Arbeitskreis „Technische und organisatorische Datenschutzfragen" der Konferenz der Datenschutzbeauftragten beraten –
8. Übereinkommen des Europarats zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten – Auszug –

Stichwortregister
für alle seit 1979 veröffentlichten Jahresberichte

1. Zur Situation

Gesetzgebung als dringliche Aufgabe

Der Datenschutz wird zunehmend bereichsspezifisch geregelt. Im Jahre 1984 galt dies vor allem für das Kabelpilotprojektgesetz und das Landeskrankenhausgesetz, im Jahre 1985 besonders für das Meldegesetz, aber auch das Gesetz für psychisch Kranke. Diese **bereichsspezifischen Regelungen** sind nicht zuletzt das Ergebnis einer engen Zusammenarbeit mit dem Abgeordnetenhaus, die darauf abzielt, die vom Bundesverfassungsgericht im Volkszählungsurteil entwickelten Grundsätze durch Landesgesetze zu konkretisieren. Allerdings darf nicht verkannt werden, daß insbesondere noch folgende z. T. umfangreiche und schwierige Vorhaben vorbereitet und parlamentarisch behandelt werden müssen:

- Krankenhausgesetz (Novelle)
- Statistikgesetz
- Archivgesetz
- Bibliotheksgesetz
- Beamtengesetz (Novelle) – Personaldaten –
- Verordnungen zum Meldegesetz
- Allgemeines Sicherheits- und Ordnungsgesetz (Novelle)
- Verfassungsschutzgesetz (Novelle)
- ADV-Gesetz
- Datenschutzgesetz (Novelle).

Dabei muß auch die – in Anlage 1 – dargestellte Abhängigkeit einzelner Vorhaben vom Fortgang entsprechender Projekte auf Bundesebene berücksichtigt werden.

Die Entwicklung des Datenschutzrechts wird schließlich auch an dem seit Herbst 1985 geltenden Übereinkommen des Europarats zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten[1] deutlich, das die Bundesrepublik Deutschland als fünfter Staat ratifiziert hat. Es handelt sich um die erste internationale Regelung des Datenschutzes, die dazu beiträgt, daß der Schutz der Bürger in Europa schrittweise verbessert und vereinheitlicht wird; angesichts der Zunahme des grenzüberschreitenden Datenverkehrs kommt dem wachsende Bedeutung zu.

Auf untergesetzlicher Ebene sind im vergangenen Jahr verschiedene **Verordnungen** und **Verwaltungsvorschriften** in Kraft getreten, die für den spezialrechtlichen Datenschutz von Bedeutung sind. Zu erwähnen sind auf Bundesebene insbesondere die Neufassung der Anordnung über Mitteilungen in Strafsachen und mehrere allgemeine Verwaltungsvorschriften zur Durchführung des Bundeszentralregistergesetzes sowie des Titels XI – Gewerbezentralregister – der Gewerbeordnung; von großer Bedeutung für den Datenschutz in der Berliner Verwaltung ist das Inkrafttreten der Neufassung der Gemeinsamen Geschäftsordnung I (GGO I) am 1. März 1985.

Ferner wurde ich u. a. in die Beratungen über die inzwischen erlassene Verordnung über den Gebrauchtwaren-, Edel- und Altmetallhandel, die Zweite Verordnung zur Änderung der Verordnung zur Durchführung des Bundesbaugesetzes (mit Regelungen des Zugriffs auf die Kaufpreissammlung) und die Ausführungsvorschriften über die Führung von Schülerbogen einbezogen.

Die Rechtsentwicklung findet auch in der **Rechtsprechung** ihren Ausdruck. Von hervorragender praktischer Bedeutung ist insbesondere die Entscheidung des Bundesgerichtshofes[1] über die Unwirksamkeit der bisher verwendeten „Schufa-Klausel". Die Banken hatten bisher bei Kontoeröffnung, aber auch bei anderen Geschäften (z. B. Kreditvergabe, Bürgschaften) eine pauschale Einwilligung des Kunden eingeholt. Ende 1983 hatte jedoch das Oberlandesgericht Hamburg entschieden, daß diese Schufa-Klausel unwirksam sei, da sie gegen die Grundsätze des Gesetzes zur Regelung der Allgemeinen 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 – BDSG –). Der Bundesgerichtshof hat dieses Urteil bestätigt.

Ihre besondere Bedeutung gewinnt die Entscheidung, weil sie das Massengeschäft der Kleinkredite betrifft, bei denen ein Datenaustausch zwischen Kreditinstituten und Schufa stattfindet.

Falsch verstandener Datenschutz

Bevor im folgenden die Datenschutzprobleme vor allem des Verwaltungsvollzugs beschrieben werden, sollen einige vermeintliche Datenschutzfragen und ihr wirklicher Hintergrund erhellt werden: Sie sind teils in der Öffentlichkeit unter dem Stichwort „Datenschutz" behandelt worden, teils haben Politiker, Verwaltungen oder Bürger geglaubt, sich zur Durchsetzung eigener Interessen des Datenschutzes bedienen zu können. Dadurch entsteht ein verzerrtes Bild vom Datenschutz.

Eine Ursache ist die **Bemäntelung von Fehlern oder bloßem bürokratischem Vorgehen** mit Datenschutzgründen. Hierzu gehören z. B. die folgenden, von der Presse aufgegriffenen Vorgänge:

„Datenschutz legt Hilfsbereitschaft Steine in den Weg"

Drei Freundinnen hatten fast gleichzeitig ein gesundes Kind geboren und wollten aus Dankbarkeit einem behinderten Kind Geld spenden. Dieses Vorhaben scheiterte am „Datenschutz", da das Sozialamt den Spendern keine Familie nennen konnte. Der Beamte, der diese Auskunft gab, hätte – ohne rechtliche Schwierigkeiten – lediglich zum Telefonhörer greifen und eine entsprechende Familie anzurufen brauchen. Warum er das nicht getan hat, bleibt sein Geheimnis. Ich hoffe, daß es sich hierbei um einen bedauerlichen Einzelfall gehandelt hat, der nicht für die öffentliche Verwaltung typisch ist.

„Daten-Irrsinn am Flughafen Tegel"

Eine Zeitung berichtete, braungebrannte Teneriffa-Urlauber müßten in Tegel doppelt so lange wie früher bei der Paßkontrolle warten. Schuld daran sei der Datenschutzirrsinn. Bisher hatten

[1] Anlage 8

[1] III ZR 213/83

immer zwei Beamte gleichzeitig kontrolliert, dabei hatte einer die Personalien laut abgelesen und telefonisch durchgegeben. Dies durfte aufgrund einer Anordnung der Polizei nicht mehr sein.

Der Flughafen Tegel wurde so konzipiert, daß kein Raum für Fluggastkontrollen vorgesehen war. Dies hat von Anfang an zu einer Fülle von provisorischen Maßnahmen geführt. Bei mir hatte sich u. a. die Liga für Menschenrechte darüber beschwert, daß das alte Abfertigungsverfahren es ermöglichte, persönliche Angaben (nicht nur Name und Vorname) anderer Passagiere mitzuhören. Ich habe daher Senat und Polizei empfohlen, eine diskretere Kontrolle durchzuführen. Dies nicht zuletzt auch deshalb, weil im westlichen Ausland die Diskretion bei Schalterabfertigungen - wie im übrigen auch im Bank- und selbst im Postbereich - wesentlich besser gewährleistet ist als in der Bundesrepublik. Die Abfertigung an Schaltern ohne Berücksichtigung der Diskretion bemängeln aber nicht nur ausländische Besucher, die dies in ihren Heimatländern in dieser Form nicht kennen, sondern in zunehmendem Maße auch Deutsche. Die von mir nicht gewollte Erschwernis bei der Abfertigung der ankommenden Fluggäste konnte zwischenzeitlich beseitigt werden. Es steht zu hoffen, daß angesichts der Größe und Bedeutung des Flughafens Tegel auch befriedigende bauliche Voraussetzungen für eine ordnungsgemäße Abfertigung geschaffen werden. Inzwischen sind weitere bauliche Maßnahmen vorgesehen.

Falsche Vorstellungen über den Datenschutz vermitteln auch Berichte aus dem Sicherheitsbereich, die in allen mir bekannten Fällen von **unrichtigen Sachverhalten oder einer falschen Beurteilung der Rechtslage** ausgehen:

„Datenschutz für Mord"

Sehr bedenkliche Auswirkungen können entstehen, wenn die Presse irreführende öffentliche Äußerungen aufgreift. So wurde der Anschlag eines Libyers mit dem Datenschutz in Verbindung gebracht. Der Libyer war, obwohl mehr als ein Anfangsverdacht gegen ihn vorlag, nur zur Grenzfahndung ausgeschrieben worden. Die Ausländerbehörde erhielt keine Kenntnis. Datenschutzvorschriften standen einer Weitergabe der Daten jedoch nicht entgegen. Die beteiligten Dienststellen haben sich auch nicht auf den Datenschutz berufen. Wenn trotz dieses eindeutigen - jederzeit durch einfache Rückfrage ermittelbaren - Sachverhalts öffentliche Beiträge diesen Fall mit dem Datenschutz in Verbindung bringen, dann müssen die Informanten folgendes verantworten: Eine ungerechtfertigte Diskreditierung des Datenschutzes und damit nicht zuletzt auch der Parlamentarier, die diese Bestimmungen beschlossen haben. Darüber hinaus birgt diese Informationspolitik vor allem die Gefahr, daß die wirklichen Schwachstellen bei den beteiligten Behörden verdeckt werden und damit eine Wiederholung von Fehlern ermöglicht wird.

Ähnliches ist auch bei der Diskussion der Spionagefälle in der letzten Zeit zu beobachten, obwohl dort ebenfalls kein Fall bekanntgeworden ist, bei dem Datenschutzfragen eine wesentliche Rolle gespielt haben.

Zu Unrecht wurde auch der folgende Fall als Datenschutzproblem behandelt, der sogar das Abgeordnetenhaus beschäftigte:

„Ich lebe von Einbrüchen. Ich möchte Wohngeld."

Der Petent hatte beim Wohngeldamt eines Bezirksamtes im Zusammenhang mit einem Antrag auf Wohngeld angegeben, er bestreite seinen Lebensunterhalt aus Erspartem, mündlich abgeschlossenen Kreditverträgen und Delikten wie Diebstahl, Raub, Betrug, Hehlerei usw., wolle aber die Höhe des Einkommens nicht angeben. Der Mitarbeiter des Wohngeldamtes griff zum Telefon und unterrichtete die Polizei. Diese leitete ein Ermittlungsverfahren mit dem Tatvorwurf „Verdacht einer Straftat" ein. Der Petent bat mich um Überprüfung der Zulässigkeit der Information an die Polizei. Obwohl ich das Bezirksamt zunächst nur um Stellungnahme gebeten hatte, mutmaßte eine Boulevardzeitung bereits, ich wolle „Ärger machen".

Die Überprüfung des Falles hat ergeben, daß die Übermittlung der Angaben vom Wohngeldamt an die Polizei datenschutzrechtlich nicht zu beanstanden ist. Nach § 71 Sozialgesetzbuch X (SGB X) ist die Offenbarung personenbezogener Daten zur Abwendung einer der in § 138 Strafgesetzbuch (StGB) genannten Straftaten zulässig. Danach wird bestraft, wer - unter anderem - von dem Vorhaben oder der Ausführung eines Raubes zu einer Zeit, zu der die Ausführung oder der Erfolg noch abgewendet werden kann, glaubhaft erfährt und es unterläßt, der Behörde oder dem Bedrohten rechtzeitig Anzeige zu machen.

Allerdings hatte das Bezirksamt entsprechende Überlegungen nicht angestellt, sondern allein auf den „gesunden Menschenverstand" hingewiesen. Zwar sollte dieser in der öffentlichen Verwaltung keineswegs vernachlässigt werden, jedoch sollte er - um Irrtümer zu vermeiden - am Gesetz gemessen werden. So sollte gerade im empfindlichen Sozialbereich bei einer Offenbarung eine genaue Prüfung der Zulässigkeit anhand der klaren gesetzlichen Regelung des Sozialgesetzbuchs stattfinden.

Schließlich zeigt der folgende Vorgang, daß auch beim Bürger **Mißverständnisse über die Reichweite des Datenschutzes** bestehen:

Bruch des Adoptionsgeheimnisses?

Eine Frau, die als Kind adoptiert worden war, fand bei ihren Adoptiveltern zufällig die Unterlagen über die Adoption. Sie suchte daraufhin ihre leibliche Mutter auf. Diese sah darin, daß ihre Daten dem Adoptivkind bekannt geworden sind, eine Verletzung des Datenschutzes.

Aus der Regelung des Adoptionsgeheimnisses (§ 1758 BGB) ergibt sich, daß ein Schutz vor Entdeckung der leiblichen Eltern nicht gewährt wird. Vielmehr liegt es in der Hand der Annehmenden, wann und wie sie die Namen der leiblichen Eltern dem Adoptivkind offenbaren. Nur die Adoptiveltern sind gesetzlich davor geschützt, daß die leiblichen Eltern die Adreßdaten der Adoptiveltern ohne deren Einverständnis erfahren. Der Datenschutz hat hinter dem Bedürfnis des Kindes zurückzustehen, seine leiblichen Eltern kennenzulernen.

2. Brennpunkte des Datenschutzes

2.1 Personalcomputer: Die kleinen großen Brüder

Das Vordringen kleiner, billiger, aber relativ leistungsfähiger Rechner (Homecomputer, Personalcomputer, Mikrocomputer) hat vor den öffentlichen Stellen Berlins nicht Halt gemacht. Die faszinierende Möglichkeit, selbst kleinere Anwendungsbereiche für die automatische Datenverarbeitung zu erschließen, die sich durch den zentralen Großrechnereinsatz nicht ohne weiteres abdecken lassen, wird zunehmend insbesondere in dezentralen Bereichen der Berliner Verwaltung, z. B. in Bezirksämtern, Schulen und Krankenhäusern, genutzt.

In der Regel ist der Einsatz solcher Rechner nicht mit dem sonst üblichen Aufwand an vorzuhaltendem Fachwissen und organisatorischen Umstellungen verbunden, da die Anlagen am Arbeitsplatz der Sachbearbeiter („Stand-Alone-Rechner") stehen. Im allgemeinen werden diese Rechner einschließlich der Anwendungsprogramme von den Lieferfirmen bereitgestellt, so daß nur noch geringfügige fachliche Anpassungen erforderlich sind.

Neben dieser „Konfektionsdatenverarbeitung" gibt es auch Personalcomputeranwendungen, bei denen Sachbearbeiter als Autodidakten Anwendungsprogramme auf dienstlich oder in Einzelfällen auch privat beschafften Kleinrechnern zur Bearbeitung dienstlicher Aufgaben einsetzen.

Der Einsatz privater Computer zu dienstlichen Zwecken ist für den Senator für Inneres Anlaß gewesen, mit Schreiben vom 29. April 1985 interne Regelungen für seine Senatsverwaltung zu erlassen, die die Rahmenbedingungen für den Einsatz solcher Rechner definieren. Danach kann ein solcher ADV-Einsatz nur genehmigt werden, wenn

- sichergestellt ist, daß die Verwaltung jederzeit über die im System gespeicherten Daten verfügen kann und daher personengebundene Nutzungsbeschränkungen ausgeschlossen sind;
- eine strikte Trennung des Einsatzes für Verwaltungszwecke und für private Zwecke außerhalb der Dienstzeit gesichert ist;

- die volle Einhaltung des Berliner Datenschutzgesetzes einschließlich der Veröffentlichungs- und Meldepflichten sowie meine Kontrollbefugnis sichergestellt sind.

Zusammengefaßt kommt der Senator für Inneres zum Ergebnis, daß aufgrund dieser Voraussetzungen der Betrieb privater Mikrocomputer für dienstliche Zwecke im allgemeinen kaum genehmigt werden kann.

Die vorsichtige Haltung des Senators für Inneres ist zu begrüßen. Aus datenschutzrechtlicher Sicht können private Computer nur zugelassen werden, wenn damit keinerlei Einschränkungen der Befugnisse der anwendenden Behörde, der Kontrollrechte von Kontrollinstanzen, der Ordnungsmäßigkeit der Datenverarbeitung und der Sicherheit personenbezogener Datenbestände vor unbefugter Offenbarung verbunden sind.

Auch der mir vorliegende Entwurf der „Ausführungsvorschriften über die Führung von Schülerbogen - AV-Schülerbogen -" des Senators für Schulwesen, Berufsausbildung und Sport geht auf die Verwendung privater Datenverarbeitungsgeräte ein. Er verweist darauf, daß für die Anwendung privater Rechner gleiche Bestimmungen gelten wie für die aus öffentlichen Mitteln beschafften Rechner, und daß ich ferner meinen Kontrollaufgaben ungehindert nachkommen können muß.

In der Fachliteratur kommt ebenfalls zum Ausdruck, daß die Einstellung privater und öffentlicher Organisationen zum Einsatz von Mikrocomputern im Rahmen individueller Datenverarbeitung einem Wandel unterzogen ist. Die ursprünglich vorherrschende Annahme, die individuelle Datenverarbeitung könnte die zentrale Großrechneranwendung dadurch ergänzen, daß sie die Automatisierungsschwelle senkt und bis in die Sachbearbeiterebene hinein flexible Anwendungen ermöglicht, wird durch die Sorge überlagert, daß die Ordnungsmäßigkeit, Kontrollierbarkeit und Transparenz der betrieblichen oder behördlichen Datenverarbeitung zu kurz kommen könne und somit unwägbare Risiken für das Finanz- und Entscheidungsgebaren sowie für den Datenschutz entstehen könnten.

Einzelne Anwendungen

Ich habe in letzter Zeit zu verschiedenen Personalcomputer-Anwendungen Stellung bezogen:

Für die Speicherung von **Personaldaten von Referendaren** beabsichtigt das Kammergericht, ein Textverarbeitungssystem einzusetzen. Nach einer Überprüfung der Zulässigkeit der dort zu speichernden Daten habe ich die Stelle darauf hingewiesen, daß zur Gewährleistung des Datenschutzes die technisch-organisatorischen Kontrollmaßnahmen in Form einer Geschäftsanweisung getroffen werden sollten, die den Kreis der Benutzer und die Modalitäten des Umgangs mit dem System regeln. Bei solchen Kleinrechneranwendungen ist vor allem auch die räumliche Sicherung besonders zu beachten. Das Kammergericht hat mir mittlerweile den Entwurf der Geschäftsanweisung über den Betrieb des Textautomaten für die Verwendung personenbezogener Daten übermittelt. Der Entwurf setzt in bemerkenswerter Konsequenz meine Empfehlungen um, die ich bereits im Jahresbericht 1983 für den Betrieb isolierter Rechner veröffentlicht habe.

Ein beliebtes Anwendungsgebiet für den Einsatz von Kleinrechnern ist das Schulwesen. Meist handelt es sich dabei um **Schülerdatenverwaltung,** wobei neben den persönlichen Daten auch Kurswahlen und Semesterdaten gespeichert werden. Dazu kommt häufig die Verwaltung von Lehrerdateien. Ich habe in jedem Fall empfohlen, den Betrieb des Rechners durch schriftliche Organisationsanweisungen zu regeln. Wenn der gleiche Rechner auch für den Informatikunterricht genutzt werden soll, ist im besonderen Maße auf die Unterbringung und Verwendung der Disketten mit personenbezogenen Daten sowie auf die klare Funktionentrennung zwischen Unterrichts- und Verwaltungsaufgaben zu achten.

Zur rationelleren Gestaltung des Verfahrens im **bezirklichen Friedhofswesen** wird von den Bezirksämtern geplant, ein einheitliches ADV-Verfahren für Kleinrechner als Ersatz für die Friedhofskartei zu entwickeln, das nach einer Pilotanwendung im Bezirksamt Tempelhof von den Friedhofsämtern aller anderen Bezirke Berlins übernommen werden soll. Das Verfahren umfaßt die Auskunftserteilung, Listenausdrucke, Suchläufe, interne Terminplanungen und Statistiken. Es sollen dabei nur Angaben gespeichert werden, die auch in den bisher verwendeten manuellen Verfahren festgehalten wurden.

Das Landesforstamt beabsichtigt den Einsatz eines Personalcomputers für das **Lohnabrechnungsverfahren der Berliner Forsten.** Gegen den geplanten Einsatz dieses schlüsselfertigen ADV-Systems habe ich keine datenschutzrechtlichen Bedenken erhoben. Zur Unterstützung bei der zukünftigen Gestaltung des Verfahrens habe ich dem Landesforstamt Hinweise zum Einsatz isolierter ADV-Systeme gegeben.

Grundsätze

Es ist ausdrücklich festzuhalten, daß dem Einsatz von Arbeitsplatzcomputern zur Verarbeitung personenbezogener Daten ebensowenig grundsätzliche Bedenken entgegenstehen wie der Verarbeitung solcher Daten in Rechenzentren. Dies setzt aber voraus, daß dem Einsatz solcher Rechner in der Organisation ein Gesamtkonzept zugrundeliegt, welches sorgfältig abgestimmt und geplant wird.

Um dieses Ziel zu fördern, habe ich die von mir im Jahresbericht 1983 und mit Erläuterungen als „Materialien zum Datenschutz" veröffentlichten **„Grundsätze für die organisatorischen und technischen Maßnahmen beim Einsatz isolierter ADV-Systeme"** für den Spezialfall des personengebundenen oder des einem Verfahren gewidmeten Einsatzes von Personalcomputern konkretisiert. Diese Grundsätze sind in der Anlage 6 dargestellt. Sie bilden den Rahmen, innerhalb dessen spezielle organisatorische und technische Maßnahmen in einer dem Schutzzweck angemessenen Weise zu realisieren sind. Dabei habe ich folgende Prinzipien zugrundegelegt:

- Daten dürfen nicht deshalb schlechter geschützt sein, weil sie auf einem Personalcomputer verarbeitet werden.
- Automatischen Einrichtungen zum Datenschutz gebührt auch bei Personalcomputern der Vorrang gegenüber nicht automatisierten Ersatzmaßnahmen.
- Der Einsatz eines Personalcomputers ist jeweils detailliert durch schriftliche Dienstanweisung zu regeln.
- Auf den datenschutzgerechten Umgang mit beweglichen Datenträgern (Disketten) ist besonderes Augenmerk zu richten.
- Die Ordnungsmäßigkeit und Kontrollierbarkeit der Anwendung von Programmen, die personenbezogene Daten verarbeiten, müssen auch beim Personalcomputer sichergestellt sein.

Ein Spezialfall der Anwendung von Kleinrechnern ist die Verwendung leistungsfähiger **Textautomaten** zur Verarbeitung personenbezogener Daten aus Dateien. Sie erfolgt häufig zur Zusammenstellung von Telefonverzeichnissen, Geschäftsverteilungsplänen und zur Adressierung von Rundschreiben an einen bestimmten Adressatenkreis. Die meisten in der Berliner Verwaltung eingesetzten Textautomaten sind durch Betriebs- und Anwendungssysteme sowie bestimmte Hardware-Gestaltung auf die Textverarbeitung spezialisierte ADV-Systeme. Durch eine Veränderung der Programmausstattung können solche Systeme ohne weiteres - wenn auch nicht mit vergleichbarem Komfort - für andere Zwecke wie für numerische Berechnungen oder Verwaltung von Dateien eingesetzt werden.

Alle Anlagen, mit denen Dateien auf automatisch lesbaren Speichermedien geführt werden können und deren Hardware es erlaubt, die in § 4 Abs. 3 Nr. 3 Berliner Datenschutzgesetz beschriebenen Operationen bei geeigneter Programmierung durchzuführen, sind ADV-Systeme, die den Bestimmungen des Berliner Datenschutzgesetzes unterliegen. Dies gilt daher auch für die genannten Textverarbeitungssysteme.

Obwohl diese Auffassung in den meisten Fällen nicht bestritten wurde und die von mir empfohlenen Maßnahmen bei solchen Textverarbeitungsanwendungen durchgeführt wurden, mußte ich in Einzelfällen beanstanden, daß trotz mehrfachen Anmahnens - auch durch interne Datenschutzinstanzen - keine Meldungen zum Dateienregister erfolgten. Gerade beim Einsatz von dezen-

tralen ADV-Anlagen sind solche Meldungen für mich von besonderer Bedeutung, da sonst eine datenschutzrechtliche Kontrolle durch mich faktisch ausgeschlossen ist.

Eine Sonderstellung nehmen **Kleinrechner** ein, **die über eine Datenübertragungsleitung mit Rechenzentren verbunden sind** und somit die Vorzüge individueller Datenverarbeitung mit dem Zugang zu Großrechnerkapazitäten verbinden. Für solche **„intelligenten Schnittstellen"** gelten die oben skizzierten Grundsätze nicht. Die mit dem unter Umständen programmgesteuerten dezentralen Zugriff auf umfangreiche Datenbestände verbundenen weitergehenden Risiken erfordern, daß zusätzliche Anforderungen an die organisatorischen und technischen Maßnahmen beim Personalcomputer und im Rechenzentrum zu stellen sind. Diese Problematik wird mit dem Einstieg in die offene Vernetzung der Berliner Verwaltung verstärkt aufgeworfen werden, und es ist zu hoffen, daß bei der Konzeption des Netzes von Anfang an der Schutz vor unbefugtem Zugriff auf zentrale Datenbestände eine bestimmende Rolle spielt.

Datenschutzrechtlich ist daher auch das Vorhaben eines Vermessungsamtes, technische Daten zum Rechenzentrum Spandau von einem Mikrocomputer aus zu übertragen, im Hinblick darauf interessant, ob dadurch sogenannten Hackern ein Zugang zu anderen personenbezogenen Datenbeständen ermöglicht werden könnte.

2.2 Der registrierte Einwohner

Meldegesetz

Am 31. Januar 1985 wurde in der letzten Sitzung der vergangenen Legislaturperiode des Abgeordnetenhauses das Gesetz über das Meldewesen in Berlin (Meldegesetz) beschlossen. Damit wurde ein langjähriges und kompliziertes Gesetzgebungsverfahren abgeschlossen[1]. Zu den verfassungsrechtlichen Fragen, insbesondere zu den Folgerungen aus dem Volkszählungsurteil des Bundesverfassungsgerichts hatte Prof. Dr. Benda eine Stellungnahme abgegeben, die wesentlich zur Klärung problematischer Punkte beitrug.

Die intensive und gründliche Behandlung des Melderechts hat sich aus meiner Sicht gelohnt, denn das jetzt vorliegende Gesetz entspricht im wesentlichen den Datenschutzanforderungen. Dies gilt insbesondere für folgende Punkte:

- § 1 Meldegesetz enthält eine genaue Definition der Aufgaben der Meldebehörde, die den Anforderungen an die Transparenz besser entspricht als § 1 Melderechtsrahmengesetz.
- Die Rechte der Bürger konnten klargestellt und erweitert werden.
- Die Meldebehörde wird organisatorisch vom Polizeipräsidenten getrennt und als Landeseinwohneramt eingerichtet. Die seit über 100 Jahren bestehende organisatorische Verbindung entfällt damit. Im Laufe dieser Zeit hat sich das Meldewesen vom obrigkeitsstaatlichen Überwachungsinstrument zu einem multifunktionalen Auskunftssystem gewandelt, bei dem der Datenschutz durch geeignete Maßnahmen sicherzustellen war. Dieses geänderte Verständnis war ursächlich für die Forderung, das Meldewesen aus dem Zuständigkeitsbereich des Polizeipräsidenten auszugliedern und zu verselbständigen. Auf diese Weise ist auch ein angemessenes Verfahren zum Ausgleich denkbarer Interessenkollisionen zwischen Ordnungs- und Vollzugsaufgaben möglich.
- Die Seriennummer des Personalausweises wird nicht ins Melderegister eingetragen. Damit wird der Gefahr begegnet, daß diese Nummer zu einem Substitut eines Personenkennzeichens werden könnte.
- Die Übermittlungsregelungen (§§ 25 ff. Meldegesetz) sind übersichtlich und für den Bürger verständlich formuliert. Der Zugriff der Polizei unterliegt hinsichtlich sensibler Daten angemessenen Einschränkungen, die die Effektivität polizeilicher Arbeit nicht beeinträchtigen.
- Die Übermittlung des internen Ordnungsmerkmals an andere Stellen ist unzulässig.
- Erkennungsdienstliche Maßnahmen gegen den Willen des Betroffenen sind nicht möglich.
- Auskünfte über einen Aufenthalt im Krankenhaus sind nur unter sehr engen Voraussetzungen und unter Beachtung der ärztlichen Schweigepflicht zulässig.
- Insassen von Justizvollzugsanstalten sind nur dann meldepflichtig, wenn sie keine Wohnung außerhalb der Justizvollzugsanstalt haben.
- Das Gastgewerbe muß Hotelmeldescheine nicht täglich bei den Meldestellen anliefern, sondern nur bereithalten.

Prof. Dr. Benda hatte gegen die Verfassungsmäßigkeit der bereits im Melderechtsrahmengesetz festgelegten Hotel- und Krankenhausmeldepflichten Bedenken geltend gemacht. Der Senator für Inneres ist daher an den Bundesminister des Innern herangetreten, um eine bundeseinheitliche Klärung zu erreichen.

Aus dem Meldegesetz sind verschiedene Konsequenzen zu ziehen:

- Durch den Erlaß von Rechtsverordnungen, bei dem der Datenschutzbeauftragte zu hören ist, sind die Aufbewahrung der Daten vor der Löschung, die Form der Meldescheine für Beherbergungsstätten und insbesondere die regelmäßigen Datenübermittlungen zu regeln.
- Die Organisation des Meldewesens und das Informationssystem Einwohnerwesen ist bis spätestens 31. März 1986 an das Melderecht anzupassen.
- Die Löschung nicht mehr zulässiger und nicht mehr erforderlicher Daten aus dem Melderegister hat bis zum 1. Oktober 1986 zu erfolgen.
- Da gemäß § 1 für bestimmte Daten die Bezirksämter als Meldebehörde zuständig sind, muß zwischen den verschiedenen Meldebehörden eine differenzierte Zugriffskontrolle erfolgen. Das bedeutet, daß auch unter den zwölf Bezirksämtern bezogen auf ihren örtlichen Zuständigkeitsbereich eine Zugriffskontrolle erfolgen muß.
- Aus der Zweckbindung der in § 2 Abs. 2 genannten Daten ergibt sich, daß der Zugriff auf diese Daten on-line nur solchen Behörden gewährt werden darf, die mit der jeweils definierten Aufgabe betraut sind.
- Da das Ordnungsmerkmal nicht mehr übermittelt werden darf, ist sicherzustellen, daß es außer bei den Dienststellen des Meldewesens nicht mehr auf dem Bildschirm oder auf Ausdrucken erscheint.
- Die Gewährleistung der Rechte der Betroffenen, insbesondere der datenschutzrechtlichen Sperrung, die bisher in der Einwohnerdatenbank nur unzureichend möglich war, muß programmtechnisch sichergestellt werden.
- Um sicherzustellen, daß die Meldebehörde den Betroffenen über die Erteilung einer erweiterten Melderegisterauskunft gemäß § 28 Abs. 2 Meldegesetz unterrichten kann, sollte die Protokollierung derartiger Auskünfte automatisch erfolgen.

Stadtadreßbuch

Nachdem im neuen Meldegesetz mit § 29 Abs. 3 die Übermittlung von Meldedaten an Adreßbuchverlage geregelt wurde, bat mich ein bekannter deutscher Verlag um Bestätigung, daß meine früheren Bedenken gegen die Herausgabe solcher Daten nicht mehr bestünden.

Eine Übermittlung von Adreßdaten der überwiegenden Anzahl der Berliner Bevölkerung ist nach der Rechtslage allerdings weiterhin nicht ohne weiteres möglich, da das Meldegesetz Personen, die sich an- oder ummelden, die Möglichkeit des Widerspruchs gegen eine Übermittlung ihrer Adreßdaten an Adreßbuchverlage einräumt, aber der Wille aller zuvor im Bestand des Melderegisters geführten Personen nicht bekannt ist.

Mit der gesetzlichen Regelung hatte der Berliner Gesetzgeber die Erstellung und Herausgabe eines Adreßbuches grundsätzlich

[1] Vgl. Jahresbericht 1984, 4.4

befürwortet. Ein Adreßbuch hat nur einen Sinn, wenn es möglichst vollständig ist. Daraus muß zwar gefolgert werden, daß nicht etwa beabsichtigt war, die Bereitstellung von Bestandsdaten aus der Zeit vor Inkrafttreten des Gesetzes auszuschließen. Es ist daher erforderlich, daß die bereits im Datenbestand vorhandenen Personen die gleichen Rechte erhalten wie die Personen, die nach Inkrafttreten des Gesetzes eine An- bzw. Ummeldung vornehmen.

Da eine Einzelbefragung sämtlicher gemeldeter Personen praktisch kaum durchführbar wäre, müssen geeignete Wege für eine öffentliche Bekanntmachung des Widerspruchsrechtes gefunden werden, wie sie im übrigen auch in den Meldegesetzen der meisten Bundesländer festgeschrieben sind.

Ich habe dem Senator für Inneres detaillierte Vorschläge, insbesondere zur Form der Veröffentlichung und zu den Widerspruchsfristen, unterbreitet.

Der Senator für Inneres hat meine Rechtsauffassung bestätigt. Er hält dabei eine von der Meldebehörde zu veranlassende Bekanntmachung im Amtsblatt und im Landespressedienst mit dem Hinweis auf eine dreimonatige Widerspruchsfrist für „Altfälle" für angemessen.

2.3 Das Informationssystem der Sicherheitsbehörden

Suche nach einem neuen Polizeirecht

Eine der wesentlichsten Auswirkungen des Volkszählungsurteils betrifft die rechtliche Regelung der polizeilichen Datenverarbeitung: Bereits in meinem Jahresbericht 1984 hatte ich auf das Mißverhältnis zwischen dem Umfang der gesetzlichen Regelung bei der polizeilichen Datenverarbeitung und deren Bedeutung hingewiesen (S. 10 ff.) und die Aspekte und Maßnahmen beschrieben, die sowohl aus der Sicht des Datenschutzes aber auch der Polizei[1] einer Regelung bedürfen. Dabei erfordern nicht nur rechtsförmliche Gründe, sondern auch die zunehmende Bedeutung der Datenverarbeitung im Bereich der Polizei eine hohe Sorgfalt bei der Gesetzgebung.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat als Grundlage für die gebotene Beratung beim Gesetzgebungsverfahren Vorstellungen für eine gesetzliche Regelung entwickelt. Die wesentlichen Gesichtspunkte sind im Beschluß vom Januar 1985 zusammengefaßt[2].

Auf Seiten der Verwaltung hatte die Innenministerkonferenz frühzeitig ihren zuständigen Arbeitskreis beauftragt, ebenfalls Vorschläge für neue polizeirechtliche Regelungen zu entwickeln. Der Arbeitskreis legte einen Vorentwurf zur Änderung des Musterentwurfs eines einheitlichen Polizeigesetzes des Bundes und der Länder vor, den die Innenministerkonferenz in ihrer Sitzung im April 1985 zur Grundlage für die weitere Beratung erklärte. Den Datenschutzbeauftragten, die bis zu diesem Zeitpunkt nicht beteiligt waren, wurde Gelegenheit zur Stellungnahme gegeben.

In meiner Stellungnahme habe ich versucht, unter Aufrechterhaltung der Struktur des Vorentwurfs die in den Papieren der Konferenz der Datenschutzbeauftragten enthaltenen Grundgedanken auf den Vorentwurf zu übertragen.

Folgende wesentliche Probleme wirft der Vorentwurf auf:

Da die Zulässigkeit der Informationsverarbeitung von der Aufgabenzuweisung an die jeweilige Behörde abhängt, ist auch aus datenschutzrechtlicher Sicht eine präzise Umschreibung der jeweils zugeordneten Aufgaben vonnöten. Das Polizeirecht umschreibt die Aufgaben nur teilweise. Insbesondere fehlen bisher klare Aussagen darüber, in welchem Umfang die Polizei zur Prävention von Straftaten („vorbeugende Verbrechensbekämpfung") und Gefahrenlagen („Gefahrenvorsorge") zuständig sein soll, obwohl gerade für diese Aufgabenstellungen Datensammlungen von erheblichem Umfang geführt werden. Ich habe vorgeschlagen, den Vorentwurf um entsprechende Definitionen zu ergänzen, wobei das Vorliegen tatsächlicher Anhaltspunkte entscheidende Voraussetzung für die Maßnahmen zur vorbeugenden Verbrechensbekämpfung sein sollte. Im Bereich der Gefahrenvorsorge sollten Daten überhaupt nur verarbeitet werden, wenn diese auf freiwilliger Basis oder aus allgemein zugänglichen Quellen erhoben werden. Ein Beispiel für eine derartige Datensammlung ist die sogenannte „Strukturdatei" in den Polizeiabschnitten, in denen personenbezogene Daten der Personen enthalten sind, die für bestimmte Grundstücke verantwortlich sind.

Die Zulässigkeit der Datenerhebung für Zwecke der vorbeugenden Straftatenbekämpfung muß grundsätzlich auf Straftaten mit erheblicher Bedeutung eingeschränkt werden. Neben dem Grundsatz, daß personenbezogene Daten beim Betroffenen erhoben werden sollen, muß der Vorrang offener Datenerhebung gegenüber der verdeckten Form hervorgehoben werden.

Bei der beabsichtigten Regelung der Bild- und Tonaufnahmen im Zusammenhang mit öffentlichen Veranstaltungen muß der enge Zusammenhang zur Veranstaltung deutlich gemacht werden. Aufnahmen sollten erst dann zulässig sein, wenn eine Gefährdung der öffentlichen Sicherheit und Ordnung konkret eintritt. Zu vermissen ist eine Regelung, ob und unter welchen Voraussetzungen bei geschlossenen Versammlungen Daten erhoben werden dürfen.

Sollten trotz der nach wie vor bestehenden rechtlichen Bedenken maschinenlesbare Personalausweise eingeführt werden, wäre zumindest eine Regelung besonders wichtig, die die Verwendung automatischer Lese- oder Aufzeichnungsgeräte einschränkt. Ich habe sicherheitshalber vorgeschlagen, hier einen ausdrücklichen Gesetzesvorbehalt einzubringen, nach dem in der jeweiligen spezialgesetzlichen Materie die Voraussetzung für den Einsatz festgelegt werden muß. Dessenungeachtet fühle ich mich durch die Diskussion - auch auf internationaler Ebene - in meiner seit jeher bestehenden Auffassung bestärkt, daß ich jedermann von der Einführung des maschinenlesbaren Ausweises abraten muß.

Erhebliche Diskussionen hat schon seit langem die „polizeiliche Beobachtung" hervorgerufen, d. h. die Aufzeichnung personenbezogener Daten über Personen, gegen die noch kein hinreichender oder gar kein Tatverdacht besteht, deren Bewegungen aber im Zusammenhang mit der Aufklärung einer Straftat oder der Gefahrenabwehr von Interesse sind. Derartige Maßnahmen sollten auf wenige Sonderfälle beschränkt werden, etwa auf die Straftaten nach den §§ 129, 129 a StGB.

Die von mir mehrfach erhobene Forderung, in einem polizeilichen Informationssystem den Zugriff auf Tatverdächtige bzw. Störer von dem Zugriff auf Daten anderer Personen zu trennen, sollte auch in der rechtlichen Regelung ihren Niederschlag finden.

Der Vorentwurf der Innenministerkonferenz enthält keine Regelungen zur Datenübermittlung an zentrale Stellen, bezüglich der Verpflichtung zur Überprüfung der Daten vor einer Datenübermittlung und zur Mitteilung der Veränderung wesentlicher Gesichtspunkte an Stellen, die zuvor Daten erhalten haben. Ferner berücksichtigt der Entwurf nicht, daß auch die Vorschriften über Identitätsfeststellungen sowie über Maßnahmen zur erkennungsdienstlichen Behandlung im Hinblick auf das informationelle Selbstbestimmungsrecht einer Präzision bedürfen.

Ein wesentliches Defizit des Vorentwurfes besteht darin, daß die besonderen Bedingungen des Einsatzes automatischer Datenverarbeitung bei der Verarbeitung polizeilicher Daten keine Berücksichtigung finden. Hier sollten sowohl materielle als auch verfahrensmäßige Vorschriften für die Automation geschaffen werden. Die Konferenz der Datenschutzbeauftragten hatte hierzu Formulierungsvorschläge entwickelt, die im wesentlichen darauf abzielen sicherzustellen, daß die möglichen Verwendungen in einem angemessenen Verhältnis zu den Gefahren für die schutzwürdigen Belange der Betroffenen stehen. Durch die Automatisierung darf keine unangemessene Verkürzung oder Verzerrung des Sachverhaltes entstehen.

Die Innenministerkonferenz hat inzwischen beschlossen, die von den jeweiligen Datenschutzbeauftragten abgegebenen Stellungnahmen bei einer Überarbeitung des Entwurfs mit einzubeziehen.

[1] Vgl. dazu insbesondere die Ausführungen des früheren Präsidenten des BKA, Horst Herold, (Dokumentation der Frankfurter Rundschau vom 27. Juni 1985)
[2] Vgl. Anlage 2

Um die derzeit bestehende völlig unzureichende Rechtslage zu verbessern, sollte der Landesgesetzgeber umgehend das Berliner Polizeirecht novellieren.

Die anderen Begleitgesetze

Das Volkszählungsurteil gebietet nicht nur eine Novellierung der Polizeigesetze, sondern auch aller anderen Gesetze im Sicherheitsbereich. Besondere Bedeutung kommt dabei dem Plan zu, einen fälschungssicheren und maschinenlesbaren Personalausweis sowie einen entsprechenden Reisepaß einzuführen: Die Datenschutzbeauftragten hatten frühzeitig festgestellt, daß die Einführung eines derartigen Ausweises nur hingenommen werden kann, wenn es im überwiegenden Allgemeininteresse geboten ist, den Personalausweis maschinenlesbar zu gestalten. Für ein derartiges überwiegendes Allgemeininteresse sind nach meiner Auffassung bisher keine überzeugenden Gründe genannt worden. Daher sind die Bedenken gegen die sachliche Erforderlichkeit und die rechtliche Zulässigkeit nicht zerstreut worden.

Herausragende Bedeutung kommt der Regelung der Informationsverarbeitung im Rahmen der (repressiven) Strafverfolgung zu. Die Strafprozeßordnung enthält bislang keine derartigen Bestimmungen, obwohl der Einsatz der Datenverarbeitung gerade bei der Verbrechensbekämpfung eine zentrale Rolle spielt. Ziel der datenschutzrechtlichen Regelungen muß es sein, eine Parallelität zwischen polizeirechtlichen und strafprozessualen Regelungen herzustellen. Normvorstellungen der Justizminister des Bundes und der Länder, die zwischenzeitlich vorgelegt worden sind, werden diesem Anliegen nur teilweise gerecht. Bemühungen um eine Angleichung sind im Gange, auch die Konferenz der Datenschutzbeauftragten hat einen entsprechenden Arbeitskreis eingerichtet. Vor einer Harmonisierung beider Regelungsbereiche ist auch der Erlaß polizeirechtlicher Vorschriften nicht zu erwarten.

Auch der Bereich der Nachrichtendienste (Verfassungsschutzämter, Bundesnachrichtendienst, Militärischer Abschirmdienst) ist regelungsbedürftig. Es ist beabsichtigt, die Datenverarbeitung der Verfassungsschutzämter einerseits (Verfassungsschutzgesetze), deren Zusammenarbeit mit den Polizeibehörden andererseits (Zusammenarbeitsgesetz) getrennt zu regeln. Die bisher hierzu bekannt gewordenen Entwürfe entsprechen bei weitem nicht den Anforderungen an eine datenschutzgerechte, selbstverständlich die Sicherheitsinteressen hinreichend berücksichtigende Regelung. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat in ihrer Sitzung vom 13. September 1985 hierzu ebenfalls Grundsätze verabschiedet[1].

Informationssystem für Verbrechensbekämpfung

Die systematische Überprüfung des Informationssystems für Verbrechensbekämpfung (ISVB) war einer der Schwerpunkte meiner Kontrolltätigkeit.

Das ISVB ist das ADV-Informationssystem des Polizeipräsidenten, das nach seiner Zielsetzung alle im Zusammenhang mit der Verbrechensbekämpfung anfallenden Informationen speichert, verarbeitet und sie den Polizeibeamten automatisch oder auf Anfragen unmittelbar und sofort zur Verfügung stellt. Das System ist in das die Datenverarbeitung des Bundeskriminalamtes (BKA) und die Datenverarbeitung der übrigen Landespolizeien umfassende gesamtpolizeiliche Informationssystem INPOL integriert.

Die Einrichtung des Systems geht auf einen Beschluß des Abgeordnetenhauses von Berlin vom September 1970 zurück. Das ursprüngliche Grundkonzept sah zunächst vor, die „Vorgangsverwaltung", d.h. die Aufnahme, Steuerung und Bearbeitung von Ermittlungsvorgängen zu unterstützen, sowie den Zugriff auf die Kriminalaktensammlung, der bisher nur über Karteikarten möglich war, zu erleichtern. Insbesondere sollten die Sachbearbeiter selbst durch unmittelbaren Zugang zur Datenverarbeitung über gewidmete Terminals die Steuerung der Vorgangsverwaltung übernehmen („Vorgangsverwaltung im Sachbearbeiterprinzip"). Die dabei entstehende Dokumentation des Bearbeitungsstandes sollte die bisherige Dokumentation in Form von Tagebüchern ersetzen.

Parallel zu diesen auf die Vorgangsverwaltung bezogenen Planungen entwickelte das Bundeskriminalamt zusammen mit den Landeskriminalämtern seit 1972 ein Konzept für ein gemeinsames arbeitsteiliges Informations- und Auskunftssystem. Innerhalb dieses Systems sollen im Datenverbund zwischen BKA und Landeskriminalämtern mit einer Reihe genau definierter „Bausteine" einzelne Aufgabenbereiche der Kriminalpolizei EDV-mäßig unterstützt werden. Die Realisierung von INPOL begann mit den Aufgabenbereichen Personen- und Sachfahndung. Schrittweise wurde bzw. wird INPOL um die Aufgaben Kriminalaktennachweis, Haftdatei, erkennungsdienstliche Daten, Aktenerschließungssysteme und Tatmittelnachweise ergänzt.

Technisch und organisatorisch sind die einzelnen Aufgabenbereiche von INPOL unterschiedlich ausgestaltet:

Während für die Aufgabenbereiche Personen- und Sachfahndung die Datenbestände in Bund und (einzelnen) Ländern parallel geführt werden (mit der Folge, daß das ISVB selbst einen entsprechenden Datenbestand enthält, der ständig mit dem INPOL-Bestand abgeglichen wird), muß auf die Daten im Rahmen der anderen Aufgabenbereiche über eigene nur dem Rechner des BKA zugeordnete Terminals zugegriffen werden.

Soweit eine Paralleldatenverarbeitung vorgesehen war, wurde für das ISVB die Entscheidung getroffen, eine integrierte Speicherung der für die Vorgangsverwaltung und für den INPOL-Verbund erforderlichen Daten vorzusehen. Die anderen vom Land Berlin für den Verbund anzuliefernden Daten werden teilweise ebenfalls im ISVB generiert und auf Stromwegen in den Verbund eingegeben, jedoch nicht gesondert im ISVB abgespeichert. Bei weiteren im Rahmen von INPOL gespeicherten Daten ist das ISVB (bisher) nicht beteiligt, die Zulieferung der Daten vollzieht sich vielmehr außerhalb des ISVB mit traditionellen Datenträgern, insbesondere Formularen (z. B. erkennungsdienstliche Daten).

Zur Realisierung der Zielsetzungen ist das ISVB in mehrere Datenbankabschnitte gegliedert. Von besonderer Bedeutung sind

- die **Vorgangsdatei (VD),** in der alle einem Ermittlungsvorgang zugeordneten Daten gespeichert sind. Der Personenbezug wird über die Angabe des bzw. der Geschädigten oder Betroffenen und der Tatverdächtigen hergestellt;
- die **Zentraldatei (ZD),** in der personenbezogene Daten aller in der Vorgangsdatei als Anzeigenerstatter, Geschädigte, Betroffene, Zeugen oder Tatverdächtigte notierte Personen erfaßt sind. Auf die Schuld- oder Geschäftsfähigkeit kommt es dabei nicht an. Zu den Grunddaten werden weitere Merkmale zugespeichert, die im Rahmen des INPOL-Verbundes angefallen sind (Fahndungen) oder für die im Rahmen der Strafverfolgung oder der Gefahrenabwehr die Erforderlichkeit des unmittelbaren personenbezogenen Zugriffs unterstellt wird;
- die **Berechtigtendatei (BD),** in der personenbezogene Daten über die ISVB-berechtigten Polizeibeamten gespeichert sind. Über diese Datei wird die Zugriffsberechtigung auf die einzelnen Datensätze und Programme gesteuert.

Für jede in der ZD enthaltene Person wird eine EDV-Nr. vergeben, mit deren Hilfe die Verknüpfung von ZD und VD hergestellt wird. Außerhalb des ISVB wird diese Nummer nicht verwendet, so daß sie nicht als Surrogat einer Personenkennziffer betrachtet werden kann.

Der Zugriff auf die Daten ist prinzipiell von jedem Terminal möglich, die differenzierten Zugriffsberechtigungen werden über verschiedene Benutzerausweise realisiert. Abgesehen von einigen speziellen Berechtigungen wird im wesentlichen differenziert zwischen kriminaldienstverrichtender Vollzugspolizei (VB-Sachbearbeiter) und nicht-kriminaldienstverrichtender Vollzugspolizei (S-Sachbearbeiter). Für Änderungsfunktionen wird als zusätzliches Kriterium der aktuelle Sachbearbeiter geführt. Während VB-Sachbearbeiter grundsätzlich auf alle Daten zugreifen können, ist der Zugriff bei S-Sachbearbeitern auf wenige Einzeldaten beschränkt.

Die Zugriffssicherung wird dadurch realisiert, daß bei den einzelnen Aktivitäten die Berechtigung des Benutzers an Hand eines

[1] Vgl. Anlage 4

Vergleichs der eingelesenen Berechtigungskarte und der Berechtigtendatei überprüft wird. Die Kontrollierbarkeit wird durch eine Protokollierung der Aktivitäten gesichert.

Als zusätzliche Sicherungsmaßnahme ist aufgrund der Geschäftsanweisung über den Schutz personenbezogener Daten in der Berliner Polizei eine zentrale Datenschutzstelle eingerichtet worden, zu deren Aufgaben die

- Regelung von Grundsatzangelegenheiten des Datenschutzes,
- Beratung, Kontrolle, Empfehlungen und Weisungen in Fragen des Datenschutzes,
- Sammlung und Unterrichtung des Polizeipräsidenten über Fälle des Datenmißbrauchs

gehören.

Die technische Abwicklung des ISVB erfolgt im Auftrag des Polizeipräsidenten hinsichtlich des Rechnerbetriebs und der Systembetreuung durch das Landesamt für Elektronische Datenverarbeitung (LED). Die Anwenderprogramme werden von der Abteilung Automatische Datenverarbeitung des Polizeipräsidenten (ZD II) erstellt und betreut. Darüber hinaus ist diese Stelle für das Datenfernübertragungsnetz sowie die Datenendgeräte im Polizeibereich zuständig.

Die Bewertung des komplexen Systems mußte vor dem Hintergrund der in der Vergangenheit beobachteten tatsächlichen Gefahren erfolgen.

Dabei war von dem Erfahrungssatz auszugehen, daß mit zunehmender Größe und Komplexität eines Datenverarbeitungssystems, insbesondere der zunehmenden Zahl der Datensätze und der zugriffsberechtigten Personen die Gefahr von Fehlern und des Mißbrauchs wächst.

Trotz der umfangreichen Maßnahmen zur Datensicherung besteht die Gefahr, daß Bedienstete unbefugt auf die Daten des ISVB zugreifen. Die bisherigen Erfahrungen zeigen, daß dies aus bloßer Neugier geschehen kann (z. B. bei Ermittlungsverfahren gegen Prominente), aber auch aus dem Bestreben, die Daten des ISVB im privaten Bereich zu benutzen, sei es zur Überprüfung von Verwandten, Freunden und Freundinnen, oder um sich im gesellschaftlichen Leben eine bessere Position zu verschaffen, indem man über fundierte Kenntnisse anderer Personen verfügt und dies auch zu erkennen gibt. In einem Einzelfall sind bei einem Beamten über hundert unaufgeklärte Abfragen festgestellt worden. In einem anderen Fall ließ sich nicht aufklären, ob Beamte Daten für Kriminelle abgefragt haben.

Der Polizeipräsident mißt Beanstandungen wegen mißbräuchlicher Zugriffe auf das ISVB durch Polizeiangehörige große Bedeutung zu. In allen bekanntgewordenen Fällen sind gegen die Beamten disziplinarische Maßnahmen eingeleitet worden, in einem Fall ist die Entlassung aus dem Polizeidienst ausgesprochen worden. Aufklärung und wiederholte Schulungsmaßnahmen sollen den Mißbrauch verhindern.

Daneben stehen jene Gefahren, die sich für den Bürger ergeben, wenn falsche, unvollständige oder veraltete Daten über ihn erfaßt werden, so daß er etwa aufgrund einer Verwechselung als zur Fahndung ausgeschrieben gespeichert ist - mit allen sich daraus ergebenden Konsequenzen.

So kann die Nichtberücksichtigung der Löschungsfristen zu einer Erschwerung der Resozialisierung führen. Dies gilt insbesondere für Daten von Jugendlichen. Dies ist ein Komplex, dessen Überprüfung nicht abgeschlossen werden konnte, da der Polizeipräsident die von mir erwünschte Stichprobenauswertung zunächst für nicht möglich erklärte, sodann nur zögernd vornahm.

Angesichts der Sensibilität der Ermittlungsdaten ist davon auszugehen, daß auch bei unbefugten dritten Stellen ein großes Interesse an der Kenntnis der Daten besteht. Ein beachtliches Risiko in dieser Hinsicht besteht derzeit noch darin, daß insbesondere die Übermittlung der Daten im INPOL-Verbund (über das Gebiet der DDR) in unverschlüsselter, d.h. mithörbarer Form erfolgt. Der Polizeipräsident hat angekündigt, daß künftig eine Verschlüsselung vorgenommen wird.

Die Überprüfung führte zu folgenden Ergebnissen:

Das System hält im wesentlichen den datenschutzrechtlichen Kriterien stand. Dennoch waren einzelne Mängel festzustellen:

Das Verfahren ist über lange Zeit gewachsen, einzelnen Verfahrensteilen liegen daher unterschiedliche Konzeptionen zugrunde; Teile sind veraltet. Insgesamt stellt sich das Verfahren als heterogen und nicht in allen Teilen transparent dar. Dies wirkt sich sowohl auf die Benutzung durch die Mitarbeiter der Polizei, als auch die Kontrollierbarkeit des Systems durch die Polizei selbst, die Aufsicht und andere Kontrollinstanzen negativ aus. Ich habe daher empfohlen, die Transparenz des Verfahrens zu verbessern. Der Polizeipräsident hat eine Nachdokumentation im realisierbaren Umfang in Aussicht gestellt.

Neben die zum erheblichen Teil entwicklungsbedingte Schwäche treten folgende konzeptionellen Grenzen:

Das ISVB und der Verbund beruhen auf der Annahme, die zentrale Datenverarbeitung sei in allen Fällen ein geeignetes Instrument der Verarbeitung personenbezogener Informationen zum Zwecke der Bekämpfung von Straftaten. Dies muß aufgrund der Erfahrung relativiert werden. Die Feststellungen legen nahe, daß es in sensiblen Bereichen zu riskant ist, eine Speicherung von Daten in dem zentralen System vorzunehmen.

Ich habe empfohlen zu prüfen, ob nicht für derartige Bereiche isolierte Lösungen (z. B. gewidmete Systeme) in Betracht zu ziehen sind; in einzelnen Bereichen hat eine derartige Prüfung stattgefunden, in einem Fall setzt die Polizei bereits einen isolierten Rechner ein.

Die Sicherstellung der Ordnungsmäßigkeit der Datenverarbeitung, die für den Datenschutz von herausragender Bedeutung ist, setzt eine klare funktionale Trennung der DV- von der Fachverantwortung voraus.

Dies ist bei der derzeitigen Organisation nicht erkennbar. Vielmehr deckt teilweise die Abteilung Automatische Datenverarbeitung in sich beide Verantwortungsbereiche ab. Zwar soll die beim Dezernat Verbrechensbekämpfung eingerichtete Verbindungsstelle den Kontakt mit ZD II garantieren; tatsächlich birgt die bestehende Organisation aber die Gefahr, daß letztlich doch stärker die technischen Vorgaben die Anwendungsbedingungen definieren. Ich habe daher eine weitere Stärkung der Fachverantwortung in der Landespolizeidirektion und eine Konzentrierung der Aufgaben der Abteilung Datenverarbeitung auf die technische Umsetzung empfohlen. Dies sollte insbesondere in einer Neuorganisation des Programmfreigabeverfahrens seinen Ausdruck finden. Der Polizeipräsident reagierte bisher mit einer stärkeren Einbindung der Dezernate Verbrechensbekämpfung und Öffentliche Sicherheit in die Programmfreigabe. Ich werde beobachten, wie sich diese Regelung bewährt.

Aufgrund der Größe des Systems, der Zahl der Zugriffsberechtigten und der bekanntgewordenen Fälle ist eine effektive Innenrevision erforderlich. Der Polizeipräsident geht davon aus, daß diese Aufgaben von der beim Stab eingerichteten zentralen Datenschutzstelle wahrgenommen werden.

Die Geschäftsanweisung über den Schutz personenbezogener Daten in der Berliner Polizei bringt dies allerdings nur teilweise zum Ausdruck. Ich habe empfohlen, ausdrücklich zu regeln, daß folgende Aufgaben von dieser Stelle wahrgenommen werden:

- Überprüfung aller Mißbrauchsfälle und Fehler,
- Auswertung der Protokolle im Hinblick auf Mißbrauchsfälle,
- stichprobenhafte Kontrolle vor Ort,
- Entwicklung von Vorschlägen zur Verbesserung der Sicherheit.

Eine entsprechende Überarbeitung der Dienstanweisung wurde angekündigt.

In Einzelfällen habe ich festgestellt, daß die technischen Maßnahmen zur Datensicherung trotz ihres relativ hohen Niveaus intern unterlaufen werden können.

Auch die Datenstruktur weist Mängel auf. Ein erheblicher Mangel liegt z. B. im Fehlen von Informationen über das weitere Schicksal von Vorgängen, die von der Polizei angelegt worden sind. Hier ist insbesondere an den Ausgang gerichtlicher Ent-

scheidungen zu denken (z. B. Freisprüche). Entsprechend einem Beschluß der Innenministerkonferenz wird derzeit vom Senator für Inneres unter Einschaltung des Senators für Justiz und Bundesangelegenheiten geprüft, wie sich ein entsprechendes Rückmeldeverfahren realisieren läßt.

Offengeblieben sind nach der Stellungnahme des Polizeipräsidenten folgende Probleme, die aus meiner Sicht nach wie vor einer Klärung bedürfen:

- deutlichere Trennung des Zugriffs auf Daten Verdächtiger und anderer Personen,
- besondere Behandlung der Daten von Kindern,
- Umfang der Speicherung und Zugriff auf personengebundene Hinweise.

2.4 Der Postaustausch der Behörden: Eine Schwachstelle der öffentlichen Informationsverarbeitung

Das Verfahren des Postaustausches zwischen Berliner Behörden unter Zuhilfenahme der Hauptverteilungsstelle beim Landesverwaltungsamt, an dem verschiedene Bundesbehörden beteiligt sind, gab zu erheblichen datenschutzrechtlichen Bedenken Anlaß.

In einer Reihe von Eingaben wurde darauf hingewiesen, daß Unterlagen mit personenbezogenen Daten verschiedenster Sensitivität regelmäßig in offenen Umlaufmappen oder anderen unverschlossenen Versendungsformen über den Fachaustauschdienst unter den Behörden ausgetauscht würden. So lagen Hinweise z. B. auf die Versendung von schulpsychologischen Gutachten, Vergleichsmitteilungen zur Gewährung des Kindergeldes mit Sozialdaten, EDV-Ausdrucken über Sozialhilfeempfänger, nichtanonymisierten Urteilsabschriften über Straftaten nach dem Betäubungsmittelgesetz vor.

Bereits in meinem Jahresbericht 1982 habe ich auf entsprechende Feststellungen hingewiesen[1].

Im November 1984 habe ich in der Hauptverteilungsstelle beim Landesverwaltungsamt stichprobenweise die durchlaufende Post daraufhin überprüft, ob und wie sie gegen die unbefugte Einsichtnahme geschützt ist.

Dabei wurden von den Mitarbeitern Hunderte von Vorgängen festgestellt, bei denen schutzwürdige personenbezogene Daten im offenen Fachpostverkehr versandt wurden. Absender waren ebenso öffentliche Stellen des Landes Berlin wie öffentliche Stellen des Bundes (Bundesanstalt für Arbeit). Lediglich die Post des Generalbundesanwaltes (Bundeszentralregister) war verschlossen.

Für Daten, die aus Dateien übermittelt werden, schreibt § 5 Abs. 1 BlnDSG angemessene technische und organisatorische Maßnahmen auch für die Sicherung vor unbefugter Kenntnisnahme vor. Ziff. 9 der Anlage zu dieser Bestimmung präzisiert diese Generalklausel dahingehend, daß zu gewährleisten ist, daß bei der Übermittlung sowie beim Transport entsprechender Datenträger personenbezogene Daten nicht unbefugt gelesen, verändert oder gelöscht werden können (Transportkontrolle). Diese unmittelbar für automatisierte Dateien geltende Vorschrift muß sinngemäß auch auf herkömmliche Dateien angewandt werden.

Nur ein Teil der festgestellten Vorgänge erfüllt diese Voraussetzungen (z. B. Mitteilungen in Grundbuchsachen, Mitteilungen über Haftbefehle, Steuerkarten, Einweisungsbeschlüsse gem. § 15 Unterbringungsgesetz, Lebensbescheinigungen einer Meldestelle, Krankenhausrechnungen eines Klinikums an das Sozialamt, Benachrichtigungen über das Vorliegen von Forderungen der Bundesanstalt für Arbeit an die Finanzbehörden, Kostenübernahmerklärungen eines Krankenhauses an das zuständige Bezirksamt, Bewilligungsbescheide der WBK Berlin an Finanzämter, Kostenübernahmeerklärungen der AOK an Kliniken und Krankenhäuser).

Der unverschlossene Versand dieser Unterlagen stellt einen Verstoß gegen das Berliner Datenschutzgesetz (bei Sozialdaten und bei Bundesbehörden: des Bundesdatenschutzgesetzes) dar, weil die in den Unterlagen enthaltenen Daten einem nicht überschaubaren Kreis von Personen offenbart werden können. Zur Einsichtnahme in die in den Unterlagen enthaltenen Daten sind weder die für Botengänge eingesetzten Mitarbeiter der absendenden Behörde oder der empfangenden Behörde noch Mitarbeiter des Landesverwaltungsamts als vermittelnde Behörde befugt. Insbesondere auf Seiten der empfangenden Behörde kann nicht sichergestellt werden, daß zunächst nichtbefugte Mitarbeiter Einsicht in die Unterlagen erhalten.

Soweit die Datenschutzgesetze nicht gelten, weil die Daten nicht aus Dateien übermittelt werden, ist der verfassungsrechtliche Verhältnismäßigkeitsgrundsatz unmittelbar anzuwenden. Wenn besondere Amts- oder Berufsgeheimnisse bestehen (medizinische Daten, statistische Daten, Sozialdaten, Steuerdaten usw.), ergibt sich entweder unmittelbar aus den Geheimhaltungsvorschriften oder aber zumindest mittelbar aus den entsprechenden Strafvorschriften (insbesondere § 203 StGB), daß der Absender für einen hinreichenden Verschluß der Unterlagen zu sorgen hat.

Auch im übrigen wird im Hinblick auf das informationelle Selbstbestimmungsrecht der Betroffenen der Schutz vor unbefugter Einsichtnahme durch das beteiligte Personal durch Verschluß zu gewährleisten sein.

Auf der Ebene der Verwaltungsvorschriften sieht die Gemeinsame Geschäftsordnung für die Berliner Verwaltung vom 4. Dezember 1984 (GGO I, in Kraft seit 1. März 1985) vor, daß auch in Angelegenheiten, für die keine ausdrücklichen gesetzlichen Geheimhaltungsgebote gelten, fremde Geheimnisse, insbesondere die zum persönlichen Lebensbereich gehörenden Geheimnisse zu wahren sind. In diesen Fällen sind verschlossene Umlaufmappen oder verschlossene Umschläge zu verwenden (§ 48). Persönliche oder vertrauliche Schriftstücke sind besonders zu kennzeichnen (§ 68).

Ich habe die festgestellten Mängel gegenüber den absendenden Stellen beanstandet und den Senator für Inneres als für die Geschäftsordnung zuständige Senatsverwaltung unterrichtet. Soweit Bundesbehörden beteiligt sind, sind die entsprechenden Feststellungen dem Bundesbeauftragten vorbehalten. Ich habe ihm die Überprüfungsergebnisse übermittelt.

Ein durch die Datenschutzgesetze ungeklärtes Problem bleibt die Frage, in welchem Umfang die vermittelnde Stelle (hier das Landesverwaltungsamt) befugt oder sogar verpflichtet ist, gegen Verstöße gegen die Transportsicherungspflicht vorzugehen. Es besteht insoweit eine problematische Situation, als datenschutzrechtlich die Postverteilungsstelle als Auftragnehmer (§ 2 BlnDSG) zu betrachten ist, der ausschließlich den Weisungen der Auftraggeber unterliegt. Die Folge ist die, daß der Auftragnehmer keine Veranlassung hat, das Ausmaß der Datensicherung höher anzusetzen, als dies der Auftraggeber vorgibt.

Diese Lage ist unbefriedigend. Es kann nicht akzeptiert werden, daß die den Fachpostverkehr betreibende (und damit auch beobachtende Stelle) offensichtliche Verstöße gegen die Transportsicherung ohne eigene Reaktionen hinnimmt.

Aus diesem Grund muß darauf hingewirkt werden, daß das Landesverwaltungsamt künftig nicht ordnungsgemäß gesicherte Sendungen zurückweist.

Den Senator für Inneres als Aufsichtsbehörde für das Landesverwaltungsamt habe ich aufgefordert, den Fachpostverkehr durch Verwaltungsvorschriften dahingehend neu zu regeln, daß die Teilnehmer sich einerseits verpflichten, hinreichende Transportsicherungsmaßnahmen zu ergreifen, daß das Landesverwaltungsamt andererseits ermächtigt wird, Anlieferungen, die offensichtlich nicht hinreichend gesichert sind, zurückzuweisen.

Die mir bisher vorliegenden Stellungnahmen der betroffenen Verwaltungen lassen erkennen, daß die aufgetretenen Probleme beseitigt werden.

So hat der Senator für Inneres veranlaßt, daß alle Dienstkräfte seines Geschäftsbereiches ausdrücklich darauf hingewiesen werden, sämtliche Schriftstücke und Akten mit personenbezogenen Daten ausnahmslos verschlossen zu versenden.

[1] Jahresbericht 1982, S. 18

Auch die übrigen betroffenen Behörden haben zugesagt, die Mitarbeiter über die aufgetretenen Probleme und die einzuhaltenden Vorschriften zu unterrichten.

Einzelne Bezirksämter wollen darüber hinaus durch eigene Stichproben in den bezirklichen Verteilungsstellen feststellen, ob die Transportkontrolle gewährleistet ist.

Ich gehe davon aus, daß auch die Verwaltungen, die durch meine Stichprobenuntersuchung nicht betroffen waren, ebenfalls geeignete Maßnahmen durchführen.

Unabhängig davon werde ich zu gegebener Zeit auch nochmals überprüfen, ob die festgestellten Mängel beim Fachaustauschverkehr nach alledem beseitigt sind.

2.5 Der Bürger im Visier von Planung und Statistik

Auch in diesem Jahr löste die Frage nach dem zulässigen Umfang der Erhebung personenbezogener Daten für Zwecke der Planung und der Statistik erhebliche Diskussionen aus. Im Mittelpunkt stand naturgemäß die Frage, wann und unter welchen Bedingungen die nächste **Volkszählung** stattfinden sollte. Im Laufe der Monate ergab sich ein politischer Konsens, der zur Verabschiedung des Volkszählungsgesetzes 1987 im September 1985 führte.

Danach findet die nächste Volkszählung am 25. Mai 1987 statt. Sie ist ebenfalls wieder als Totalerhebung angelegt und umfaßt im wesentlichen die gleichen Fragestellungen wie die geplante Volkszählung 1983. Die Durchführung der Volkszählung folgt jedoch den Vorgaben des Bundesverfassungsgerichts, die ihrerseits nicht zuletzt auf den Vorstellungen der Datenschutzbeauftragten zu einer datenschutzgerechten Durchführung einer Volkszählung beruhten.

Offen geblieben ist die auch vom Bundesverfassungsgericht lediglich aufgeworfene und nicht gelöste Frage, in welcher Form eine moderne staatliche Statistik ihre Daten sammelt. Kann sie wirklich nur - wie eine Ordnungsverwaltung - auf der Grundlage spezieller Statistikgesetze mit der Regelung gesetzlicher Auskunftspflicht und Bußgeldandrohung zuverlässig den statistischen Status der Bürger ermitteln? Oder muß sie sich nicht stärker an Methoden der Wirtschaft und der Wirtschaftsforschung orientieren? In welchem Umfang muß eine amtliche Statistik die klassische und wann die anderen Methoden wählen?

Sicher handelt es sich dabei nicht nur um eine Datenschutzfrage, aber das Datenschutzrecht zwingt zu Lösungen, die sich am vom Bundesverfassungsgericht anerkannten Selbstbestimmungsrecht der Bürger an ihren Daten orientieren.

Auch der **Mikrozensus 1985,** der in den beiden Vorjahren u. a. an datenschutzrechtlichen Bedenken gescheitert war, wurde mit einer umfassenden Auskunftspflicht durchgeführt.

Das der Erhebung zugrundeliegende Mikrozensusgesetz 1985 sowie die auf seiner Grundlage erlassene Verordnung, die den Fragenkatalog im einzelnen enthält, entsprechen den Anforderungen des Bundesverfassungsgerichts. Zu erwähnen ist im wesentlichen:

- Es wird zwischen Erhebungsmerkmalen und Hilfsmerkmalen unterschieden.
- Welche Daten abgefragt werden dürfen, ist in der Verordnung genau festgelegt.
- Die Erhebungsstellen sind die Statistischen Landesämter.
- Die Interviewer dürfen nicht in der unmittelbaren Nähe ihrer Wohnung oder bei der Möglichkeit von Interessenkonflikten eingesetzt werden. Sie dürfen die aus der Tätigkeit gewonnenen Erkenntnisse nicht in anderen Verfahren oder für andere Zwecke verwenden.
- Das Gesetz enthält genaue Bestimmungen zur Trennung der Hilfs- von den Erhebungsmerkmalen und zur Löschung der Hilfsmerkmale.

Die relativ geringe Anzahl von Beschwerden bei der Durchführung des Mikrozensus zeigt, daß eine datenschutzfreundliche Ausgestaltung der Erhebung und eine angemessene Aufklärung der Bevölkerung einen großen Beitrag zur Akzeptanz der amtlichen Statistik leisten können. Im Gegensatz zur nächsten Volkszählung sieht das am 10. Juni 1985 verabschiedete Mikrozensusgesetz zusätzlich vor, daß einige Daten probeweise unter 0,25 % der Bevölkerung ohne Auskunftspflicht erhoben werden sollen. Es ist davon auszugehen, daß die weitere Entwicklung der amtlichen Statistik erheblich vom Ergebnis dieser Probeerhebung abhängt.

Weniger positiv zu beurteilen ist die im Frühjahr durchgeführte **Handels- und Gaststättenzählung 1985.** Sie war die erste Bundesstatistik, die nach dem Urteil des Bundesverfassungsgerichts zur Volkszählung als Totalerhebung durchgeführt wurde. Sie war deshalb ein aufschlußreiches Beispiel dafür, wie Zählungen aufgrund bestehender Gesetze durchgeführt werden, die den Grundsätzen des Bundesverfassungsgerichts zu statistischen Erhebungen nicht mehr entsprechen. In einer Entschließung stellte die Konferenz der Datenschutzbeauftragten von Bund und Ländern dazu einige Mängel fest.

So war festzustellen, daß eine Beteiligung der Datenschutzbeauftragten bei der Vorbereitung der Zählung nicht ermöglicht wurde. Verschiedene Aspekte der Zählung (Umfang der Fragen, Trennung der Hilfsmerkmale von den Erhebungsmerkmalen, Löschungsfristen, Nutzung der von den Finanzbehörden bereitgestellten Daten) entsprachen nicht oder nicht in vollem Umfang den heute an eine Statistik zu stellenden Anforderungen.

Im Frühjahr 1986 beabsichtigen mehrere Institutionen, im Auftrag der BVG ein Konzept für den künftigen öffentlichen Personennahverkehr, insbesondere unter Einbeziehung des S-Bahn-Netzes, zu erarbeiten. Als eine wesentliche Grundlage für die Prognose der Verkehrsnachfrage wird eine **Befragung** von ca. 5 % **der Berliner Haushalte** dienen, die - auf freiwilliger Basis Auskunft darüber geben sollen, welche Verkehrsmittel sie benutzen.

Dazu werden die Adressen von ca. 50 000 Personen aus dem Melderegister an ein privates Institut, das mit der Erhebung beauftragt ist, übergeben. Dieser Personenkreis wird über die Ziele der Befragung schriftlich informiert und um Teilnahme gebeten. Einige Tage später werden Interviewer dann die Bürger aufsuchen und einen Fragenkatalog über die benutzten Verkehrsmittel, Wegstrecken und andere relevante Aspekte vorlegen.

Die Fragebögen werden nach der anonymen Übertragung in eine Tabelle vernichtet, so daß keine personenbezogenen Daten mehr vorhanden sind.

Von dem Institut, das die Erhebung und Auswertung durchführt, bin ich frühzeitig über das Gesamtkonzept informiert und um Bewertung der datenschutzrechtlichen Aspekte gebeten worden. Ich habe Empfehlungen für die Durchführung der Erhebung gegeben.

2.6 Archive und Bibliotheken: Schutz für Betroffene und Leser

Zu beachtlichen öffentlichen Diskussionen hat der Datenschutz in zwei Bereichen geführt, die normalerweise nicht im Brennpunkt des öffentlichen Interesses stehen: Der Schutz personenbezogener Daten in Archiven und Bibliotheken. Über den Bedarf an landesgesetzlichen Regelungen auf dem Gebiet des Archivwesens habe ich bereits früher berichtet[1].

Für Berlin wird eine derartige Regelung immer dringlicher, da gerade hier eine große Zahl hochsensibler Archivbestände besteht, ohne daß der Zugang gesetzlich geregelt wäre. Von besonderer Bedeutung sind dabei Unterlagen aus der Zeit des Nationalsozialismus oder aus der Nachkriegszeit mit entsprechendem Bezug. Zur Erläuterung einige Zahlen:

Allein im Berlin Document Center werden ca. 27 Millionen Einzelbestände in Akten oder Karteien verwaltet; in der Wehrmachtsauskunftsstelle befinden sich ca. 20 Millionen Akten; bei den Entschädigungsämtern liegen ca. 210 000 Akten, bei den Entschädigungskammern der Justiz ca. 70 000 Akten; im Krankengeschichtenarchiv der Karl-Bonhoeffer-Nervenklinik befinden sich ca. 100 000 Krankengeschichten, dabei auch die Vorgänge zur Euthanasie. Nicht zu nennen sind hier die nur schwer schätzbaren Unterlagen in den Erbgesundheitsabteilungen der Gesund-

[1] Jahresberichte 1980, S. 18; 1982, S. 20; 1983, S. 10; 1984, S. 3

heitsämter, im Krankenbuchlager, die Rückerstattungsakten des Obersten Rückerstattungsgerichts sowie natürlich auch die Akten, die sich schon beim Landesarchiv befinden. Grob geschätzt warten ca. 50 bis 60 Millionen Einzelbestände personenbezogener Unterlagen auf eine gesetzliche Archivierungsregelung in Berlin, ohne die eine wissenschaftliche Aufarbeitung dieses dunklen Kapitels der deutschen Geschichte nicht möglich ist.

Daß auch die Erforschung der Bewältigung der Folgen dieser Zeit große Probleme aufwirft, zeigt ein Forschungsprojekt, das auf die Aufklärung der Gründe zielte, aus denen Entschädigungen für Naziopfer gewährt oder verweigert wurden. Forschungsgegenstand sollten die Akten der Justiz zu entsprechenden Prozessen sein. Da mehr oder weniger in jeder Entschädigungs- bzw. Wiedergutmachungsakte ärztliche Gutachten enthalten sind, kann die Einsichtnahme nur mit Einwilligung des Betroffenen gewährt werden. Auch bei Berücksichtigung des § 299 ZPO scheitert eine Einsicht in Gerichtsakten an dem aus Art. 2 Abs. 1 GG abgeleiteten allgemeinen Persönlichkeitsrecht. Danach gehört die Entscheidung über die Weitergabe ärztlicher Gutachten grundsätzlich zum „unantastbaren Bereich privater Lebensgestaltung“[1], so daß auch hier - ohne spezialrechtliche Regelung – eine Einsicht nur mit Einwilligung des Betroffenen möglich ist. Nur ein Archivgesetz könnte einen gewissen Zugang zu den Daten ermöglichen.

Dem Bundestag liegt zur Beratung der Entwurf für ein Bundesarchivgesetz vor; im Oktober sind Sachverständige dazu angehört worden.

Der Senator für Kulturelle Angelegenheiten hat noch in der vergangenen Legislaturperiode einen Vorentwurf für ein Berliner Archivgesetz erarbeitet, der sich eng an einen „Entwurf eines bundeseinheitlichen Gesetzes über die Sicherung und Nutzung von Archivgut“ anlehnt, den ein besonderer Arbeitskreis der Konferenz der Datenschutzbeauftragten erarbeitet hatte. Die weitere Erörterung dieses Entwurfs ist auch vom Fortgang auf Bundesebene abhängig, da insbesondere bei den Fristen, ab denen die Nutzung des Archivgutes für jedermann oder für bestimmte Zwecke gestattet sein soll, eine einheitliche Regelung erforderlich ist. Unter Hinweis auf das Kunsturhebergesetz neigt der Senator für Kulturelle Angelegenheiten bei Archivgut, das Verstorbene betrifft, zu einer relativ kurzen Schutzfrist.

In meiner Stellungnahme zu dem Vorentwurf habe ich vertreten, daß für die Einsichtnahme im Rahmen eines Forschungsprojektes eine derart kurze Frist akzeptiert werden kann, wenn entsprechende Rahmenbedingungen vorliegen. Ich habe folgende Formulierung vorgeschlagen:

> „Im Einzelfall oder bei bestimmten Archivgruppen kann die Nutzung des Archivgutes vor Ablauf der Sperrfrist nach § 7 Abs. 3 und 4 durch das Landesarchiv genehmigt werden, wenn ein rechtlicher, wirtschaftlicher, kultureller oder gesellschaftlicher Vorgang erforscht werden soll, der über den privaten Bereich eines Betroffenen hinaus eine besondere öffentliche Bedeutung erlangt hat und daher für das Verständnis der Gegenwart und der Zeitgeschichte von erheblicher Bedeutung ist. Bei personenbezogenen Daten, die einem besonderen Schutz unterliegen, darf die Frist nicht auf einen Zeitraum von unter zehn Jahren nach dem Tod des Betroffenen verkürzt werden. Die Genehmigung darf nur anerkannten unabhängigen Forschungsinstituten erteilt werden.“

Durch Berliner Behörden wird auch landesfremdes Archivgut verwaltet. Sofern eine vertragliche Regelung über die Nutzung nicht getroffen wurde, muß das Archivgesetz Nutzungskriterien zur Verfügung stellen, nach denen einheitlich verfahren werden kann. Dies betrifft vor allem auch das Berlin Document Center, für welches dem Senator für Inneres in bestimmten Fällen von den Alliierten die Verfügungsgewalt übertragen wurde. Damit alliierte Vorbehaltsrechte oder zwischenstaatliche Vereinbarungen bei der Regelung des Zugangs zum Berlin Document Center nicht beeinträchtigt werden, habe ich folgende Formulierung empfohlen:

> „Die Benutzung des im Landesarchiv gelagerten Archivgutes bedarf der Genehmigung durch das Landesarchiv Berlin. Soweit andere Behörden oder öffentliche Stellen des Landes Berlin befugt sind, über die Nutzung von Archivgut zu entscheiden, das von anderen Stellen aufbewahrt wird, ist über den Nutzungsantrag entsprechend den nachfolgenden Bestimmungen zu entscheiden. Bestehende Informationsrechte oder besondere Vereinbarungen mit Eigentümern privaten Archivgutes bleiben unberührt.“

[1] BVerfGE 27, 350 ff.

3. Beobachtungen beim Betrieb von Bildschirmtext und bei der Entwicklung anderer Neuer Medien

Gemäß § 3 Abs. 3 Satz 3 Bildschirmtext-Zustimmungsgesetz und § 55 Abs. 1 Satz 1 Kabelpilotprojektgesetz berichte ich im folgenden dem Abgeordnetenhaus von Berlin über festgestellte Mängel und über meine Vorschläge zur Verbesserung des Datenschutzes bei Bildschirmtext und dem Kabelpilotprojekt.

3.1 Bildschirmtext

Situation

Die Verbreitung von Bildschirmtext ist bisher hinter den Erwartungen zurückgeblieben. Im September 1985 betrug die Teilnehmerzahl ca. 33 000. Dies hat einerseits zur Folge, daß die Bedeutung datenschutzrechtlicher Probleme durch die noch geringe Verbreitung des Dienstes relativiert wird, daß aber andererseits die Möglichkeiten zur Korrektur einzelner Mängel oder Fehlentwicklungen noch besser gegeben sind.

Die von mir im Jahresbericht 1984 ausführlich dargestellten Defizite hinsichtlich der bundesrechtlichen Regelungen über Bildschirmtext sind bisher nicht beseitigt worden. Nach wie vor ist der rechtliche Handlungsrahmen der Deutschen Bundespost nicht mit den Regelungen des Bildschirmtext-Staatsvertrages vergleichbar. Es gilt allerdings die Zusage der Deutschen Bundespost, daß sie nach den in Art. 9 Bildschirmtext-Staatsvertrag enthaltenen Grundsätzen zum Datenschutz bei Bildschirmtext handeln würde. Die Praxis steht nicht im Widerspruch zu dieser Zusage.

Fortschritte

Bei verschiedenen Gesprächen zwischen Vertretern der Konferenz der Datenschutzbeauftragten von Bund und Ländern mit Vertretern der Deutschen Bundespost und des Bundesministeriums für das Post- und Fernmeldewesen wurde deutlich, daß die anfangs starre Haltung der Deutschen Bundespost gegenüber den Datenschutzinstanzen einer kooperativeren Politik weichen würde. Dies ist mit Abstrichen auch für das Informationsgebaren der Deutschen Bundespost hinsichtlich technischer Fragen gegenüber den Landesdatenschutzbeauftragten bei der Behandlung von Einzelfällen festzustellen. Nach wie vor fehlen jedoch verbindliche schriftliche Unterlagen über interne technische Zusammenhänge des Bildschirmtextsystems, so insbesondere das Bildschirmtext-Host-Handbuch. Nur diese würden es möglich machen, die Einhaltung des Bildschirmtext-Staatsvertrages durch die Deutsche Bundespost, Anbietern und Teilnehmern zu beobachten oder die datenschutzrechtliche Relevanz von Bürgereingaben zu den Gebaren von Post, Anbietern und Teilnehmern auch ohne wohlwollendes Entgegenkommen der Deutschen Bundespost im Einzelfall zu bewerten.

Im April 1985 sind von der Deutschen Bundespost verschiedene Verbesserungen der Software des Bildschirmtextsystems vorgenommen worden, die auch den Datenschutz betreffen. So wird nunmehr die Definition bestimmter leicht erratbarer Kennwörter wie Folgen gleicher Zahlen und Buchstaben, aufsteigende oder absteigende Folgen von Zahlen und Buchstaben, bereits vom System abgewiesen. Zusammen mit der Beseitigung des offensichtlichen Systemmangels, der unter bestimmten Voraussetzungen bei der Verwendung des Editiersystems zur zufälligen Einspielung fremder Teilnehmerdaten führte, sind damit Verbesserungen des Schutzes vor unbefugter Verwendung des Systems erreicht worden. Weitere Verbesserungen wären hier allerdings noch durchführbar und wünschenswert.

Die Einblendung des genauen Zeitpunktes einer Seitenaktualisierung durch den Anbieter bei jedem Aufruf der Seite - ein

Merkmal, welches gelegentlich Anlaß von Bürgerbeschwerden war - ist ebenfalls mit der Systemmodifizierung im April 1985 beendet worden.

Die Deutsche Bundespost hat ferner im Rahmen ihrer Programmumstellung wirksame Maßnahmen ergriffen, um die nachträgliche Veränderung von Mitteilungen durch den Absender zu verhindern.

Eine weitere Softwareänderung im Oktober 1985 hat zu einer zusätzlichen Verbesserung geführt:

Die Umgehung der alten Schutzmaßnahmen oder die häufige Kennworterprobung wird nunmehr damit verhindert, daß nach neun Fehlversuchen pro Tag der Anschluß gesperrt wird.

Defizite

Neben den ausstehenden Fortschritten bei der **bundesrechtlichen** Regelung des Datenschutzes bei Bildschirmtext ist als Defizit festzuhalten, daß verschiedene im Jahresbericht 1984 bereits ausführlicher dargestellte Mängel des Schutzes vor unbefugter Verwendung des Systems (Art. 9 Abs. 8 Bildschirmtext-Staatsvertrag) noch nicht behoben worden sind:

- Abhörbarkeit von Anschlußkennung und geheimem Kennwort (fehlende Verschlüsselung),
- fehlende Unterrichtung des richtigen Anschlußinhabers bei Versuchen, sein Kennwort auszuforschen,
- fehlender besonderer Schutz der Editierfunktion. Daran ändert auch die Systemänderung von Oktober 1985 nichts, wonach für die Durchführung des Editierens die erneute Eingabe des persönlichen Kennwortes erforderlich ist. Wirksam ist der Schutz nur, wenn es sich dabei um ein anderes Kennwort als das für die Teilnehmernummer handeln würde. Eine solche Änderung des Verfahrens ist allerdings von der Deutschen Bundespost angekündigt.

Diese Defizite der Zugriffskontrolle bei Bildschirmtext, die noch im Verantwortungsbereich der Deutschen Bundespost liegen, werden in Zukunft weiter abgebaut, wenn die Berechtigungs-Chip-Karte für Bildschirmtext angeboten wird. Die Realisierung des Projekts ist bereits in Auftrag gegeben, so daß frühestens ab 1987 die Einführung der Chipkarte erwartet werden kann. Bei den bekannt gewordenen Fällen der mißbräuchlichen Verwendung von Bildschirmtext-Anschlüssen ist allerdings der leichtsinnige Umgang von Teilnehmern mit den angebotenen Sicherungstechniken Hauptursache von solchen Mißbräuchen:

- Der von Presse und Rundfunk mit Aufmerksamkeit verfolgte Fall, in dem ein Hamburger „Hacker-Club" unter der Identität eines Kreditinstituts für 135 000,– DM gebührenpflichtige Seiten zu seinen Gunsten abgerufen hat - auf das Geld wurde verzichtet, es ging um die Öffentlichkeitswirkung - erwies sich, nachdem die Deutsche Bundespost dem zuständigen Hamburgischen Datenschutzbeauftragten die erbetenen technischen Auskünfte endlich erteilt hatte, nicht als Folge eines Systemfehlers, der zu dem Zeitpunkt tatsächlich beobachtet wurde, sondern als Folge unbedachten Umgangs mit dem geheimen Kennwort bei der Demonstration des Bildschirmtextdienstes durch das Kreditinstitut.
- Von einem öffentlichen Bildschirmtextterminal eines Berliner Unternehmens konnte ein Benutzer das offensichtlich lückenhafte Programm zur Abwehr unerwünschter Aufrufe kostenpflichtiger Seiten umgehen und so einem Anbieter in großem Umfang Spenden zukommen lassen.
- In einem weiteren Fall beklagte ein Berliner Teilnehmer, daß ein Dritter unter seiner Teilnehmerkennung gebührenpflichtige Seiten aufgerufen - und sogar sein persönliches Kennwort geändert habe. Dies war möglich, weil er sich dem System gegenüber als freizügig deklariert hatte, um von fremden Anschlüssen aus das Bildschirmtextsystem benutzen zu können und darüber hinaus sein persönliches Kennwort unbedacht weitergegeben hatte.

Von grundsätzlicher Bedeutung ist die an mich herangetragene Frage, ob in Fällen mißbräuchlicher Verwendung von der Deutschen Bundespost rekonstruiert werden kann, von welchem Anschluß aus wann mit welcher Identität das Bildschirmtextsystem genutzt wurde. Die Deutsche Bundespost hat einem Petenten gegenüber erklärt, daß dies grundsätzlich möglich, aus datenschutzrechtlichen Gründen jedoch zweifelhaft sei. Eine abschließende Klärung steht noch aus.

Weitere, im Jahresbericht 1984 dargestellten Probleme sind nach wie vor aktuell:

- Die Speicherung von Abrechnungsdaten im Entgelt- und Gutschriftensatz in der Bildschirmtext-Leitzentrale erfolgt immer noch differenziert nach Leitseiten. Da ein Anbieter sein Programm durch Verwendung diverser Leitseiten inhaltsbezogen differenzieren kann, ist dieser Widerspruch zu Art. 9 Abs. 3 Satz 1 Bildschirmtext-Staatsvertrag noch nicht behoben.
- Verschiedene Eingaben und Hinweise von Bildschirmtextteilnehmern haben erneut auf die Praxis unseriöser Anbieter hingewiesen, Antwortseiten so zu gestalten, daß bei der Absendung der Antwortseite personenbezogene Daten des Absenders unbemerkt von ihm an den Anbieter übermittelt werden. Erneut wurde gegen Art. 9 Abs. 8 Nr. 2 Bildschirmtext-Staatsvertrag verstoßen, indem die Daten farbgleich zum Hintergrund eingeblendet wurden und so nicht erkannt werden konnten, wenn nicht die Attributtaste des Bildschirmtext-Endgerätes gedrückt wurde.

Zwei weitere Praktiken zur unbemerkten Erlangung von personenbezogenen Daten von Absendern von Antwortseiten sind mir vorgeführt worden. Konkrete Verstöße gegen den Staatsvertrag aufgrund dieser Tricks sind bisher nicht bekannt geworden. Aus Gründen der Sicherheit werden diese Praktiken hier nur grob beschrieben:

- Mit Hilfe von sogenannter Telesoftware veranlaßt der Anbieter solcher Software intelligente Decoder der abrufenden Teilnehmer zur unbemerkten Absendung von Antwortseiten mit Absenderangaben[1].
- Anbieter lassen sich personenbezogene Absenderdaten unsichtbar auf der ersten Zeile der Antwortseite übermitteln. Sichtbar ist auf dieser Zeile sowohl für Absender als auch für den Empfänger der von der Post automatisch dort eingeblendete Name des empfangenden Anbieters. Die Kenntnisnahme der unsichtbar übertragenen Daten erfolgt unter Verwendung von Personalcomputern beim Empfänger.

Eine weniger besorgniserregende, aber überaus lästige Praxis ist die massenweise Übermittlung von Werbemitteilungen (Rundsendungen) im Mitteilungsdienst, ohne daß der Teilnehmer die Möglichkeit hat, sich dagegen zu wehren. Mitteilungen müssen in einem relativ zeitraubenden Verfahren abgerufen werden, bevor man sie löschen kann und somit Platz in seinem eigenen Mitteilungsspeicher schaffen kann. Nach eigenen Beobachtungen ist davon auszugehen, daß mehr als 90 % aller empfangenen Mitteilungen ungezielte Rundsendungen sind, die von Bildschirmtextwerbeträgern unter Verwendung von Computern in das System eingebracht werden. Eine übergreifende Einrichtung, die mit der Robinson-Liste des Allgemeinen Direktwerbe- und Direktmarketing-Verbandes e.V. zur Abwehr schriftlichen Werbematerials vergleichbar wäre, existiert bisher immer noch nicht. Lediglich einige Btx-Werbeagenturen haben für sich solche Listen eingerichtet, in die man sich über Bildschirmtext eintragen kann. In der dringenden Empfehlung an die Deutsche Bundespost, zentral eine solche Möglichkeit zur Abwehr aller oder bestimmter Werbemitteilungen zu schaffen, sehe ich eine Anregung, die auch der Akzeptanz des Dienstes förderlich sein kann.

Ausblick

Die zukünftige Ausgestaltung des Bildschirmtext-Dienstes ist auch unter dem Aspekt zu betrachten, daß in wenigen Jahren mit dem ISDN (Integrated Services Digital Network) für die Telekommunikation einschließlich des Fernsprechens ein wesentlich leistungsfähigeres digitales Netz mit erheblich höheren Datenübertragungsraten bereitstehen wird. Dies wird auch nicht ohne Einfluß auf Bildschirmtext sein. Die Datenschutzbeauftragten in Bund und Ländern bereiten sich derzeit auf die Einführung

[1] Vgl. Jahresbericht 1984, S. 15

dieses Netzes vor, um den technischen und rechtlichen Regelungsbedarf zu erkunden. Dabei werden folgende Überlegungen von Bedeutung sein.

Der vorgesehene Ausbau der Kommunikationsinfrastruktur läßt erwarten, daß eine Vielfalt von neuen Kommunikationsdiensten eingerichtet werden wird, die verschiedene Formen administrativer, industrieller und privater Kommunikation befriedigen sollen. Die bestehenden oder derzeit in Erprobung befindlichen Kommunikationsdienste (z.B. Telefon, Telex, Teletext, TEMEX, Telefax, Bildschirmtext, Datex-L und -P) werden durch das neue integrierende Netz mit größerem Leistungsumfang ausgestattet werden und weitere Dienste könnten erfunden und eingeführt werden. Die rechtlichen Regelungen zu diesen Diensten werden an die neuen Verhältnisse anzupassen sein oder neu formuliert werden müssen. Dies gilt auch für die datenschutzbezogenen Regelungen.

Die Einflußnahme der Datenschutzbeauftragten auf die datenschutzgerechte Gestaltung eines Kommunikationsdienstes sowie seiner organisatorischen und rechtlichen Umgebung erfaßt

- Gestaltungsempfehlungen zur datenschutzgerechten technischen Gestaltung des Dienstes,
- Empfehlungen zur organisatorischen Einbettung der Dienste,
- Aufzeigen des rechtlichen Regelungsbedarfs,
- Empfehlungen zur rechtlichen Regelung.

Ein solcher Anspruch läßt sich nur einlösen, wenn die Erfahrungen aus den datenschutzrechtlichen Beratungen zum Bildschirmtext-Staatsvertrag und zum Kabelpilotprojektgesetz durch die Ableitung allgemeinerer Prinzipien auf die Behandlung weiterer neuer Medien übertragen werden können.

Zunächst muß unterschieden werden zwischen neuen Diensten, bei denen Teilnehmer untereinander in gleichberechtigter Weise kommunizieren (Teilnehmerdienste, z.B. Fernsprechen, Datex-Dienste, Telefax, Teletext, Bildschirmtext-Mitteilungsdienst) und solchen, bei denen Anbieter eine Dienstleistung bereithalten, die von Teilnehmern genutzt werden kann (z.B. Bildschirmtext, Kabelfernsehen, TEMEX).

Personenbezogene Daten, auf deren Schutz datenschutzrechtliche Bestimmungen und technisch-organisatorische Maßnahmen zu richten sind, fallen bei solchen Diensten in verschiedenen Zusammenhängen an:

- Inhalte von Kommunikationsvorgängen und Informationsangeboten bei Betreibern, Anbietern und Teilnehmern,
- Abrechnungsdaten bei Betreibern und Anbietern,
- Teilnehmerstammdaten bei Betreibern und Anbietern,
- Anbieterstammdaten bei den Betreibern,
- Verbindungsdaten bei den Betreibern.

Daraus ergeben sich datenschutzbezogene Risikofelder:

- Offenbarung von personenbezogenen Daten im Angebot bei Anbieterdiensten,
- Offenbarung von Kommunikationsinhalten bei Teilnehmerdiensten oder von Daten über die Inanspruchnahme von Angeboten bei Anbieterdiensten gegenüber Dritten,
- Rückschlüsse auf Verhaltensmerkmale (Persönlichkeitsprofile) von Personen aufgrund differenzierter Abrechnungsdaten und aufgrund von Verbindungsdaten,
- Nutzung technischer Schwachstellen zum unbefugten Zugriff auf personenbezogene Daten.

Für die Beherrschung dieser Risikobereiche ergeben sich daraus folgende Schlußfolgerungen:

1. In der Gestaltungsphase eines Dienstes ist darauf hinzuwirken, daß das Design so gewählt wird, daß für Abrechnungs- oder Verbindungszwecke möglichst wenig Daten erforderlich sind. Die verbleibenden erforderlichen Daten sollen möglichst wenig zu einem Persönlichkeitsprofil des Benutzers beitragen. Die Verbindungsdaten sind nach Beendigung der Verbindung nicht mehr weiter erforderlich und sollten dann automatisch physisch gelöscht werden.
2. Es sollte in der Designphase ferner berücksichtigt werden, daß Abrechnungsdaten bzw. andere nutzungsbeschreibende personenbezogene Daten - wenn überhaupt - nur dort anfallen, wo aufgrund der rechtlichen Struktur, der Interessenlage und der technischen Kompetenz davon ausgegangen werden kann, daß die Wahrscheinlichkeit eines Mißbrauchs und die Verlockung dazu möglichst gering ist. Durch eine derartige Konzentration ist die Effektivität der Kontrolle besser sicherzustellen. Z.B. ist es als vorteilhaft anzusehen, daß die Deutsche Bundespost als Betreiber von Bildschirmtext auch die Speicherung der Abrechnungsdaten über die Inanspruchnahme der Angebote übernimmt, also die anfallenden finanziellen Transfers zwischen Anbietern und Teilnehmern vermittelt.
3. Die genannten Maßnahmen zur technischen Gestaltung eines Dienstes, die die Datenschutzrisiken von vornherein reduzieren sollen und die zur Abwehr unbefugter Handlungen in technische und organisatorische Maßnahmen zum Datenschutz umzusetzenden Kontrollanforderungen müssen ebenso wie der Umgang mit personenbezogenen Daten in allen Zusammenhängen des Dienstes rechtlich geregelt sein. Damit können rechtmäßiger Gebrauch und Mißbrauch der Daten eindeutig voneinander getrennt werden.
4. Teilnehmer, Betreiber und Anbieter haben im Rahmen ihrer Verantwortung technische und organisatorische Maßnahmen zu realisieren, die nötig sind, um die unbefugte Offenbarung von personenbezogenen Daten zu verhindern.

Ein wesentlicher Beitrag zur Sicherung des authentischen Zugangs zu solchen Kommunikationsdiensten, so auch des zukünftigen Bildschirmtext-Dienstes wird in dem Einsatz von **Chipkarten** gesehen. Es wird erwartet, daß solche Chipkarten, ausgestattet mit Speichern und Prozessoren, sehr flexible Anwendungsmöglichkeiten finden werden, z.B.

- Identifikation und Authentifikation von Teilnehmern eines Dienstes,
- Verschlüsselung von sensitiven Daten, z. B. geheime Kennworte,
- Zählen von verbrauchten Gebühreneinheiten.

Der Einsatz der Chipkarte spielt auch im beispielhaften Konzept des österreichischen Bildschirmtext-Dienstes eine Rolle, der heute bereits den anonymen Zugang zum System zuläßt, solange nicht kostenpflichtige Seiten aufgerufen werden oder Mitteilungen versandt werden. In diesen Fällen muß sich der Teilnehmer nach wie vor identifizieren und hinterläßt in der Bildschirmtextzentrale seine persönlichen Daten.

Mit dem Einsatz einer kostenpflichtigen Chipkarte, deren „Kapital" mit der sukzessiven Abbuchung der Gebühren für gebührenpflichtige Seiten aufgezehrt wird, ließe sich auch ein sicheres Konzept zum anonymen Aufruf gebührenpflichtiger Seiten realisieren. Hinzu kommt die Überlegung, übersandte Mitteilungen statt in der Bildschirmtextzentrale im Endgerät des Empfängers zu speichern, bis dieser sie löscht, so daß der Dienst aus der Sicht der Bildschirmtextzentrale vollständig anonymisiert gestaltet werden kann.

Dieser österreichische Ansatz zeigt, daß bereits bei der technischen Gesamtkonzeption eines Dienstes entscheidende Weichen zugunsten des Datenschutzes gestellt werden können.

Es erscheint geboten, daß diese besonders datenschutzfreundlichen Aspekte des österreichischen Konzepts auch beim Ausbau des Bildschirmtextsystems mit dem Ziel der Übernahme erwogen werden.

3.2 Fernwirkdienst TEMEX

Die Erprobung des Fernwirkdienstes der Deutschen Bundespost TEMEX (Telemetry Exchange) wird in der nächsten Zeit in verschiedenen Städten beginnen. Im Rahmen von Systemversuchen, in denen die Art der Dienstleistung von TEMEX erkundet und Sinn und Bedarf des Dienstes ermittelt werden sollen, wer-

den die Städte München und Ludwigshafen als erste den Fernwirkdienst im Zusammenwirken mit der Deutschen Bundespost erproben. Weitere Städte - auch Berlin - beabsichtigen die Erprobung von TEMEX im Rahmen von Betriebsversuchen, in denen die technischen Bedingungen des Verfahrens erprobt und eine Vielfalt von Anwendungsformen und Endgeräten auf Tauglichkeit und Marktgerechtigkeit geprüft werden sollen.

In vereinfachter Darstellung wird TEMEX in folgender Weise abgewickelt:

Durch ein Endgerät im Hause oder der Wohnung des Teilnehmers werden die TEMEX-Daten erfaßt. Welcher Art das Endgerät oder die TEMEX-Daten sind, hängt von der Art des Dienstangebotes des TEMEX-Anbieters ab. So kann z. B. über Sensoren geprüft werden, ob ein bestimmtes Ereignis eingetreten ist (Alarmmeldungen) oder der Stand von Meßeinrichtungen und Zählern abgelesen werden. Die erfaßten Daten werden an einem TEMEX-Netzabschluß in die Telefonleitung eingespeist, ohne daß dabei der Fernsprechdienst beeinträchtigt wird. Die Daten werden zunächst an die zuständige Ortsvermittlungsstelle übertragen, dort von den Fernsprechsignalen getrennt und danach in der TEMEX-Unterzentrale (einem Rechner) daraufhin überprüft, ob sie ignoriert werden können (etwa bei Alarmdiensten, wenn alles in Ordnung ist) oder an eine TEMEX-Hauptzentrale weitergeleitet werden müssen. In der Unterzentrale erfolgt abgesehen von Pufferungen keine Datenspeicherung.

In der Hauptzentrale wird ermittelt, wer der absendende TEMEX-Anschluß war und für welchen TEMEX-Anbieter die Daten bestimmt sind. Dann werden die Daten nach Vereinbarungen behandelt, die zwischen dem Betreiber, also der Post, und dem Anbieter getroffen wurden. In der Regel wird es sich dabei um Modalitäten für die unverzügliche Weiterleitung an den Anbieter oder die Zwischenspeicherung der TEMEX-Daten handeln. Die Operationen der Hauptzentrale werden über eine Stammdatei der Teilnehmer und Anbieter gesteuert. In der Hauptzentrale erfolgt ferner die Gebührenabrechnung. Die weiteren, vom Angebot abhängenden Reaktionen des Anbieters auf die eingehenden TEMEX-Daten sind dann Sache der Ausgestaltung des Vertrages zwischen Teilnehmern und Anbietern.

In Berlin ist ebenfalls ein TEMEX-Betriebsversuch vorgesehen. Mehrere Firmen haben als Anbieter Interesse an dem Versuch bekundet. In § 53 Kabelpilotprojektgesetz besteht bereits eine Datenschutzvorschrift für solche Versuche. Im Zusammenhang mit Planungen für den Betriebsversuch haben mit der Deutschen Bundespost und den zuständigen Senatsverwaltungen für Wirtschaft und Arbeit und für Kulturelle Angelegenheiten Gespräche stattgefunden.

Auf Seiten der Bundespost ist bisher wenig Bereitschaft vorhanden, ihre Versuchsplanung unter die Schutzwirkung dieser Regelung zu stellen. Ich habe versucht, verständlich zu machen, daß angesichts des hohen Risikos für die Persönlichkeitssphäre Betroffener eine angemessene Akzeptanzquote bei diesem neuen Kommunikationssystem nur dann erreicht werden kann, wenn durch Schutzvorschriften sichergestellt ist, daß widerrechtliche Eingriffe in die Privatsphäre unterbunden werden können und die Systeme von Anfang an so ausgelegt werden, daß der Betroffene „Herr der Wirkungsweise" dieser Systeme bleibt und nicht zum bloßen Objekt ferngesteuerter Meß- und Wirkvorgänge wird. So habe ich die Auslegung und Anwendungsformen des § 53 Kabelpilotprojektgesetz mehrfach erörtert, um verständlich zu machen, daß durch diese Regelung eine ausgewogene Gestaltung der Interessen der Anbieter und Nutzer erreicht wurde. Mit einem der Interessenten, den Berliner Wasserwerken, die z. Z. als wichtigster Anbieter in Berlin in Frage kommen, habe ich Gespräche über datenschutzrechtliche Anforderungen beim Einsatz von fernlesbaren Wasseruhren geführt.

Das Gesetz geht in § 53 Kabelpilotprojektgesetz davon aus, daß beim Betroffenen ein Gerät installiert sein muß, welches anzeigt, wann es in Betrieb ist (durch eine Lampe, einen Zeiger etc.), und daß es grundsätzlich durch den Betroffenen abschaltbar sein soll. Unter Berücksichtigung einer Analyse der Risiken des Fernlesens der beim Wasserverbrauch aufgelaufenen akkumulierten Meßwerte, insbesondere unter Berücksichtigung der Tatsache, daß in Berlin im Regelfall der Wasserverbrauch sich auf mehrere Wohnungen verteilt, erscheint es mir vertretbar, den § 53 Abs. 3 Kabelpilotprojektgesetz dahingehend auszulegen, daß eine Abschaltvorrichtung in diesem speziellen Fall nicht erforderlich ist. Voraussetzung dafür ist jedoch eine entsprechend klare Regelung des „Vertragszwecks" im Sinne des § 53 Abs. 3 Satz 1 letzter Halbsatz. Ich habe empfohlen, dementsprechend einen Mustervertrag für die Testzeit und einen Mustervertrag für die folgende Zeit zu entwerfen. Wird auf die Abschaltvorrichtung im Hinblick auf den vereinbarten Vertragszweck verzichtet, so gewinnt die „Betriebsanzeige", durch die ein Teilnehmer erkennen kann, wann ein Dienst in Anspruch genommen wird, besonderes Gewicht. Sie ist gesetzlich unverzichtbar und sollte in ihrer technischen Gestaltung dem Gefährdungspotential und der Sensibilität der anfallenden Daten entsprechen. Der Bürger soll dadurch auf einfache Weise davon in Kenntnis gesetzt werden, daß eine Übertragung von Meßdaten stattfindet oder stattgefunden hat. Wenn möglich sollte angezeigt werden, wie häufig eine Übertragung erfolgte. Zu begrüßen wäre es, wenn auch das letzte übertragene Meßergebnis für den Bürger ablesbar wäre.

Gerade diesen Zweig der „Neuen Medien" werde ich im Hinblick auf die damit verbundenen Gefahren auch in Zukunft besonders beobachten.

3.3 Kabelpilotprojekt Berlin

Am 28. August 1985 begann in Berlin das Kabelpilotprojekt mit der Übertragung der fünf über den Äther empfangbaren Fernsehprogramme sowie weiterer nur über Kabel empfangbarer Programme über das in Berlin bereits installierte Kabelnetz. Bei diesen Programmen handelt es sich vorläufig um reine Verteilprogramme, so daß datenschutzrechtlich bedeutsame Risiken, wie z. B. die Möglichkeit zur personenbezogenen Erfassung von Sehgewohnheiten, noch keine Bedeutung haben. Im derzeitigen Stadium ist insbesondere zu prüfen, ob im Inhalt der Fernsehprogramme personenbezogene Daten nur entsprechend der für Übermittlungsvorgänge geltenden Vorschriften über den Datenschutz offenbart werden (§ 52 Abs. 4 Kabelpilotprojektgesetz).

Die Entscheidung, mit welchen Konvertern die Hausverteilung von Pay-TV und Pay-per-view in Berlin vorgenommen werden soll, ist noch offen. Nachdem der bei anderen Kabelpilotprojekten eingesetzte sogenannte FAT-Konverter aus technischen Gründen in Berlin nicht einzusetzen war, soll ein anderes Modell eingesetzt werden. Bei diesem Modell handelt es sich um ein Gerät, welches Funktionen eines Konverters und eines Decoders vereinigt. Das Gerät empfängt ein von einem Rechner der Zentrale an den bestimmten Teilnehmer adressiertes Signal, wählt den gewünschten Kanal an und entschlüsselt dann das verschlüsselt eingehende Programm. Die Wünsche des Teilnehmers würden nicht über einen im Kabel integrierten Rückkanal, sondern auf anderem Wege (Telefon, Postkarte etc.) an die Zentrale gerichtet werden. Die Entscheidung über die fernmeldetechnische Zulassung dieses Konverters durch das FTZ war bei Drucklegung des Berichts jedoch noch nicht getroffen und es bestand Unsicherheit darüber, ob eine positive Entscheidung fallen würde.

Nach Angaben der Projektgesellschaft Kabelkommunikation wäre bei einer negativen Entscheidung noch völlig offen, wie Pay-TV und Pay-per-view in Berlin realisiert werden.

Das dann denkbare Spektrum technischer Lösungen reicht vom zentralgesteuerten Dienst mit Rückkanal, der die Speicherung differenzierter Benutzerdaten erforderlich macht, bis zur dezentralen Erfassung der Kosten (z. B. mit Hilfe von Chipkarten), wobei nur kurzfristig anschlußbezogene Verbindungsdaten über Rückkanal an den Betreiber zu übermitteln wären.

Erst wenn klar ist, mit welchen technischen Methoden Pay-TV und Pay-per-view realisiert werden sollen, kann ich bei dieser Entscheidungslage zu den datenschutzrechtlichen Problemen dieser Dienste Stellung beziehen.

3.4 Workshop „Datenschutz und Neue Medien"

Im Rahmen der Internationalen Funkausstellung wurde erstmals das „Medienforum Berlin" veranstaltet, an dessen Planung und Durchführung ich beteiligt war. In einem ganztägig durchgeführten Workshop „Datenschutz und Neue Medien" wurde

internationalen Experten auf dem Gebiet des Mediendatenschutzes, in der Mehrheit Mitarbeiter der jeweiligen Datenschutzbehörden, Gelegenheit gegeben, Einzelprobleme aus der Sicht ihres Landes darzustellen.

Die sehr erfolgreiche Veranstaltung, bei der auch der Senator für Kulturelle Angelegenheiten die Bedeutung des Datenschutzes für eine vorurteilsfreie Akzeptanz der Neuen Medien unterstrich, dokumentiert die internationale Bedeutung des Problems: Ein großer Teil der von mir beobachteten Probleme und Mängel der Neuen Medien sind auch in anderen europäischen Ländern Gegenstand der Erörterung. So wurde von mißbräuchlicher Verwendung elektronischer Mitteilungsdienste (Großbritannien), Problemen der privaten Nutzung von Bildschirmtext für die Geschäftsabwicklung (Schweiz), der Zweckentfremdung der bei der Kabelkommunikation anfallenden Nutzungsdaten (USA, Kanada), der versteckten Speicherung von Benutzungsdaten (Frankreich) und Problemen der Anonymisierung (Österreich) berichtet.

Die anwesenden Vertreter der in- und ausländischen Datenschutzbeauftragten hatten am Vortag eine Beschlußvorlage für die internationale Konferenz der Datenschutzbeauftragten Ende September 1985 in Luxemburg erarbeitet, in der dieses Gremium zu einer verstärkten Beschäftigung mit Problemen des Datenschutzes bei Neuen Medien aufgefordert wird[1]. Dies ist insbesondere deswegen unausweichlich, weil sowohl auf dem Gebiet der schmal- als auch der breitbandigen Kommunikation eine internationale Vernetzung in den nächsten Jahren zu erwarten ist.

4. Weitere Fragen aus der Kontroll- und Beratungspraxis

4.1 Systematische Überprüfungen

Neben der oben bereits dargestellten umfangreichen Überprüfung des Informationssystems Verbrechensbekämpfung beim Polizeipräsidenten in Berlin wurde eine Reihe weiterer systematischer technisch-organisatorischer Überprüfungen bei öffentlichen Stellen durchgeführt. So erfolgten Prüfungen bei

- den Berliner Stadtreinigungs-Betrieben (BSR),
- der Wohnungsbau-Kreditanstalt und der Berliner Pfandbrief-Bank,
- den Bezirksämtern Wilmersdorf und Kreuzberg.

Die Ergebnisse der Überprüfung beim Bezirksamt Kreuzberg liegen noch nicht vor. Dafür werden die Ergebnisse der Überprüfung des Bezirksamts Steglitz berücksichtigt, die im Jahresbericht 1984 noch nicht behandelt werden konnten.

Schwerpunkte solcher technisch-organisatorischer Überprüfungen liegen in der Beachtung der Bestimmungen des § 5 Abs. 1 BlnDSG und der Anlage dazu sowie des § 16 BlnDSG (Überwachbarkeit der ordnungsgemäßen Programmanwendung) und des § 22 BlnDSG (Meldepflicht zum Dateienregister).

Berliner Stadtreinigungs-Betriebe

Die Überprüfung der BSR hatte durch zahlreiche Presseberichte und eine parlamentarische Anfrage[2] im Vorfeld der Prüfung zusätzliche Aktualität erhalten.

Bereits während der Vorbereitung der routinemäßigen Prüfung ging ich Hinweisen auf On-line-Anschlüsse in Privatwohnungen nach, von denen einige Mitarbeiter der BSR Zugriff auf den BSR-Datenbestand hatten[3]. Diese von der Geschäftsleitung gebilligten Anschlüsse sollten den betreffenden Mitarbeitern im Störungsfall ein sofortiges Eingreifen in die Verfahrensabläufe ermöglichen. Mit der Einrichtung der privaten On-line-Verbindung war ein Zugriff auf personenbezogene Daten möglich, welche die BSR zur Abwicklung ihrer Geschäfte benötigte. Da der Umgang mit personenbezogenen Daten in Privatwohnungen weder durch die BSR noch durch mich kontrollierbar ist, empfahl ich dringend, die On-line-Anschlüsse unverzüglich abzuschalten. Die BSR ist dieser Empfehlung gefolgt.

Bei der Prüfung war festzustellen, daß die BSR sich bemüht, organisatorische Mängel der Datenverarbeitung, die auch in der Presse Aufmerksamkeit gefunden hatten, nach Kräften abzubauen. Meine Prüfung war deshalb unter dem Gesichtspunkt zu sehen, daß ich zu dieser Konsolidierungsphase mit Anregungen zur datenschutzrechtlichen Gestaltung der betrieblichen Datenverarbeitung beitragen wollte. Soweit derzeit erkennbar ist, setzt die BSR meine Empfehlungen zur Verbesserung des Datenschutzes zügig um.

Die bei der BSR festgestellten Mängel betrafen:

- die Organisation und Anwendungsweise des Zugangskontrollsystems,
- die Anwendung der vorhandenen Programme zur Zugriffssicherung,
- die räumlichen und personellen Funktionentrennungen im Bereich des Rechenzentrums,
- die Archivverwaltung,
- die Transportkontrolle beim Datenträgeraustausch,
- die Organisation der Vernichtung von EDV-Listen,
- die Anonymität der Testdatenbank, auf die externer On-line-Zugriff durch Programmier- und Beratungsfirmen gestattet wird.

Wohnungsbau-Kreditanstalt und Berliner Pfandbrief-Bank

In Fortführung meiner Prüfung der Kreditinstitute habe ich die Wohnungsbau-Kreditanstalt und gleichzeitig auch die Berliner Pfandbrief-Bank geprüft.

Die Prüfung hat ergeben, daß die Berliner Pfandbrief-Bank und die Wohnungsbau-Kreditanstalt weitgehend die erforderlichen Vorkehrungen zur Gewährleistung des Datenschutzes getroffen haben.

Das gemeinsame Rechenzentrum unterliegt der Verantwortung der Berliner Pfandbrief-Bank. Durch eine klare Aufgabenbeschreibung und -trennung zwischen den Anstalten ist die Auftragskontrolle durch die Wohnungsbau-Kreditanstalt gegenüber der Berliner Pfandbrief-Bank gewährleistet.

Diese Trennung wird durch logische und physische Zugriffskontrollen, die ständig von der Revision der Wohnungsbau-Kreditanstalt auf ihre Wirksamkeit hin überprüft wird, realisiert.

Besonders hervorzuheben ist die Tatsache, daß die nach § 16 Satz 2 Nr. 2 BlnDSG geforderte Überwachbarkeit der ordnungsgemäßen Anwendung der Datenverarbeitungsprogramme durch eine gute Programmdokumentation sichergestellt wird, so daß auch für prüfende Instanzen die notwendige Transparenz der Datenverarbeitung vorhanden ist.

Für die Organisation des Rechenzentrums und die Durchführung von Programmtests habe ich Empfehlungen ausgesprochen, die die Gefahr einer unbefugten Kenntnisnahme personenbezogener Daten weiter verringern sollen.

Bezirksämter

Die wichtigsten Ergebnisse bei den Bezirksämtern Steglitz und Wilmersdorf fasse ich im folgenden zusammen:

In den Bezirksämtern stellen sich in besonderem Maße jene Probleme, die sich aus der Dezentralität dieser Verwaltungen ergeben, und über die ich in den Abschnitten 2.1 und 2.4 ausführlich berichtet habe:

- der Einsatz von Personalcomputern am Arbeitsplatz der Sachbearbeiter,
- Speicherung von Dateien auf Textautomaten,
- Postverteilung und Postversand.

Darüber hinaus bleibt zu berichten:

In der personalaktenführenden Stelle eines Bezirksamtes wurde festgestellt, daß sämtliche Kindergeldvorgänge integraler Bestandteil der Personalakte sind. Die entsprechenden Unterlagen sind mit den Personalvorgängen in chronologischer Reihenfolge abgeheftet und durchlaufend paginiert.

[1] Vgl. Anlage 5.
[2] Kleine Anfrage Nr. 4298 vom 19. November 1984
[3] Jahresbericht 1984, S. 18

In dem Rundschreiben II Nr. 41/1984 vom 11. Juli 1984 des Senators für Inneres wird darauf hingewiesen, daß Kindergeldvorgänge nicht mehr in der Personal-(Haupt-)akte geführt werden dürfen. Dieser Auffassung schließe ich mich an. Ich habe den Stellen empfohlen, für die Übergangszeit alle neuen Kindergeldvorgänge getrennt zu führen und die alten Unterlagen nach und nach hinzuzufügen.

In einem Bezirksamt wird eine Grundstückseigentümerkartei geführt, die dadurch auf den neuesten Stand gebracht wird, daß von den Amtsgerichten Bescheide übersandt werden, die aktuelles Datenmaterial über die Grundstückseigentümer enthalten. Dabei wird u. a. auch über die Schulden der Grundstückseigentümer Auskunft gegeben. Darüber hinaus soll die Kartei zur Vorbereitung der nächsten Volkszählung verwendet werden.

Diese Kartei ist nicht erforderlich, da Daten von Grundstückseigentümern auch aus dem Liegenschaftskataster erhältlich sind. Eine Notwendigkeit, die Grundstückseigentümerkartei für die Vorbereitung zur Volkszählung zu verwenden, sehe ich nicht, zumal hierfür in einer gesonderten Aktion alle für diese Aufgabe notwendigen Daten erhoben werden.

Im Wohnungsamt eines der geprüften Bezirksämter werden bei zwei automatisierten Verfahren sämtliche Unterlagen mikroverfilmt. Dabei wurden bisher jedoch keine Sicherungskopien erstellt. Diese Verfahrensweise entspricht nicht dem Grundsatz einer ordnungsgemäßen Datenverarbeitung, da bei einem möglichen Verlust des Originals der Aufwand der Rekonstruktion in keinem Verhältnis zu einer - ohne großen Aufwand vorstellbaren - Sicherungskopie steht.

4.2 Wahlen zum Abgeordnetenhaus 1985

Im Vor- und Nachfeld der Wahlen entstanden Datenschutzfragen, die auch zu zahlreichen Anfragen und Eingaben der Bürger geführt haben.

Wahlwerbung mit Einwohnerdaten

So haben sich viele Bürger an mich gewandt, die persönlich adressierte Wahlwerbung von Parteien erhalten hatten. Sie fragten, auf welche Weise eine Partei an die Adressen gelangen könne und ob das Verfahren rechtmäßig sei. Das seinerzeit geltende Landeswahlgesetz sah in § 30 Abs. 2 vor, daß den Parteien aus dem Melderegister Listen mit Angaben über Namen, Adressen und akademische Grade von Bürgern für Wahlzwecke zur Verfügung gestellt werden konnten. Insoweit lag eine gesetzliche Grundlage für die Adressenweitergabe vor. In allen mir vorliegenden Fällen wurden die gesetzlichen Bestimmungen beachtet und die Einwohnerlisten nicht an unbefugte Stellen weitergeleitet, im übrigen unverzüglich nach der Wahl ordnungsgemäß vernichtet.

Parallel zu den mir vorgelegten Eingaben hatten sich Bürger an das Verwaltungsgericht gewandt mit dem Antrag feststellen zu lassen, daß § 30 Abs. 2 Landeswahlgesetz verfassungswidrig sei und eine Auskunftserteilung das allgemeine Persönlichkeitsrecht verletze. Während das Verwaltungsgericht die Regelung des Landeswahlgesetzes für mit dem informationellen Selbstbestimmungsrecht nicht vereinbar hielt, stellte sich das daraufhin angerufene Oberverwaltungsgericht auf den Standpunkt, daß damit kein unverhältnismäßiger Eingriff in die Rechte des Bürgers verbunden sei. Vielmehr ergebe sich aus einer Abwägung zwischen den Belangen der Wahlberechtigten und dem Recht der Partei, ihre Programme und Ziele im Zusammenhang mit anstehenden Wahlen zu verbreiten, die Zulässigkeit der Regelung im Landeswahlgesetz.

Nach meiner Auffassung entspricht weder das Verbot der direkten Wahlwerbung noch eine völlige Freigabe bestimmter Daten aus dem Melderegister zu Wahlwerbezwecken einem sachgerechten Interessenausgleich zwischen Bürgern und Parteien. Ich hatte daher bei den Beratungen zum neuen Meldegesetz seit Jahren gefordert, eine Regelung aufzunehmen, die dem Bürger ein Widerspruchsrecht gegen die Weitergabe einräumt, damit dieser selbst über die Zusendung von Wahlwerbung entscheiden könne. Diese Lösung ist in § 29 Abs. 1 Meldegesetz umgesetzt worden. Sie ist für beide Seiten vorteilhaft:

Einerseits hat es der Bürger in der Hand, sich von unerwünschter Wahlwerbung freizuhalten, andererseits versenden die Parteien kein Material an Personen, die sich damit nicht beschäftigen wollen.

Einsatz von Bildschirmtext zur Präsentation der Wahlergebnisse

Erstmals wurde bei einer Wahl ein Btx-Rechnerverbund erprobt, über den die von der Wahlzentrale im Statistischen Landesamt ermittelten Ergebnisse präsentiert wurden. Somit konnten neben dem Bezirksamt Schöneberg auch die anderen Bezirksämter laufend über die aktuellen Wahlergebnisse informiert werden.

Bereits im Vorfeld der Wahl habe ich mich davon überzeugt, daß aus Datenschutzgründen am Wahlabend auf den eingesetzten Rechnern **nur** die Wahlprogramme zum Einsatz kamen.

Aus Kapazitätsgründen wurde der Abruf der Wahlergebnisse (Hochrechnungen der Erst- und Zweitstimmen, namentliche Zusammensetzung des Abgeordnetenhauses) auf das Rathaus Schöneberg und die Bezirksämter beschränkt.

Erst nach der Feststellung des amtlichen Endergebnisses konnten über den eingesetzten externen Rechner die verschiedensten Ergebnisse von allen Btx-Teilnehmern abgerufen werden. Die Präsentation erfolgte unter voller Beachtung des Datenschutzes.

Die Speicherung der Wählerdaten

Entgegen den Erfahrungen bei den Wahlen im Jahre 1981 waren in diesem Jahr kaum Beschwerden betroffener Bürger über unrichtige Wahldaten zu verzeichnen.

Nur in einem Fall ist bei der Nutzung der beim Statistischen Landesamt zentral für Berlin geführten Straßenkartei durch einen Erfassungsfehler die Adresse des Betroffenen falsch eingetragen worden. Für den Druck der Wahlbenachrichtigungskarten wurde hierauf zurückgegriffen, so daß es zur Verarbeitung der fehlerhaften Adresse und somit zu einer Fehlzustellung gekommen ist.

Das Landesamt für Elektronische Datenverarbeitung hat die Fehlspeicherung im Einwohnerverfahren korrigiert und veranlaßt, daß die Straßendatei des Statistischen Landesamtes berichtigt wird. Ich habe beim bezirklichen Wahlamt darauf hingewirkt, daß das Wählerverzeichnis berichtigt wird und dem Ehepaar noch rechtzeitig vor der Wahl ihre Wahlbenachrichtigungskarten ordnungsgemäß zugestellt werden.

In einem anderen Falle hatte ein Bürger, der Anfang des Jahres umgezogen war, zwei Wahlbenachrichtigungskarten erhalten. Meine Überprüfungen haben ergeben, daß der Betroffene bis kurz vor dem Stichtag des Ausdruckes der Wahlbenachrichtigungskarten in seiner alten Wohnung gewohnt und sich erst nach Ausdruck polizeilich umgemeldet hatte. Als dem Bezirkswahlamt die neue Adresse bekannt wurde, wurde dem Wahlberechtigten mit einer neuen Wahlbenachrichtigungskarte mitgeteilt, wo sich nunmehr sein Wahllokal befindet. In diesem Zusammenhang wurde der Name im alten Wählerverzeichnis gestrichen. Somit war sichergestellt, daß der Betreffende nur einmal wählen konnte.

Briefwahl im Strafvollzug

Durch mehrere Eingaben bin ich auf das Verfahren bei der Wahl zum Abgeordnetenhaus in den Justizvollzugsanstalten hingewiesen worden. Kritikpunkt war insbesondere ein Formblatt, welches dazu dienen sollte, Gefangenen, die nicht selbst mit dem für sie zuständigen Bezirkswahlamt in Verbindung traten, Briefwahlunterlagen zu besorgen.

Dabei wurde das Formblatt über den Leiter der Justizvollzugsanstalt an das Einwohnermeldeamt geleitet, welches es - nach Feststellung einer Adresse in Berlin - an das zuständige Bezirkswahlamt sandte.

Da es nach dem Meldegesetz originäre Aufgabe des Einwohnermeldeamtes ist, verbindliche Auskünfte über den Wohnsitz zu geben, war das Verfahren datenschutzrechtlich nicht zu beanstanden.

Allerdings habe ich Bedenken geäußert gegen einige Fragen auf dem Formblatt (z. B. Tag der Festnahme zur jetzigen Haft; ob

sich der Gefangene z. Z. in Untersuchungs- oder Strafhaft befindet etc.), da diese Fragen für die Aufgabenerfüllung nicht notwendig gewesen sind. Gleiches galt für die Frage danach, ob der Gefangene von seinem Wahlrecht Gebrauch machen wolle oder nicht. Da ich jedoch davon ausgehen konnte, daß die Gefangenen die genannten Fragen bereits während des laufenden Wahlverfahrens nicht beantworten mußten, und daß die genannten Angaben in Zukunft nicht mehr erhoben werden, habe ich von einer förmlichen Beanstandung abgesehen.

Soweit die Formblätter oder Vermerke über die Absendung der Formblätter zu den Gefangenenakten genommen wurden, habe ich die zuständigen Stellen darauf hingewiesen, daß die Formblätter und Vermerke mit Ablauf der in § 25 Landeswahlordnung vorgesehenen Frist aus den Akten wieder entfernt und ordnungsgemäß vernichtet werden müssen.

Geburtsdaten von Wahlbewerbern

Die nach der Landeswahlordnung vorgeschriebene Bekanntmachung von Angaben über jeden Wahlbewerber dient dazu, den Wähler über die Person des Bewerbers umfassend zu informieren. Dabei schreibt die Landeswahlordnung auch die Veröffentlichung des genauen Geburtsdatums vor. Nach meiner Auffassung genügt die Angabe des Geburtsjahres.

Der Senator für Inneres ist ebenfalls der Auffassung, daß für die Entscheidung des Wählers im Normalfall höchstens das Geburtsjahr, nicht jedoch das genaue Geburtsdatum maßgeblich sein dürfte. Andererseits stellte er sich auf den Standpunkt, daß hier nur ein verhältnismäßig geringer Eingriff in die Privatsphäre des Wahlbewerbers vorliege, dem ein öffentliches Interesse an einer genauen Identifikation, insbesondere bei Sammelnamen, gegenüberstehe. Darüber hinaus verzichte ein Kandidat für einen Sitz im Parlament bis zu einem gewissen Grade freiwillig auf die Geheimhaltung seiner persönlichen Sphäre.

Die Entscheidung über die Veröffentlichung des genauen Geburtsdatums sollte zumindest jedem einzelnen Bewerber überlassen bleiben. Ich würde eine entsprechende Änderung der Landeswahlordnung begrüßen.

4.3 Der Umgang mit Personaldaten

Personaldaten: eine heilige Kuh?

Obwohl seit Beginn meiner Tätigkeit die Art und Weise, wie personenbezogene Daten öffentlicher Bediensteter verarbeitet werden, Gegenstand einer Vielzahl von Beschwerden und Nachfragen war, gestaltet sich gerade auf diesem Gebiet die Kontrolle der Einhaltung des Datenschutzes schwierig. Dies liegt in erster Linie daran, daß gesetzliche Vorschriften trotz der mit der Führung von Personalakten verbundenen Eingriffe in das informationelle Selbstbestimmungsrecht fehlen. Die von der Rechtsprechung entwickelten Grundsätze sind äußerst lückenhaft; zudem ist fraglich, in welchem Umfang sie den von der neuen Rechtsprechung des Bundesverfassungsgerichtes entwickelten Kriterien standhalten.

Meinen Bemühungen, Beschwerden von Betroffenen über den Umfang der Datenerhebungen oder -offenbarungen nachzugehen, wird häufig die Frage nach der Kontrollbefugnis des Datenschutzbeauftragten entgegengehalten. Dies wird auch aus der Stellungnahme des Senats zu meinem Jahresbericht 1984 deutlich, in dem mir auf diesem Gebiet nur eine sehr beschränkte Kontrollbefugnis zugestanden wird: Eine unmittelbare Geltung des Berliner bzw. (wegen eines entsprechenden Verweises in § 1 Abs. 4 BlnDSG) Bundesdatenschutzgesetzes scheide mangels Dateibezug aus. Auch formatisierte Teile von Personalakten (z. B. Aktenvorblätter) fielen nicht unter den Dateibegriff, da sie nach dem Prinzip der Vollständigkeit der Personalakten nicht zum Zwecke der Sortierung aus ihnen entnommen werden dürfen. Andererseits sei der Begriff der „anderen Vorschriften über den Datenschutz", deren Einhaltung der Datenschutzbeauftragte zugegebenerweise auch kontrolliere, eng auszulegen. Insbesondere könne der Datenschutzbeauftragte die Einhaltung allgemeiner Verfassungsgrundsätze wie Erforderlichkeit und Verhältnismäßigkeit nicht überprüfen.

Dem ist entschieden entgegenzutreten.

Bereits die Behauptung, die Personalakten oder zumindest Teile davon erfüllten den Dateibegriff nicht, kann so nicht aufrechterhalten werden. Die Personalakten bestehen in weiten Teilen aus einer im wesentlichen gleichartigen Aneinanderreihung von formatisierten Vorgängen (Personalfragebogen, Formulare für verschiedene Berechnungen, vorgefertigte Verfügungen, Dienstleistungsberichte usw.). Dieses Ausmaß der Formatisierung ermöglicht jederzeit eine Auswertung nach bestimmten Merkmalen, aber auch in bestimmtem Umfang ein Umsortieren. Daß dies aus tatsächlichen oder rechtlichen Gründen nicht geschieht, spielt keine Rolle; die Definition des Dateibegriffes (§ 4 Abs. 3 Ziff. 3 BlnDSG) stellt allein auf die Möglichkeit der Umordnung und Auswertung ab („umgeordnet und ausgewertet werden **kann**, ungeachtet der dabei angewendeten Verfahren"). Die Begrenzung des Dateibegriffes durch den Begriff der Akte ist demgegenüber insbesondere im Hinblick auf das Verfassungsgebot der Gewährleistung der informationellen Selbstbestimmung restriktiv zu sehen. Sie läßt Raum nur für die Privilegierung solcher Akten, die sich wegen des Fehlens eines gleichartigen Aufbaus dem datenschutzrechtlichen Regelinstrumentarium, soweit es in den Datenschutzgesetzen niedergelegt ist, entziehen (z. B. chronologische Ablage von Korrespondenz).

Hinzu kommt, daß eine Vielzahl der in den Personalakten enthaltenen Daten im Rahmen des Personalbezügeverfahrens, zunehmend aber auch im Rahmen automatisierter Verfahren der Personalbewirtschaftung in automatisierten Dateien geführt werden. Es ist weithin herrschende Meinung, daß der Dateibegriff von formal als Akten geführten Unterlagen dann erfüllt wird, wenn automatisch geführte Dateien auf den Aktenbeständen beruhen.

Die Kontrollbefugnis des Berliner Datenschutzbeauftragten bei Personaldaten ergibt sich aber auch unter einem anderen, erheblich gewichtigeren Aspekt: Die Möglichkeit, die Verarbeitung personenbezogener Daten durch den Datenschutzbeauftragten überprüfen zu lassen, wird weithin als Voraussetzung für die Legitimität der Datenverarbeitung betrachtet, insbesondere in Gebieten, die wegen ihrer Komplexität oder auch ihrer Geheimhaltungsbedürftigkeit der Einsicht des Bürgers entzogen sind. Das Bundesverfassungsgericht hat im Volkszählungsurteil die Befugnisse des Datenschutzbeauftragten unter dem Aspekt des vorbeugenden Rechtsschutzes gewürdigt. Hieraus ergibt sich, daß der Kontrolle durch den Datenschutzbeauftragten gerade in wenig transparenten Gebieten besondere Bedeutung zukommt.

Ein solcher Fall liegt aus meiner Sicht gerade dann vor, wenn – wie bei Personaldaten – eine beträchtliche Diskrepanz zwischen dem Umfang der gesammelten Informationen auf der einen Seite, der mangelhaften Gesetzeslage auf der anderen Seite besteht. Eine andere Sichtweise, wie sie in der Stellungnahme des Senats zum Ausdruck kommt, würde dazu führen, daß der Datenschutz gerade in gesetzlich schlecht strukturierten und für das informationelle Selbstbestimmungsrecht besonders problematischen Verwaltungsbereichen nur unzureichend kontrolliert werden kann.

Hieraus ist zu folgern, daß in kritischen Rechtsbereichen die Kontrollbefugnisse des Datenschutzbeauftragten unmittelbar auf Verfassungsgrundsätze gestützt werden müssen. Der Datenschutzbeauftragte befindet sich hier in einer Situation, die derjenigen der Rechtsprechung vergleichbar ist: Auch diese muß, um zulässigen Begehren von Klägern gerecht zu werden, ihre Judikatur in bestimmten Fällen unmittelbar auf die Verfassung stützen und kann ihre Zuständigkeit nicht mit einem Verweis auf fehlende Kodifizierungen ablehnen.

Ich sehe mich deshalb berechtigt und verpflichtet, den Beschwerden öffentlicher Bediensteter gegen den Umgang mit Personaldaten in der Personalakte und anderen Datensammlungen nachzugehen und bestehende Datenschutzmängel zu beanstanden. Soweit sich aus anderen Quellen Hinweise auf Mißbräuche ergeben, werde ich diesen ebenfalls nachgehen. Die möglicherweise hinter der Stellungnahme des Senats stehende Befürchtung, der Datenschutzbeauftragte könnte in einem über das erforderliche Ausmaß hinausgehenden Umfang Personalakten einsehen, ist unbegründet.

Ein Prüfergebnis

Welche Bedeutung die Datenschutzkontrolle für die Rechte der Bediensteten hat, zeigen die Ergebnisse einer Überprüfung der Personaldatenführung in einer Einrichtung einer Universität, die eine Einsichtnahme in einzelne Personalakten nicht erforderlich machte und nur die Struktur der Personaldatenverarbeitung betraf:

Abgesehen davon, daß die Zuständigkeit für die Personalaktenführung und damit die datenschutzrechtliche Verantwortung unzureichend geregelt ist, erhält ein für Einzelpersonalangelegenheiten unzuständiges Organ regelmäßig eine aus personenbezogenen Daten bestehende monatliche Gesamtübersicht über das Personal. Es ist nicht auszuschließen, daß diese Daten auch an weitere Stellen weitergegeben werden. In den Personalakten selbst werden Beihilfeunterlagen und Kindergeldunterlagen geführt, die auch bei der Weitergabe der Personalakte z. B. im Zusammenhang mit Bewerbungen nicht oder nur teilweise ausgesondert werden. Insbesondere das Einheften der Beihilfeunterlagen ermöglicht nicht nur den mit der Bearbeitung von Beihilfevorgängen beauftragten Mitarbeitern, sondern jeder Person, die Zugang zur Personalakte hat, die Einsicht in die dort enthaltenen medizinischen Daten.

Wegen der Besonderheit des Betriebes fertigt das Landesamt für Elektronische Datenverarbeitung von den Daten aus dem Verfahren nach den Zahlungsbestimmungen für Personalbezüge Abzüge, die in der Einrichtung weiter verarbeitet werden. Es konnte bei der Prüfung nicht festgestellt werden, in welchem Verfahren Aufträge zur Auswertung dieser Daten erteilt werden. Insbesondere wurde nicht klar, in welchem Umfang Organe der Einrichtung auf diese Daten zugreifen.

In mindestens einem Institut werden auf einem isolierten Rechner weitere automatisierte Dateien mit Personaldaten geführt. Hierzu gehört auch eine Erfassung der Fehlzeiten einzelner Mitarbeiter. Es war sogar geplant, einen Ausdruck aus der Fehlzeitendatei zum Aushang zu bringen. Besondere Anweisungen zur Führung von Personaldaten in nachgeordneten Institutionen bestehen nicht. Die erforderlichen Anmeldungen zum Dateienregister wurden nicht vorgenommen. Personalakten werden in einfachen Holzschränken aufbewahrt, die zuvor als Kleiderschränke benutzt worden waren. Ein Datensichtgerät, mit dem Personaldaten abgerufen werden können, war in einem Vorzimmer so aufgestellt, daß jeder Besucher unbeschränkte Einsicht in die Daten erhielt.

Derartige Mängel, die den Beteiligten oft unbewußt sind, können nur beseitigt werden, wenn eine hinreichende Kontrolle gewährleistet ist.

Veröffentlichung von Personaldaten

In den unterschiedlichsten Zusammenhängen wird die Frage an mich herangetragen, ob der öffentliche Dienstherr oder Arbeitgeber bestimmte Personaldaten veröffentlichen oder seine Bediensteten sogar verpflichten darf, von sich aus Daten zu offenbaren.

Hier ist nicht das Berliner Datenschutzgesetz anzuwenden. Übermittlungen von Daten zu dienst- oder arbeitsrechtlichen Rechtsverhältnissen richten sich gemäß § 1 Abs. 4 BlnDSG nach § 24 BDSG.

Danach sind Veröffentlichungen von Personaldaten nur zulässig, wenn sie unmittelbar der Zweckbestimmung dieser Rechtsverhältnisse dienen, oder soweit sie zur Wahrung berechtigter Interessen erforderlich sind und schutzwürdige Belange der Betroffenen nicht beeinträchtigt werden. Dabei ist bei Anwendung der zweiten Alternative im Hinblick auf die Rechtsprechung zum Personaldatenrecht größte Zurückhaltung geboten.

Bereits hieraus ist ersichtlich, daß eine einheitliche Beurteilung nicht möglich ist, vielmehr die unterschiedlichen Sachlagen jeweils an diesen Kriterien gemessen werden müssen.

Entscheidungsrelevant ist dabei auch der Umfang der zu veröffentlichenden Daten. Hier muß unterschieden werden zwischen der Veröffentlichung

- von Name, Funktionsbeschreibung, Dienstanschrift und Diensttelefon und
- darüber hinausgehender Daten wie Geburtsdatum, Jubiläumsdaten, Privatanschriften u.ä.

Wegen des sich unmittelbar aus der Funktion bzw. der zugewiesenen Aufgabenstellung ergebenden Öffentlichkeitsbezuges müssen zumindest

- Behördenleiter,
- öffentlich bestellte oder gewählte Gremienvertreter,
- Bedienstete, zu deren Aufgaben ausdrücklich die Öffentlichkeitsarbeit gehört (z.B. Pressereferenten, Btx-Beauftragte) und
- Bedienstete, die mit bestimmten Aufgaben öffentliche Stellen nach außen hin vertreten,

eine Bekanntgabe von Namen, Funktionsbeschreibung, Dienstanschrift und Diensttelefon, auch in Publikationen, hinnehmen. So können diese Daten von Abteilungs-, Unterabteilungs-, Referats-, Amtsleitern u.ä. veröffentlicht werden. Wenn Sachbearbeiter einzelne Aufgaben mit Öffentlichkeitswirkung wahrnehmen und hierbei auch den Bürger beraten, müssen auch sie die Veröffentlichung dieser Daten hinnehmen.

Unberührt bleibt davon die Verpflichtung aller öffentlichen Bediensteten, gegenüber den Bürgern im Einzelfall und auf besonderes Verlangen selbst den Namen und ihre Funktion zu benennen. Dies hat seinen Niederschlag in § 22 Abs. 6 und 7 GGO I gefunden.

Über die bisher genannten Angaben hinausgehende Daten wie Geburtsdatum, Jubiläumsdatum, Privatanschrift usw. dürfen jedoch nur mit Zustimmung der Betroffenen veröffentlicht werden, da für die Veröffentlichung solcher Daten keine vertragliche oder vertragsähnliche Verpflichtung besteht, andererseits aber immer Grund zur Annahme besteht, daß schutzwürdige Belange der Betroffenen beeinträchtigt werden können.

Angehörige von Berufsgruppen, deren dienstliche Tätigkeit sich auch auf den häuslichen Bereich erstreckt (z.B. Hochschullehrer), müssen gleichwohl die Publikation von Privatadressen hinnehmen, wenn sie nicht besondere schutzwürdige Belange geltend machen können, die eine Veröffentlichung unverhältnismäßig erscheinen lassen.

Personalrat und Datenschutz

Nach den Bestimmungen des Personalvertretungsgesetzes (PersVG) sind Personalräte Organe der jeweiligen Verwaltung und insoweit auch zur Einhaltung der Datenschutzgesetze verpflichtet. Wegen ihrer allgemeinen Bedeutung gebe ich an dieser Stelle einige Vorgänge aus diesem Bereich wieder:

Mir ist vorgetragen worden, daß der Personalrat der Lehrer und Erzieher eines Bezirksamtes auf die Vorlage sämtlicher **Bewerbungsunterlagen** von Lehrern durch das Schulamt dränge.

Ungeachtet der nach dem PersVG vorgesehenen vertrauensvollen Zusammenarbeit zwischen der Dienststelle und dem Personalrat kommt es hier aus datenschutzrechtlicher Sicht darauf an, daß Rechte betroffener Bewerber gewahrt bleiben, ohne bestehende Rechte des Personalrats einzuengen.

Zwar besteht für den Personalrat im Rahmen seiner Mitbestimmungsbefugnis bei **konkreten** Einstellungsvorgängen nach höchstrichterlicher Rechtsprechung ein sehr umfangreiches Informationsrecht auch im Interesse der Bewerber. Sofern jedoch Bewerbungen unabhängig von einem konkreten Einstellungsvorgang eingehen, ist dies noch nicht der Fall.

Wenn die Dienststelle allerdings beabsichtigt, nicht alle auf diesem Wege eingehenden Bewerbungen mangels offener Stellen abzulehnen, vielmehr eine vorläufige Auswahl nach bestimmten Bedarfskriterien trifft, die einzelne Bewerber für zukünftige Stellenbesetzungen in Betracht kommen lassen, muß der Personalrat zumindest in die Lage versetzt werden, zu beurteilen, ob seine Mitbestimmungsrechte nicht bereits zu diesem Zeitpunkt berührt werden.

Hierfür ist es ausreichend, dem Personalrat geeignete Informationen in anonymisierter Form zukommen zu lassen. Dies könnte etwa dadurch geschehen, daß die Dienststelle dem Personalrat die Anzahl abgelehnter Bewerbungen unter Angabe konkreter Ablehnungsgründe mitteilt.

Über die aufrechterhaltenen Bewerbungen könnte ihm die Dienststelle in angemessenen Zeiträumen aktualisierte Übersichten zukommen lassen, aus denen in anonymisierter Form die vorhandenen Bewerbungen mit dem konkreten Hinweis auf den Grund der Aufbewahrung ersichtlich sind. Dies würde den Personalrat bei konkreten Besetzungen jederzeit in die Lage versetzen zu prüfen, ob ihm tatsächlich auch aus dem allgemeinen Bewerbungsbestand alle für die zu besetzende Stelle in Betracht kommenden Bewerber im Rahmen seiner Mitbestimmungsrechte genannt wurden.

Im Zusammenhang mit einer Personalratswahl habe ich die Weitergabe der Namen der die **Wahlvorschläge** unterstützenden Dienstkräfte beanstandet. Diese Unterlagen sind nicht Bestandteil der Wahlunterlagen i. S. von § 22 Wahlordnung (WO). In § 12 WO wird ausdrücklich bestimmt, daß die Namen der die Wahlvorschläge Unterstützenden nicht bekanntgegeben werden dürfen. Es ist ausschließlich Aufgabe des Wahlvorstandes, diese Namen im Rahmen der Prüfung der Gültigkeit eines Wahlvorschlages zur Kenntnis zu nehmen und unmittelbar nach Ablauf der Wahlanfechtungsfrist zu vernichten, weil für eine weitere Aufbewahrung kein Rechtsgrund mehr besteht.

Wenn dem Personalrat entgegen dem Willen des Verordnungsgebers dennoch diese Namen mit den Wahlunterlagen nach § 22 WO zur Aufbewahrung überlassen wurden, war nach § 12 WO i. V. m. § 11 PersVG ihre Geheimhaltung vorgeschrieben und somit in besonderem Maße erforderlich.

Diverse Wahlvorstände befürchteten, daß viele der von den Dienststellen im allgemeinen listenmäßig zur Verfügung gestellten personenbezogenen Daten mit den **Wählerverzeichnissen** zur Einsichtnahme ausgelegt würden.

Ungeachtet der Tatsache, daß von den Dienststellen gem. § 10 BlnDSG nur die für eine ordnungsgemäße Aufgabenerfüllung der Wahlvorstände unbedingt notwendigen Daten zur Verfügung gestellt werden dürfen, hat zumindest der jeweilige Wahlvorstand dafür Sorge zu tragen, daß ausschließlich Daten zur Einsicht ausgelegt werden, die für die Erfüllung des in § 2 WO beschriebenen Aufgabenzwecks erforderlich sind. Hiernach ist vorgeschrieben, daß das Verzeichnis der wahlberechtigten Dienstkräfte getrennt nach den Gruppen der Angestellten, Arbeiter und Beamten aufgestellt wird. Zweck des Wählerverzeichnisses ist, den Bediensteten die Möglichkeit zu geben, rechtzeitig vor der Wahl evtl. vorhandene Gründe vorzutragen, die eine Wahlbeteiligung anderer Bediensteter ausschließen könnten (Einspruchsrecht).

Dazu müssen die jeweils einzeln aufgeführten Personen hinreichend bestimmt sein. Dies dürfte durch Angabe des Namens, Vornamens und des Dienst- oder Arbeitsbereiches gewährleistet sein. Selbst wenn diese Merkmale auf mehrere angeführte Personen zutreffen sollten, wäre kein Grund für die Angabe weiterer personenbezogener Daten gegeben, da der Wahlvorstand bei Einsprüchen eine Entscheidungsverpflichtung hat und im Rahmen dieser Entscheidung ohnehin eine genaue Identitätsprüfung vornehmen muß.

Zu diesem Zweck ist es dem Wahlvorstand unbenommen, für sich parallel eine Liste zu führen, die auch Geburtsdaten und Wohnanschriften sowie Angaben über den jeweiligen Zeitpunkt des Eintritts in die Dienststelle enthält. Für eine allgemeine Offenbarung auch dieser Angaben besteht jedenfalls weder ein Erfordernis noch eine rechtliche Grundlage.

Nach der Wahl hatte in einem Städtischen Krankenhausbetrieb der Vorsitzende des Personalrats die gesamten **Wahlunterlagen der Personalratswahl** (Wählerverzeichnis mit Geburtsdaten, Berufsbezeichnungen und Anschriften, die Wahlvorschlagsliste mit den Unterschriften der unterstützenden Dienstkräfte sowie Briefwahlunterlagen) zur Auswertung an eine Gewerkschaft weitergeleitet.

Er war von der Rechtmäßigkeit seines Handelns ausgegangen, weil die Beauftragten der Gewerkschaft, die die Wahlanalysen durchzuführen hatten, nicht Mitarbeiter der Krankenanstalt, sondern als Mitarbeiter des Fachbereichs Politische Wissenschaften der FU tätig waren und somit die bloße Kenntnis der Unterlagen seines Erachtens keinen Schluß auf konkrete Personen und Funktionen bei den Beauftragten zuließ.

Der Personenbezug spielte hier jedoch keine Rolle, da hinsichtlich der Datensicherungspflicht für Personalratsmitglieder § 11 PersVG als spezialgesetzliche Datenschutznorm unmittelbar gilt.

Hiernach sind Personalratsmitglieder verpflichtet, über die im Amt bekannt gewordenen Angelegenheiten und Tatsachen u. a. Stillschweigen dann zu bewahren, wenn deren Geheimhaltung vorgeschreiben oder ihrer Bedeutung nach erforderlich ist. Eine Ausnahmeregelung zu Forschungszwecken ist weder im PersVG noch in der Wahlordnung zum PersVG enthalten.

Da die WO eine Reihe von Veröffentlichungspflichten vorschreibt, dem Personalrat jedoch gem. § 22 ausschließlich die Verpflichtung zur Aufbewahrung von Wahlunterlagen bis zur nächsten Personalratswahl auferlegt, wird der Rahmen der Geheimhaltungspflicht deutlich eingegrenzt.

Eine Übermittlung von Wahlunterlagen war nur insoweit datenschutzrechtlich unbedenklich, als es sich um Abschriften der allgemein zugänglichen, sogar zur Veröffentlichung vorgeschriebenen Wählerverzeichnisse (§ 2 WO), Wahlvorschläge (§ 12 WO) und Bekanntmachungen der gewählten Bewerber (§ 21 WO) handelte. Eine Geheimhaltung der hiermit verbundenen personenbezogenen Daten war ihrer Bedeutung nach - auch nach Erledigung des Aufgabenzwecks - nicht erforderlich, eine Übermittlung insoweit zulässig. Dies gilt selbstverständlich nicht für Wählerverzeichnisse, aus denen hervorgeht, wer an der Wahl teilgenommen hat.

4.4 Gesundheitswesen

Änderung des Landeskrankenhausgesetzes

Unter der Federführung der Berliner Krankenhausgesellschaft e. V. und meiner Mitwirkung wurde ein Formulierungsvorschlag zur weiteren Novellierung des § 15 Landeskrankenhausgesetz entwickelt, der die schon in meinem Jahresbericht 1984 erwähnten, noch verbleibenden Defizite bei der Regelung der ärztlichen Schweigepflicht im Krankenhausbereich beseitigen soll. Dieser Entwurf muß noch mit Krankenkassen und Krankenhäusern erörtert werden.

Neben einer Regelung zur Durchführung der kassenärztlichen Abrechnung enthält er vor allem eine Aussage zum Einsichtsrecht des Patienten in die Krankengeschichte und andere medizinische Daten.

Dieser Entwurf steht im Einklang mit der jüngsten Entwicklung der Rechtsprechung zum Einsichtsrecht des Patienten. Hatte der Bundesgerichtshof noch im Jahre 1982[1] lediglich das Einsichtsrecht des Patienten in seine objektiven Daten (die sogenannten Untersuchungsbefunde) befürwortet, nicht jedoch die Einsicht in die subjektiven Informationen (d. h. diagnostische Wertungen und persönliche Urteile eines Arztes), zeichnet sich durch eine weitere Entscheidung[2] eine deutliche Wende zur Verstärkung der Rechtsposition eines Patienten gegenüber dem Arzt ab.

Nunmehr wird dem Patienten grundsätzlich auch die Einsicht in den subjektiven Teil (d. h. auch in psychiatrische Unterlagen) ermöglicht. Wenn den Umständen nach keine therapeutischen Bedenken gegen eine Offenlegung der Krankengeschichte bestehen, mißbrauche der Arzt vielmehr sein Recht auf Zurückhaltung der Krankenunterlagen. Allerdings könne der Arzt sich nach wie vor auf den allgemeinen Hinweis beschränken, daß die Krankengeschichte aus therapeutischen Gründen nicht zu offenbaren sei.

Diese Beschränkung des Einsichtsrechts des Patienten halte ich noch immer für zu weitgehend, da sie weder dem Patienten noch einem Gericht eine Nachprüfung ermöglicht.

[1] BGH-Urteil vom 23. November 1982, VI ZR 222/79

[2] BGH-Urteil vom 2. Oktober 1984, VI ZR 311/82

Um diesen Bedenken Rechnung zu tragen, enthält der von der Arbeitsgruppe vorgeschlagene Formulierungsentwurf lediglich noch die Einschränkung, daß die Einsicht verweigert werden kann, wenn Rechte Dritter gefährdet werden oder sich der Patient in einem die freie Willensbildung ausschließenden krankhaften Zustand der Geistestätigkeit befindet. Diese Tatsachen hat der Arzt nachzuweisen.

Gewährleistung des Datenschutzes in Krankenhäusern

Die bestehenden datenschutzrechtlichen Regelungen des Landeskrankenhausgesetzes können den Schutz der Patientendaten nur sicherstellen, wenn organisatorische Maßnahmen dem Gesetz auch Wirkung verschaffen. In Betracht könnte z. B. eine Dienstanweisung für Ärzte und Pflegepersonal kommen.

Es ist zu begrüßen, daß meine Anregung, in den Krankenhausbetrieben entsprechend § 28 BDSG einen Fachberater für Datenschutzfragen zu schaffen, aufgegriffen wurde. Über die fachlichen Merkmale und Qualifikationen einer solchen Tätigkeit haben Gespräche mit den zuständigen Gesundheitsstellen, mit Verwaltungsleitern der Krankenhäuser und mit der Berliner Krankenhausgesellschaft stattgefunden. In einem derzeit diskutierten Merkmalskatalog sind im wesentlichen meine Empfehlungen berücksichtigt.

Der Schwerpunkt der Mängel, die mir bekannt geworden sind, liegt hauptsächlich im Bereich der Organisation. So hätten sich Beschwerden von Patienten vermeiden lassen, über die entweder durch den Pförtner oder durch die Telefonauskunft zu viele Daten offenbart wurden. Zwar hatten die Patienten die Auskunftsermächtigung unterzeichnet, jedoch stellt diese Erklärung keinen Freibrief für jedwede Datenoffenbarung dar. Vielmehr ist die Datenoffenbarung auf das erforderliche Minimum zu reduzieren. So halte ich es für datenschutzrechtlich nicht hinnehmbar, einem Dritten, der nicht imstande ist, einen Patienten hinreichend genau zu bezeichnen, seitens der Krankenhausverwaltung eine Anzahl von weiteren persönlichen Daten zu offenbaren, um ihn in die Lage zu versetzen, den vielleicht (!) richtigen Patienten zu identifizieren.

Vermeidbar ist es auch, im Zimmer des Patienten detaillierte medizinische Daten offen auszuhängen. In einem Falle mußte ich jedoch eine solche Verfahrensweise beanstanden.

Zu beanstanden waren in einem Krankenhaus EDV-mäßig erstellte und für den Arbeitgeber bestimmte Krankenbescheinigungen, die auf einem unzureichend geschwärzten Feld die chiffrierte, jedoch entschlüsselbare Codierung des Krankheitsbildes enthielten. Nicht gerechtfertigt war auf der anderen Seite, einem Patienten, der privat abrechnen wollte, „aus Datenschutzgründen" keine Spezifikation über die Behandlung und Diagnose zu geben.

Datenschutz im öffentlichen Gesundheitsdienst

Die Presse griff eine Dateimeldung im Amtsblatt auf, nach der Daten von Geschlechtskranken durch die Gesundheitsämter regelmäßig an andere näher bezeichnete Stellen übermittelt würden.

Ich habe aufgrund der Meldung die Beratungsstellen für Geschlechtskranke insbesondere unter dem Gesichtspunkt der „regelmäßigen Übermittlung" überprüft. Dabei habe ich festgestellt, daß die im Amtsblatt ausgedruckten Empfänger nicht in dem zu befürchtenden Umfang Daten erhielten, sondern nur im Rahmen der rechtmäßigen Aufgabenerfüllung mit Einwilligung der jeweiligen Patienten oder aufgrund besonderer Rechtsvorschriften im Einzelfall.

Dieser Fall warf die Frage auf, was das Datenschutzgesetz unter „regelmäßiger Übermittlung" in § 12 Abs. 1 Ziff. 4 versteht. Die Veröffentlichungspflicht soll die Datenspeicherung und Datenübermittlung für jeden Bürger transparent machen. Eine solche Meldung hat den optimalen Informationswert für den Bürger allerdings nur dann, wenn sie überschaubar ist, wenn sie substantiierte Informationen enthält und schlüssig auf Funktionszusammenhänge verweist. Der Begriff der Regelmäßigkeit muß daher für den Bürger in einem aus sich selbst heraus verständlichen Sinne ausgelegt werden. Er ist daher zu verstehen als „regelgemäße" Übermittlung von Daten, d. h. es muß ein abstrakt durch Gesetz oder Verwaltungsvorschrift geregeltes Übermittlungsverfahren definiert sein. Datenübermittlungen, die ausschließlich aufgrund von Einwilligungen erfolgen, sind keine „regelmäßigen Übermittlungen", weil der Grund für die Übermittlung nicht in einer „Regelung" liegt, sondern in der unmittelbaren Einwilligung des Betroffenen. Eine Ausnahme kommt nur in Betracht, wenn die Einwilligung aufgrund einer Mitwirkungspflicht (z. B. beim Sozialleistungsverfahren) erfolgen muß.

Gewährung und Abrechnung von Leistungen

Von Ärzten bin ich darauf hingewiesen worden, daß für die Abrechnung mit den Krankenkassen ein neues Formular zum „Antrag auf weitere Kostenübernahme für Krankenhauspflege - psychiatrische Behandlungsfälle -" erprobt werden sollte. Die Neufassung des Formulars enthielt Fragen, die weit über das für den Patienten Zumutbare hinausgingen. Da dieses Formular nicht nur einmalig, sondern in gleichbleibenden Abständen hätte ausgefüllt werden sollen, wäre mit der entstehenden Formularsammlung ein komplettes Krankheitsabbild mit höchst privaten Angaben entstanden. Der Versuch wurde nach meiner Beanstandung abgebrochen.

Die Probleme der Datenübermittlung zu Abrechnungszwecken zwischen Krankenhäusern und Krankenkassen bestehen auch zwischen Krankenhäusern und dem Träger der Sozialhilfe. Von einem Bezirksamt wurde ich angesprochen, weil die „Erste-Hilfe-Bogen", die zwecks Kostenübernahme an den Kostenträger der Sozialhilfe gesandt werden, sehr detailliert Unfallhergang, Vorgeschichte, medizinische Befunde, Diagnose, Therapievorschlag usw. enthalten. Generell sollten detaillierte medizinische Informationen nicht an Sozialämter übermittelt werden. Die Unterscheidung von Gesundheitsämtern und Sozialbehörden bietet die Möglichkeit, das Patientengeheimnis auf optimale Weise zu gewährleisten. Ähnlich wie bei den Krankenkassen der Vertrauensärztliche Dienst für die medizinischen Daten zuständig ist, können auch hier medizinische Unterlagen bei den Gesundheitsämtern bleiben. Die Sozialbehörde muß lediglich über das Untersuchungsergebnis informiert werden. Das Verwaltungsverfahren würde dadurch nicht behindert, sondern insofern vereinfacht, als die den Bescheid erlassende Sozialleistungsbehörde nicht mit medizinischen Informationen belastet wird, zu denen sie in der Regel keine Aussagen zu machen braucht und die einen erhöhten Aufwand zum Schutz der Daten bedingen.

Damit ist ohne Einwilligung des Patienten eine Übermittlung dieser Informationen an das Sozialamt nicht zulässig. Ist ein Patient jedoch nicht erklärungsfähig oder ist er nicht in der Lage, finanziell für sich selbst einzutreten, so daß entweder eine Krankenkasse oder der Sozialleistungsträger einstandspflichtig wären, dann entscheidet zunächst der mutmaßliche Wille des Patienten (abhängig von den jeweils gegebenen Umständen). Im zweiten Fall ist eine gesetzliche Regelung vonnöten, die ein Zusammenwirken von Krankenhaus, Krankenkasse und Sozialleistungsträger insoweit zuläßt, als es erforderlich ist, um die Kostenträgerschaft rechtlich abzuklären.

Ich habe das Verfahren nach dem Gesetz über die Gewährung von Leistungen an Zivilblinde, Gehörlose und Hilflose (ZGHG) im Hinblick auf die Pflege durch Sozialstationen überprüft. Die Prüfung der medizinischen Aspekte eines Leistungsantrags auf Pflege durch die Sozialstationen ist auf das Landesamt für zentrale soziale Dienste - Landesversorgungsamt - übertragen worden. Von den Bezirksämtern sind zusätzlich die weiteren sozialrechtlichen Voraussetzungen zu prüfen, für deren Beurteilung eine Kenntnis detaillierter medizinischer Daten allerdings nicht erforderlich ist. Nach eingehenden Erörterungen mit der Senatsverwaltung für Gesundheit und Soziales wurde das Verfahren so geregelt, daß die „Pflegedokumentation", die von den Sozialstationen erstellt wurde, direkt an den Ärztlichen Dienst des Landesversorgungsamtes weitergeleitet wird und dieser sie nach Einsicht und Auswertung direkt an die zuständige Sozialstation zurücksendet. Gegenüber dem Bezirksamt werden vom Ärztlichen Dienst des Landesversorgungsamtes keine detaillierten medizinischen Daten offenbart, sondern es wird vielmehr eine prüfärztliche Stellungnahme übersandt, die die gesetzlichen Voraussetzungen der Leistungsgewährung bestätigt, ohne daß die medizini-

schen Grundlagen für diese Entscheidung offenbart werden. Die Mitwirkung des Ärztlichen Dienstes des Landesversorgungsamtes hat zwar keine bindende Wirkung für den Bewilligungs- oder Ablehnungsbescheid des Bezirksamtes, jedoch sind die medizinischen Aspekte dadurch hinlänglich überprüft. Ähnlich wie in anderen Bereichen hat sich hierbei die Erkenntnis durchgesetzt, daß medizinische Daten von den dafür eingerichteten staatlichen Stellen zu erheben und unter dem Blickwinkel der geltend gemachten Anspruchsgrundlage zu beurteilen sind. Keine Kenntnis von solchen Daten dürfen jene Stellen haben, die nach der Geschäftsverteilung nicht dazu berufen sind, diese fachspezifische Aufgabe zu erfüllen.

4.5 Sozialverwaltung

Mitwirkungspflicht des Leistungsempfängers

Die Verpflichtung des Leistungsempfängers zur Abgabe einer Einwilligung stellt ein schwieriges Problem dar. Häufig hängen Sozialleistungen von der Mitwirkungsbereitschaft des Antragstellers oder Leistungsempfängers ab. Die Mitwirkung eines Antragstellers ist dabei auch Grundlage für die erforderlichen Datenübermittlungen. Allerdings darf die Behörde sich auf sie nur insoweit beziehen, als dies für die Durchführung eines Leistungsverhältnisses unter Berücksichtigung des Verhältnismäßigkeitsprinzips unbedingt erforderlich ist.

Anschaulich wurde dies bei der Beratung eines Amtes für Familien- und Heimpflege. Ein wichtiger Aufgabenbereich dieses Amtes ist die Vermittlung von Kindern in Heime oder Pflegefamilien. Die Suche und Auswahl eines geeigneten Platzes für ein Kind erfordert es, persönliche Entscheidungskriterien in Bezug auf das Kind gegenüber Heimen und Pflegefamilien zu offenbaren. Dies sollte aber nach Möglichkeit anonym geschehen, da der Name in dem frühen Stadium der Vermittlungstätigkeit von untergeordneter Rolle ist. In erster Linie kommt es auf die soziale und persönliche Situation des Kindes an, die auch ohne Preisgabe der Identität mit den Familien oder Heimen erörtert werden kann.

Ein Petent, der nach der Beendigung seines Studiums Sozialhilfe bezogen und in diesem Zusammenhang eine Erklärung unterschrieben hatte, daß er die Sozialleistung gemäß § 92 a Bundessozialhilfegesetz zu ersetzen habe, wenn er durch vorsätzliches oder grob fahrlässiges Verhalten bedürftig geworden war, beschwerte sich darüber, daß er vom Sozialamt aufgefordert wurde, seine Kostenersatzfähigkeit nachzuweisen, bevor überhaupt seine Kostenersatzpflichtigkeit festgestellt worden war. Er trug vor, daß er nicht durch vorsätzliches oder grob fahrlässiges Verhalten bedürftig geworden sei. Meine Überprüfung ergab, daß der Behörde keine Tatsachen über ein solches Verhalten bekannt geworden waren. Auch stellte ich fest, daß es sich bei dieser Verfahrensweise nicht um einen Einzelfall handelte. Vielmehr wurden die Formulare zum Einkommensnachweis in der Regel auch ohne vorherige Feststellung der Kostenersatzpflichtigkeit versandt. Aufgrund meiner Bemängelung wurde zugesichert, daß künftig die Hilfeempfänger nur dann zum Nachweis der Kostenersatzfähigkeit aufgefordert werden, wenn die Kostenersatzpflichtigkeit feststeht.

In einem Fall habe ich festgestellt, daß die Allgemeine Ortkrankenkasse medizinische Unterlagen über einen Versicherten an den ärztlichen Dienst des Landesarbeitsamtes Berlin übersandt hatte, ohne daß eine Einwilligungserklärung des Betroffenen vorgelegen hatte, und ohne daß dieser auf sein Widerspruchsrecht nach § 76 SGB X verzichtet hatte. Ich habe die Maßnahme beanstandet und die Zusicherung erhalten, daß Daten über Versicherte, die medizinische Tatbestände enthalten, nur dann an Dritte offenbart werden, wenn der Betroffene entweder eingewilligt oder auf sein Widerspruchsrecht verzichtet hat.

Offenbarung von Sozialdaten

Wiederholt wurde ich vor die Frage gestellt, in welchem Verhältnis das Sozialgeheimnis zu den **Prozeßordnungen** steht, insbesondere, in welchem Umfang eine Aussagegenehmigung vor Gericht durch den zuständigen Vorgesetzten erteilt werden darf. Hintergrund war in einem Fall, daß ein Kind den Unterhaltsanspruch gegen den Vater dahingehend abändern lassen wollte, daß der Vater Unterhalt in Form einer monatlichen Geldrente und nicht durch Aufnahme in den väterlichen Haushalt zu gewähren habe. Ein Vormundschaftsgericht hatte das Jugendamt aufgefordert, hierzu Auskunft zu erteilen. Das Jugendamt hat, nachdem der Vater seine Einwilligung zur Datenoffenbarung verweigert hatte, dies abgelehnt und eine Aussagegenehmigung nicht gewährt. Einhellig besteht die Ansicht, daß die Vorschrift des Sozialgeheimnisses in § 35 Abs. 1 und insbesondere Abs. 3 SGB I klarstellt, daß auch Prozeßordnungen das Sozialgeheimnis nicht durchbrechen. Die Regelungen der Zivilprozeßordnung über den Beweis durch Zeugenvernehmung, also insbesondere die §§ 376 Abs. 1 und 383 Abs. 1 Nr. 6 werden somit ergänzt und für den Bereich der in § 35 SGB I genannten Stellen insofern konkretisiert, als Zeugenaussagen nur im Rahmen der Offenbarungsbefugnisse nach §§ 68 ff. SGB X rechtmäßig sind. Dies gilt auch für vormundschaftsgerichtliche Verfahren, da § 15 FGG die Vorschriften der Zivilprozeßordnung für anwendbar erklärt. Besonderheiten könnten allenfalls bei der Auslegung der §§ 68 ff. SGB X bestehen, wenn im vormundschaftsgerichtlichen Verfahren das Amtsermittlungsprinzip herrscht, nicht jedoch beim Grundsatz des § 35 SGB I. Dies folgt schon daraus, daß bei dem noch strengeren Amtsermittlungsgrundsatz des Strafverfahrensrechts ebenfalls § 35 SGB I zu berücksichtigen ist und Offenbarungen nur im Rahmen der §§ 69 Abs. 1 Ziff. 1 und 73 SGB X erfolgen dürfen. Eine Offenbarungsbefugnis aus § 74 SGB X konnte in dem mir vorgelegten Fall des vormundschaftsgerichtlichen Verfahrens nicht angenommen werden, da die Bestimmungsänderung des Unterhalts nach § 1612 Abs. 2 Satz 2 BGB in das Vorfeld der von § 74 Ziff. 1 SGB X erfaßten Problematik fällt.

Im vorangegangenen Jahr hatte ich auf ein Rundschreiben verwiesen, das zur Auslegung des § 68 SGB X bei der Gewährung von Auskünften zum Zwecke der Strafverfolgung an die Polizei verfaßt wurde[1]. Meine Beobachtungen haben ergeben, daß dadurch eine wesentliche Beruhigung und Klärung im Zusammenwirken von Polizei und Sozialbehörden eingetreten ist. Mißverständnisse sind vor allem noch dort aufgetreten, wo dieses Rundschreiben nicht hinreichend bekannt geworden ist.

Die Regelung wird durch folgenden Fall illustriert:

Die Polizei hatte die Kopie eines Haftbefehls gegen einen Sozialhilfeempfänger einem Sozialamt übersandt, mit der Bitte, diesen beim Abholen der Sozialhilfe festzuhalten und die Polizei entsprechend zu informieren. Diesem Ersuchen konnte nicht ohne weiteres nachgekommen werden, weil die Voraussetzungen des § 68 SGB X nicht vorlagen und ein Haftbefehl nicht mit der richterlichen Anordnung gemäß § 73 SGB X gleichzusetzen ist. Der zuständige Sachbearbeiter des Bezirksamtes bat daher den Hilfeempfänger vorsorglich um seine Einwilligung, um wegen des Haftbefehls bei der Polizei nachfragen zu dürfen. Dabei stellte sich heraus, daß der Haftgrund schon entfallen war und nach dem Hilfeempfänger nicht mehr gefahndet wurde. Es war lediglich der Umsicht des zuständigen Sachbearbeiters zu danken, daß dem Hilfeempfänger größte Unannehmlichkeiten erspart blieben.

Noch unbefriedigend ist die in der Verwaltungsvorschrift zur Änderung der Ausführungsvorschriften über die Gewährung von Hilfe nach dem Bundessozialhilfegesetz an **Ausländer** geregelte Verfahrensweise bei Auskünften über den Sozialhilfeempfang von Ausländern an die Ausländerbehörde. Gemäß Ziff. 33 b sollen auch die Ausländer an die Ausländerbehörde gemeldet werden, auf die das europäische Fürsorgeabkommen anzuwenden ist. Diese aus meiner Sicht nicht zulässige Regelung war Gegenstand mehrerer Beschwerden. Meiner Auffassung wurde bisher entgegengehalten, daß durch das internationale Fürsorgeabkommen lediglich die Ausweisung beschränkt wird, jedoch nicht andere ausländerrechtliche Maßnahmen, und daß daher die Übermittlung des Sozialhilfeempfangs erforderlich sei. Diese Auffassung ist jedoch unzutreffend, weil gemäß § 71 Abs. 2 SGB X lediglich eine Datenübermittlung für die Zwecke nach § 10 Abs. 1 Nr. 7, 9 und 10 und § 11 Ausländergesetz zulässig ist. Eine Datenübermittlung zur Vorbereitung anderer ausländerrechtlicher Maßnahmen sieht das Sozialgesetzbuch nicht vor. Da die Offenbarungsbefugnisse jedoch dort abschließend geregelt sind,

[1] Vgl. Anlage 3

kann mithin eine Datenübermittlung zu anderen ausländerrechtlichen Zwecken nicht zulässig sein.

Vertraulichkeit

Die datenschutzgerechte Abwicklung der Dienstgeschäfte in zahlreichen Ämtern, die die Vorschriften des Sozialgesetzbuches zu beachten haben, bereitet vielen Ämtern Schwierigkeiten. Die mithörsichere Beratung ist hierbei nach wie vor zu nennen, obwohl sich eine zunehmende Bereitschaft zeigt, im Einzelfall auf besonderen Wunsch individuell zu beraten. Eine gravierende Beeinträchtigung des Sozialgeheimnisses sah ich in einem Bezirk darin, daß alle Besucher des Sozialamtes sich in eine im Wartezimmer ausliegende Liste eintragen mußten (mit Name, Adresse und dem Grund ihres Besuchs), so daß jeder Neuankömmling die Anliegen der anderen Besucher zur Kenntnis nehmen konnte. Ich habe die Abschaffung dieses Verfahrens empfohlen. Ähnlich zu beurteilen war die in dem gleichen Bezirk bei einem anderen Amt festgestellte Verwendung einer „Scheckliste", in der die Scheckempfänger mit Namen, Anschrift und Leistungsgrund eingetragen waren und selbst durch ihre Unterschrift den Empfang des Schecks quittieren mußten. Angeblich sollte die Liste jeweils abgedeckt sein. Es ist jedoch praktisch kaum zu kontrollieren, ob dies wirklich geschieht.

Ein Hilfeempfänger beschwerte sich darüber, daß zur Nachprüfung seiner Unterhaltsfähigkeit die Nachweise über seine Einkommens- und Vermögensverhältnisse fälschlicherweise fotokopiert worden und dann „im Papierkorb" gelandet seien. Die zuständige Verwaltung sicherte zu, daß künftig an Stelle von Fotokopien derartige Nachweise durch einen entsprechenden Aktenvermerk des Sachbearbeiters nach Vorlage der Urkunden erfolgen würden, und daß der Inhalt der Papierkörbe „datenschutzgerecht" in einem verschlossenen Keller der Abteilung Sozialwesen aufbewahrt und von Mitarbeitern des Amtes in der Müllverbrennungsanlage Ruhleben vernichtet wird.

Auch bei der Auswahl der Beweismittel ist der Grundsatz der Verhältnismäßigkeit zu beachten. Dementsprechend habe ich dem Landesversorgungsamt abgeraten, den Nachweis der Einkünfte aus Kapitalvermögen bei Empfängern von Hinterbliebenenrenten durch das Ablichten von Sparbüchern zu führen. Künftig wird über die Zinseinkünfte aus Sparbucheinlagen ein Kontoauszug unter Verwendung eines neugeschaffenen Vordrucks, der zu den Akten genommen wird, Beweis geführt.

Besondere Leistungen

In der Öffentlichkeit wurden Befürchtungen laut, daß beim Betrieb des **Telebusses** Aufzeichnungen über Einzelfahrten vorgenommen würden. Dies trifft nicht zu. Die Software des Telebusfahrdienstes läßt es nicht zu, Benutzerprotokolle mit personenbezogenen Daten zu erstellen. Die Aufbewahrungsfrist der Fahrtwunschkarten mit personenbezogenen Daten ist auf vier Wochen reduziert. Bei der Durchführung des Telebusdienstes ist im Berichtsjahr eine grundsätzliche Änderung eingetreten. Bisher erfolgte die Erteilung der Telebusberechtigung durch den Berliner Zentralausschuß selbst, wobei die Erteilung der Berechtigung im Auftrage der Senatsverwaltung für Gesundheit, Soziales und Familie erfolgte. Diese Aufgabe ist auf das Landesversorgungsamt verlagert worden. Daraus ergab sich die Frage, ob im Zuge der Aufgabenverlagerung die beim Berliner Zentralausschuß befindliche Datei der Telebusberechtigten dem Landesversorgungsamt übermittelt werden durfte und ob das Landesversorgungsamt nach Erteilung eines Bewilligungsbescheides dem Berliner Zentralausschuß eine Mitteilung über die Bewilligung der Telebusberechtigung geben darf. Da der Berliner Zentralausschuß privatrechtlich organisiert ist, ist die Übermittlung der Datei an das Landesversorgungsamt an den Vorschriften des Bundesdatenschutzgesetzes zu messen. Der hier einschlägige § 24 BDSG regelt allerdings nur die Datenübermittlung, nicht jedoch die Übertragung von Aufgabenbereichen. Da der Vorgang in seiner Wirkung einer Datenübermittlung gleichkommt, muß der Rechtsgedanke des § 24 BDSG gleichwohl angewandt werden. Nach § 24 BDSG kann eine Datenübermittlung scheitern, wenn schutzwürdige Belange der Betroffenen entgegenstehen. Schutzwürdige Belange konnten daher berührt werden, wenn mehr als lediglich die Tatsache, daß der Betroffene „berechtigt" ist, den Telebus zu benutzen, mitgeteilt werden sollten. Für Daten, die dem Schutz des § 203 StGB oder des Sozialgesetzbuches unterstehen, habe ich die besondere Schutzwürdigkeit der Belange der Betroffenen bejaht und deshalb gefordert, eine Einwilligung für die Datenübermittlung zum Zwecke der Aufgabenübertragung einzuholen. Auch bei der Übermittlung des Bewilligungsbescheides vom Landesversorgungsamt an den Berliner Zentralausschuß kommt es auf die besondere Schutzwürdigkeit der Daten gemäß § 76 SGB X an, denn das Landesversorgungsamt ist seinerseits unmittelbar an das Sozialgesetzbuch gebunden. Die Übermittlung von Gesundheitsdaten ist danach unzulässig, wenn ein Betroffener von seinem Widerspruchsrecht Gebrauch gemacht hat. Auf dieses Widerspruchsrecht muß er hingewiesen worden sein. Allerdings könnte die Ausübung des Widerspruchsrechtes leistungsrechtliche Konsequenzen haben. Das Landesversorgungsamt hat die Berücksichtigung dieser Grundsätze zugesagt.

Die neu gegründete **Stiftung Hilfe für die Familie - Stiftung des Landes Berlin** - unterliegt als öffentlich-rechtliche Organisation meiner Kontrollbefugnis, jedoch ist diese Stiftung kein Sozialleistungsträger im Sinne des Sozialgesetzbuches, obwohl sie in sozial problematischen Fällen schwangeren Frauen Unterstützung gewähren soll. Die zu verteilenden Mittel werden aufgrund eines Antrags gewährt, über den nach den „Richtlinien für die Vergabe von Mitteln der Stiftung Hilfe für die Familie - Stiftung des Landes Berlin -" entschieden wird. Problematisch war es hier, eine interessen- und zugleich datenschutzgerechte Klausel für die Datenübermittlung und Datenerhebung zu finden. Obwohl das Sozialgesetzbuch formal nicht gilt, muß sich die Stiftung im Hinblick auf den Sozialdatenschutz wegen der engen funktionalen Verwandtschaft der Tätigkeit entsprechend am Sozialgesetzbuch orientieren.

5. Nachtrag zu Feststellungen aus den Vorjahren

Nachweis der Berechtigung zum Bezug von Leistungen (Jahresbericht 1984, S. 27)

Aufgrund eines erneuten Vorstoßes erteilt nunmehr das Landesarbeitsamt auf Antrag aus der automatischen Leistungsdatei Bescheinigungen, die zur Gewährung von Fahrpreisermäßigungen bei der BVG vorgelegt werden können.

Fehlauskünfte aus dem Melderegister (Jahresbericht 1984, S. 21 f.)

Zur Vermeidung von Fehlauskünften ist der Polizeipräsident in Berlin meiner Empfehlung gefolgt und hat in einer Geschäftsanweisung die von mir aufgeführten Kriterien für eine ordnungsgemäße Identitätsfeststellung von gesuchten Personen festgelegt.

Anordnung über Mitteilungen in Strafsachen (Jahresbericht 1984, S. 24)

Eine gesetzliche Grundlage für die Mitteilungen in Strafsachen ist nach wie vor nicht vorhanden. Für eine Übergangszeit haben jedoch die Landesjustizverwaltungen und der Bundesminister der Justiz eine Neufassung der Anordnung vereinbart, die seit dem 1. April 1985 in Kraft ist.

Übermittlung personenbezogener Daten vom Amtsarzt an die Dienstbehörde (Jahresbericht 1984, S. 9 f.)

Mit dem Senator für Gesundheit und Soziales wurde im Ergebnis Übereinstimmung darin erzielt, daß auch ohne ausdrückliche Einwilligung der Betroffenen bei amtsärztlichen Begutachtungen Art und Ausmaß der Funktionseinbuße mitgeteilt werden dürfen, die den Beamten zur weiteren Ausübung seines Dienstes unfähig machen.

Schülerdaten
(Jahresbericht 1980, S. 13; Jahresbericht 1981, S. 11 f.; Jahresbericht 1982, S. 19 f.; Jahresbericht 1983, S. 24; Jahresbericht 1984, S. 28[1])

Der Entwurf von Ausführungsvorschriften über Schülerbogen, der meine Empfehlungen weitgehend aufgegriffen hat, lag den Gremien nach dem Schulverfassungsgesetz zur Zustimmung vor. Im Laufe des Verfahrens konnten weitere datenschutzrechtliche Fortschritte erzielt werden.

Betriebsdatenbank
(Jahresbericht 1982, S. 17)

Unter der Bezeichnung Gewerbedatenbank plant der Senator für Wirtschaft und Arbeit den Aufbau eines Dialog-Verfahrens für die Bezirksämter (Abteilung Wirtschaft) zur Erfassung, Speicherung und Auswertung von Daten aus den Anzeigen nach den §§ 14 und 55 c der Gewerbeordnung sowie § 1 Gewerbeanzeigen-Verordnung. Dieses Verfahren stellt eine Modifizierung des ursprünglich für die Verarbeitung der Gewerbeanzeigen konzipierten Teils des ADV-Projektes „Betriebsdatenbank" dar. Es wird als Pilotprojekt für das Bezirksamt Wilmersdorf von Berlin, Abteilung Finanzen und Wirtschaft, in diesem Jahr begonnen und soll 1986 auf die übrigen Bezirke übertragen werden.

Eine wesentliche Neuerung zum ehemals geplanten Projekt „Betriebsdatenbank" ist die Verlagerung der Zuständigkeit auf die speichernde Stelle, nämlich die für Wirtschaft zuständige Abteilung des jeweiligen Bezirksamtes. Ursprünglich wurden der Senatsverwaltung umfangreiche Kompetenzen eingeräumt, die zum Teil den Datenschutzvorschriften, hier speziell § 4 Abs. 3 Ziff. 1 BlnDSG zuwiderliefen.

Ein anderes Problem - nämlich das der Zugriffsregelung auf den Datenbestand der Gewerbedatenbank durch die Gewerbesachbearbeiter der Bezirksämter - ist ebenfalls aufgrund meiner damaligen Bedenken modifiziert worden. Durch technisch-organisatorische Maßnahmen soll nun gewährleistet sein, daß die jeweiligen Sachbearbeiter eines bestimmten Bezirksamtes nur auf den Teil des Gesamtdatenbestandes zugreifen dürfen, der für die Erfüllung ihrer Aufgaben notwendig ist.

6. Zusammenarbeit mit anderen Stellen

Datenschutzbeauftragte des Bundes und der Länder

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

22. Konferenz am 23./24. Januar 1985:
- Beschluß über Anforderungen an Datenschutzregelungen im Polizeirecht[2]

23. Konferenz am 9./10. Mai 1985:
- Beschluß über die Handels- und Gaststättenzählung 1985
- Beschluß zum Datenschutz bei der Perinataldokumentation

Sonderkonferenz am 16. September 1985:
- Beschluß über Anforderungen an Datenschutzregelungen für den Verfassungsschutz[3]
- Beschluß zu den Mitteilungen in Zivilsachen (MiZi)

24. Konferenz am 14./15. November 1985:
- Beschluß zur Speicherung personengebundener Hinweise im INPOL-System

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

Abgeordnetenhaus

Vor Ablauf der 8. Legislaturperiode des Abgeordnetenhauses von Berlin konnten im Januar 1985 noch das Meldegesetz und das Gesetz für psychisch Kranke verabschiedet werden. Die in beiden Gesetzen enthaltenen datenschutzrelevanten Bestimmungen sind das Ergebnis einer intensiven Zusammenarbeit mit dem Ausschuß für Inneres, Sicherheit und Ordnung und dem Ausschuß für Gesundheit, Soziales und Familie sowie den im Abgeordnetenhaus vertretenen Fraktionen. Darüber hinaus bestanden in Einzelfragen Kontakte zum Petitionsausschuß und zum Ausländerausschuß sowie zu dem Unterausschuß des Innenausschusses „Berichte des Berliner Datenschutzbeauftragten", der seine Arbeit inzwischen aufgenommen hat. Die von mir unter Datenschutzgesichtspunkten als vordringlich angesehenen Gesetzgebungsvorhaben habe ich oben (1.) und in der Anlage 1 dargestellt. Fortschritte in diesen Bereichen können nur erzielt werden, wenn sich die bisher positive Zusammenarbeit zwischen dem Parlament, den Fraktionen und einzelnen Abgeordneten und dem Datenschutzbeauftragten auch in Zukunft weiter fortsetzt.

Aufsichtsbehörde für nicht-öffentliche Stellen

Im Rahmen der bewährten Zusammenarbeit mit der Aufsichtsbehörde für den Datenschutz beim Senator für Inneres wurden u.a. die folgenden Fragen behandelt: Gemeinsame Probleme der Bildschirmtext-Aufsicht, Datenschutz bei Banken, Einsicht in Krankenunterlagen, Erhebung personenbezogener Daten durch Wohnungsvermieter.

7. Aufgaben des Berliner Datenschutzbeauftragten

7.1 Im Berichtsjahr 1985

Die Zahl der **schriftlichen Eingaben** ist gegenüber dem Vorjahr leicht gestiegen. Sie entfallen nach der Häufigkeit geordnet insbesondere auf folgende Gebiete:

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

Ähnlich wie im Vorjahr haben sich in mehr als 50 % der Eingaben Mängel herausgestellt.

Die Bearbeitung der Eingaben konnte in der Regel mit Unterstützung der betroffenen Behörden zügig und sachgerecht erfolgen. Dennoch traten auch in diesem Jahr in Einzelfällen Verzögerungen deswegen ein, weil die von mir angesprochenen speichernden Stellen, teilweise auch nach mehrfacher Mahnung, der gesetzlich vorgeschriebenen Unterstützungspflicht nicht oder nur nach ungebührlich langer Bearbeitungszeit nachkamen. Häufig wird dies damit begründet, daß vor einer Stellungnahme eine oder mehrere Aufsichtsbehörden eingeschaltet werden müßten. Hierzu ist festzuhalten, daß auch die Mitwirkung anderer Stellen die speichernde Stelle nicht von ihren eigenen Pflichten befreit.

Zu mißlichen Folgen führen zu lange Bearbeitungszeiten insbesondere dann, wenn - wie bei den Straftaten wegen Verletzung des persönlichen Lebens- und Geheimbereichs (§§ 201 ff. StGB) oder der Datenschutzbestimmungen (§ 28 BlnDSG, § 41 BDSG) - die dreimonatige Strafantragsfrist läuft. Häufig möchten die Betroffenen den Sachverhalt auf seine tatsächliche und rechtliche Relevanz vom Datenschutzbeauftragten prüfen lassen, bevor sie sich dazu entschließen, einen Strafantrag zu stellen. Dieser - verständliche - Wunsch wird vereitelt, wenn die Antragsfrist während der Bearbeitungszeit abläuft.

---

[1] Aufgrund eines technischen Versehens wurde in der gedruckten Fassung meines Jahresberichtes auf Seite 28 unter der Überschrift „Schülerdaten" der falsche Text abgedruckt:
Der Senator für Schulwesen, Jugend und Sport hat den Entwurf von Ausführungsvorschriften über die Führung von Schülerakten und ergänzt. Die derzeit vorliegende Fassung berücksichtigt weitestgehend meine Empfehlungen. Hervorzuheben ist, daß erstmals auch die automatische Verarbeitung von Schülerdaten, insbesondere auch in Kleincomputern geregelt wird.

[2] vgl. Anlage 2

[3] vgl. Anlage 4

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

Auch bei den Beratungsersuchen (§ 21 Abs. 1 letzter Satz BlnDSG) war wiederum eine Zunahme zu beobachten.

Das von mir zu führende **Dateienregister** enthält nunmehr 1234 Dateien (Vorjahr 1006) von 269 (256) speichernden Stellen. Es gibt jetzt einen guten Überblick über die automatisierten Dateien des öffentlichen Bereichs. Daher hat sich das Register auch zu einem wirksamen Instrument für die Kontrolle der Datenverarbeitung in Berlin entwickelt. Um die Transparenz der öffentlichen Verwaltung zu erhöhen, werde ich den allgemeinen, jedermann zugänglichen Teil des Datenregisters auszugsweise veröffentlichen.

7.2 Voraussichtliche Schwerpunkte

Aufgrund der bisherigen Erfahrungen ergeben sich folgende Schwerpunkte für das Jahr 1986:

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

- Kleincomputern;
- Anwendung der Fernverarbeitung, insbesondere in offenen Netzen;
- weiteren öffentlichen Stellen, u. a. auch bei den Bezirksämtern.

Berlin, 16. Dezember 1985

Der Berliner Datenschutzbeauftragte
Dr. Kerkau

Anlage 1

Übersicht der wesentlichen datenschutzrelevanten Gesetzesvorhaben auf Landesebene

Gesetzesvorhaben	Datenschutzrelevante Punkte	Abhängigkeit von Vorhaben auf Bundesebene	Verfahrensstand in Berlin	Bemerkungen
1. LandeskrankenhausG Novellierung	Insbesondere Regelung des Rechts des Patienten, in seine Krankenunterlagen Einsicht zu nehmen.		Vorschläge einer Arbeitsgruppe einschließlich einer Stellungnahme des BlnDSB liegen vor.	Beratung im Abgeordnetenhaus ist ca. 1986 zu erwarten.
2. LandesstatistikG	Regelung des Statistikgeheimnisses. Aufbewahrung/Löschung von Daten, Abgrenzung Verwaltungsstatistik/Statistik des StaLa, Neuregelung der Struktur- und Planungsdatenbank, Auftragsstatistiken für Dritte.	Beratung der Novelle des Bundesstatistikgesetzes durch den Bundestag hat im Herbst 1985 begonnen.	Referentenentwurf und Stellungnahme des BlnDSB liegt vor.	Der Zeitpunkt der Beratungen im Abgeordnetenhaus (ca. 1986/87) hängt nicht zuletzt vom Fortschritt der Beratungen des Bundestages über das Bundesstatistikgesetz ab.
3. LandesarchivG	Regelung des Zugangs zu den Archiven (Fristen) und Art der Verwertung.	BundesarchivG Beginn der Beratungen im Bundestag Herbst 1985.	Referentenentwurf, Stellungnahme des BlnDSB und Beschluß der Konferenz der DSB liegen vor.	Der Zeitpunkt der Beratungen im Abgeordnetenhaus (ca. 1986/87) hängt vom Fortgang der Beratungen auf Bundesebene ab.
4. BibliotheksG	Art und Umfang der zu erhebenden Daten der Benutzer, Löschung dieser Daten.			
5. LandesbeamtenG Novellierung	Umgang mit Personaldaten, Personalakten.	Der Bundestag hat einen Bericht angefordert, der 1986 von einer interministeriellen Arbeitsgruppe erstattet werden soll. Mit gesetzlichen Maßnahmen auf Bundesebene wird vorerst nicht gerechnet.	**Entwurf** des Senators für Inneres von **Verwaltungsvorschriften** über die Führung von Personalakten der Dienstkräfte des Landes Berlin (Stand August 1984) und Stellungnahme des BlnDSB (Dezember 1984).	Eine gesetzliche Regelung ist frühestens gegen Ende der laufenden Legislaturperiode des Abgeordnetenhauses zu erwarten. Jedenfalls sollten die Verwaltungsvorschriften alsbald verabschiedet werden.
6. Meldewesen				
6.1 MelderechtsrahmenG	Überprüfung aufgrund des Benda-Gutachtens (u. a. Krankenhausmeldepflicht).	Eine Regelung in Berlin hängt direkt von einer Bundesregelung ab. Eine Reaktion des Bundes auf das Benda-Gutachten ist nicht bekannt.	Entscheidend ist die Entwicklung auf Bundesebene.	Berlin sollte über den Bundesrat initiativ werden.
6.2 Durchführung des LandesmeldeG (Erlaß der Durchführungsvorschriften)	Unter anderem Meldescheine für Hotels, regelmäßige Datenübermittlungen.		Referentenentwurf. Eine Anhörung des BlnDSB ist vorgeschrieben. Stellungnahme des BlnDSB liegt vor.	(Die geplante Aufstellung der regelmäßigen Datenübermittlungen im Jahresbericht kann erst nach Inkrafttreten der Durchführungsvorschriften erfolgen.)
7. ASOG Novellierung	Regelung der Informationssammlung und -verwertung, z. B. Videoüberwachung, Rasterfahndung.	Die Innenministerkonferenz strebt einen Musterentwurf für Polizeigesetze an. Ein erster Entwurf liegt vor. Eine Novellierung der StPO wird vom BMI vorbereitet. Ein erster Entwurf liegt ebenfalls vor.	Stellungnahme des BlnDSB und Beschluß der Konferenz der DSB liegen vor.	Es sollte angestrebt werden, das ASOG noch in dieser Legislaturperiode des Abgeordnetenhauses zu novellieren.
8. VerfassungsschutzG Novellierung	Regelung der Informationssammlung und -verwertung.	Erste Entwürfe liegen vor.	Stellungnahme der Konferenz der DSB und des BlnDSB liegen vor.	Die Regelung auf Bundesebene sollte abgewartet werden.
9. ADVG	Gesetzliche Regelung des ADV-Einsatzes im öffentlichen Bereich. Unter anderem Regelung der Verfahrensabwicklung des Kleincomputereinsatzes, des LED, der öffentlichen Datennetze etc.		Es muß geprüft werden, ob eine derartige Regelung sinnvoll ist.	Die Prüfung durch den BlnDSB ist für 1986/87 vorgesehen.
10. BlnDSG Novellierung	Anpassung an die technische Entwicklung. Berücksichtigung der Rechtsprechung etc.	Die Verabschiedung eines novellierten BDSG sollte abgewartet werden.		

Anlage 2

Anforderungen an Datenschutzregelungen im Polizeirecht

Beschluß der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 24. Januar 1985

I.

Notwendigkeit bereichsspezifischer Regelungen

1. Die Datenschutzbeauftragten des Bundes und der Länder haben seit Jahren auf die Notwendigkeit präziser gesetzlicher Regelungen für die Datenverarbeitung durch die Vollzugspolizei hingewiesen. Einzelne Maßnahmen wie z. B. die polizeiliche Beobachtung oder die Verarbeitung von Daten Unbeteiligter stehen weitgehend im Widerspruch zum geltenden Polizei- und Strafverfahrensrecht. Gesetzlich nicht hinreichend abgedeckt sind insbesondere die Erhebung und Nutzung personenbezogener Daten zu Zwecken der vorbeugenden Bekämpfung von Straftaten.

   Spätestens seit dem Urteil des Bundesverfassungsgerichts zum Volkszählungsgesetz ist eine bereichsspezifische Regelung der polizeilichen Informationsverarbeitung unerläßlich. Dabei kann es nicht darum gehen, die derzeitige, durch eine Ausweitung der Datenverarbeitung gekennzeichnete Praxis der Datenverarbeitung festzuschreiben, sie muß vielmehr überprüft und der Umfang zulässiger Informationsverarbeitung durch spezielle Befugnisnormen konkret bestimmt und begrenzt werden.

2. Eine solche Regelung muß zumindest die nachfolgenden Grundsätze beachten. Diese Grundsätze sollten - evtl. differenziert je nach spezifischer Aufgabenzuweisung - sowohl in den Polizeigesetzen des Bundes und der Länder als auch in der Strafprozeßordnung, soweit es um gleichartige Maßnahmen geht, berücksichtigt werden.

II.

Grundsätze polizeilicher Informationsverarbeitung

1. Allgemeine Prinzipien

1.1 Die gesetzlichen Regelungen über die Informationsverarbeitung müssen die polizeilichen Befugnisse klar und rechtsstaatlich umschreiben. Dies bedeutet

- dem Gebot der Normenklarheit entsprechende Spezialregelung und damit die Zurückdrängung von Generalklauseln,
- Beachtung des Grundsatzes der Verhältnismäßigkeit,
- prinzipielle Beschränkung auf die Aufgaben Gefahrenabwehr und Strafverfolgung,
- Beachtung des Grundsatzes der Zweckbindung der Daten.

1.2 In Übereinstimmung mit dem vom Bundesverfassungsgericht anerkannten Recht auf informationelle Selbstbestimmung müssen die Regelungen jede Art und Form der Verarbeitung personenbezogener Daten durch die Polizei erfassen.

Sowohl die Erhebung als auch jede Nutzung von Daten sind in die Regelung mit einzubeziehen.

Die Form der Verarbeitung ist bei der Intensität der einzelnen Regelung zu berücksichtigen.

Die Speicherung personenbezogener Merkmale wie Krankheit oder besonderer Verhaltensweisen, insbesondere mit Hilfe automatischer Verfahren, ist nur zulässig, wenn die möglichen Verwendungen in einem angemessenen Verhältnis zu den Gefahren für die schutzwürdigen Belange der Betroffenen stehen. Durch die Automatisierung darf keine Verzerrung oder unangemessene Verkürzung des Sachverhalts entstehen.

2. Für die Datenverarbeitung sollten folgende Grundsätze Beachtung finden:

2.1 Zum Erheben und Speichern personenbezogener Daten

2.1.1 Grundsätze

Die Verarbeitung von Daten muß grundsätzlich der Abwehr einer im einzelnen Fall bestehenden (konkreten) Gefahr oder der Aufklärung einer konkreten Straftat dienen.

- Eine darüber hinausgehende Verarbeitung kann nur in eng begrenzten Fällen zugelassen werden. Insbesondere bedürfen Befugnisse zur vorbeugenden Bekämpfung von Straftaten einer klaren abschließenden Umschreibung im Gesetz.
- Für die Erfüllung spezialgesetzlich zugewiesener Aufgaben stehen der Polizei nur die jeweiligen spezialgesetzlichen Befugnisse zu.
- Der Bürger muß - wie zuletzt auch das Bundesverfassungsgericht im Volkszählungs-Urteil festgestellt hat - grundsätzlich unbeobachtet von staatlichen Stellen an Versammlungen teilnehmen können. Bei Befugnissen zur Informationserhebung in Versammlungen ist stärker als in der bisherigen Praxis dem Grundrecht der Versammlungsfreiheit Rechnung zu tragen.

Werden personenbezogene Informationen in Dateien gespeichert, müssen die Herkunft und die Richtigkeit der Informationen in Akten oder anderen Unterlagen nachweisbar sein. Werden Bewertungen gespeichert, muß erkennbar sein, wer die Bewertungen vorgenommen hat und wo die Erkenntnisse gespeichert sind, die ihnen zugrundeliegen.

2.1.2 Datenerhebung und -speicherung

- Die Gewinnung von Informationen muß grundsätzlich offen geschehen; heimliche Informationserhebung ist nur dann zulässig, wenn dies zur Aufgabenerfüllung im Einzelfall unerläßlich ist.
- Die Erhebung durch selbsttätige Lese- und Aufzeichnungsgeräte ist gesetzlich zu regeln.
- Bei Erhebung von Daten unter Mitwirkung des Betroffenen ist dieser in der Regel auf seine Aussage- oder Mitwirkungspflicht oder auf die Freiwilligkeit hinzuweisen.
- Werden heimlich erhobene Daten gespeichert, ist der Betroffene grundsätzlich nach Wegfall der Zweckgefährdung zu informieren.
- Die Anfertigung und Aufbewahrung erkennungsdienstlicher Unterlagen muß präziser und restriktiver geregelt werden. Vorschriften über die Anfertigung und Verarbeitung von erkennungsdienstlichen Unterlagen dürfen nicht durch neue technische Möglichkeiten umgangen werden (z. B. Überwachung bestimmter Orte durch Videogeräte, automatische Stimmerkennung).
- Die Übernahme der in Strafermittlungsverfahren erhobenen Informationen in Unterlagen für Zwecke der Gefahrenabwehr und vorbeugenden Bekämpfung von Straftaten ist an strenge Voraussetzungen zu knüpfen.
- Der Abgleich von oder mit Fremddatenbeständen darf künftig nur zur Abwehr erheblicher gegenwärtiger Gefahren sowie zur Aufklärung abschließender festgelegter schwerer Straftaten zugelassen werden. Die hierbei gewonnenen Daten müssen einer strengen Zweckbindung unterliegen. Voraussetzungen, Art und Umfang des Abgleichs, Verwertung und Dauer der Aufbewahrung sind im Gesetz abschließend zu regeln.
- Der Einsatz besonderer Verfahren, die über ein Aktenhinweissystem hinausgehen (z. B. Spurendokumentationsverfahren), bedarf einer gesetzlichen Regelung.
- Personenbezogene Daten dürfen grundsätzlich nur bei der sachbearbeitenden Dienststelle in kriminalpolizeilichen Sammlungen oder entsprechenden Dateien gespeichert werden. Die Speicherung dieser personenbezo-

genen Daten bei polizeilichen Zentralstellen ist nur aufgrund ausdrücklicher gesetzlicher Regelung zulässig.

- Erkenntnisfragen oder Bitten um Amtshilfe dürfen bei den angefragten Stellen grundsätzlich nicht zur Anlage kriminalpolizeilicher Personenakten oder -dateien führen. Gleiches muß für bloße Unterrichtungen gelten.

2.2 Übermittlung von Daten

2.2.1 Die zu polizeilichen Zwecken gewonnenen Daten sind grundsätzlich zweckgebunden zu verwerten.

2.2.2 Bei der Übermittlung an Polizeibehörden ist hinsichtlich Art und Inhalt nach der konkreten polizeilichen Funktion und Zuständigkeit zu unterscheiden. Die Datenübermittlung an zentrale Stellen ist restriktiv zu regeln; das gilt auch für Erkenntnisanfragen und deren Beantwortung.

2.2.3 Eine Übermittlung an andere als Polizeibehörden und sonstige öffentliche Stellen sowie an Privatpersonen ist nur im Einzelfall zulässig und nur

- zur Abwendung einer konkreten Gefahr, einer erheblichen sozialen Notlage oder
- zur Verfolgung von öffentlich-rechtlichen oder zivilrechtlichen Ansprüchen in Fällen von Beweisnot,

und nur, wenn hierfür eine ausdrückliche gesetzliche Regelung besteht. Bei Anfragen, deren Beantwortung in die Zuständigkeit anderer Stellen fällt, hat die Polizei grundsätzlich an diese Stellen zu verweisen. Die Vorschriften des Bundeszentralregistergesetzes dürfen nicht durch polizeiliche Auskunft unterlaufen werden.

Eine Datenübermittlung an Nachrichtendienste darf wegen der verfassungsrechtlich gebotenen Trennung von polizeilicher und nachrichtendienstlicher Tätigkeit entgegen der derzeitigen Praxis nur in engen Grenzen zugelassen werden. Ein geeigneter Maßstab sind die Übermittlungsregelungen nach dem Gesetz zu Art. 10 GG.

Bei der Übermittlung an ausländische Stellen ist durch geeignete Absprachen und durch die Vereinbarung internationaler Regelungen sicherzustellen, daß die innerstaatlichen Grundsätze des Datenschutzes nicht gefährdet werden.

2.2.4 Vor jeder Übermittlung hat die auskunftgebende Stelle grundsätzlich die Richtigkeit der vorhandenen Unterlagen und deren Erforderlichkeit für die eigene Aufgabenerfüllung zu überprüfen. Wenn ein Verfahren noch nicht abgeschlossen ist, ist darauf hinzuweisen. Eine Übermittlung hat zu unterbleiben, wenn die Unterlagen zu vernichten sind.

2.2.5 Tatsache und Inhalt der Übermittlung sind in der Akte festzuhalten. Bei Veränderung wesentlicher Gesichtspunkte (z. B. Löschung) hat die übermittelnde Stelle die Änderung nachzuberichten, soweit dadurch nicht schutzwürdige Belange des Betroffenen beeinträchtigt werden.

2.3 Löschungs- und Überprüfungsvorschriften

Für die Aufbewahrung der Daten muß der Gesetzgeber differenziert Löschungs- und Überprüfungsvorschriften gesetzlich vorsehen. Insbesondere ist zu unterscheiden

- nach Alter des Betroffenen,
- nach der Schwere der Gefahr und der Straftat,
- nach der Art der Tatbegehung,
- nach der Art der Daten,
- nach dem Ausgang des Verfahrens.

Die gegenwärtig praktizierten Regelfristen (für Kinder 2 Jahre, für Jugendliche 5 Jahre, für Erwachsene 10 Jahre) dürfen nicht verlängert werden.

Daten, die allein zur Personenfeststellung erhoben wurden, sind unmittelbar nach Zweckerreichung zu vernichten.

2.4 Transparenz

Entsprechend der verfassungsmäßigen Garantie des Rechtsweges (Art. 19 Abs. 4 GG) hat der Einzelne grundsätzlich ein Recht auf vollständige Auskunft. Dieses umschließt

- die zu seiner Person gespeicherten Informationen,
- Zweck, Rechtsgrundlage und vorgesehene Dauer der Speicherung,
- Art der Gewinnung oder Herkunft der Informationen,
- die Tatsache und den Inhalt der Übermittlung an andere Stellen.

Ausnahmen hiervon sollten nur dann zulässig sein, wenn hierdurch die Erfüllung polizeilicher oder anderer Sicherheitsaufgaben gefährdet oder erheblich erschwert wird, überwiegende Interessen Dritter entgegenstehen oder die Erfüllung des Auskunftsanspruchs nur mit unverhältnismäßigem Aufwand möglich wäre.

Die Bearbeitung von Auskunftsersuchen muß getrennt von polizeilichen Informationssammlungen erfolgen. Die Tatsache der Antragstellung darf nicht zum Nachteil des Betroffenen verwertet werden.

2.5 Notwendige organisatorische Maßnahmen

Für die Anlage neuer und für die Überprüfung vorhandener personenbezogener Sammlungen sowie für Verbunddateien muß der Erlaß von Errichtungsanordnungen gesetzlich vorgesehen werden, die Regelungen enthalten über

1. die Bezeichnung, den Zweck und die Rechtsgrundlage der Sammlung,
2. den in die Sammlung aufzunehmenden Personenkreis,
3. die Art und den Umfang der zu speichernden Informationen, die der Erschließung dienen können,
4. die Übermittlung von Informationen,
5. die Dauer der Aufbewahrung der Informationen und
6. die zuständige Stelle für die Anlage und Führung von Sammlungen.

Diese Errichtungsanordnungen sind zu veröffentlichen.

Daten, die zur Vorgangsverwaltung oder nur zum Nachweis polizeilichen Handelns geführt werden, sind von Datensammlungen zur Gefahrenabwehr und Strafverfolgung zu trennen.

Anlage 3

Rundschreiben über die Offenbarung von Sozialdaten im Rahmen der Amtshilfe nach § 68 SGB X vom 22. März 1984 GesSozFam DSB - SGB X -; SchulJugSport DSB - SGB X -; ArbB DSB - SGB X -

Es muß festgestellt werden, daß noch immer Unsicherheit bei der Anwendung datenschutzrechtlicher Vorschriften im sozialen Bereich besteht und manche Rechtsfragen - trotz ihrer Bedeutung für die Alltagspraxis - nach wie vor kontrovers diskutiert werden. Hierzu gehört insbesondere die Frage der Amtshilfe nach § 68 SGB X gegenüber Nicht-Sozialleistungsträgern (wie z. B. den Strafverfolgungsbehörden).

Die Offenbarungsbefugnis nach § 68 SGB X besteht - unbeschadet der weiteren Regelungen in den § 69 ff SGB X - gegenüber allen Stellen, die Aufgaben der öffentlichen Verwaltung wahrnehmen, auch gegenüber den Strafverfolgungsbehörden (§ 1 Abs. 2 SGB X).

Dazu wird empfohlen:

1. Der Dezernent bestimmt den zuständigen Bediensteten im Sinne des § 68 Abs. 2 SGB X und ordnet ihm ein neutrales Stellenzeichen zu. Diese Kontaktperson ist allen bekannten potentiellen Anfragern zu benennen.
2. Bei der Datenoffenbarung im Wege der Amtshilfe ist sicherzustellen, daß Rückschlüsse auf ein konkretes Sozialleistungsverhältnis nicht möglich sind.
3. Soweit Daten mündlich offenbart worden sind, ist ein Vermerk über Umfang und Empfänger der Auskunft anzufertigen.
4. Die Datenoffenbarung ist auf die in § 68 Abs. 1 SGB X genannten Daten zu beschränken:
   - Vor- und Familiennamen
   - Geburtsdatum und -ort
   - derzeitige Anschrift
   - Namen und Anschriften des derzeitigen Arbeitgebers.

   Als Anschrift gelten insbesondere
   - der Wohnsitz (§ 30 Abs. 3 SGB I),
   - der gewöhnliche Aufenthalt (§ 30 Abs. 3 SGB I) oder
   - der tatsächliche Aufenthalt von längerer Dauer, z. B. in Heimen und Anstalten sowie anderen Orten des tatsächlichen Wohnens.

Amtshilfe darf nicht geleistet werden, wenn Grund zu der Annahme besteht, daß schutzwürdige Belange des Betroffenen beeinträchtigt werden (§ 68 Abs. 1 Satz 1 SGB X). Bei der Prüfung der schutzwürdigen Belange des Betroffenen - dabei kann es sich um wirtschaftliche, soziale oder persönliche Gründe handeln - ist auf den Einzelfall abzustellen. Das bloße Bewahren vor Strafverfolgung ist nicht schutzwürdig.

Die Offenbarung von Sozialdaten von Personengruppen ist hiernach nicht zulässig.

Amtshilfe braucht nicht geleistet zu werden, wenn

1. die ersuchende Behörde nicht dargelegt hat, daß sie sich die Angaben auf andere Weise nicht - oder nicht ohne unverhältnismäßigen Aufwand - beschaffen kann (§ 68 Abs. 1 Satz 2 SGB X).
2. die ersuchte Behörde unter Berücksichtigung der Aufgaben der ersuchenden Behörde durch die Offenbarung die Erfüllung ihrer eigenen Aufgaben ernstlich gefährden würde (§ 4 Abs. 3 Nr. 3 SGB X).

Anlage 4

Anforderungen an Datenschutzregelungen für den Verfassungsschutz

Beschluß der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 13. September 1985

I.

Notwendigkeit bereichsspezifischer Regelungen

1. Gerade für die Datenverarbeitung der Verfassungsschutzbehörden sind präzise gesetzliche Grundlagen erforderlich, da sie in besonderem Maße in das informationelle Selbstbestimmungsrecht eingreift, weil sie fast vollständig im Geheimen und somit unter Ausschluß der Öffentlichkeit und der Kontrolle durch den Betroffenen stattfindet.

   Ebenso wie im Polizeirecht kann es auch beim Verfassungsschutz nicht darum gehen, die derzeitige Praxis gesetzlich festzuschreiben. Vielmehr muß der Umfang zulässiger Informationsverarbeitung der Verfassungsschutzbehörden auf der Grundlage des Volkszählungsgesetz-Urteils des Bundesverfassungsgerichts überprüft und durch spezielle Aufgaben- und Befugnisnormen konkretisiert und begrenzt werden. Die Neuregelung muß zumindest die nachfolgenden Grundsätze beachten.
2. Ähnliche Regelungen für den MAD und den BND sind unter Berücksichtigung der Besonderheiten der jeweiligen Aufgabenstellung geboten.

II.

Allgemeine Grundsätze der Datenverarbeitung durch den Verfassungsschutz

1. Die Regelung der Informationsverarbeitung durch den Verfassungsschutz muß den Anforderungen der Normenklarheit entsprechen. Da über die Datenverarbeitung im Einzelfall meist nichts bekannt wird, ist es für den Bürger von besonderer Bedeutung, daß er den gesetzlichen Bestimmungen entnehmen kann, aus welchem Anlaß, in welcher Form und zu welchem Zweck der Verfassungsschutz personenbezogene Daten verarbeiten darf.
2. Diese Vorschriften müssen zwischen den unterschiedlichen Aufgaben der Verfassungsschutzbehörden differenzieren. Was beispielsweise für die Abwehr von Spionen vertretbar ist, ist nicht auch für die Mitwirkung an Sicherheitsüberprüfungen angemessen.
3. Der Grundsatz der Zweckbindung gilt auch für die Verfassungsschutzbehörden. Das bedeutet: Angesichts der Vielfalt ihrer Aufgaben reicht eine pauschale Bindung an „Zwecke des Verfassungsschutzes" nicht aus. Vielmehr dürfen die für die unterschiedlichen Aufgaben erhobenen Daten grundsätzlich nur für die jeweilige Aufgabe verwendet werden.
4. Die Regelung der Verarbeitung personenbezogener Daten durch den Verfassungsschutz muß die Erhebung sowie jegliche andere Art der Verarbeitung und Verwendung einbeziehen.

5. Regelungsbedürftig sind auch die Voraussetzungen für die jeweilige Form der Datenverarbeitung: Wesentliche Schritte der Automatisierung sollten beispielsweise nur zugelassen werden, wenn diese für die Erfüllung der jeweiligen Aufgabe gerechtfertigt sind und hierdurch schutzwürdige Belange der Betroffenen nicht unverhältnismäßig beeinträchtigt werden. Dies gilt insbesondere für Systeme der Datenverarbeitung, die über einen Aktennachweis hinausgehen oder durch Übernahme von Akteninhalten neue Verwendungs- und Verknüpfungsmöglichkeiten eröffnen.
6. Für jede automatisierte oder manuelle Datei ist eine detaillierte Errichtungsanordnung zu erlassen.

III.
Erheben und Sammeln personenbezogener Daten

1. Der Einsatz nachrichtendienstlicher Mittel muß klar geregelt sein. Dies gilt sowohl für die Voraussetzung der Anwendung als auch für die Frage, gegen wen nachrichtendienstliche Mittel eingesetzt werden dürfen. Die nachrichtendienstlichen Mittel sollten soweit wie möglich gesetzlich festgelegt werden. Zumindest sollten die Verfassungsschutzbehörden verpflichtet werden, alle in Frage kommenden Mittel im einzelnen intern zu beschreiben und ihren Einsatz zu dokumentieren. Die Anwendung nachrichtendienstlicher Mittel entbindet nicht von der Beachtung der allgemeinen Rechtsordnung.
2. Holt der Verfassungsschutz bei anderen Behörden Auskünfte ein, so soll er sein Ersuchen begründen, wenn nicht besondere Gründe entgegenstehen (z. B. schutzwürdige Belange des Betroffenen oder Sicherheitsinteressen des Staates). Entfällt danach die Begründung, so sind die Gründe des Ersuchens intern zu dokumentieren. Für Kontrollzwecke sollte ein eigenes Verzeichnis eingerichtet werden.
3. Eine Verpflichtung anderer Behörden, dem Verfassungsschutz von sich aus Informationen zu übermitteln, muß auf solche Bestrebungen beschränkt werden, die auf Anwendung von Gewalt oder geheimdienstliche Tätigkeit gerichtet sind. Darüber hinaus dürfen Behörden von sich aus nur unter weiteren gesetzlich festzulegenden Einschränkungen den Verfassungsschutz über personenbezogene Vorgänge informieren. Übermittlungen „auf Verdacht" sind unzulässig und können sich schädlich für das Verhältnis des Bürgers zu den Behörden auswirken.
4. Bei der Regelung der Informationsbeziehungen zwischen Polizei und Verfassungsschutz ist das verfassungskräftige Trennungsgebot zu beachten, das inhaltlicher ebenso wie organisatorischer Natur ist. Der Verfassungsschutz darf deshalb die Polizei z. B. nicht um Maßnahmen ersuchen, die die Anwendung polizeilicher Befugnisse erfordern. On-line-Verbindungen zwischen Polizei und Verfassungsschutz sind mit dem Trennungsgebot nicht vereinbar. Ein geeigneter Maßstab für Datenübermittlungen der Polizei an den Verfassungsschutz im Einzelfall sind die Verwertungsregelungen nach dem Gesetz zu Art. 10 GG.
5. Es ist sicherzustellen, daß spezielle Verwertungsbestimmungen - z. B. des Strafverfahrensrechts - beachtet werden; dies gilt z. B. für Erkenntnisse, die im Rahmen der Telefonüberwachung oder bei Durchsuchungen gewonnen wurden.

IV.
Speichern personenbezogener Daten

1. Die Befugnis zur Speicherung ist differenziert nach den unterschiedlichen Aufgabenbereichen zu regeln.

   So muß der Extremismusbezug in der Person desjenigen erfüllt sein, dessen Daten personenbezogen auswertbar im Rahmen der Extremismusbeobachtung gespeichert werden sollen. Hierbei ist außerdem zu beachten, daß Personendaten nur gespeichert werden dürfen, wenn dies zum Zwecke der Beobachtung extremistischer Bestrebungen erforderlich ist. Der Praxis, die immer mehr von der Beobachtung von Organisationen zur Erfassung von Einzelpersonen übergeht, muß entgegengewirkt werden.
2. Die Gründe für eine Speicherung müssen aus den Unterlagen des Verfassungsschutzes nachvollziehbar sein. Werden Bewertungen gespeichert, so muß erkennbar sein, wer sie vorgenommen hat und welche Unterlagen ihnen zugrundeliegen.
3. Es sind gesetzliche Regelfristen für die Überprüfung und Löschung der gespeicherten Daten festzulegen. Dabei ist zwischen den einzelnen Aufgabenbereichen (etwa Extremismusbeobachtung/Spionageabwehr), nach der Relevanz der einzelnen Informationen (etwa: vager Verdacht / gesicherte Informationen) sowie nach dem Alter der Betroffenen zu differenzieren. Dies gilt auch für die Speicherung in Akten.

V.
Mitwirkung an Personenüberprüfungen
(Sicherheitsüberprüfungen - § 3 Abs. 2 BVerfSchG)

1. Im Rahmen von Sicherheitsüberprüfungen werden sowohl beim Verfassungsschutz als auch bei einer Reihe weiterer Stellen Daten erhoben und verarbeitet. Hierfür sind besondere gesetzliche Grundlagen erforderlich.
2. Für die Mitwirkung des Verfassungsschutzes sind folgende Prinzipien zu beachten:
   - Die Sicherheitsüberprüfungen sind auf das erforderliche Maß zu beschränken. Dies gilt insbesondere für die Intensität der Prüfung, die sich nach der Gefährdung im Einzelfall richten muß.
   - Die Sicherheitsüberprüfung soll erst durchgeführt werden, wenn nur noch davon die Aufnahme der sicherheitsrelevanten Tätigkeit abhängig ist. Für den personellen Sabotageschutz ist zudem die exakte Beschreibung der sicherheitsempfindlichen Bereiche und die Begrenzung der Überprüfung auf tatsächlich in diesem Bereich eingesetzte Personen zu fordern.
   - Die Verfahrensregelungen müssen andere Ermittlungsformen ausschließen.
   - Die Voraussetzungen, unter denen im Rahmen der Sicherheitsüberprüfung auch Nachforschungen über Dritte angestellt werden dürfen, sind gesetzlich festzulegen. Soweit Dritte, z. B. Ehegatten, einbezogen werden, ist deren Einwilligung erforderlich. Die Speicherung von Daten über diese Personen ist auf ein Minimum zu beschränken und darf grundsätzlich nicht personenbezogen erschließbar sein.
   - Das Verfahren muß für die Betroffenen (einschließlich der Dritten) transparent sein. Sie sind über die Tatsache, den Ablauf, die beteiligten Stellen und das Ergebnis der Sicherheitsüberprüfung zu unterrichten. Im Fall von Sicherheitsbedenken ist dem Überprüften Gelegenheit zur Stellungnahme zu geben. Ausnahmen von dieser Unterrichtungspflicht sind eng zu fassen. Auch Auskunftspersonen sind über den Zweck der Befragung zu unterrichten, um Fehlschlüsse zu Lasten des Betroffenen zu vermeiden, und auf die Freiwilligkeit ihrer Angaben hinzuweisen.
   - Stellt der Betroffene einen Auskunftsantrag nach den Datenschutzgesetzen, so ist diesem zu entsprechen, soweit die Speicherung im Rahmen der Sicherheitsüberprüfung erfolgt ist.
   - Die speziell für die Sicherheitsüberprüfung beim Betroffenen oder bei anderen Stellen erhobenen Daten dürfen in der Regel nur für diesen Zweck verwendet werden. Die Trennung von Sicherheits- und Personalakten ist strikt zu wahren.

VI.

Übermittlung von Daten durch Verfassungsschutzbehörden

1. Verfassungsschutzbehörden dürfen untereinander personenbezogene Daten nur austauschen, soweit dies zu ihrer jeweiligen gesetzlich festgelegten Aufgabenerfüllung erforderlich und verhältnismäßig ist.
2. Die Übermittlung personenbezogener Daten durch den Verfassungsschutz an andere Sicherheitsbehörden (z. B. Polizei, Staatsanwaltschaft, BND u. a.) muß unter Beachtung des Zweckbindungsgrundsatzes präziser und restriktiver als in den derzeit praktizierten Zusammenarbeitsrichtlinien in Staatsschutzsachen geregelt werden. Die Voraussetzungen einer Übermittlung müssen konkret festgelegt werden. Allein die Begründung, daß die Übermittlung mit „dem Zweck des Verfassungsschutzes" vereinbar sei, ist nicht ausreichend. An Strafverfolgungsbehörden darf der Verfassungsschutz Informationen, die er mit nachrichtendienstlichen Mitteln erlangt hat, nur weitergeben, wenn tatsächliche Anhaltspunkte für die Einleitung eines Ermittlungsverfahrens wegen einer Straftat der in § 7 Abs. 3 Gesetz zu Art. 10 GG genannten Art vorliegen.
3. Eine Übermittlung an andere Behörden kann nur zur Erfüllung eigener Aufgaben des Verfassungsschutzes in Betracht kommen. Ausnahmen bedürfen einer gesetzlichen Regelung.
4. Eine Übermittlung von personenbezogenen Daten an private Stellen (z. B. Firmen, Gewerkschaften, Parteien) ist nur im Rahmen der gesetzlich vorgesehenen Sicherheitsüberprüfungen und nur in dem dafür unerläßlichen Rahmen oder aus Gründen der Spionage- und Terrorismusabwehr zulässig. Bei Übermittlungen außerhalb der Sicherheitsüberprüfung ist außerdem die Zustimmung der obersten Dienstbehörde einzuholen.
5. Eine Übermittlung an ausländische Dienststellen einschließlich der Nachrichtendienste ist an besonders enge Voraussetzungen zu knüpfen. Es ist – längerfristig durch völkerrechtliche Übereinkommen – zu gewährleisten, daß im Inland geltende Schutzrechte des Betroffenen nicht gefährdet werden.
6. Vor jeder Übermittlung hat die auskunftgebende Verfassungsschutzbehörde die Richtigkeit der vorhandenen Unterlagen und deren Erforderlichkeit für die eigene Aufgabenerfüllung zu überprüfen. In allen Fällen ist die Übermittlung personenbezogen zu dokumentieren. Über die Änderung wesentlicher Gesichtspunkte ist die Empfängerbehörde zu unterrichten, soweit dadurch nicht schutzwürdige Belange des Betroffenen beeinträchtigt werden.
7. Eine Unterrichtung der Öffentlichkeit über personenbezogene Erkenntnisse des Verfassungsschutzes ist grundsätzlich ausgeschlossen.

VII.

Auskunft an den Betroffenen

Die Verfassungsschutzbehörden dürfen Auskunftsersuchen der Bürger nicht, wie dies derzeit die meisten Ämter handhaben, schematisch ablehnen. Der Gesetzgeber sollte daher von folgenden Grundsätzen ausgehen:

Die Auskunft ist zu erteilen

- in aller Regel, wenn die Speicherung nur auf einer Sicherheitsüberprüfung beruht,
- im übrigen nach Abwägung im Einzelfall.

Im Falle einer Auskunftsverweigerung sind die Gründe im einzelnen zu dokumentieren.

Die Bearbeitung von Auskunftsersuchen muß getrennt von anderen Informationssammlungen erfolgen. Die Tatsache der Antragstellung darf nicht zum Nachteil der Betroffenen verwertet werden.

VIII.

Rechte der Datenschutzbeauftragten

Die Kontrollkompetenz der Datenschutzbeauftragten erstreckt sich auf die gesamte Datenverarbeitung der Verfassungsschutzbehörden und umfaßt auch Akten und sonstige Unterlagen. Auch die Datenverarbeitung im Rahmen des Gesetzes zu Art. 10 GG muß der Kontrolle der Datenschutzbeauftragten unterliegen. Dies ist unerläßlich für die Durchsetzung des Rechts auf informationelle Selbstbestimmung gerade im Bereich des Verfassungsschutzes.

Anlage 5

Datenschutz und Neue Medien

Beschluß der nationalen Datenschutzbeauftragten
nach einem Erfahrungsaustausch
im Rahmen der Internationalen Funkausstellung 1985
am 4. September 1985 in Berlin

1. Die internationale Konferenz der Datenschutzbeauftragten hat am 18. Oktober 1983 auf ihrer Sitzung in Stockholm einen Beschluß zum Thema Neue Medien gefaßt, in dem gefordert wurde, daß durch geeignete Maßnahmen, insbesondere der Gesetzgebung, in jedem Land die Betriebsbedingungen so gestaltet werden, daß durch den Einsatz der Neuen Medien Persönlichkeitsrechte nicht beeinträchtigt werden (vgl. unten).
2. Die Weiterentwicklung der Neuen Medien in den einzelnen Staaten bestätigt einerseits die Notwendigkeit der Forderungen, zeigt aber andererseits auch zusätzliche Gefährdungen auf:
   - Die internationale Standardisierung der Telekommunikationsdienste und die zunehmende grenzüberschreitende Vernetzung der Systeme machen internationale Vereinbarungen auch über den Datenschutz bei neuen Informations- und Kommunikationsdiensten dringlich.
   - Der beginnende Aufbau von Glasfasernetzen, die anstehende Einführung der Breitbandkommunikation und die Integration der einzelnen Telekommunikationsdienste, verbunden mit der Digitalisierung von schmal- und breitbandigen Übertragungsnetzen werden zu einer erheblichen Zunahme der Informationsströme führen. Gleichzeitig werden Integration und Digitalisierung zu einer besseren Auswertbarkeit mit Hilfe automatischer Anlagen führen und damit die Gefahr des unbefugten Aufzeichnens und Auswertens der übermittelten Informationen erhöhen.
   - Der Einsatz von Satelliten zur Kommunikation schafft im Hinblick auf die Datenintegrität und den Schutz vor unbefugtem Abhören ebenfalls Risiken.
3. Die anläßlich des Erfahrungsaustausches versammelten Vertreter der nationalen Datenschutzinstitutionen appellieren daher an die internationale Konferenz der Datenschutz-

beauftragten, den in ihrem Beschluß vom 18. Oktober 1983 enthaltenen Forderungen gegenüber den nationalen Regierungen Nachdruck zu verleihen und auf eine Verstärkung der internationalen Zusammenarbeit bei der Überwachung Neuer Medien hinzuwirken.

Neue Medien

Beschluß der Internationalen Konferenz
der Datenschutzbeauftragten vom 18. Oktober 1983

1. Die Internationale Konferenz der Datenschutzbeauftragten geht übereinstimmend davon aus, daß der Einsatz Neuer Medien, die über Kabelnetze verbreitet werden, eine erhebliche Gefährdung für die Persönlichkeitsrechte mit sich bringen kann.

   Soweit bei den Neuen Medien die Kommunikation zwischen Informationsanbietern und Teilnehmern durch elektronische Datenverarbeitungsanlagen gesteuert wird, ist - im Gegensatz zu herkömmlichen Medien - die Speicherung personenbezogener Daten in einem gewissen Umfang erforderlich.

   So werden beim Medium „Bildschirmtext" (Videotex) Verbindungs- und Abrechnungsdaten gespeichert. Bei manchen Diensten werden die vom Teilnehmer abgerufenen Sendungen registriert. Das Recht der Unverletzlichkeit der Wohnung wird berührt, wenn mit neuen Diensten von außen in den Wohnungen Wirkungen ausgelöst und Messungen vorgenommen werden.

   Über die auf diese Weise an zentralen Stellen automatisiert entstehenden Sammlungen personenbezogener Daten könnten Persönlichkeitsprofile aller Benutzer erstellt werden. Deren soziale Beziehungen und Verhaltensweisen können damit zum Gegenstand von Maßnahmen gemacht werden.

   Darüber hinaus können mit Hilfe der Neuen Medien personenbezogene Daten jeglicher Art mit geringem Aufwand und in großem Umfang verbreitet werden. Erfahrungen mit Bildschirmtext haben gezeigt, daß Anbieter und Benutzer mißbräuchlich sensible Daten über die Neuen Medien veröffentlichen.

Anlage 6

Grundsätze für organisatorische und technische Maßnahmen zum Datenschutz beim Einsatz von Personalcomputern (PC)

Diese Grundsätze betreffen den Einsatz von Personalcomputern (PC). Sie präzisieren die „Grundsätze für die organisatorischen und technischen Maßnahmen beim Einsatz isolierter ADV-Systeme".

1. **Definitionen**

1.1 ADV-Systeme im Sinne dieser Grundsätze sind alle Einrichtungen zur automatisierten Datenverarbeitung, mit denen Dateien auf automatisch lesbaren Speichermedien geführt werden können und deren Hardware es erlaubt, die in § 2 Abs. 3 Nr. 3 Bundesdatenschutzgesetz (§ 4 Abs. 3 Nr. 3 Berliner Datenschutzgesetz) beschriebenen Operationen auf Dateien durchzuführen.

1.2 Isolierte ADV-Systeme im Sinne dieser Grundsätze sind ADV-Systeme,

- die nicht im Rahmen eines arbeitsteilig organisierten Rechenbetriebes eingesetzt werden,
- die vom Benutzer selbst bedient werden,
- auf die nicht ohne Veranlassung durch den Benutzer von außen zugegriffen werden kann,
- sofern sie mehrere interaktive Schnittstellen besitzen, diese im Teilhaberbetrieb und alle nur im räumlich isolierten Bereich des Rechners eingesetzt werden können,
- deren anwendungsbezogene Datenträger ausschließlich vom berechtigten Benutzer verwaltet werden.

1.3 Ein ADV-System heißt gewidmet, wenn es ausschließlich zur Abwicklung eines einzigen Anwendungsverfahrens eingesetzt wird (Dedicated System).

1.4 Ein ADV-System heißt personengebunden, wenn es nur eine Person gibt, die zur Benutzung des Systems berechtigt ist.

2. **Geltungsbereich**

2.1 Diese Grundsätze betreffen den Einsatz von Personalcomputern (2.2) zur Verarbeitung personenbezogener Daten gemäß § 2 Abs. 1 Bundesdatenschutzgesetz (§ 4 Abs. 1 Berliner Datenschutzgesetz).

2.2 Personalcomputer sind isolierte ADV-Systeme, die gewidmet oder personengebunden sind. Für andere Einsatzformen sind die weitergehenden „Grundsätze für die organisatorischen und technischen Maßnahmen beim Einsatz isolierter ADV-Systeme" anzuwenden.

Daher gelten diese Grundsätze nicht für ADV-Systeme, die

- nicht isoliert sind, also etwa als intelligente Terminals den Zugang zu zentralen Systemen oder Netzen eröffnen;
- weder gewidmet noch personengebunden sind, da hier wegen der komplexen Benutzungsorganisation die Grundsätze für die organisatorischen und technischen Maßnahmen beim Einsatz isolierter ADV-Systeme anzuwenden sind.

3. **Allgemeine Grundsätze**

3.1 Der Grad der Schutzbedürftigkeit personenbezogener Daten ergibt sich insbesondere aus ihrer Natur und aus dem Zusammenhang, in dem sie verwendet werden. Die Art der eingesetzten ADV-Anlage und ihrer Einsatzform spielen daher bezüglich der Anforderungen an den Datenschutz eine geringe Rolle.

3.2 Der für den technischen und organisatorischen Datenschutz betriebene Aufwand hat zwar in einem angemessenen Verhältnis zum Schutzzweck und zum Aufwand für das ADV-System zu erfolgen. Daten dürfen aber nicht deswegen schlechter geschützt sein, weil sie auf einem Personalcomputer verarbeitet werden.

3.3 Bei Personalcomputern kann ein wirksamer organisatorischer und technischer Datenschutz in der Regel mit relativ geringen Mitteln erreicht werden. Allerdings setzen eine wirksame Speicher-, Benutzer- und Zugriffskontrolle bei Systemen mit festem peripherem Speicher die Anwendung entsprechender hard- bzw. softwaretechnischer Maßnahmen voraus.

3.4 Darüber hinaus sind soweit möglich technische Einrichtungen einzusetzen, die die Maßnahmen zur Durchführung des Datenschutzes unterstützen.

3.5 Auch bei Personalcomputern haben die zuständigen Organe der speichernden Stelle die Ausführung des Datenschutzgesetzes sicherzustellen (§ 16 Berliner Datenschutzgesetz). Dies bedeutet insbesondere, daß die interne Verantwortlichkeit für den Betrieb des Personalcomputers eindeutig festgelegt wird.

Sofern für die Durchführung der jeweiligen Aufgabe überhaupt der Einsatz eines Personalcomputers in Betracht kommt, ist hierzu schriftlich festzulegen,

- wer den Personalcomputer benutzen darf,
- welche Daten zu welchem Zweck verarbeitet werden dürfen,
- welche EDV-Programme eingesetzt werden dürfen,
- wie die Personalcomputer-Anwendung in die Aufbau- und Ablauforganisation des Gesamtbetriebes eingebunden werden muß.

Dies gilt auch dann, wenn die Benutzung privater Personalcomputer für dienstliche Zwecke in den Diensträumen oder in der Privatwohnung gestattet werden soll. In diesen Fällen ist sicherzustellen, daß die internen und externen Datenschutzkontrollinstanzen die gespeicherten Daten, die verwendeten Programme und die technischen und organisatorischen Maßnahmen zur Datensicherung überprüfen können. Hierzu empfiehlt sich eine entsprechende Erklärung des Eigentümers, die im zweiten Fall auch das Recht zur Prüfung in der Privatwohnung umfaßt.

Die Erfüllung der vorgeschriebenen Veröffentlichungs- und Meldepflichten ist von der speichernden Stelle sicherzustellen.

3.6 Die speichernde Stelle hat im Rahmen ihrer Weisungsbefugnis gegenüber den Benutzern für die datenschutzgerechte Ausstattung des technischen Systems, der Computerarbeitsplätze, des Raumes und der Möbel, in denen sich Datenträger befinden, im angemessenen Verhältnis zum Schutzzweck zu sorgen.

3.7 Die aus diesen Grundsätzen folgenden Bedingungen des Einsatzes von Personalcomputern regelt die speichernde Stelle durch schriftliche Dienstanweisung.

4. Organisatorisch-technische Maßnahmen beim Einsatz von Personalcomputern

4.1 Zur Nutzung eines Personalcomputers befugt sind

- bei personengebundenem Betrieb ausschließlich die eine nutzungsberechtigte Person,
- bei gewidmeten Systemen die im Dienst befindlichen und mit dem Anwendungsverfahren betrauten Personen.

4.2 Während des Betriebes von Personalcomputern ist sicherzustellen, daß bei Darstellung personenbezogener Daten auf Bildschirmen oder Druckern Unbefugten die Einsicht verwehrt wird.

4.3 Solange der Personalcomputer bei Aufrechterhaltung der Stromversorgung betriebsbereit bleibt, hat er unter der ununterbrochenen Aufsicht des Benutzers zu sein. Kurzfristige Unterbrechungen der Aufsicht sind nur tolerierbar, wenn Unbefugten der Zugang an das System durch wirksamen Raumverschluß verwehrt wird.

4.4 Wird der Personalcomputer nicht benutzt, so ist die Stromversorgung zu unterbrechen und sind die beweglichen Datenträger, die personenbezogene Daten oder Betriebsprogramme enthalten, dem Personalcomputer zu entnehmen und ordnungsgemäß aufzubewahren.

4.5 Bewegliche Datenträger mit personenbezogenen Daten oder Betriebsprogrammen sind, solange sie nicht unter wirksamer Aufsicht stehen, mit Sicherheitsverschluß verschlossen aufzubewahren.

4.6 Die datenschutzgerechte Vernichtung von Belegen und ADV-Listen, die beim Einsatz des Personalcomputers anfallen, ist zu gewährleisten.

4.7 Soweit durch das technische System keine wirksameren Protokollierungen erfolgen, ist mindestens folgendes über die Nutzung des Personalcomputers in einem Benutzerbuch zu protokollieren:

Bei personengebundenem Betrieb:

- Datum und Uhrzeit von Anfang und Ende der Benutzung,
- Art der Anwendung (u. U. Angabe der verwendeten Anwendungssoftware),
- Namen der benutzten personenbezogenen Dateien,
- Nummern der verwendeten beweglichen Datenträger.

Bei gewidmeten Systemen:

- Name des Benutzers,
- Datum und Uhrzeit von Anfang und Ende der Benutzung,
- Nummern der verwendeten beweglichen Datenträger.

4.8 Ein fester peripherer Speicher ist ein Speicher, der über die Arbeitsspeicherausstattung eines Personalcomputers hinaus an den Personalcomputer direkt angeschlossen ist und folgende Eigenschaften besitzt:

a) Die Datenträger können im Regelfall dem direkt angeschlossenen Laufwerk nicht entnommen werden.

b) Der Inhalt der Datenträger wird durch die Unterbrechung der Stromversorgung nicht beeinträchtigt.

Ist ein Personalcomputer mit einem solchen festen peripheren Speicher zusätzlich zu oder an Stelle von Speichern mit beweglichen Datenträgern ausgestattet, so sind über die bereits beschriebenen Maßnahmen hinaus folgende Maßnahmen zu treffen:

Der Personalcomputer ist zur Realisierung einer wirksamen Speicher-, Benutzer- und Zugriffskontrolle mit folgenden Einrichtungen auszustatten:

- Schlüsselschalter für die Inbetriebnahme des Personalcomputers
- bei gewidmeten Systemen:
  Betriebssystem oder zusätzliche Datenschutz-Software, welche die individuelle Benutzeridentifikation und -authentifikation und die differenzierte Zugriffsberechtigung auf Programme und Daten ermöglicht.

5. Ordnungsmäßigkeit der Datenverarbeitung beim Einsatz von Personalcomputern

5.1 Anwendungsprogramme dürfen auch auf Personalcomputern nur aufgrund eines in der Verantwortung der speichernden Stelle liegenden formalen Freigabeverfahrens angewendet werden.

5.2 Für die Freigabe ist zu prüfen,

- ob ein Abschlußtest nachweist, daß das Programm den dienstlichen Erfordernissen des Anwenders entspricht;
- ob das Programm so aufgebaut und dokumentiert ist, daß sachverständige Dritte in angemessen kurzer Zeit die Pflege und Anwendungsbetreuung des Programms voll verantwortlich übernehmen können.

5.3 Die Dokumentation des formalen Freigabeverfahrens, die Ergebnisse des Abschlußtests, die Programmdokumentation, die Dokumentation der Programmänderungen und der aktuelle Text des Quellprogramms sind in einer Programmakte zusammenzufassen.

5.4 Bei Programmen, die von Dritten gegen Entgelt überlassen worden sind, kann von der Führung einer vollständigen Programmakte i. S. von 5.3 abgesehen werden, sofern durch die Vertragsgestaltung mit dem Hersteller und die Bereitstellung anderweitiger Unterlagen sichergestellt ist, daß die Ordnungsmäßigkeit und die Kontrollierbarkeit der Programmanwendung durch die verantwortliche speichernde Stelle gewährleistet werden kann.

5.5 Jedes freigegebene System- und Anwendungsprogramm ist auf einem Datenträger zu speichern, welcher mit zusätz-

licher Schreibsperre vor unbefugten Änderungen des Inhaltes gesichert ist.

5.6 Jeder bewegliche Datenträger, der Programme enthält, muß durch unverfälschbare Merkmale dem Personalcomputer eindeutig zuordenbar sein. Jeder bewegliche Datenträger, der personenbezogene Daten enthält, ist in gleicher Weise dem Personalcomputer zuzuordnen oder ggf. eindeutig als für den Datenträgeraustausch vorgesehen zu kennzeichnen.

Anlage 7

Technische und organisatorische Datensicherungsmaßnahmen bei der Wartung und Fernwartung von DV-Anlagen

(Im Arbeitskreis
„Technische und organisatorische Datenschutzfragen"
der Konferenz der Datenschutzbeauftragten
beratende Orientierungshilfe)
Stand: 1985

Bei der Wartung und beim Einsatz der Fernwartung von DV-Systemen durch den Hersteller hat der Kunde (Betreiber des Rechenzentrums) die Einhaltung folgender Datensicherungsmaßnahmen zu beachten:

1. **Maßnahmen zur Zugangskontrolle**

1.1 Zugangskontrolle der Wartung vor Ort

Das Personal, das die Wartungsarbeiten an der DV-Anlage durchführt, muß sich den gleichen kundenspezifischen Zugangsregelungen unterziehen, wie das eigene Personal (Legitimationsprüfung).

1.2 Sicherstellung, daß vom Maschinenbediener nur die Wartungszentrale angerufen werden kann

Bei Benutzung des Datex-L-Netzes bietet die Deutsche Bundespost eine Einrichtung für Direktruf (Kosten mtl. DM 5,–) an, mit der ausschließlich eine bestimmte Fernsprechnummer, die in den Rechner einprogrammiert wurde, angewählt werden kann. Im herkömmlichen Fernsprechnetz kann der Spezial-Fernsprechapparat Typ 756 DD (Kosten mtl. DM 5,80) nach Eingabe der Rufnummer nur zu dieser Rufnummer die Verbindung herstellen. Die Rufnummerneingabe läßt sich durch einen Schlüssel sichern. Auf diese Weise wird verhindert, daß ein unbefugter Teilnehmer Zugriff auf das System erhält, wenn er einen Komplicen am Rechner hat.

1.3 Kontrolle des Fernwartungsvorgangs

Der Fernwartungsvorgang muß vom Betreiber der DV-Anlage jederzeit abgebrochen werden können.

2. **Organisation der Abgangskontrolle**

2.1 Prüfung der aus dem Rechenzentrumsbereich hinausgehenden Datenträger

Bevor Datenträger mit personenbezogenen Daten aus dem Rechenzentrumsbereich zu Wartungszwecken oder zur Fehleranalyse hinausgegeben werden, ist eine besondere Erlaubnis durch autorisiertes Rechenzentrumspersonal einzuholen. Mit Rechenzentrumspersonal ist das für die Bedienung der Datenverarbeitungsanlage vom Betreiber der Anlage eingesetzte und mit entsprechender Befugnis versehene Personal gemeint. Auf einem Begleitschein, der zugleich als Beleg für die Abgangs- und Rücklaufkontrolle verwendet wird, ist die Art der Daten und des Datenträgers zu vermerken.

2.2 Behandlung wartungseigener Datenträger

Es ist sicherzustellen, daß das Wartungspersonal nicht mit den eigenen mitgebrachten Datenträgern (Magnetbänder und Magnetplatten) die Wartung durchführt, sondern ausschließlich mit Duplikaten arbeitet, die im Rechenzentrum erstellt werden und dort für Kontrollzwecke (mindestens 1 Jahr) aufzubewahren sind. Werden Test- und Service-Programme des Herstellers auf der Anlage gespeichert, sind diese unter einer besonderen Kennung abzulegen.

3. **Maßnahmen zur Speicherkontrolle**

Der Betreiber des Rechenzentrums muß Dateien und Programme durch Paßworte schützen, soweit diese bei der Wartung physisch im Zugriff bleiben.

3.1 Vergabe und Verwaltung der Paßwörter

Die Vergabe und Verwaltung der Paßwörter muß ausschließlich den dazu autorisierten Personen des Rechenzentrumspersonals obliegen.

3.2 Wartung der heißen Anlage

Müssen Wartungs- und Diagnosearbeiten an der Herstellersoftware im laufenden Betrieb durchgeführt werden, so dürfen diese nur unter ständiger Kontrolle eines sachkundigen Mitarbeiters des Rechenzentrums erfolgen. (Nach den VDE-Schutzbestimmungen dürfen auch Arbeiten an Starkstromgeräten nie ohne Anwesenheit weiterer Personen ausgeführt werden).

3.3 Zugriff auf personenbezogene Daten

Ist für Wartungszwecke ein Zugriff auf personenbezogene Daten erforderlich, kann das nur nach ausdrücklicher Genehmigung durch die verantwortliche Stelle erfolgen. Der Zugriff auf personenbezogene Daten sollte allerdings nur den Ausnahmefall darstellen. Nicht benötigte Dateien sind aus dem direkten Zugriff zu entfernen.

3.4 Einspielen neuer Releases ins Betriebssystem und in systemnahe Software

Das Einspielen von Änderungen ins Betriebssystem und in systemnahe Software unmittelbar durch die Fernwartung ist abzulehnen. Solche Änderungen sind ausschließlich vom Rechenzentrum durchzuführen. Im Zuge der Fernwartung notwendige Änderungen sind ausschließlich in einer besonderen Datei im System des Rechenzentrums einzuspeichern. Die Durchführung der Änderungen ist erst nach Freigabe durch autorisiertes Rechenzentrumspersonal vorzunehmen.

Bei der Wartung vor Ort hat die Änderung des Betriebssystems und der systemnahen Software nur durch den Systemverantwortlichen bzw. im Beisein einer sachkundigen Person des Betreibers der DV-Anlage zu erfolgen.

4. **Maßnahmen zur Zugriffskontrolle**

4.1 Offenbarung von Kundenpaßwörtern

Für den Fall, daß in einem Wartungsvorgang ein Zugriff auf Dateien mit personenbezogenen Daten oder direkt auf die Paßwortdatei notwendig ist, sind nach Abschluß der Wartungsarbeiten die der Wartung offenbarten Paßwörter unverzüglich zu ändern.

4.2 Überprüfen der Wartungsprotokolle

Die Aktivitäten eines Wartungsvorgangs, die in einer Protokolldatei festzuhalten sind, sind zu überprüfen und mindestens ein Jahr aufzubewahren. Die Verpflichtung des Systemverantwortlichen, den Wartungsvorgang am Bildschirm zu verfolgen und die Verbindung in kritischen Fällen zu unterbrechen, bleibt davon unberührt.

5. Maßnahmen zur Auftragskontrolle

5.1 Wartungsvertrag

Im Wartungsvertrag sind klare Regelungen hinsichtlich der Abgrenzung der Kompetenzen und Pflichten zwischen Wartungs- und Rechenzentrumspersonal zu treffen. Art und Umfang der Wartung (Hard- und Software) sind schriftlich festzulegen.

5.2 Sicherheitsanforderungen an das Wartungspersonal

Der Hersteller muß vertraglich versichern, daß das Wartungspersonal sicherheitsüberprüft und auf das Datengeheimnis verpflichtet ist.

5.3 Weitergabe der übertragenen Daten

Eine Weitergabe der Daten, die der Wartung übergeben oder bei der Fernwartung übertragen wurden, ist vertraglich zu untersagen bzw. streng zu reglementieren.

5.4 Behandlung der übergebenen bzw. übertragenen Daten nach Aufgabenerledigung

Soweit es sich nicht um reine Hardwaredaten handelt, ist vertraglich zu vereinbaren, daß übergebene bzw. übertragene Daten im Wartungszentrum nur temporär aufbewahrt bzw. gespeichert werden dürfen und nach Erledigung sofort zu vernichten bzw. zu löschen sind.

5.5 Vereinbarung über den Einsatz der Fernwartung

Hinsichtlich der Fernwartung wird empfohlen, einen separaten schriftlichen Vertrag abzuschließen, in dem die Einhaltung besonderer Datensicherungsmaßnahmen, die festzulegen sind, vereinbart wird.

6. Maßnahmen zur Transportkontrolle

6.1 Transportweg

Der Transportweg für Datenträger (Magnetbandrollen, Listen usw.) und die am Transportweg beteiligten Personen sind festzulegen. Darüber hinaus empfiehlt es sich, eine Sicherheitsanalyse durchzuführen.

6.2 Materielle Datensicherungsmaßnahmen

Es ist zu prüfen, ob beim Versand von Datenträgern für Wartungszwecke die Versandart angemessen und ausreichend ist. Darüber hinaus ist eine Vollständigkeitsprüfung vorzusehen. Beim Transport von Datenträgern sind grundsätzlich Begleitpapiere zu benützen.

7. Maßnahmen zur Organisationskontrolle

7.1 Dokumentation

Der Betreiber des Rechenzentrums ist gehalten, das Wartungs- bzw. Fernwartungskonzept schriftlich zu dokumentieren (Kontrolle der technischen und organisatorischen Maßnahmen zum Datenschutz).

Anlage 8

Übereinkommen des Europarats zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten

(Straßburg, 28. Januar 1981)

– Auszug –

Kapitel II Grundsätze für den Datenschutz

Artikel 4 Pflichten der Vertragsparteien

(1) Jede Vertragspartei trifft in ihrem innerstaatlichen Recht die erforderlichen Maßnahmen, um die in diesem Kapitel aufgestellten Grundsätze für den Datenschutz zu verwirklichen.

(2) Jede Vertragspartei trifft diese Maßnahmen spätestens zu dem Zeitpunkt, zu dem dieses Übereinkommen für sie in Kraft tritt.

Artikel 5 Qualität der Daten

Personenbezogene Daten, die automatisch verarbeitet werden,

a) müssen nach Treu und Glauben und auf rechtmäßige Weise beschafft sein und verarbeitet werden;

b) müssen für festgelegte und rechtmäßige Zwecke gespeichert sein und dürfen nicht so verwendet werden, daß es mit diesen Zwecken unvereinbar ist;

c) müssen den Zwecken, für die sie gespeichert sind, entsprechen, dafür erheblich sein und dürfen nicht darüber hinausgehen;

d) müssen sachlich richtig und wenn nötig auf den neuesten Stand gebracht sein;

e) müssen so aufbewahrt werden, daß der Betroffene nicht länger identifiziert werden kann, als es die Zwecke, für die sie gespeichert sind, erfordern.

Artikel 6 Besondere Arten von Daten

Personenbezogene Daten, welche die rassische Herkunft, politische Anschauungen oder religiöse oder andere Überzeugungen erkennen lassen, sowie personenbezogene Daten, welche die Gesundheit oder das Sexualleben betreffen, dürfen nur automatisch verarbeitet werden, wenn das innerstaatliche Recht einen geeigneten Schutz gewährleistet. Dasselbe gilt für personenbezogene Daten über Strafurteile.

Artikel 7 Datensicherung

Für den Schutz der personenbezogenen Daten, die in automatisierten Dateien/Datensammlungen gespeichert sind, werden geeignete Sicherungsmaßnahmen getroffen gegen die zufällige oder unbefugte Zerstörung, gegen zufälligen Verlust sowie unbefugten Zugang, unbefugte Veränderung oder unbefugtes Bekanntgeben.

Artikel 8 Zusätzlicher Schutz für den Betroffenen

Jedermann muß die Möglichkeit haben,

a) das Vorhandensein einer automatisierten Datei/Datensammlung mit personenbezogenen Daten, ihre Hauptzwecke sowie die Bezeichnung, den gewöhnlichen Aufenthaltsort oder den Sitz des Verantwortlichen für die Datei/Datensammlung festzustellen;

b) in angemessenen Zeitabständen und ohne unzumutbare Verzögerung oder übermäßige Kosten die Bestätigung zu erhalten, ob Daten über ihn in einer automatisierten Datei/Datensammlung mit personenbezogenen Daten gespeichert

sind, sowie zu erwirken, daß ihm diese Daten in verständlicher Form mitgeteilt werden;

c) gegebenenfalls diese Daten berichtigen oder löschen zu lassen, wenn sie entgegen den Vorschriften des innerstaatlichen Rechts verarbeitet worden sind, welche die Grundsätze der Artikel 5 und 6 verwirklichen;

d) über ein Rechtsmittel zu verfügen, wenn seiner Forderung nach Bestätigung oder gegebenenfalls nach Mitteilung, Berichtigung oder Löschung im Sinne der Buchstaben b und c nicht entsprochen wird.

Artikel 9 Ausnahmen und Einschränkungen

(1) Ausnahmen von den Artikeln 5, 6 und 8 sind nicht zulässig, abgesehen von den in diesem Artikel vorgesehenen.

(2) Eine Abweichung von den Artikeln 5, 6 und 8 ist zulässig, wenn sie durch das Recht der Vertragspartei vorgesehen und in einer demokratischen Gesellschaft eine notwendige Maßnahme ist

a) zum Schutz der Sicherheit des Staates, der öffentlichen Sicherheit sowie der Währungsinteressen des Staates oder zur Bekämpfung von Straftaten;

b) zum Schutz des Betroffenen oder der Rechte und Freiheiten Dritter.

(3) Die Ausübung der Rechte nach Artikel 8 Buchstabe b, c und d kann durch Gesetz für automatisierte Dateien/Datensammlungen mit personenbezogenen Daten eingeschränkt werden, die Zwecken der Statistik oder der wissenschaftlichen Forschung dienen, wenn offensichtlich keine Gefahr besteht, daß der Persönlichkeitsbereich der Betroffenen beeinträchtigt wird.

Artikel 10 Sanktionen und Rechtsmittel

Jede Vertragspartei verpflichtet sich, geeignete Sanktionen und Rechtsmittel für Verletzungen der Vorschriften des innerstaatlichen Rechts, welche die in diesem Kapitel aufgestellten Grundsätze für den Datenschutz verwirklichen, festzulegen.

Artikel 11 Weitergehender Schutz

Dieses Kapitel ist nicht so auszulegen, als ob es die Möglichkeit begrenze oder auf andere Weise beeinträchtige, daß eine Vertragspartei den Betroffenen ein größeres Maß an Schutz als das in diesem Übereinkommen vorgeschriebene gewährt.

Kapitel III Grenzüberschreitender Datenverkehr

Artikel 12 Grenzüberschreitender Verkehr personenbezogener Daten und innerstaatliches Recht

(1) Werden personenbezogene Daten, die automatisch verarbeitet werden oder für eine solche Verarbeitung beschafft worden sind - mittels welcher Datenträger auch immer -, über die Staatsgrenzen hinweg weitergegeben, so finden die folgenden Bestimmungen Anwendung.

(2) Eine Vertragspartei darf allein zum Zweck des Schutzes des Persönlichkeitsbereichs von Betroffenen den grenzüberschreitenden Verkehr personenbezogener Daten in das Hoheitsgebiet einer anderen Vertragspartei nicht verbieten oder von einer besonderen Genehmigung abhängig machen.

(3) Jede Vertragspartei ist jedoch berechtigt, von Absatz 2 abzuweichen,

a) soweit ihr Recht für bestimmte Arten von personenbezogenen Daten oder automatisierten Dateien/Datensammlungen mit personenbezogenen Daten wegen der Beschaffenheit dieser Arten besondere Vorschriften enthält, es sei denn, die Vorschriften der anderen Vertragspartei sehen einen gleichwertigen Schutz vor;

b) um zu verhindern, daß ihr Recht dadurch umgangen wird, daß eine Weitergabe aus ihrem Hoheitsgebiet in das Hoheitsgebiet einer Nichtvertragspartei auf dem Weg über das Hoheitsgebiet einer anderen Vertragspartei erfolgt.

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, Bd. 2, Datenschutz in Berlin 1979-1983

Abgangskontrolle 104
Abgeordnetenhaus 14, 121; 1984/28; 1985/17
Abiturienten 118
Ablichtung 42, 55, 87, 113
Abonnentenverwaltung 106
Abruf, unbefugter 76, 107
Adoption 108, 109; 1985/4
Adrema-Platten 115
Adressenmittlung 26
Adreßbuch 1985/6
Adreßlisten 58, 115
ADV-Gesetz 1985/3
ADV-Gesetz 1985/26
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
Aktenvernichtung 63
Allgemeine Geschäftsbedingungen 1984/6
Allgemeine Ortskrankenkasse 1984/16
Allgemeines Sicherheits- und Ordnungsgesetz 107; 1984/3, 10; 1985/3, 7, 26, 27
Amerika-Gedenkbibliothek 85; 1984/28
Amtsanwaltschaft, s. Staatsanwaltschaft
Amtsarzt 1984/9; 1985/23
Amtsblatt, Dateiveröffentlichung 57
Amtsgeheimnis 55
Amtsgericht 54
Amtshilfe 25
Anonymisierung 34, 40, 51, 104
Anordnung über Mitteilungen in Strafsachen 40, 41, 44, 108; 1984/12, 24; 1985/3, 23
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; 1985/11, 26
Archivgesetz 1985/3
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; 1985/24
Auftragsdatenverarbeitung 112; 1984/17
Ausbildungsförderung, s. Bundesausbildungsförderungsgesetz
Auskunft 25, 35, 52, 116; 1985/23
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; 1985/3, 26
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; 1985/3, 26
Berichtigungsanspruch 35
Berliner Datenschutzgesetz 24, 121; 1985/26
Berliner Entwässerungswerke 105
Berliner Pfandbriefbank 1985/16
Berliner Philharmonisches Orchester 106
Berliner Stadtreinigungsbetriebe 57; 1985/16
Berliner Wasserwerke 105
Beschwerden s. Anrufung
Betriebsdatenbank 85; 1985/24
Betriebskrankenkasse des Landes und der Stadt Berlin 1984/17
BEWAG 36
Bezirksämter 109, 116; 1984/16; 1985/16
Bezirkseinwohneramt 54
Bezirksverordnetenversammlungen 15, 73
Bibliotheken 85, 105; 1985/11, 26
Bibliotheksgesetz 1985/3
Bildschirmtext 33, 37, 45, 59, 67, 75, 87, 101; 1984/12, 28; 1985/12
Bildschirmtext, Anbieter 1984/14; 1985/17
Bildschirmtext, Betreiber 1984/14
Bildschirmtext, externe Rechner 101
Bildschirmtext, Staatsvertrag 75, 88, 123
Bildschirmtext, Zustimmungsgesetz 101, 120
Blutspendedienst 1984/8
Breitbandkommunikation 59, 101
Broschüren 27
Bundesausbildungsförderungsgesetz 63
Bundesbaugesetz 119
Bundesdatenschutzgesetz, Novellierung 65, 88, 89, 120, 121
Bundeskindergeldgesetz s. Kindergeld
Bundeskriminalamt 44
Bundessozialhilfegesetz 72
Bundesstatistikgesetz 31
Bundeszentralregister, unbeschränkte Auskunft 40, 56, 88, 120; 1984/28
Bußgeldverfahren 1984/22
BVG 104; 1985/23
Chipkarte 1985/14
Codes 34, 60, 77, 101; 1984/6
Computerkriminalität 1984/5
Computermißbrauch 1984/4
Datei 25, 31, 49, 55, 58; 1985/18
Dateienregister 12, 24, 26, 27, 30, 43, 57, 64, 86, 88, 105, 120, 121; 1985/24
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 1o5
Einsichtsrecht 25, 41, 59, 66, 100; 1985/20
Einsichtsrecht, Schülerbogen 41
Einwilligung 24, 26, 31, 34, 51, 57, 59, 67; 1985/22
Einwohnerdatenbank, s. Melderegister
Epidemiologie, s. Forschungsprojekte
Erforderlichkeit 25, 41, 58, 61
Erhebung 40, 51, 56, 110, erkennungsdienstliche Unterlagen 1984/11
EUROCAT 50,
Europarat 28, 46; 1985/3, 35
Europäische Gemeinschaften 28, 50
externe Schreibkräfte 1984/9
Fachpostverkehr, siehe Postaustausch
Fahndung, Kraftfahrzeuge 79
Fahrzeugregister 1984/22
Familienkrankenhilfe 72
Fehlbelegungsabgabe 72, 75
Fehleintragung 54
Fehlspeicherung 107
Fensterbriefumschläge 43
Ferngespräche, Erfassung, s. Telefondatenerfassung
Fernmeldeordnung 1984/12
Fernwartung 63; 1985/34
Fernwirkdienste 101, 102; 1984/16; 1985/14

Feuersozietät 1984/16
Feuerwehr 79
Finanzverwaltung 88
Flughafen 1985/4
Formulare 26
Forschung 33, 51, 59, 61, 82, 112, 117
Forschung, Sozialgesetzbuch X 82
Forschungsprojekte 50, 61, 87, 118
Fremdfirmen 63, 84, 86
Friedhöfe 1985/5
Forsten 1985/5
Funk 42
Führungszeugnis 57
Funktionentrennung 86, 101, 114; 1984/6
GASAG 36, 104
Geburtsdaten 41; 1985/18
Gebührenpflicht bei Auskünften 28
Gemeinsame Geschäftsordnung für die Berliner Verwaltung 89, 106; 1985/3, 10
Geschäftsverteilungsplan 115
Gesetz über Abbau der Fehlsubventionierung s. Fehlbelegungsabgabe
Gesetz über psychisch Kranke 121; 1985/3
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
Handels- und Gaststättenzählung 1985/11
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
Informationssystem Verbrechensbekämpfung 79,; 1985/8
Informationsverarbeitung, Entwicklung 49
INPOL-System 44; 1985/8
Institutionsleihe 44
intelligente Schnittstelle 1985/6
interner Datenschutzbeauftragter 105, 112, 116
internes Dateienregister 105
Intimbereich 39
isolierte Rechner 63, 114; 1985/5
ISVB, s. Informationssystem Verbrechensbekämpfung
Jugendgerichtshilfe 58, 110
Justizverwaltung 50, 60
Justizvollzugsanstalten 55, 81, 87; 1985/17
Kabelkommunikation 33, 37, 39, 46, 67, 102
Kabelpilotprojekt 101; 1984/15; 1985/3, 15
Kammergericht 1985/5
KAN, s. Kriminalaktennachweis
Kaufpreissammlung 119; 1984/27
Kindergeld 72, 100; 1984/19
Kirchen 24, 27, 32
Kirchensteuerstelle 1984/17
Klassenliste 118
Kleinrechner 84, 114; 1985/4, 6
Klinische Nachsorgeregister 50
Konferenz der Datenschutzbeauftragten 18, 43, 64, 88, 120; 1984/28; 1985/24
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
Krankenkassen 1985/21
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; 1985/3, 20, 26
Landesstatistikgesetz 104; 1984/3; 1985/3, 26
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
Medienforum Berlin 1985/15
Medienprivileg 8, 38, 65, 68
medizinische Daten 25, 27, 31, 40, 49, 63, 100, 112, 120; 1984/3, 7; 1985/20
Meldegesetz 35, 45, 53, 64, 77, 107, 121; 1984/3, 21; 1985/3, 6, 26
Meldepflicht, s. Landesmeldegesetz, Melderechtsrahmengesetz
Melderechtsrahmengesetz 27, 31, 44, 55, 100; 1985/26
Melderegister 54, 63, 64, 78, 87, 107; 1984/21; 1985/6, 23
Menschenrechtskonvention 28
Mieterlisten 73
Mietobergrenzen 1984/27
Mietpreisstellen 73
Mikrocomputer 1984/18
Mikroverfilmung 1984/32
Mikrozensus 1984/23; 1985/11
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; 1985/31
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; 1985/6
Organleihe 44
Orwell 99
Öffentliche Lebensversicherung 1984/16
öffentliche Wirtschaftsunternehmen 1984/16
Öffentlichkeitsarbeit 33, 50, 89, 121; 1984/29
Paß 126; 1985/8
Pay - TV 102; 1985/15
Personalakten 26, 40, 67; 1984/18; 1985/18
Personalausweis 26, 31, 42, 55, 87, 106, 120, 126; 1985/6
Personalausweisgesetz 44, 100, 106; 1984/4
Personalbezügedatei 1984/24
Personalcomputer 1985/4, 32
Personaldaten 25, 32, 40, 45, 49, 56, 66, 67; 1984/9, 18; 1985/5, 18
Personalfragebogen 1984/19
Personalrat 1985/19
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; 1985/11
Polizei, Ordnungsaufgaben, s. Allgemeines Sicherheits- und Ordnungsgesetz,

Ausländerbehörde, Melderegister, Paß, Personalausweis
Polizei, Strafverfolgung, s. Fahndung, Informationssystem Verbrechensbekämpfung, INPOL-System, KAN, KpS-Richtlinien, Strafverfolgung, Strafprozeßordnung
Polizeiliche Beobachtung 1984/11; 1985/7
Postaustausch 1985/15
Postkarte 43
Postzustellungsurkunde 43
private Computernutzung 1984/18; 1985/4
private EDV-Unternehmen 84
Programmdokumentation 106, 114
Programmtests 86, 113
Protokollisten 116
Prozeßordnungen 1984/25; 1985/22
psychiatrische Daten 53, 66; 1984/8; 1985/20
psychiatrische Gutachten 41
Quellabzugsverfahren 57
Rasterfahndung 33, 35, 43; 1984/11
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; 1985/3
Schuldnerverzeichnis 61; 1984/28
Schule 25, 32, 36, 41, 50, 57, 87, 118, 120; 1984/28; 1985/5, 24
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; 1985/22
Sozialgesetzbuch X 25, 26, 27, 31, 44, 50, 58, 64, 72, 81, 109; 1984/25; 1985/22
Sozialgesetzbuch X, Aktenführung 1984/25, 34
Sozialgesetzbuch X, Ausländer 100, 111; 1985/22
Sozialgesetzbuch X, Datenschutzbeauftragte 112
Sozialgesetzbuch X, Offenbarung für Forschung und Planung 59, 82
Sozialgesetzbuch X, Offenbarung für Strafverfahren 82, 100, 111; 1984/26; 1985/4, 22, 29
Sozialgesetzbuch X, Zweckbindung 83
Sozialgesetzbuch X, 3. Kapitel 83, 100
Sozialhilfe, Ausländer 58, 82
Sozialhilfe, 58, 87
Sozialhilfestatistik 64
Sozialleistungsträger 1984/16
Sozialwissenschaftliche Untersuchungen 33
Sparkasse der Stadt Berlin West 1984/16
speichernde Stelle 62, 109
Sperrung 1984/22; 1985/6
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; 1985/11
Städtebauförderungsgesetz 74
Steuerfahndung 88
Steuerverwaltung 88
Strafgesetzbuch, 200 81
Strafprozeßordnung 1984/10; 1985/8
Strafverfolgung 37, 79; 1984/10; 1985/7
Strafvollzug, s. Justizvollzugsanstalten
Studentendaten s.Hochschulen
Taxifahrer 62; 1984/28
Technische Prüfstellen für den Kraftfahrzeugverkehr 64
Telebus 1984/26; 1985/23
Telefon, Benutzung 42
Telefondatenerfassung 63, 87, 120
Teletex 37, 38
TEMEX, siehe Fernwirkdienste
Testdaten 86, 113; 1984/18
Textverarbeitung 84, 85; 1985/5
Todesursachenstatistik 104
Transparenz der Datenverarbeitung 30, 86, 104, 114
Transportkontrolle 86
Umwandlung von Mietwohnungen 73
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
Verfassungsschutzgesetz 1985/3, 8, 26, 29
Vermessungsamt 1985/6
Verkehrszählung 1985/11
Vernichtung von Datenträgern 63, 115
Veröffentlichung von Verurteilungen 81
Versand von Schriftstücken 54
Vertraulichkeit 111; 1984/9; 1985/23
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; 1985/11
Vordrucke 53, 87
Wahlen 54, 55, 59, 68; 1985/17
Warnkartei 40
Wählerliste, s. Wahlen
Werbung 28
Wettbewerbsunternehmen, Krankenhäuser 112
Wirtschaftskriminalität 77; 1984/6
Wohnung 100
Wohnungsbau-Kreditanstalt 1985/16
Wohnungsbau-Rechenzentrum 85, 120; 1984/17
Zentrale Vormundschaftskasse / Unterhaltsvorschußkasse 85
Zugriffsberechtigung 55
Zugriffskontrolle 86; 1985/8
Zustimmung, s. Einwilligung
Zweckbindung 66

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	89	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