Abgeordnetenhaus von Berlin

10. Wahlperiode

Drucksache 10/2652 neu

16. 12. 88

Dieses Blatt ist auszutauschen, da die Nummer der Vorlage zur Kenntnisnahme in 133 geändert worden ist.

Mitteilungen des Präsidenten

- Nr. 311 -

Inhaltsübersicht

Druckschluß: 14. Dezember 1988

Ausgegeben am 16. Dezember 1988

Der Präsident
Peter Rebsch

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

Abgeordnetenhaus von Berlin

10. Wahlperiode

Drucksache 10/2652

16. 12. 88

Mitteilungen des Präsidenten

- Nr. 311 -

Inhaltsübersicht

Druckschluß: 14. Dezember 1988

Ausgegeben am 16. Dezember 1988

Der Präsident
Peter Rebsch

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

Vorlage zur Kenntnisnahme

Bericht des Berliner Datenschutzbeauftragten zum 31. Dezember 1988

Inhaltsverzeichnis

Der Berliner Datenschutzbeauftragte gibt zu Beginn des Jahresberichts 1988[1] einen Überblick über die Situation des Datenschutzes (1). Sie wird durch die dynamische Entwicklung der Informationstechnik, den Aufbrauch des von der Verwaltung in Anspruch genommenen und von einigen Gerichten eingeräumten Übergangsbonus und das Bestreben des Gesetzgebers, Informationseingriffe zu regeln, bestimmt. In den folgenden Abschnitten 2 - 4 werden die Ergebnisse der Datenschutzkontrolle und Beratung dargelegt. Dabei wird unter 3 - entsprechend den gesetzlichen Vorschriften[2] - über die Beobachtungen beim Betrieb von Bildschirmtext und bei der Entwicklung anderer neuer Medien berichtet. Weiter werden neue Entwicklungen zur Feststellung aus den Vorjahren (5) und die Zusammenarbeit auf dem Gebiet des Datenschutzes (6) dargestellt

[1] Nach § 26 Abs. 2 Berliner Datenschutzgesetz erstattet der Berliner Datenschutzbeauftragte dem Abgeordnetenhaus und dem Regierenden Bürgermeister jährlich

[2] § 5 Abs. 3 Gesetz zum Staatsvertrag über Bildschirmtext (GVBl. S. 871 und § 23 Abs. 1 Kabelpilotprojektgesetz, GVBl. S. 565)
Die Bestimmungen lauten gleichermaßen: „Der Berliner Datenschutzbeauftragte berichtet dem Abgeordnetenhaus von Berlin über von ihm festgestellte Mängel und seine Vorschläge zur Beseitigung und zur Verbesserung des Datenschutzes"

Abgeordnetenhaus von Berlin - 10. Wahlperiode Drucksache 10/2652

Vorlage zur Kenntnisnahme

Bericht des Berliner Datenschutzbeauftragten zum 31. Dezember 1988

Inhaltsverzeichnis

Der Berliner Datenschutzbeauftragte gibt zu Beginn des Jahresberichts 1988[1] einen Überblick über die Situation des Datenschutzes (1). Sie wird durch die dynamische Entwicklung der Informationstechnik, den Aufbrauch des von der Verwaltung in Anspruch genommenen und von einigen Gerichten eingeräumten Übergangsbonus und das Bestreben des Gesetzgebers, Informationseingriffe zu regeln, bestimmt. In den folgenden Abschnitten 2 - 4 werden die Ergebnisse der Datenschutzkontrolle und Beratung dargelegt. Dabei wird unter 3 - entsprechend den gesetzlichen Vorschriften[2] - über die Beobachtungen beim Betrieb von Bildschirmtext und bei der Entwicklung anderer neuer Medien berichtet. Weiter werden neue Entwicklungen zur Feststellung aus den Vorjahren (5) und die Zusammenarbeit auf dem Gebiet des Datenschutzes (6) dargestellt

1. Zur Situation
1.1 Neue Formen der Datenverarbeitung
1.2 Übergangsbonus
1.3 Europa ohne Datenschutz?

2. Brennpunkte des Datenschutzes
2.1 Gesundheitsreform durch Datenverarbeitung?
2.2 Das genetische Personenkennzeichen
2.3 Der Bürger im Objektiv der Videokameras
2.4 Volkszählung: Zu viel Zwang - zu wenig Freiwilligkeit
Erhebung
Arbeitsstättenzählung
Durchsetzung der Auskunftspflicht
Aufbereitung
Bewertung

3. Neue Medien
3.1 Telekommunikation
3.2 Bildschirmtext
Entwicklung des Dienstes
Bildschirmtext in der Berliner Verwaltung
Anbieterprüfungen
3.3 Kabelpilotprojekt
3.4 Neue Telekommunikationsdienste

4. Weitere Fragen aus der Kontroll- und Beratungspraxis
4.1 Abgeordnetenhaus und Senatskanzlei
4.2 Bau- und Wohnungswesen
4.3 Finanzwesen
Steuerverwaltung
Haushaltswesen
4.4 Gesundheit und Soziales
Datenverarbeitung im Gesundheitswesen
AIDS
Forschung und Planung mit Patientendaten
Transparenz im Gesundheitswesen - nur nicht für den Patienten?
Sozialversicherungsausweis und Rentenversicherungsnummer
Amtshilfe zwischen Polizei und Sozialamt?
Forschung in der Sozialverwaltung
Technisch-organisatorische Maßnahmen
4.5 Inneres
Amtliche Statistik
Personalwesen
Öffentliche Sicherheit
Meldewesen
4.6 Justiz
Automation bei der Staatsanwaltschaft
Zentrales Handelsregister
Datenschutzdelikte
4.7 Kulturelle Angelegenheiten
Archivwesen
Bibliotheken
4.8 Schulwesen
4.9 Verkehr und Betriebe
Führerscheindatei
Neue Fahrkarten bei der BVG
4.10 Wirtschaft und Arbeit
Mitgliedererfassung durch die IHK
Kreditwesen
4.11 Wissenschaft und Forschung
Rasterfahndung in der Hochschule
Stellenbesetzungslisten
4.12 Organisation und Geschäftsordnung
Postaustausch in der Berliner Verwaltung
Aktenaufbewahrung
Mitschnitt von Telefonaten

5. Nachträge zu Feststellungen aus den Vorjahren
Arbeitsunfähigkeitsbescheinigung (Jahresbericht 1986, Ziff. 5.3)
Vordrucke (Jahresbericht 1987, Ziff. 5.7)
Vordrucke (Jahresbericht 1985, Ziff. 4.5)
Bezirksämter - Führung der Grundstückseigentümerkartei (Jahresbericht 1985, Ziff. 4.1)
Schulpsychologischer Dienst (Jahresbericht 1987, Ziff. 5.5)

6. Zusammenarbeit mit anderen Stellen
Konferenz der Datenschutzbeauftragten
Abgeordnetenhaus
Aufsichtsbehörde nach dem Bundesdatenschutzgesetz
Meldungen zum Dateienregister

[1] Nach § 26 Abs. 2 Berliner Datenschutzgesetz erstattet der Berliner Datenschutzbeauftragte dem Abgeordnetenhaus und dem Regierenden Bürgermeister jährlich

[2] § 5 Abs. 3 Gesetz zum Staatsvertrag über Bildschirmtext (GVBl. S. 871 und § 23 Abs. 1 Kabelpilotprojektgesetz, GVBl. S. 565)
Die Bestimmungen lauten gleichermaßen: „Der Berliner Datenschutzbeauftragte berichtet dem Abgeordnetenhaus von Berlin über von ihm festgestellte Mängel und seine Vorschläge zur Beseitigung und zur Verbesserung des Datenschutzes"

2

EEM 10/2652 2

Anlagen

1. Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 6. Juni 1988 zur Neufassung des Bundesdatenschutzgesetzes.
2. Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 6. Juni 1988 zum Entwurf eines Gesetzes zur Strukturreform im Gesundheitswesen.
3. Beschluß der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 14. März 1988 betr. Polizeiliche Datenverarbeitung bis zum Erlaß bereichsspezifischer gesetzlicher Regelungen.
4. Beschluß der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 10. Oktober 1988 zur Sicherstellung des Datenschutzes bei der Poststrukturreform.
5. Beschluß der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 10. Oktober 1988 über aktuelle Probleme des Datenschutzes in der Telekommunikation.
6. Ausführungsvorschriften über den Schulpsychologischen Dienst vom 18. August 1988.
7. Beschluß der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 10. Oktober 1988 über Datensicherheit beim Einsatz kleinerer Datenverarbeitungsanlagen.
8. Informationen zur Datenträgervernichtung.

Stichwortregister

für alle seit 1979 veröffentlichten Jahresberichte

1. Zur Situation

Die Situation des Datenschutzes wird durch drei Entwicklungslinien bestimmt:

- die dynamische Entwicklung der Informationstechnik, die - wie in der Berliner Verwaltung deutlich zu beobachten - die Schwelle zu einer neuen Phase der Datenverarbeitung überschritten hat;
- den Verbrauch des „Übergangsbonus", den die Rechtsprechung der Verwaltung nach dem Volkszählungsurteil des Bundesverfassungsgerichts[1] eingeräumt hat und der eine umfassende und normenklare rechtliche Regelung des Umgangs mit personenbezogenen Informationen erzwingt;
- die zunehmende Bedeutung der Europäischen Gemeinschaft, die das völlige Fehlen des Datenschutzes auf Gemeinschaftsebene zu einem wachsenden Problem macht.

1.1 Neue Formen der Datenverarbeitung

Die vorhergesagte *Entwicklung der Informationstechnik* zeigt sich nun auch in der Praxis der Berliner Verwaltung immer deutlicher. Sie ist durch die rasche Zunahme von Personalcomputern (PCs) - wobei diese Bezeichnung angesichts der hohen Leistungskraft der Geräte in die Irre führt -, den steigenden Einsatz von Bürosystemen mit mehreren Endgeräten, den Aufbau von Netzen (z. B. Verwaltungsnetz) und den Anschluß von Großrechnern, Bürosystemen und PCs an die Netze gekennzeichnet. Für den Datenschutz bedeutet dies, daß einmal neben den Großrechenzentren immer mehr dezentrale Rechner im Auge behalten werden müssen, und zum anderen bei vernetzter Datenverarbeitung die Kommunikation über Netze immer schwerer kontrollierbar wird. Die qualitativen und quantitativen Anforderungen an die datenschutzrechtliche Kontrolle haben sich damit erheblich erhöht und werden mit fortschreitendem Einsatz weiter steigen.

[1] BVerfGE 65, 1 ff.

Für den Anwender macht sich dies als Tendenz zur Rückkehr der Verarbeitung von Informationen in die Fachbehörde und -abteilung bemerkbar. Die Datenverarbeitung kann in Zukunft auf Grund einer besseren Identifikation mit der Fachaufgabe gestaltet werden, da die Betriebssysteme, Datenbanken, Büroinformationssysteme, Menüentwicklungssysteme und viele Komponenten mehr für die Verwendung durch den nicht speziell vorgebildeten Mitarbeiter geeignet sein sollen. Die Aufgaben der DV-Fachleute in der Verwaltung sollen sich dagegen von der Systemgestaltung zur Beratung bei der Auswahl und Einführung der Systeme verlagern. Die Anwendungsflexibilität der Datenverarbeitung kann mit der zunehmenden Unabhängigkeit von zentralen Instanzen erheblich steigen.

Dies bedeutet nicht, daß die neuen Verfahren ausschließlich isoliert betrieben werden; vielmehr stehen sie oft organisatorisch oder technisch im Zusammenhang mit umfassenderen Verfahren, denn der bereits beschriebene Trend[1] zur Vernetzung der Datenverarbeitung der Berliner Verwaltung hält an: Für das automatisierte Haushaltswesen, für die Umstellung des Besteuerungsverfahrens der Oberfinanzdirektion und für das Senatsinformationssystem sind landesweite vernetzte Systeme geplant, zu denen ich im einzelnen Stellung nehmen werde.

Daneben stehen weitere Dezentralisierungstendenzen: Verschiedene Verwaltungsabläufe werden mit Hilfe von PCs automatisiert, die bisher in manueller Form oder mit zentraler Datenverarbeitung abgewickelt werden. Zu den vielen individuellen Insellösungen, die in den letzten Jahren zu verzeichnen waren, treten jetzt koordiniert entwickelte PC-Verfahren, deren ordnungsgemäße und datenschutzgerechte Gestaltung weniger dem Zufall überlassen wird. Beispiele dafür sind das geplante neue Lehrer-Informations- und Verwaltungssystem auf der Basis dezentraler PC-Netze als Ersatz für die alte Lehrerindividualdatei, Personalplanungs- und -verwaltungssysteme, Automationsprojekte im Sozialwesen.

Die Dezentralisierungstendenzen in der Datenverarbeitung, verbunden mit dem fortschreitenden Ausbau der Netze, sind angesichts der technologischen Entwicklungstrends unausweichlich. Im Hinblick darauf hat der Senat eine Umorganisierung der Datenverarbeitung mit dem *Orientierungsrahmen zu ADV-Planung und -Einsatz in der Berliner Verwaltung* in die Wege geleitet. Mit den darin zum Ausdruck kommenden Deregulierungsvorstellungen soll die bisher als zu unflexibel und bürokratisch geltende, die schnelle Umsetzung der technischen Entwicklung zur Verwaltungsautomation behindernde Organisation der ADV-Planung abgelöst werden.

Wesentliche Merkmale dieses Orientierungsrahmens sind statt des bisherigen Gesamtplanungsverfahrens:

- Festlegungen und Standards in Form von Mindest- und Rahmenbedingungen, in deren Rahmen die einzelnen Verwaltungen in eigener Verantwortung die Projekte planen und durchführen sollen;
- die verstärkte Einbindung externen Sachverstandes durch Einbindung leistungsfähiger Unternehmen der Privatwirtschaft.

Das Landesamt für Elektronische Datenverarbeitung (LED), künftig Berliner Datenverarbeitungszentrale, wird eingeschränkt auf die zentralen Dienstleistungsaufgaben, die von der öffentlichen Verwaltung unabweisbar selbst erfüllt werden müssen, d. h. die Durchführung von Großverfahren, die Betreuung und Verwirklichung des Verwaltungsnetzes sowie die Betreuung und Planung anwendungsneutraler Datenbanken. Systemanalyse als Projektentwicklung, Anwendungsprogrammierung sowie Wartung und Pflege der Anwendungsprogramme werden zukünftig nicht mehr vom LED, sondern von den einzelnen Verwaltungen unter Einbeziehung externen Sachverstandes selbst geleistet.

Wenngleich es den Datenschutz fördern kann, wenn neue organisatorische Rahmenbedingungen die Modernisierung der Datenverarbeitung in der Verwaltung vorantreiben, darf nicht übersehen werden, daß viele Produkte der modernen Datenverarbeitung die Lösung neuer Datenschutzprobleme erzwingen:

[1] Jahresbericht 1987, Ziff. 3

Die heutigen Betriebssysteme nach dem Industriestandard bringen keinen Fortschritt des technischen Datenschutzes, moderne relationale Datenbanken und integrierte Büroinformationssysteme stellen neue Grundsatzfragen an die Nachvollziehbarkeit der rechtmäßigen Anwendung, die offenen Datenverarbeitungsnetze (so auch das ISDN) bieten nur wenige Antworten, wie die Rechtmäßigkeit einerseits und die Sicherheit der Datenflüsse andererseits sichergestellt werden kann. Preisgünstigkeit, Schnelligkeit, Flexibilität und Anwendungskomfort werden mit verblüffender Dynamik entwickelt, die Entwicklung adäquater „Bremsen" zur Sicherstellung von Datenschutz und Ordnungsmäßigkeit, noch allgemeiner: der Sozialverträglichkeit, ist bisher nicht als vordringlich angesehen worden.

Alarmierende Beispiele aus jüngster Zeit sind die Ausbreitung eines eingeschleusten Virusprogramms, das den Speicherplatz von ca. *sechstausend* amerikanischen Computern - darunter auch Rechner des Verteidigungsministeriums - so belegte, daß die regulären Programme nicht ablaufen konnten, und der Fall, daß ein Hacker die elektronische Post des belgischen Premierministers mitlesen konnte. In beiden Fällen wurde nicht zuletzt von politischen und wissenschaftlichen Führungskräften sowie Fachkräften der Herstellerfirmen die alte Binsenweisheit übersehen: *ungehinderter Datenaustausch und Datenschutz sind miteinander unvereinbar.* Gute und sichere Systeme müssen zwischen beiden Extremen einen vernünftigen Mittelweg einhalten. Nur wenn sich die Entwicklung in Berlin auf dieser Mittellinie bewegt, sind vergleichbare Vorfälle zu vermeiden.

Ob der Orientierungsrahmen ausreicht, um eine dementsprechende bürger- und sachgerechte Datenverarbeitung der Berliner Verwaltung zu fördern, erscheint noch recht zweifelhaft.

Die *Verlagerung der Verantwortung* für die Planung und Umsetzung von DV-Projekten vom LED auf Senats- und Bezirksverwaltungen setzt voraus, daß diese über die nötige Professionalität - qualifiziertes Personal und Sachmittel in angemessenem Umfang - verfügen, die es ermöglicht, ordnungsgemäße und effektive ADV-Verfahren unter Berücksichtigung allgemein verbindlicher Standards zu realisieren. Demgegenüber lassen Erfahrungen vergangener Jahre in manchen Fällen den Schluß zu, daß einzelne Mitarbeiter ihre „Privatstandards" gegen die Interessen einer ordnungsgemäßen und effektiven Verwaltung einführen konnten. Dem muß Einhalt geboten werden, wenn die Transparenz und damit die Kontrollierbarkeit der Datenverarbeitung nicht (vollends) verloren gehen soll.

Auch der *Einsatz privater Unternehmen* hat in der Vergangenheit nicht nur positive Effekte erzeugt. Prüfungen in diesem Bereich haben mehrfach gezeigt, daß die auftraggebenden öffentlichen Stellen ihre Verantwortung nicht mehr in ausreichendem Maße wahrnehmen konnten. So ist den öffentlichen Auftraggebern gelegentlich mit dem Hinweis auf Firmengeheimnisse der Zugang zu Dokumentationsmaterialien versagt worden, die für die Überwachung der ordnungsgemäßen Datenverarbeitung jedoch notwendig gewesen wären. Ein bekanntes Beispiel für die Probleme eines vollständig an Private vergebenen Projektes bietet der Bildschirmtext[1].

Insgesamt ist festzustellen, daß - die mit dem Orientierungsrahmen angestrebte - Deregulation bisher nicht ausreicht, um die Probleme zu lösen, die sich aus den neuen Formen der Datenverarbeitung ergeben. Vielmehr sind Regeln und Maßnahmen erforderlich, die Datenschutz und Datensicherheit ebenso wie die Wirtschaftlichkeit garantieren. Insoweit bestehen Defizite, die dringend geschlossen werden müssen.

1.2 Übergangsbonus

Spätestens seit dem *Volkszählungsurteil des Bundesverfassungsgerichts* steht fest, daß der Umgang mit Informationen im wesentlichen vom Parlament entschieden werden muß. Dies gilt insbesondere für Informationseingriffe durch die öffentliche Verwaltung. Allerdings hat das Bundesverfassungsgericht dem Gesetzgeber in der Vergangenheit Übergangsfristen zur Beseitigung derartiger Regelungsdefizite zugebilligt, wenn damit eine sonst eintretende Funktionsunfähigkeit staatlicher Einrichtungen vermieden werden kann, die der verfassungsmäßigen Ordnung noch ferner stünde als der bisherige Zustand.

Verschiedene Gerichte haben seit dem Urteil daher konsequenterweise festgestellt, daß die Verarbeitung personenbezogener Daten zwar ohne hinreichende gesetzliche Grundlage erfolge, dieser Zustand für eine gewisse Zeit aber hinzunehmen ist; für die polizeiliche Datenverarbeitung hat dies als bisher höchstes Gericht der Bayerische Verfassungsgerichtshof festgestellt[1].

Der Übergangsbonus kann jedoch weder zeitlich noch sachlich unbegrenzt in Anspruch genommen werden: Der Gesetzgeber muß, sobald ihm dies möglich ist, Initiativen ergreifen, um die Regelungslücken zu schließen: Das Bundesverfassungsgericht hat in anderen Fällen ausdrücklich darauf hingewiesen, daß der Gesetzgeber eine Neuregelung nicht ungebührlich verzögern darf.

In der Übergangsfrist sind aber auch nicht beliebige Eingriffe zulässig. Vielmehr reduziert sich die Befugnis auf diejenigen Maßnahmen, die für die geordnete Weiterführung eines funktionsfähigen Betriebes unerläßlich sind. Jede Einführung neuer Verfahren muß daher besonders streng am Maßstab der Unerläßlichkeit gemessen werden.

Diesen für alle Verwaltungszweige geltenden Tatbestand hat die Konferenz der Datenschutzbeauftragten des Bundes und der Länder für den Bereich der polizeilichen Datenverarbeitung besonders betont[2].

Für das Land Berlin hatte ich bereits im letzten Jahresbericht darauf hingewiesen, daß aus meiner Sicht der Übergangsbonus für Berlin mit dieser Legislaturperiode abläuft[3].

Nach dem Volkszählungsurteil setzten relativ frühzeitig Aktivitäten in Bund und Ländern ein, um für die *Sicherheitsbehörden* die für erforderlich gehaltenen gesetzlichen Grundlagen für ihre informationellen Tätigkeiten zu schaffen, denn bisher sind zahlreiche Formen der Datenerhebung und Datenverarbeitung nicht oder nur punktuell geregelt. Neuregelungen sind jedoch nur vereinzelt, und dann nicht im Hinblick auf die Verbesserung der Gewährleistung des Datenschutzes erfolgt[4]. Eine umfassende Novellierung des Polizeirechts und der Datenverarbeitung bei der Strafverfolgung steht dagegen aus.

Seit Jahren habe ich konkrete Vorschläge unterbreitet und dafür geworben, daß Berlin - trotz der bekannten Berliner Unlust, Bundesgesetze konzeptionell zu beeinflussen - sich für eine Novellierung der Strafprozeßordnung (StPO) engagiert. Herausgekommen sind bisher nur punktuelle, wenig überzeugende Änderungen der StPO.

Auch im Bereich des Polizeirechts hat man sich bedeckt gehalten, obwohl bereits in mehreren Ländern Gesetze vorliegen oder beraten werden. Der Innensenator begründete dies damit, daß man möglichst bundeseinheitlich vorgehen und auch die Bundesregelung in der StPO berücksichtigen solle. Dies ist richtig, allerdings sind die Verhältnisse nicht so, daß in Berlin die Hände länger in den Schoß gelegt werden könnten.

Auch eine parlamentarische Initiative, nach der zum 1. April 1988 vom Senat der Entwurf eines novellierten Allgemeinen Sicherheits- und Ordnungsgesetzes (ASOG) vorgelegt werden sollte, führte lediglich zu einem Zwischenbericht, in dem auf den Abstimmungsbedarf mit der Bundesgesetzgebung hingewiesen wurde. Ein daraufhin vorgelegter Entwurf der F.D.P.-Fraktion greift manche Anregungen der Konferenz der Datenschutzbeauftragten auf, konnte aber in den zuständigen Ausschüssen nur noch anberaten werden. Ein letztlich doch im zuständigen Referat des Innensenators konzipierter Entwurf, der sich eng an den Musterentwurf hält, wurde mir erst sehr spät zugeleitet.

Zu Beginn der kommenden Legislaturperiode muß die Novellierung des Polizeirechts hohe Priorität erhalten, da anderenfalls die gesamte polizeiliche Informationsverarbeitung beanstandet werden müßte.

---

[1] vgl. insbesondere meine Jahresberichte für die Jahre 1980 - 1985 und den Bericht des Bundesrechnungshofes, Bundestag Drs. 11/3056.

[1] Urteil vom 9. 7. 1985 (21 B 82 A. 2261)

[2] Entschließung vom 1. 4. 88, vgl. Anlage 3

[3] Jahresbericht 1987, Ziff. 5.3

[4] z. B. Gesetz zur Änderung der Strafprozeßordnung v. 19. 4. 86 (§ 163 d StPO); Gesetz zur Änderung des Straßenverkehrsgesetzes v. 28. 1. 87 (ZEVIS)

Auch auf anderen Gebieten ist die Landesgesetzgebung zwar vorangekommen, hat jedoch nicht die erwünschten Fortschritte gemacht. Regelungen der Informationsverarbeitung sind insbesondere auf folgenden Gebieten erörtert worden:

Die *Landesstatistik* soll entsprechend meiner seit Jahren erhobenen Forderung erstmals auf eine gesetzliche Grundlage gestellt werden. An den Vorarbeiten bin ich von Anfang an beteiligt worden. Der Senatsentwurf ist inzwischen eingebracht worden und wird im Abgeordnetenhaus beraten[1].

Keine erkennbaren Fortschritte haben dagegen die Arbeiten an einem *Landesarchivgesetz*[2] gemacht: Nachdem das Bundesarchivgesetz in Kraft getreten ist, sollte eine Regelung in Berlin alsbald nachfolgen, zumal hier aufgrund der Bedeutung Berlins umfangreiches Material vorhanden ist, dessen rechtliche Behandlung für eine Auswertung durch Forscher bisher ungeklärt ist. Im Kulturressort wird nach wie vor die Schaffung eines *Bibliotheksgesetzes*[3] abgelehnt, obwohl die Arbeiten an der Ausleihautomation weiterhin fortgeführt werden, und ich zumindest den Verbund der Bibliotheken nur auf einer hinreichenden gesetzlichen Grundlage für möglich halte. Es steht zu hoffen, daß diese Vorhaben jedenfalls zu Beginn der neuen Legislaturperiode erledigt werden.

Außerdem steht im Krankenhauswesen eine Regelung für das *Einsichtsrecht des Patienten* aus. Obwohl in der ablaufenden Legislaturperiode bereits eine weitgehende Einigkeit unter den Politikern zu beobachten war, wurde auch nach Fristsetzung durch den Unterausschuß Datenschutz kein Gesetzentwurf vorgelegt.

Die Situation auf *Bundesebene* ist durch große Reformvorhaben gekennzeichnet, die auch auf den Datenschutz beträchtliche Auswirkungen haben. Hier ist vor allem die *Gesundheitsstrukturreform* zu nennen, mit der sich die Datenschutzbeauftragten eingehend auseinandergesetzt haben[4]. Vor allem ist zu fordern, daß die im Zusammenhang mit Leistungen der gesetzlichen Krankenversicherung vorgesehene automatisierte Verarbeitung von Daten der Versicherten, Ärzte und Zahnärzte vom Gesetzgeber wegen des damit verbundenen gravierenden Eingriffs in das Selbstbestimmungsrecht der Versicherten nur zugelassen werden darf, wenn damit tatsächlich auch die erklärten Ziele des Gesetzgebungsvorhabens gefördert, namentlich wesentliche Beiträge zur Kostendämpfung geleistet werden können und sich dies nicht auch durch weniger einschneidende Maßnahmen erreichen läßt. Wenn auf die näheren Einzelheiten erst weiter unten eingegangen wird, so bleibt jedoch generell festzuhalten, daß wiederum ein großes Reformvorhaben mit der umfassenden Speicherung von sensiblen personenbezogenen Daten verbunden wird. Die daran geknüpfte Hoffnung, daß die Datenverarbeitung wesentliche Vorteile bietet, war in der Vergangenheit bei zahlreichen Großprojekten anzutreffen; sie hat sich jedoch in den wenigsten Fällen erfüllt.

Das *Gesetz über die Sozialversicherungsnummer* ist inzwischen verabschiedet worden. Seine Auswirkungen lassen sich noch nicht voll übersehen. Aus Datenschutzsicht besteht jedoch die Sorge, daß sich die Nummer zu einer Art Personenkennzeichen in vielerlei Bereichen entwickeln wird. Diese Gefahr wird durch die geplante Einführung eines *Sozialversicherungsausweises* noch verstärkt.

Deutlich weniger Engagement zeigte die Bundesregierung bei der Reform der *Strafprozeßordnung,* von deren Realisierung die Innenministerkonferenz auch die Fortschritte bei der Polizeirechtsnovellierung abhängig gemacht hat. Die Vielzahl der vorliegenden Entwürfe, die gleichwohl noch lückenhaft sind, lassen eine rechtzeitige Verabschiedung in dieser Legislaturperiode kaum mehr erwarten: ein im Hinblick auf den Ablauf des Übergangsbonus äußerst mißlicher Umstand.

Von erheblicher Bedeutung für den Datenschutz ist die Anpassung der Datenschutzgesetze an die Anforderungen des Volkszählungsurteils, wenn ich auch stets die Auffassung vertreten habe, daß zunächst die spezialrechtlichen Materien zu regeln sind. Den Datenschutzgesetzen sollte im Hinblick auf die Normenklarheit nur Auffangcharakter zukommen, damit der Bürger beim Studium eines Gesetzes auch die beim Vollzug erforderlichen Informationsprozesse erkennen kann, und nicht erst Überlegungen über das Verhältnis der verschiedenen Gesetze zueinander anstellen muß.

Gleichwohl wurde vom Bundesinnenministerium ein neuer Entwurf eines *Bundesdatenschutzgesetzes* sowie eine Ergänzung des *Verwaltungsverfahrensgesetzes* vorgelegt. Ungeachtet einiger technischer Verbesserungen hat die Konferenz der Datenschutzbeauftragten ihre bereits zu dem vorhergehenden Entwurf aus der vergangenen Legislaturperiode vorgebrachte Kritik erneuert[1]. Der Entwurf wird wesentlichen Forderungen der Datenschutzbeauftragten nicht gerecht und bedarf spätestens in der parlamentarischen Beratung erheblicher Verbesserungen.

Im Gegensatz dazu haben die Länder Hessen, Bremen und Nordrhein-Westfalen bei der Novellierung ihrer Landesgesetze diese Forderungen aufgegriffen; die SPD-Fraktion im Abgeordnetenhaus hat einen Gesetzentwurf vorgelegt, der sich an diesen Gesetzen orientiert[2].

Im Mittelpunkt der *Rechtsprechung* zum Datenschutz stand die Frage, ob und wie lange der Übergangsbonus noch gewährt werden kann. Zunehmend häufiger stellen sich dabei die Gerichte auf den Standpunkt, daß fünf Jahre nach dem Volkszählungsurteil die dem Gesetzgeber eingeräumte Zeitspanne zur Anpassung der Gesetze an die Verfassungslage zu verstreichen droht. So vertritt am Beispiel der zentralen Namenskartei der Staatsanwaltschaften, deren Automatisierung mit dem Verfahren ASTA in Berlin Gegenstand der datenschutzrechtlichen Kontrolle war[3], das Oberlandesgericht Frankfurt die Auffassung, der Übergangsbonus laufe mit dem Ende der Legislaturperiode des Bundestages im Jahre 1990 ab[4]. Auf die Erforderlichkeit gesetzlicher Grundlagen für die in meinen Jahresberichten öfters kritisch erwähnte Anordnung über Mitteilungen in Strafsachen hatte zuvor auch das Berliner Kammergericht sehr deutlich hingewiesen[5].

Entgegen denjenigen Stimmen, die die Reichweite des Volkszählungsurteils unter Hinweis auf den zu engen Geltungsbereich der Datenschutzgesetze auf die Verarbeitung personenbezogener Daten in Dateien begrenzen wollen, hat das Bundesverfassungsgericht[6] betont, daß das Recht auf informationelle Selbstbestimmung generell vor staatlicher Erhebung und Verarbeitung personenbezogener Daten schütze und nicht auf den jeweiligen Anwendungsbereich der Datenschutzgesetze beschränkt sei: Es erklärte § 687 Zivilprozeßordnung für verfassungswidrig, der die öffentliche Bekanntmachung der Entmündigung einer Person wegen Verschwendung oder Trunksucht anordnete. Auf weitere Entscheidungen des höchsten deutschen Gerichts zur informationellen Selbstbestimmung darf man gespannt sein.

Wie bereits in den Vorjahren nahmen sich besonders die *Arbeitsgerichte* datenschutzrechtlicher Fragestellungen an. In der brisanten Frage, unter welchen Umständen Unterlagen aus den Personalakten zu entfernen sind, entschied das Bundesarbeitsgericht, daß der Arbeitnehmer die Entfernung eines auf einer wahren Sachverhaltsdarstellung beruhenden Schreibens aus der Personalakte verlangen kann, wenn es für die weitere Beurteilung des Arbeitnehmers überflüssig geworden ist und ihn in seiner beruflichen Entwicklungsmöglichkeit fortwirkend beeinträchtigen kann[7]. Von großem Interesse ist, in welchem Umfang auch die für die Personalaktenführung bei Beamten zuständigen Verwaltungsgerichte entscheiden werden, das hergebrachte Vollständigkeitsprinzip zugunsten der Wahrung der informationellen Selbstbestimmung differenzierter zu betrachten.

Ebenfalls Gegenstand arbeitsgerichtlicher Rechtsprechung war die Frage, in welchem Umfang von Arbeitgebern Videokameras zur Überwachung der Arbeitnehmer eingesetzt werden dürfen.

---

[1] vgl. Abgeordnetenhaus Drs. 10/2534 v. 21. 10. 88 und unten Ziff. 4.5

[2] vgl. unten 4.7

[3] ebd.

[4] vgl. Anlage 2 und unten Ziff. 2.1

[1] vgl. Anlage 1

[2] Abgeordnetenhaus Drs. 10/2440

[3] vgl. unten Ziff. 4.6

[4] Beschluß vom 14. 7. 88 (3 VAs 4/88)

[5] Beschluß vom 23. 3. 88 (4 VAs 40/87)

[6] Beschluß vom 9. 3. 88 (1 BvL 49/86)

[7] Urteil vom 13. 4. 88 (5 AZR 537/86)

Das Bundesarbeitsgericht ist der Auffassung, eine Verletzung des Persönlichkeitsrechts eines Arbeitsnehmers könne vorliegen, wenn dieser einem ständigen lückenlosen Überwachungsdruck dadurch unterworfen werde, daß der Arbeitgeber sich vorbehält, jederzeit ohne konkreten Hinweis den Arbeitnehmer durch versteckt aufgestellte Videokameras zu überwachen[1]. Etwas anderes muß allerdings gelten, wenn Aufzeichnungen aufgrund tatsächlicher Anhaltspunkte als Notwehr- oder Notstandmaßnahme gegenüber rechtswidrigem Verhalten die einzige Möglichkeit des Nachweises darstellen: So hat das Landesarbeitsgericht Berlin die Verwertung heimlicher Tonbandaufzeichnungen zum (nur so möglichen) Nachweis betrügerischen Verhaltens des Verkaufspersonals zugelassen[2].

1.3 Europa ohne Datenschutz?

Auf dem Weg zu einer dynamischen europäischen Volkswirtschaft strebt die Europäische Gemeinsschaft die Vollendung des gemeinsamen *Binnenmarktes* für das Jahr 1992 an. Obwohl eine steigende Flut von EG-Normen zu beobachten ist, die bindende Regeln für immer neue Bereiche schafft, fehlen datenschutzrechtliche Vorschriften auf Gemeinschaftsebene.

So mußte ich anläßlich einer Beschwerde eines EG-Mitarbeiters über die unbefugte Weitergabe seiner Personaldaten feststellen, daß es sowohl an einer datenschutzrechtlichen Grundlage wie an einer für diesen Fall zuständigen Datenschutzinstanz fehlt. Ein weiteres Beispiel ist die Normung auf dem Gebiet der Telekommunikation. Sie soll nach dem Grünbuch[3] wesentlich verstärkt werden, ohne daß dabei Fragen des Datenschutzes und der Datensicherung berücksichtigt werden. Das ist nicht zuletzt deshalb zu bedauern, weil nach meiner Erfahrung gerade in der Normungsphase Datenschutz- und Datensicherungsgesichtspunkte relativ leicht berücksichtigt werden könnten.

Daher ist eine Datenschutzkontrollinstitution auf europäischer Ebene erforderlich, die die Kommission berät und für die Berücksichtigung datenschutzgerechter Lösungen eintritt. Diese Stelle hätte auch die Aufgabe, mit den nationalen Datenschutzbeauftragten zusammenzuarbeiten und für die Harmonisierung des Datenschutzrechts auf einem möglichst hohen Niveau Sorge zu tragen.

2. Brennpunkte des Datenschutzes

2.1 Gesundheitsreform durch Datenverarbeitung?

Die Bundesregierung hat im April des Jahres den Entwurf eines *Gesetzes zur Strukturreform im Gesundheitswesen* (Gesundheits-Reformgesetz - GRG) beschlossen und an die parlamentarischen Gremien zur Beratung überwiesen. Ziel dieses Vorhabens ist es, die seit Jahren steigenden Beitragssätze in der gesetzlichen Krankenversicherung zu senken und dauerhaft zu stabilisieren. Neben gesundheitspolitischen Maßnahmen sollen Maßnahmen zur Erhöhung der Wirtschaftlichkeit eingeführt werden, die erheblichen Einfluß auf den Schutz der personenbezogenen Daten von Patienten, aber auch von „Leistungserbringern" (Ärzten, Zahnärzten, Apothekern) haben: Vorgesehen ist die umfassende Verarbeitung von Daten über ärztliche und ärztlich verordnete Leistungen durch die Krankenkassen und Kassenärztlichen Vereinigungen. Ein Medizinischer Dienst, der den bisherigen Vertrauensärztlichen Dienst ersetzen soll, wird zusätzliche Daten erhalten.

Bereits vor dem Beschluß der Bundesregierung habe ich dem Senator für Gesundheit und Soziales meine Bedenken eindringlich geschildert. Die umfassende automatisierte Speicherung und Verarbeitung medizinischer Daten greifen tief in das Grundrecht auf informationelle Selbstbestimmung ein und ermöglichen im Ansatz die Erstellung von Gesundheitsprofilen. Die Voraussetzungen für derartige Eingriffe sind im Gesetzgebungsverfahren nicht hinreichend dargelegt worden.

Insbesondere habe ich Zweifel daran, daß die totale Erfassung ein geeignetes Mittel ist, den angestrebten Zweck zu erreichen, und ob im Rahmen einer Güterabwägung die mit der Speicherung verbundenen Risiken richtig eingeschätzt werden.

Insbesondere habe ich an folgendem Kritik geübt:

- der mangelhaften Festlegung der Voraussetzungen für die Datenübermittlung an den Medizinischen Dienst und den fehlenden Bestimmungen über den Verwendungszweck der Daten;
- den zu weitgehenden Befugnissen der Verbände der Krankenkassen und Kassenärztlichen Vereinigungen bei der Festlegung der erforderlichen Daten;
- der ungenügenden Regelung des Auskunftsanspruchs;
- der Verwendung der Rentenversicherungsnummer im Bereich der Krankenkassen, insbesondere auch vor dem Hintergrund des (maschinenlesbaren) Krankenversicherungsausweises.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder forderte eine Verbesserung des Datenschutzes in dem Reformpaket[1]. Vor allem wurde betont, daß für die Erstellung von Statistiken, die für die Bewertung und Beeinflussung des Leistungsgeschehens wichtig sind, anonyme Datenbestände ausreichen.

Im Laufe der Beratung des Gesetzentwurfes im Bundestag konnten Verbesserungen erzielt werden; insbesondere wurde die Zweckbindung der anfallenden Daten für Wirtschaftlichkeitsprüfungen erheblich stärker betont, gerade soweit es sich um personenbezogene Daten der Leistungsempfänger handelt. Löschungsfristen für die Daten sollen verhindern, daß die Datenbestände sich zu lebenslangen gesundheitlichen Datenkonten entwickeln. Transparenz- und Auskunftsvorschriften sollen die Durchschaubarkeit für den Bürger erhöhen. Die Rentenversicherungsnummer wird von den Krankenkassen nicht (mehr) verwendet.

Gleichwohl ist festzuhalten, daß das Gesetz mit der Einführung einer Vielzahl neuer Datensammlungen und -ströme unübersehbare Risiken schafft, zumal der genaue Umfang der Datenverarbeitung unklar bleibt. Die Ermächtigung an die Vertragspartner, diesen Umfang weitgehend zu bestimmen, ist kein geeignetes Mittel, die gebotene Normenklarheit herzustellen.

2.2 Das genetische Personenkennzeichen

In einem Ermittlungsverfahren wegen Mordes und Vergewaltigung sollten anhand einer Blutprobe des Beschuldigten Genstrukturen ermittelt und mit am Tatort gesicherten Spuren verglichen werden. Auf Antrag der Staatsanwaltschaft beschloß das Amtsgericht Tiergarten, dem Beschuldigten eine Blutprobe entnehmen zu lassen. Gegenwärtig ist die Durchführung einer solchen Genomanalyse zur Erstellung eines *„Genetischen Fingerabdrucks"* nur in Großbritannien möglich. Nach der Untersuchung hält die Staatsanwaltschaft den Beschuldigten für überführt. Wie das Gericht in der Hauptverhandlung entscheiden wird, bleibt abzuwarten.

In diesem Zusammenhang ist zu fragen, unter welchen Voraussetzungen ein solcher Eingriff vom geltenden Recht gedeckt ist oder ob nicht in jedem Fall der Gesetzgeber die Anwendung der neuen Methode durch normenklare Regelungen begrenzen muß.

Bei der Erstellung eines „Genetischen Fingerabdrucks" wird das genetische Material auf bestimmte Strukturelemente hin untersucht, die die Identität des Trägers dieser Erbinformation mit sehr hoher Wahrscheinlichkeit feststellbar machen. Wenn die Analyse des am Tatort gefundenen und vom Täter stammenden Zellmaterials (z. B. Haare, Blut oder Sperma) ergibt, daß dieses die gleiche genetische Struktur aufweist wie die dem Beschuldigten entnommene Blutprobe, so ist die Wahrscheinlichkeit, daß er nicht mit dem Täter identisch ist, nach heutigen Erkenntnissen zu vernachlässigen. Praktisch bedeutet dies, daß nur bei eineiigen Zwillingen der Identitätsnachweis nicht geführt werden kann.

[1] Urteil vom 7. 10. 87 (5 AZR 116/86)
[2] Urteil vom 15. 2. 88 (9 Sa 114/87)
[3] Bundestag Drs. 11/930

[1] vgl. Anlage 2

Während herkömmliche Analysen nur an Zellen durchgeführt werden können, die nicht älter als ein halbes Jahr sind (Blutgruppenvergleich, individuelle Proteinmerkmale), kann das genetische Material auch aus bis zu zwei Jahre alten Blut- oder Spermaresten oder aus Haarwurzeln gewonnen werden.

Es liegt auf der Hand, daß diese neue Methode für die Verbrechensbekämpfung große Bedeutung bekommen kann, wenn sie auch von deutschen Gerichten als Beweismittel anerkannt wird. Nach § 81 a StPO dürfen dem Beschuldigten auch gegen seinen Willen auf richterliche Anordnung Blutproben entnommen werden, wenn kein Nachteil für seine Gesundheit zu befürchten ist. Ob eine Genomanalyse auf diese Vorschrift gestützt werden kann, ist noch ungeklärt. Das Gesetz enthält keinerlei Regelung über die Art der Untersuchungen, die an den entnommenen Blutproben durchgeführt werden dürfen. Sofern es sich um die Aufklärung von verfahrenserheblichen Tatsachen handelt, ist jede technisch mögliche Untersuchung gedeckt. Die Enquete-Kommission des Deutschen Bundestages „Chancen und Risiken der Gentechnologie" hat jedoch darauf hingewiesen, daß diese Rechtslage nur für die bisher üblichen Untersuchungstechniken hinzunehmen ist[1].

Der Ausdruck „Genetischer Fingerabdruck" ist insofern irreführend, als seine Erstellung im Gegensatz zum eigentlichen Fingerabdruck einen körperlichen Eingriff voraussetzt. Die Genomanalyse kann auch nicht mit den bisherigen Methoden der Untersuchung von Blutproben und Tatspuren gleichgesetzt werden. Sie ermöglicht einen qualitativ neuen, ungleich tieferen Eingriff in die Persönlichkeitsphäre des Betroffenen.

Die Erhebung und Nutzung genetischer Daten im Strafverfahren muß daher auf die Führung des Identitätsnachweises mit Hilfe der nicht codierenden Teile des Genoms beschränkt werden. Diese enthalten nach heutigen Erkenntnissen keine weiteren Informationen über bestimmte Erbanlagen. Nur unter dieser Voraussetzung könnte der Einsatz genomanalytischer Methoden im Strafprozeß vom geltenden Recht gedeckt sein.

Es muß sichergestellt werden, daß darüber hinausgehende genetische Informationen in Strafverfahren nicht genutzt werden. Allerdings wächst mit der fortschreitenden Entwicklung und der zunehmenden Erhebung genetischer Daten auch im Bereich der pränatalen Diagnostik oder des Neugeborenen-Screening das Interesse der Strafverfolgungsbehörden, auf solche Datensammlungen zuzugreifen. Auch könnten genetische Daten, die zu Zwecken der Strafverfolgung in einem bestimmten Verfahren erhoben worden sind, nach Abschluß dieses Verfahrens von der Polizei weiter gespeichert und für präventive Zwecke genutzt werden. Damit würden Teile der Erbinformation zu einem unveränderlichen genetischen Personenkennzeichen, das für verschiedenste Zwecke verwendet werden könnte. Schon die Einführung eines herkömmlichen Personenkennzeichens ist vom Bundesverfassungsgericht und vom Deutschen Bundestag als verfassungswidriger Schritt zur totalen Erfassung aller Bürger bezeichnet worden. Umso gravierender wäre die Erhebung und Nutzung des Wissens um die genetische Konstitution vieler Personen für eine Vielzahl von Zwecken außerhalb eines konkreten Strafverfahrens.

Auch die genetische Analyse von *Tatspuren* führt zur Erhebung personenbezogener Daten, denn mit ihrer Hilfe kann ein genetisches Profil noch unbekannter, aber identifizierbarer Personen (Täter, Opfer oder sonstwie Beteiligte) erstellt werden. Die Herstellung eines Personenbezugs ist gerade das Ziel dieser Datenerhebung[2].

Bei diesen Analysen stellt sich ebenfalls die Frage, ob sie auf „persönlichkeitsneutrale" Abschnitte der Erbinformation beschränkt werden können. Mit der Enquete-Kommission bin ich der Auffassung, daß genetische Analysen, die gegen den Beschuldigten im Verfahren nicht angeordnet werden können (weil sie über die bloße Identitätsfeststellung hinausgehen), auch nicht an Tatspuren durchgeführt werden sollten.

Die Enquete-Kommission hat dem Deutschen Bundestag deshalb empfohlen, bei der anstehenden Novellierung des Strafverfahrensrechts und bei den Diskussionen über die Entwicklung und Vereinheitlichung des Polizeirechts des Bundes und der Länder die besondere Problematik der Erhebung, Verwertung und Speicherung genetischer Analysen bei der Strafverfolgung und der polizeilichen Prävention aufzugreifen und Regelungen zu entwickeln, die den vorgetragenen Bedenken Rechnung tragen. Sie hat ferner empfohlen, daß sich die Konferenz der Datenschutzbeauftragten des Bundes und der Länder dieser Problematik annimmt und zu ihr Stellung nimmt[1].

Der Polizeipräsident beabsichtigt, die Methode des „DNA-Profiling" (Genetischer Fingerabdruck) in seiner *Direktion Polizeitechnische Untersuchungen* anzuwenden. Nach Auskunft des Senators für Inneres[2] werden die nach allen Untersuchungsmethoden gewonnenen Ergebnisse lediglich in den Laborunterlagen und den Gutachten, die Bestandteil des Ermittlungsvorgangs sind, niedergelegt. Damit sei der Datenschutz „gegenwärtig wie künftig gewährleistet". Die Polizei sei in der Lage, die Untersuchungsmethoden zu nutzen, wenn die erforderlichen Umbauten in den Labors der Direktion Polizeitechnische Untersuchungen abgeschlossen werden. Als eine gerichtlich anerkannte Methode könne der Vergleich „Genetischer Fingerabdrücke" bisher mangels entsprechender Entscheidungen deutscher Gerichte nicht bezeichnet werden. Der Polizeipräsident plant, die Genomanalyse in konkreten strafrechtlichen Ermittlungsverfahren einzusetzen, um auf diese Weise Kosten für Analyseaufträge an externe Institute einzusparen. Sobald ihm diese Methode zur Verfügung steht, hätte der Polizeipräsident aber auch die Möglichkeit, sie für Zwecke der vorbeugenden Verbrechensbekämpfung zu nutzen.

Von der Nutzung der Genomanalyse im Strafverfahren ist die Anwendung dieser Methode für *präventiv-polizeiliche Zwecke* strikt zu unterscheiden. Die Enquete-Kommission des Deutschen Bundestages hat darauf hingewiesen, daß nach geltendem Recht genetische Analysen, die die Entnahme einer Blutprobe voraussetzen, außerhalb eines Strafverfahrens z.B. zur Feststellung der Identität einer bloß verdächtigen Person (§ 163 b Abs. 1 StPO) oder als Maßnahme des polizeilichen Erkennungsdienstes (§ 81 b StPO) oder der allgemeinen polizeilichen Prävention gegen den Willen der Betroffenen unzulässig sind[3]. Ich teile die Auffassung der Enquete-Kommission, daß diese Rechtslage bekräftigt werden sollte.

Die Schaffung und Nutzung genanalytischer Laborkapazitäten beim Polizeipräsidenten halte ich nur solange für hinnehmbar, wie die von der Polizei konkret angewandten Verfahren ausschließlich zur Führung des Indentitätsnachweises geeignet sind und auf der genetischen Ebene keinen persönlichkeitsrelevanten Informationsüberschuß erzeugen. Das in der Direktion Polizeitechnische Untersuchungen gegenwärtig erprobte Verfahren schließt nach dem derzeitigen Stand der wissenschaftlichen Erkenntnis das Anfallen persönlichkeitsrelevanter Überschußinformationen (z. B. Anlagen zu Erbkrankheiten) zuverlässig aus. Soweit die Polizei in zulässigem Umfang genetische Daten in einem konkreten Strafverfahren erhebt, darf sie diese Daten nach dessen Abschluß nicht für präventive Zwecke weiter speichern.

Sobald die ständige Weiterentwicklung der wissenschaftlichen Erkenntnismöglichkeiten in diesem Bereich eine andere Bewertung erfordert oder andere genanalytische Verfahren mit weitergehenden Aussagemöglichkeiten zur Strafverfolgung angewandt werden sollen, halte ich es für geboten, daß solche genetischen Analysen ausschließlich von unabhängigen gerichtsmedizinischen Instituten durchgeführt werden. Nur so kann die genaue Begrenzung dieser weitreichenden Analysemethoden auf die Identitätsfeststellung oder Entlastung bisher verdächtiger Personen kontrollierbar gemacht werden. Diese Institute hätten die Frage des Gerichts nach der Identität des sichergestellten Zellmaterials (Tatspuren und Blutprobe des Beschuldigten) mit „ja" oder „nein" zu beantworten, aber sie dürften keine zusätzlichen genetischen Informationen, die zwangsläufig miterhoben werden, dem Gericht übermitteln. Die Institute hätten das Zellmaterial nach Abschluß der Untersuchung zu vernichten, damit es nicht in unkontrollierbarer Weise für weitere Untersuchungen verwendet werden kann.

[1] Bundestag Drs. 10/6775, S. 176

[2] vgl. Ziffer 2.3

[1] A.a.O. S. 177

[2] Antwort auf die Kleine Anfrage Nr. 4805 in Mitteilungen des Präsidenten Nr. 281, Drs. 10/2370 v. 25. 7. 88

[3] A.a.O., S. 176 f.

2.3 Der Bürger im Objektiv der Videokamera

Derselbe Kriminalfall, der in Berlin erstmals zur Anwendung der Genomanalyse im Strafverfahren Anlaß gab, war auch aus anderem Grunde spektakulär: Auf die Spur des Verdächtigen kam die Polizei durch Hinweise aus der Bevölkerung, die nach der Veröffentlichung eines Fahndungsfotos eingingen. Das Fahndungsfoto war gefertigt worden, weil auf Grund bestimmter Anhaltspunkte davon ausgegangen werden konnte, daß der Täter die Euroscheckkarte des Opfers mißbräuchlich zum Geldabheben an Geldautomaten benutzt hatte. Dabei wurde der Verdächtige von einer Videokamera aufgenommen.

Die Veröffentlichung des *Fahndungsfotos* ist datenschutzrechtlich nicht zu beanstanden: Das Kunsturhebergesetz sieht ausdrücklich vor, daß für Zwecke der Rechtspflege und der öffentlichen Sicherheit von den Behörden Bildnisse ohne Einwilligung des Abgebildeten verbreitet werden dürfen.

Probleme des informationellen Selbstbestimmungsrechts wirft aber die Frage auf, unter welchen Voraussetzungen überhaupt *Videoaufnahmen* gefertigt werden können. Die Frage ist deswegen von großer Bedeutung, weil sowohl im öffentlichen als auch im privaten Bereich zunehmend mehr Kameras eingesetzt werden: Außer den hier in Frage stehenden Geldautomaten ist insbesondere die Verwendung von Kameras zur Überwachung des öffentlichen Verkehrs diskutiert worden. Die Betreiber versprechen sich durch den verbesserten Überblick einen Sicherheitsgewinn, und zwar sowohl durch die abschreckende Wirkung auf den potentiellen Täter, der eine schnelle Entdeckung fürchten muß, als auch zur Aufklärung bestimmter Ereignisse.

Den Datenschutzbeauftragten ist schon entgegengehalten worden, es handele sich hierbei nicht um Probleme des Datenschutzes. Dagegen ist einzuwenden, daß auch Bilder personenbezogene Daten („Angaben über persönliche oder sachliche Verhältnisse einer bestimmbaren Person": vgl. § 4 Abs. 1 BlnDSG) darstellen, selbst wenn der Name der abgebildeten Person nicht allgemein bekannt ist. Da Videoaufnahmen der vorliegenden Art (im Gegensatz etwa zu Kameras, die den Verkehr an Straßenkreuzungen überwachen) dazu dienen, bestimmte Personen ausfindig zu machen, ist die Aufnahme gerade auf den Personenbezug hin orientiert. Hinzu kommt, daß in jedem Fall das Recht am eigenen Bild als besondere Ausprägung des informationellen Selbstbestimmungsrechts betroffen ist.

Es sind verschiedene *Formen des Einsatzes von Videokameras* möglich, die jeweils eine verschiedene Bewertung erfordern:

- Die Videokamera wird lediglich zur Rationalisierung der Beobachtung eingesetzt und läuft durchgehend, wobei jedoch keine Bilder aufgezeichnet werden. Hier handelt es sich um einen Ersatz der persönlichen Anwesenheit von Aufsichtspersonen. Die Eingriffe sind - abgesehen von der räumlichen Distanz - nicht anders als bei der persönlichen Beobachtung zu bewerten.
- Es werden permanent Videoaufzeichnungen gefertigt, die im nachhinein betrachtet und ausgewertet werden können.
- Die Videokamera wird so gesteuert, daß sie nur bei bestimmten Anlässen, z. B. einer Abhebung von Geldautomaten oder auf Knopfdruck eines Mitarbeiters Einzelbilder fertigt.

In der Regel werden die aufgezeichneten Aufnahmen schon aus ökonomischen Gründen nur dann ausgewertet, wenn bestimmte Ereignisse überprüft werden müssen, insbesondere strafrechtliche Ermittlungsmaßnahmen erforderlich sind. Kommt es nicht zu derartigen Ereignissen, werden die Aufnahmen nach bestimmten, in der Regel sehr kurzen Fristen gelöscht bzw. überspielt.

Weder im öffentlichen noch im privaten Bereich existieren klare Regelungen. Ich gehe von folgender *Bewertung* aus:

Sofern die Kamera nur zur - räumlich versetzten - Verbesserung der Beobachtung dient, ohne daß Aufzeichnungen hergestellt werden, halte ich die Nutzung im Rahmen der jeweiligen Aufgabenerfüllung oder - im privaten Bereich - der privatrechtlichen Rechtsbeziehung für zulässig. Auch für Behörden ergibt sich hieraus z. B., daß die Überwachung öffentlich zugänglicher Räume im Rahmen des Hausrechts zulässig ist. Zu beachten ist dabei natürlich, daß in bestimmten Fällen zusätzliche Erfordernisse an die Aufnahmen gestellt werden müssen. So sind bei der Überwachung von Bediensteten die Mitbestimmungsrechte des Personalrats zu beachten; die Auffassung des Bundesarbeitsgerichts wurde hier schon dargelegt[1]).

Eine neue Qualität erhält der Eingriff, wenn zu der kontinuierlichen Beobachtung die Aufzeichnung der Bilder hinzukommt. Hier ist zwischen öffentlicher und privater Nutzung zu unterscheiden:

Im öffentlichen Bereich - etwa beim Einsatz durch die Polizei zur Gefahrenabwehr oder Strafverfolgung - ist erneut auf die Erforderlichkeit einer spezialgesetzlichen Regelung zu verweisen.

Soweit zu anderen öffentlichen Aufgaben, etwa im Rahmen der Wahrnehmung von Ordnungsaufgaben, Kameras eingesetzt werden sollen, gilt Entsprechendes. In der Übergangszeit muß eine strenge Abwägung zwischen den verfolgten Zwecken und der Schwere des Eingriffs vorgenommen werden, die in der Regel zur Unzulässigkeit der Speicherung von Videoaufnahmen führt.

Auch im privatrechtlichen Bereich ist der Eingriff in die Persönlichkeitsrechte der betroffenen Personen nach dem Grundsatz der Verhältnismäßigkeit abzuwägen gegenüber dem Interesse der Stelle, die Videokameras einsetzt, um bestimmte Abläufe oder kriminelle Taten im konkreten Einzelfall aufklären zu können.

Dabei ist zu berücksichtigen, daß die Videokameraüberwachung auch zu Gunsten der Kunden und Gäste wirken kann: So hat eine Bank die Pflicht, die Vermögensverhältnisse solcher Kunden, denen die Scheckkarte abhanden gekommen ist oder gestohlen wurde, zu schützen.

Allerdings hat auch hier die Einwilligung der Betroffenen Vorrang: Gerade wenn man das Recht am eigenen Bild als entscheidendes Kriterium betrachtet und - was im Hinblick auf das informationelle Selbstbestimmungsrecht geboten ist - auch die Speicherung von Bildern in den Schutzbereich einbezieht, ist zumindest die Aufklärung der Betroffenen unerläßlich. Dies könnte durch entsprechende - nicht nur kleingedruckte - Hinweise in Hausordnungen oder Geschäftsbedingungen geschehen, die an den geeigneten Stellen den Betroffenen zur Kenntnis gebracht werden.

2.4 Volkszählung: Zu viel Zwang - zu wenig Freiwilligkeit

Mit der Schließung der bezirklichen Volkszählungsämter im Mai 1988 und der Beendigung der Annahme der Erhebungsbogen durch das Statistische Landesamt im September 1988 ging der für den Bürger sichtbare Teil der Volkszählung zu Ende. Mit der schrittweisen maschinellen Einlesung und Aufbereitung der Erhebungsmerkmale hatte zuvor bereits eine neue, für den Schutz der Daten des Bürgers besonders kritische Phase begonnen.

Folgende datenschutzrechtliche Mängel haben sich ergeben:

Erhebung

Zahlreiche Bürger wurden noch während der Erhebungsphase erinnert, gemahnt oder es wurde sogar ein Bußgeldverfahren gegen sie eingeleitet, obwohl sie die Volkszählungsbogen ausgefüllt hatten.

Zur Einleitung ungerechtfertigter Bußgeldverfahren trug das Verfahren der *Datenübermittlung* zwischen den Ämtern für Volkszählung und dem Statistischen Landesamt bei. Zwar wurden in allen Ämtern für Volkszählung zum 31. Dezember 1987 die für die Rücklaufkontrolle gespeicherten Daten gelöscht und nur noch Restlisten ausgedruckt, die die Namen der Auskunftspflichtigen enthielten, die bisher nicht geantwortet hatten. Gleichzeitig leiteten die Bezirke Zwangsgeldverfahren ein, für die PC-gestützt Zwangsgelddateien eingerichtet wurden. Erst im März 1988 entschied der Senator für Inneres, daß parallel zu den Zwangsgeldverfahren auch Bußgeldverfahren durchgeführt werden sollten, die das Statistische Landesamt aufgrund der Restlisten einleitete. Trotz telefonischer Rückfragen bei den Ämtern für Volkszählung erhielten so mehrfach Auskunftspflichtige, die bereits geantwortet hatten, einen Anhörungsbogen oder einen Bußgeldbescheid.

[1]) vgl. Ziff. 1.2

Dies hätte vermieden werden können, wenn rechtzeitig vor dem Ausdruck der Restlisten eine Entscheidung darüber gefallen wäre, ob das Statistische Landesamt Bußgeldverfahren durchführen sollte oder nicht. Nur dann wäre die Übermittlung der vollständigen Restlisten mit Stand vom 31. Dezember 1987 an das Statistische Landesamt auch erforderlich gewesen.

Bürger, die angaben, ihre *Erhebungsunterlagen* bereits ausgefüllt zurückgesandt zu haben, deren Unterlagen aber nicht auffindbar waren, wurden von den Ämtern für Volkszählung in der Regel nur darauf hingewiesen, daß der Auskunftspflichtige bei der Rücksendung der Unterlagen auf dem Postweg die Gefahr des Verlustes so lange trägt, bis die Erhebungsunterlagen im Amt für Volkszählung eintreffen. Zahlreiche Eingaben verdeutlichten mir, wie schwer den Auskunftspflichtigen der Sinn dieser von mir bereits im letzten Jahr kritisierten Regelung zu vermitteln war. Den Bürgern wurde dagegen nicht erläutert, daß die Volkszählungsbriefe versehentlich ungeöffnet vernichtet worden sein könnten. In diesem Fall wäre zumindest die Offenbarung von Erhebungsmerkmalen gegenüber Dritten ausgeschlossen gewesen: Das Hauptanliegen der betroffenen Bürger war es gerade sicherzustellen, daß ihre ausgefüllten Erhebungsunterlagen nicht versehentlich einem Dritten zugestellt wurden.

Derartige Fälle kamen wiederholt vor: Obwohl in einem dieser Fälle Mitarbeiter ausdrücklich angewiesen waren, nur noch druckfrische Erhebungsunterlagen bei Mahnungen und Heranziehungsbescheiden zu versenden, wurden drei Monate später im selben Volkszählungsamt fünf aneinanderhängende ausgefüllte Personenbogen aus einem Krankenheim an andere Auskunftspflichtige versandt. Zudem waren in diesem Fall die Erhebungsunterlagen aus dem Krankenheim entgegen der Arbeitsanweisung des Statistischen Landesamtes für die sensiblen Sonderzählbezirke nicht getrennt von den normalen Zählbezirken aufbewahrt worden. In anderen Fällen ließ sich nicht aufklären, wie es zum Versand ausgefüllter Erhebungsunterlagen an andere Auskunftspflichtige kommen konnte.

Arbeitsstättenzählung

Die Erhebungsstellen versandten nach dem Rücklauf der Personenbogen in zahlreichen Fällen Arbeitsstättenbogen an Personen, die auf ihren Personenbogen angegeben hatten, daß sie selbständig und/oder unter ihrer Wohnadresse berufstätig seien. Diese Nutzung von Erhebungsmerkmalen ist vom Volkszählungsgesetz gedeckt. Eine Reihe betroffener Bürger wandte sich jedoch an mich, weil sie ein irreführendes formularmäßiges Anschreiben erhalten hatten: Darin hieß es, man habe anhand allgemein zugänglicher Quellen wie z. B. Adreßbüchern festgestellt, daß der betroffene Bürger eine Arbeitsstätte unterhalte. Die Nutzung der Personenbogen wurde nicht erläutert. Dadurch wurde der - unbegründete - Verdacht einer Datenerhebung auf verbotenen Wegen ausgelöst.

Ein Amt für Volkszählung hatte das Wirtschaftsamt zur Mitteilung der Namen von Gesellschaften oder der Inhaber von Firmen aufgefordert, die noch keinen Arbeitsstättenbogen ausgefüllt hatten. Dabei nannte die Erhebungsstelle auch Arbeitsstätten wie z. B. Kindertagesstätten, die mangels Gewerbeeigenschaft dem Wirtschaftsamt gegenüber nicht anzeigepflichtig sind. Mit der Übermittlung dieser Daten wurden statistische Einzelangaben der Vollzugsverwaltung mitgeteilt. Gleichzeitig wurde offenbart, daß die Unternehmen ihrer Auskunftspflicht bisher nicht nachgekommen waren. Das Ersuchen ermöglichte dem Wirtschaftsamt einen Datenabgleich, ob die Unternehmen einen Verstoß gegen die gewerberechtliche Anzeigepflicht begangen hatten. Die Datenübermittlung habe ich daher beanstandet.

Durchsetzung der Auskunftspflicht

Zunächst war die Zahl der Personen, die auch nach Erlaß der förmlichen Heranziehungsbescheide ihre Erhebungsunterlagen nicht sofort ausfüllten, erheblich höher, als die amtliche Statistik dies erwartet hatte. Daher wurden in großem Umfang Zwangsgeldverfahren und - ab Ostern 1988 - auch Bußgeldverfahren gegen diese Personen eingeleitet.

Bereits Ende 1987 erhielt ich einen Hinweis, wonach die Oberfinanzdirektion plane, Zwangsgelder gegen Auskunftsverweigerer in erster Linie durch *Konten- oder Gehaltspfändung* zu vollstrecken. Danach sollten die Vollstreckungsstellen der Finanzämter, die auf Ersuchen der Ämter für Volkszählung die Vollstrekkung zu betreiben haben, aus den Steuerakten die Bankverbindung und den Arbeitgeber der Betroffenen entnehmen. Auf Rückfrage wurde mir erklärt, daß die Vollstreckungsstellen zwar alle rechtlich zulässigen Möglichkeiten ausschöpfen würden, um die zu erwartende hohe Zahl von Vollstreckungsersuchen zügig erledigen zu können, daß aber ein Rückgriff auf Steuerakten als Bruch des Steuergeheimnisses angesehen werde und damit ausscheide.

Das Statistische Landesamt und der Senator für Inneres hatten ohnehin - zumindest bei der Planung des Vollstreckungsverfahrens betont, daß sie wenig Interesse an Konten- oder Gehaltspfändungen hätten, weil ihnen daran liege, möglichst viele ausgefüllte Erhebungsbogen zu erhalten. Dieses Ziel hielten sie für leichter erreichbar durch einen direkten Kontakt zwischen Vollstreckungsbeamten und Auskunftspflichtigen. Die beteiligten Stellen vereinbarten deshalb ein Verfahren, wonach die Finanzämter zunächst nochmals den Auskunftspflichtigen die Vollstreckung ankündigten. Diese Mahnschreiben führten in zahlreichen Fällen dazu, daß die Erhebungsunterlagen ausgefüllt wurden. In den übrigen Fällen sollten kurzfristig Konten- und Gehaltspfändungen vorgenommen werden. Entgegen der vorherigen Auskunft vertrat nun der Senator für Finanzen in einem Erlaß vom 1. Juni 1988 die Auffassung, hierzu könne erforderlichenfalls auch in Steuerakten Einsicht genommen werden. Das Steuergeheimnis stehe dem nicht entgegen, weil insoweit ein zwingendes öffentliches Interesse gem. § 30 Abs. 4 Nr. 5 Abgabenordnung (AO) gegeben sei.

Ich habe den Senator für Finanzen sofort nach Bekanntwerden des Erlasses dringend gebeten, den Erlaß zurückzuziehen, da er nicht mit dem Steuergeheimnis (§ 30 AO) vereinbar ist: Das Steuergeheimnis gilt auch zwischen den einzelnen, mit verschiedenen Zuständigkeiten versehenen Stellen eines Finanzamtes (z. B. Steuererhebungsstelle einerseits, Vollstreckungsstelle andererseits). Zwar ist eine Datenweitergabe im zwingenden öffentlichen Interesse zulässig (§ 30 Abs. 4 Nr. 5 AO). Dieser unbestimmte Rechtsbegriff wird aber durch drei Beispielsfälle konkretisiert. Die Nichtabgabe oder verspätete Abgabe von Volkszählungsunterlagen ist mit keinem dieser gesetzlichen Beispiele gleichzusetzen. Das vom Finanzsenator angenommene zwingende öffentliche Interesse setzt die Gefahr voraus, daß schwere Nachteile für das allgemeine Wohl eintreten. Diese Gefahr lag jedoch nicht vor. Das Statistische Landesamt ging selbst davon aus, daß mit der Zusammenführung von Erhebungsmerkmalen und Regionallisten eine Einarbeitung von dann noch eingehenden Erhebungsbogen technisch nicht mehr möglich ist oder die weitere Aufarbeitung unangemessen verzögern würde. Mit diesem Zeitpunkt, der bezirksweise festgelegt wurde, ist die Vollstreckung aller Zwangsgelder eingestellt worden. Schon an diesem Verfahrensablauf ist erkennbar, daß auch dann, wenn nicht sämtliche Erhebungsbogen in das Volkszählungsergebnis eingehen, keine Gefahr schwerer Nachteile für das allgemeine Wohl besteht.

Die Rechtsprechung hat die Offenbarung von Steuerdaten auf der Grundlage des § 30 Abs. 4 Nr. 5 AO auch dann für zulässig erklärt, wenn anderenfalls die Gefahr einer erheblichen Störung der wirtschaftlichen Ordnung bestanden hätte. Der Senator für Finanzen vertrat die Auffassung, daß die durch eine „breit organisierte Nichtabgabe der Volkszählungsbögen bewirkte Gefährdung der vollständigen Erhebung dieser aktuellen Planungsdaten für das öffentliche Wohl nicht minder schwere Nachteile bringt als dies durch Handlungen bewirkt wird, die die Gefahr einer erheblichen Störung der wirtschaftlichen Ordnung zur Folge haben." Diese Auffassung teile ich nicht. Die Erfahrungen während der Vollstreckung von Zwangsgeldern haben gezeigt, daß keineswegs alle Personen, die ihren Volkszählungsbogen bisher nicht ausgefüllt hatten, sich an einer „breit organisierten Nichtabgabe" beteiligt haben. So brachen Vollstreckungsbeamte eines Finanzamtes die Wohnungstür einer 88jährigen Rentnerin in einem Altenheim auf, die alle Schreiben der Erhebungsstelle unbeachtet gelassen hatte. Auch der Direktor des Statistischen Landesamtes hat gegenüber der Presse die Auffassung vertreten, daß die meisten Auskunftspflichtigen, die bis Mitte 1988 ihre Erhebungsunterlagen nicht ausgefüllt hatten, zu einem Personenkreis zählen, der generell nicht auf Behördenschreiben reagiert.

Ich habe zwar Verständnis für das Bemühen, eine Konfrontation zwischen Vollstreckungsbeamten und Volkszählungsboykotteuren bei Hausdurchsuchungen zu vermeiden. Aber auch dies begründet kein zwingendes öffentliches Interesse an der Offenbarung von Steuerdaten. Wenn der Gesetzgeber die - im Vorfeld von mir stets kritisierte - Entscheidung getroffen hat, die Volkszählung 1987 mit einer zwangsweise durchsetzbaren und mit Bußgeld bewehrten Auskunftspflicht durchzuführen, dann muß sich die Exekutive bei der Vollstreckung in besonderem Maße an die gesetzlichen Vorschriften halten. Schließlich war die Durchbrechung des Steuergeheimnisses besonders zu einem Zeitpunkt unverhältnismäßig, als nur noch 0,3 % der Erhebungsunterlagen im Land Berlin ausstanden.

Dennoch sind in 42 Fällen die Steuerakten zum Zweck der Vollstreckung von Zwangsgeldern bei der Volkszählung herangezogen worden. Ich habe diese Fälle beanstandet. Der Senator für Finanzen hat seinen Erlaß daraufhin zurückgenommen.

In einem weiteren Fall hatte der Vollstreckungsbeamte eines Finanzamtes beobachtet, wie ein Auskunftspflichtiger, gegen den im Auftrag eines Amtes für Volkszählung ein Zwangsgeld vollstreckt werden sollte, aus einem Pkw ausstieg. Der Vollstreckungsbeamte notierte sich das Kennzeichen und ermittelte durch eine Halterabfrage bei dem für die Kraftfahrzeugsteuer zuständigen Finanzamt, daß der Auskunftspflichtige Halter dieses Fahrzeugs war. Dabei wurde auch seine Bankverbindung mit ausgedruckt. Die Vollstreckungsstelle nutzte diese Information, um das Bankkonto des Auskunftspflichtigen zu pfänden. Nachdem der Senator für Finanzen seinen Erlaß zurückgenommen hatte, wurde auch diese Pfändung aufgehoben.

Der Senator für Inneres hatte zur strikten Gewährleistung der Trennung zwischen Statistik und Verwaltungsvollzug zugesichert, daß das Statistische Landesamt bei der Einleitung von Bußgeldverfahren gegen Auskunftspflichtige, die nach dem Stichtag umgezogen sind, von *Melderegisteranfragen* absehen wird. Entsprechend meinen Empfehlungen haben die bezirklichen Ämtern für Volkszählung bei der Durchführung der Zwangsgeldverfahren von derartigen Anfragen abgesehen.

Gleichwohl hat das Statistische Landesamt in Bußgeldverfahren Anfragen an das Landeseinwohneramt gerichtet. Bis zu diesem Zeitpunkt waren rund 1 500 Briefe mit Anhörungsbogen zum Vorwurf einer Ordnungswidrigkeit im Zusammenhang mit der Volkszählung 1987 von der Post als unzustellbar an das Statistische Landesamt zurückgegeben worden. Daraufhin begaben sich drei Mitarbeiter dieses Amtes mit diesen Briefen zum Landeseinwohneramt und nannten den dort tätigen Mitarbeitern den Namen des Auskunftspflichtigen und dessen alte Adresse. Sie erhielten daraufhin die neue Anschrift und notierten sie auf dem Umschlag. Die neuen Anschriften wurden sofort in die Bußgelddatei übernommen und es wurden neue Anhörungsbogen ausgedruckt. Die alten Briefe wurden vernichtet. Beim Landeseinwohneramt wurden die Auskünfte nicht protokolliert. Auf diese Weise sollte das Risiko eines Melderegisterabgleichs ausgeschlossen werden[1].

Die mir von der zuständigen Senatsverwaltung gegebene Zusage, die ich zudem veröffentlicht hatte, ist nicht eingehalten worden.

Zwar ist das Vorgehen des Statistischen Landesamtes - im Gegensatz zu dem des Senators für Finanzen bei der Einsichtnahme in Steuerakten - rechtlich nicht zu beanstanden. Die Übermittlung neuer oder ergänzter Anschriften von Auskunftspflichtigen durch die Meldebehörde an die Erhebungsstelle ist kein verfassungswidriger Melderegisterabgleich[2].

Ich hätte es allerdings begrüßt, wenn stattdessen ein Verfahren gewählt worden wäre, bei dem die Meldebehörde nach dem Stichtag dem Statistischen Landesamt in bestimmten Zeitabständen Namen und Anschriften derjenigen Einwohner übermittelt hätte, die umgezogen sind. Anhand dieses Datenbestandes hätte das Statistische Landesamt die Adressen in seiner Bußgelddatei aktualisieren können. Bei diesem Verfahren wären zwar insoweit mehr Daten übermittelt worden, als für den Zweck der Erhebungsstelle erforderlich war, weil auch die Anschriften solcher umgezogener Bürger gemeldet worden wären, die bereits ihrer Auskunftspflicht genügt hatten. Gleichwohl erscheint dieses Verfahren datenschutzgerechter als eine Mitteilung von Namen und Anschriften solcher Personen, die bisher ihre Auskunftspflicht nicht erfüllt haben, an die Meldebehörde.

Das Rechtsamt eines Bezirks hatte gegenüber dem Verwaltungsgericht nach der Beendigung der Zwangsgeldvollstreckung die Erledigung aller noch anhängigen Rechtsstreitigkeiten in einem *Sammelschriftsatz* erklärt, der die Namen aller in diesem Bezirk wohnenden Personen enthielt, gegen die Zwangsgelder im Zusammenhang mit der Volkszählung festgesetzt worden waren und die diese Festsetzungen angefochten hatten. Das Verwaltungsgericht stellte sämtlichen Verfahrensbeteiligten Kopien dieses Sammelschriftsatzes zu, so daß jeder eine vollständige Liste aller hartnäckigen Volkszählungsgegner dieses Bezirks erhielt.

Ich habe dieses Vorgehen des Bezirksamts beanstandet. Jede öffentliche Stelle darf auch als Prozeßbeteiligte personenbezogene Daten nur in dem für das jeweilige Verwaltungsstreitverfahren erforderlichen Umfang einem Gericht übermitteln. Sammelschriftsätze und Sammelverfügungen beeinträchtigen regelmäßig das informationelle Selbstbestimmungsrecht der Betroffenen und sind zudem im Zeitalter der modernen Textverarbeitung kein taugliches Mittel der Verwaltungsvereinfachung.

Aufbereitung

Das Volkszählungsgesetz verpflichtet die amtliche Statistik, die bei der Volkszählung erhobenen Daten zum frühestmöglichen Zeitpunkt zu anonymisieren und die Erhebungs- und Organisationsunterlagen ebenfalls zum frühestmöglichen Zeitpunkt zu vernichten. Dieses gesetzliche *Beschleunigungsgebot* hat das Bundesverfassungsgericht[1] dahingehend konkretisiert, daß die Feststellung der amtlichen Bevölkerungszahl des Landes nach dem eindeutigen Gesetzeswortlaut nicht den Regelzeitpunkt, sondern den spätesten Zeitpunkt der Löschung oder Vernichtung kennzeichne. Die Statistischen Landesämter seien gehalten, für jede der Erhebungsunterlagen den jeweils frühestmöglichen Zeitpunkt zu ermitteln und die Vernichtung oder Löschung zu diesem Zeitpunkt vorzunehmen. Entsprechendes gilt für die Anonymisierung der laufenden Nummern und Ordnungsnummern des jeweiligen Datensatzes. Das Bundesverfassungsgericht hat die grundrechtssichernde Funktion der Löschungs- und Vernichtungsregelungen betont und in diesem Zusammenhang ausgeführt, daß Art und Geschwindigkeit der Aufbereitung und ihre Organisation keine verbindlichen, etwa die Gerichte bindenden, tatsächlichen Vorgaben der Statistischen Landesämter bildeten, sondern sich ihrerseits am Gebot frühestmöglicher Löschung und Vernichtung zu orientieren hätten. Vermeidbare wesentliche Verzögerungen der Datenaufbereitung hätten dabei außer Betracht zu bleiben. Die Statistischen Landesämter seien gehalten, die Aufbereitungsorganisation und die personellen und sachlichen Mittel in den Grenzen des vom Bürger vernünftigerweise erwartbaren Aufwandes an einer zügigen Aufbereitung auszurichten.

Die Programme für die *maschinelle Aufbereitung* der Volkszählungsdaten und ihre gesetzlich vorgeschriebene Anonymisierung wurden von Statistischen Bundesamt im Verbund mit bestimmten Statistischen Landesämtern erstellt. Ich habe erhebliche Zweifel, ob dieses Verfahren der Programmerstellung dem Beschleunigungsgebot des Volkszählungsgesetzes entsprochen hat. Ein Rückstand der maschinellen Aufbereitung der Volkszählungsdaten - nach vorangegangenen Verzögerungen in der Erhebungsphase - von bis zu einem halben Jahr gegenüber den eigenen Planungen der amtlichen Statistik kann nicht vernachlässigt werden. Auch bei der Einführung des Plausibilitätsprogramms gab es wiederholt Verzögerungen und nachträgliche Änderungen selbst nach Abschluß der Testphase. Das Statistische Landesamt ist als speichernde Stelle zwar verpflichtet, seinerseits die Aufbereitungsorganisation in einer Weise zu gestalten, die dem Beschleunigungsgebot Rechnung trägt. Im System der Verbundprogrammierung müssen jedoch vermeidbare Verzögerungen in der Programmerstellung, die gleichzeitig

[1] Vgl. unten Ziff. 4.5

[2] Vgl. OVG Hamburg, Beschluß vom 30. Juni 1988 (OVG Gs IV 58/88)

[1] Beschluß v. 24. 9. 1987 (1 BvR 970/87)

die Anonymisierung und Löschung bzw. Vernichtung verzögern, in erster Linie dem federführenden Statistischen Bundesamt angelastet werden.

Ursprünglich plante die amtliche Statistik, am 25. November 1988, also eineinhalb Jahre nach dem Stichtag der Volkszählung am 25. Mai 1987, die amtlichen Bevölkerungszahlen bekanntzugeben. Obwohl ungewiß war, ob dieser Termin auch in Berlin würde eingehalten werden können, hat das Statistische Landesamt zwei Wochen vorher mit der vorgeschriebenen Verfremdung der laufenden Nummern und Ordnungsnummern in jedem Einzeldatensatz und mit der Vernichtung der Erhebungsunterlagen begonnen. Wann die amtliche Bevölkerungszahl des Landes Berlin festgestellt wird, ist gegenwärtig noch offen. Spätestens innerhalb von zwei Wochen nach diesem Termin muß auch die Verfremdung der laufenden Nummern und Ordnungsnummern in jedem Einzeldatensatz abgeschlossen sein.

Gemeinsam mit dem Bundesbeauftragten für den Datenschutz und dem Hessischen Datenschutzbeauftragten habe ich das bundeseinheitliche Programm zur *Verfremdung* der laufenden Nummern und Ordnungsnummern überprüft, die den Zusammenhang jedes gespeicherten Datensatzes mit Haushalt, Wohnung und Gebäudebezeichnung festhalten. Es genügt den Anforderungen des Volkszählungsgesetzes, wenn bestimmte zusätzliche Maßnahmen zur Geheimhaltung des Verfremdungsverfahrens getroffen werden. Die praktische Umsetzung werde ich überprüfen. Eines ist jedoch schon jetzt hervorzuheben: Die Verfremdung der laufenden Nummern und Ordnungsnummern führt nicht zu einer vollständigen Anonymisierung der beim Bürger erhobenen Merkmale, sondern lediglich zu einer Verringerung des Risikos der Reidentifizierung. Das hat der Gesetzgeber ausdrücklich in Kauf genommen und deshalb eine vollständige Anonymisierung erst für den Fall vorgeschrieben, daß die Statistikämter Erhebungsmerkmale an Dritte weitergeben. Auch das Bundesverfassungsgericht hat wiederholt betont, daß die Einzelangaben selbst nach der Verfremdung der laufenden Nummern und Ordnungsnummern personenbezogen bleiben[1].

Aus Anlaß der Volkszählung habe ich das *Rechenzentrum* im Statistischen Landesamt überprüft, das ausschließlich für die technische Abwicklung der Volkszählung eingerichtet wurde. Im Vordergrund der Prüfung standen Sachverhaltsfeststellungen zur Zu- und Abgangskontrolle, Online-Verarbeitung, zum Freigabeverfahren und zur Anwendung von Datenschutz-Software.

Obwohl der Zutritt zum Rechenzentrum des Statistischen Landesamtes für die Volkszählung technisch durch ein leistungsfähiges Zugangskontrollsystem und durch Monitorüberwachung zufriedenstellend geregelt und überwachbar gemacht worden ist, waren hinsichtlich der organisatorischen Umsetzung Mängel festzustellen:

Schon unter den bestehenden räumlichen Verhältnissen ist die Anzahl der mit ständiger Zutrittsberechtigung mittels maschinenlesbarer Zugangskontrollkarte versehenen Personen zu hoch. So waren z. B. mehrere Sicherheitsbeauftragte mit solchen Ausweisen ausgestattet, obwohl sie nur gelegentlich Aufgaben im Sicherheitsbereich zu versehen hatten, die sie auch nach Eintragung in ein Besucherbuch unter Aufsicht des Rechenzentrumspersonals hätten erfüllen können.

Überdies entsprechen die baulichen Maßnahmen zur Funktionentrennung, damit zur Minimierung des zugangsberechtigten Personenkreises und Optimierung der Transparenz der Abläufe im Rechenzentrum, nicht den Anforderungen an ein sicheres Rechenzentrum. So sind die Arbeitsplätze der Anwendungs- und Systemprogrammierer im Sicherheitsbereich untergebracht, obwohl diese Aufgaben über Datenstationen außerhalb des Sicherheitsbereiches zu erfüllen wären, damit dort, wo Operator mit beweglichen Datenträgern umgehen bzw. über Operator-Konsolen in die Abläufe der Datenverarbeitung eingegriffen werden kann, keine zusätzlichen Risiken geschaffen werden. Spätestens, wenn nach Abschluß der Arbeiten für die Volkszählung das Rechenzentrum unbefristet für sensible Datenverarbeitungsaufgaben, wie sie die Verarbeitung statistischer Einzeldatensätze nun einmal darstellt, verwendet werden sollte, müßten bauliche Änderungen vorgenommen werden, die neben der heute bereits vorhandenen sicheren Abschottung nach außen auch die Datensicherheit nach innen gewährleisten können.

Bewertung

Die Beteiligungsquote bei der Volkszählung lag beim Abschluß der Annahme von Erhebungsbögen bei 99,8 % der gemeldeten Personen. Dies ist angesichts der zuvor gehegten Befürchtung, der Erfolg der Volkszählung sei wegen einer Verweigerungsquote bis in den zweistelligen Bereich gefährdet, ein sehr hoher Wert. Er konnte allerdings nur erreicht werden durch ein Ausschöpfen aller Zwangs- und Sanktionsmittel, die den Behörden zur Verfügung standen, und die sich in mehreren Wellen gegen jeden richteten, der gleich ob aus einer staatsfeindlichen Haltung, engagierter Skepsis oder schlichter Abwesenheit die geforderten Angaben nicht oder nicht vollständig gemacht hatte. Wegen der sicherlich in der Werteskala der staatlichen Ordnung nicht an erster Stelle rangierenden Statistik wurden dabei in über 60 000 Fällen Zwangsmaßnahmen ergriffen[1]: Eine in der Geschichte staatlicher Vollstreckung äußerst ungewöhnliche Größenordnung.

Ein Gewinn für die staatliche Ordnung wäre nur dann zu erwarten, wenn die amtliche Statistik aufgrund der jetzt gesammelten Erfahrungen ernsthaft über Alternativen zur Totalerhebung mit Auskunftspflicht nachdenken würde. Wenn die Bundesregierung in ihren drei Statistikberichten vom Februar 1988[2] beharrlich die Auffassung vertritt, soweit statistische Erhebungen gegenwärtig mit Auskunftspflicht durchgeführt würden, sei diese auch in Zukunft unverzichtbar, so ist sie schlecht beraten und verkennt die Aufforderung des Bundesverfassungsgerichts an den Gesetzgeber, die Diskussion im In- und Ausland über einen möglichen Verzicht auf Totalerhebungen und über Alternativen aufmerksam zu verfolgen und Konsequenzen zu ziehen, sobald sichere Ergebnisse dieser Diskussion vorliegen.

In ihrem Bericht über die Erfahrungen bei der Durchführung des Mikrozensusgesetzes hat die Bundesregierung ausführlich die ausländischen Erfahrungen dokumentiert[3]. Danach werden in 8 von 19 untersuchten europäischen und außereuropäischen Ländern Arbeitskräfte- und Mehrzweckstichproben *auf freiwilliger Basis* zum Teil mehrmals jährlich durchgeführt, wobei Antwortquoten zwischen 81 und 95 % erreicht wurden. Die Bundesregierung führt dies darauf zurück, daß die Befragten die Auskunftserteilung bei staatlichen Erhebungen in den in Betracht kommenden Ländern grundsätzlich als Bürgerpflicht ansehen[4]. Das Statistische Bundesamt ist der Auffassung, daß sich derartige Antwortquoten nach den Testerhebungen zum Mikrozensus und den Erfahrungen mit Befragungen in der empirischen Sozialforschung in der Bundesrepublik nicht erzielen lassen. Ich halte dies nicht für überzeugend, zumal eine vollständige Auswertung der Testerhebungen zum Mikrozensus noch gar nicht stattgefunden hat. Offenbar ist es der amtlichen Statistik in so unterschiedlichen Staaten wie Luxemburg oder den Vereinigten Staaten bisher besser gelungen als in der Bundesrepublik, den Bürgern die Bedeutung der Teilnahme an derartigen Erhebungen argumentativ zu verdeutlichen.

Ein weiterer Schritt auf dem Weg zu einem Volkszählungs-Ersatz, der den Erfordernissen der amtlichen Statistik genügt, könnte auch die Entwicklung eines Verfahrens sein, in dem personenbezogene Daten in Dateien des *Verwaltungsvollzugs* anonymisiert und reidentifikationssicher für statistische Zwecke ausgewertet werden.

Weder war die Volkszählung - wie von manchen ihrer Gegner behauptet - ein Schritt in den totalen Überwachungsstaat, noch haben die Gegner der Volkszählung den Rechtsstaat gefährdet, wie es zur Rechtfertigung mancher überzogener Reaktion der Be-

[1] vgl. Beschluß v. 24. 2. 1988 (1 BvR 151/88)

[1] Insgesamt wurden zur Durchsetzung der Auskunftspflicht bis zum 21. 9. 1988 62 999 Zwangsgeldfestsetzungsbescheide erlassen und 34 841 Vollstreckungsersuchen an die Finanzämter gerichtet; bis zum 24. 10. 1988 wurden daneben 7 881 Bußgeldbescheide erlassen, gegen die in 3 552 Fällen Einspruch erhoben wurde.

[2] Bundestag Drs. 11/1755, 1756, 1762 v. 3. 2. 88

[3] Bundestag Drs. 11/1756, Anhang III.2

[4] ebd., S. 5

hörden behauptet wurde. Die Auseinandersetzung um die Volkszählung 1987 hatte für beide Seiten vorwiegend symbolischen Charakter.

Will die amtliche Statistik weiterhin verläßliche und aussagekräftige Ergebnisse liefern, so muß sie sich vom staatlichen Zwang unabhängig machen und auf die Kooperationsbereitschaft des Bürgers setzen.

Insgesamt begrüße ich die lebhafte Diskussion und die zahlreichen Eingaben, die mich aus Anlaß der Volkszählung 1987 erreichten. Das Datenschutzbewußtsein in großen Teilen der Bevölkerung ist erheblich geschärft worden. Ich würde mir wünschen, daß sich dies zunehmend auch in anderen Bereichen des Umgangs mit personenbezogenen Daten niederschlägt.

3. Neue Medien

3.1 Telekommunikation

Die eingangs beschriebenen neuen Entwicklungen der Datenverarbeitung setzen voraus, daß die verschiedenen Geräte mit Leitungen untereinander verbunden sind, über die die Informationen ausgetauscht werden können. Damit kommt der Ausgestaltung der Telekommunikationsmöglichkeiten für die Entwicklung der Datenverarbeitung eine erhebliche Bedeutung zu. Eine besondere Rolle spielen dabei öffentliche Telekommunikationsnetze, die von der Deutschen Bundespost bereitgestellt werden und benutzt werden müssen, wenn die Telekommunikation über die Grenzen eines Grundstücks hinaus durchgeführt werden soll.

Der Ordnungsrahmen, in den die öffentliche Telekommunikation in der Bundesrepublik eingebettet ist, befindet sich derzeit im Umbruch:

- Das neue *Poststrukturgesetz* sieht die Liberalisierung und teilweise Privatisierung des Fernmeldewesens vor; dabei entstehen Bereiche (z. B. bei den Endgeräten), in denen die bestehenden Datenschutzregelungen nicht oder nur unzureichend gelten.
- Mit Inkrafttreten der *Telekommunikationsordnung* (TKO) am 1. Januar 1988 hat die Deutsche Bundespost den Übergang von bisher getrennten Fernmeldenetzen zu einem einzigen diensteintegrierten, digitalen Telekommunikationsnetz für die Übermittlung aller Nachrichtenarten eingeleitet; künftig fallen an zentralen Stellen erheblich mehr und leichter auswertbare personenbezogene Daten an als bisher, die je nach Dienstart mehr oder weniger präzise Rückschlüsse auf das Verhalten der Teilnehmer erlauben. Zur Gewährleistung des Datenschutzes reichen die bisherigen Regelungen der TKO nicht aus.
- Die Vorlage des *Grünbuchs der Europäischen Gemeinschaften* über die Entwicklung des gemeinsamen Marktes für Telekommunikationsdienstleistungen und Telekommunikationsgeräte zeigt, daß der Datenschutz bei der geplanten Liberalisierung des Angebots von Dienstleistungen und Geräten im wesentlichen als Hemmnis für die Entwicklung optimaler Bedingungen der Telekommunikation betrachtet wird. Es besteht die Gefahr, daß das nationale Datenschutzrecht durch ein Gemeinschaftsrecht überlagert wird und die Anforderungen nationaler Rechtsordnungen an den Datenschutz als wettbewerbswidrig angesehen werden.
- Der vom Bundesinnenminister vorgelegte Entwurf für die Neufassung des *Bundesdatenschutzgesetzes* berücksichtigt die neuen Entwicklungen der Telekommunikation nicht.
- Eine *Regelung der Nutzung* der Telekommunikationsdienste durch die Länder steht aus; somit ist der Datenschutz im Nutzungsbereich nicht gewährleistet.

An das *Poststrukturgesetz* war die Forderung zu richten, daß auch in den Bereichen, in denen Endeinrichtungen durch Private betrieben oder sonstige Netzfunktionen durch Private wahrgenommen werden, ebenso strenge Datenschutzregelungen gelten wie sie im Bereich der Bundespost notwendig sind. Hierzu reicht die Verordnungsermächtigung in § 26 Poststrukturgesetz, die die Bundesregierung nur beim Telefondienst zum Tätigwerden verpflichtet, nicht aus. Darüber hinaus könnte der Datenschutz durch private Geschäftsbedingungen unterlaufen werden. Ich halte vielmehr eine abschließende gesetzliche Regelung für notwendig, die den Umfang der Daten auf das unerläßliche Ausmaß beschränkt, eine strenge Zweckbindung vorsieht und für den Bürger die Datenflüsse offenlegt.

Dies gilt auch für personenbezogene Daten, die beim Betrieb privater Telekommunikationsdienstleistungen (§ 1 Abs. 4 Fernmeldeanlagengesetz n. F.) anfallen. Solche Dienstleistungen dürfen nur zugelassen werden, wenn sie den gesetzlichen Anforderungen entsprechen.

Die wachsende Menge personenbezogener Daten, die durch die *Digitalisierung* und die *Diensteintegration* entsteht, und deren leichtere Auswertbarkeit machen strengere Regelungen des Umgangs mit Verbindungs-, Gebühren- und Inhaltsdaten erforderlich. Die beim Einsatz der programmgesteuerten Vermittlungstechnik automatisch und permanent beim Aufbau und zur Aufrechterhaltung von Verbindungen anfallenden personenbezogenen Daten müssen unmittelbar nach Beendigung der Verbindung gelöscht werden, um der Gefahr der Bildung eines Persönlichkeitsprofils zu begegnen. Daneben fallen umfangreiche Sammlungen von Gebührendaten für die Benutzung des Telekommunikationsnetzes an (z. B. Telefongebühren), die teilweise präzise Rückschlüsse auf das Verhalten der Teilnehmer zulassen. Diese Daten dürfen nicht an fremde Privatpersonen oder Interessengruppen gelangen; hier sind ein Übermittlungsverbot und eine strenge Zweckbindung zu schaffen. Mit automatischer Spracherkennung könnten aus der Masse der Kommunikationsvorgänge (z. B. Telefongespräche) programmgesteuert einzelne Informationen (z. B. Gesprächsinhalte) herausgefiltert, gespeichert und übermittelt werden. Derartige Auswertungen sind öffentlichen und privaten Stellen ausdrücklich zu verbieten.

Die derzeitigen Regelungen der Telekommunikationsordnung zur Datensicherheit werden den speziellen Risiken der Telekommunikationsdienste nicht gerecht. Vielmehr müssen mehr als früher auch organisatorische und verfahrensrechtliche Vorkehrungen getroffen werden, die dem neuesten Stand von Wissenschaft und Technik der Datensicherung entsprechen (z. B. Verschlüsselungsverfahren, Codesicherheit, Schutz vor Fehleingaben). Das Fernmeldegeheimnis allein kann der Gefahr einer Verletzung des Persönlichkeitsrechts nicht entgegenwirken.

Wegen der durch das Grünbuch deutlich werdenden Gefahr der Aushöhlung nationaler Datenschutzvorschriften im Telekommunikationsbereich durch schwach ausgeprägte Datenschutzregelungen im *Gemeinschaftsrecht* ist die Bundesregierung aufzufordern, dafür Sorge zu tragen, daß die Liberalisierung des Telekommunikationsmarktes durch angemessene gemeinschaftsrechtliche Datenschutzregelungen begleitet wird. Ihre Durchsetzung muß durch die Einrichtung entsprechender Kontrollinstitutionen gewährleistet werden.

Bei der Novellierung des *Bundesdatenschutzgesetzes* muß vor allem sichergestellt werden, daß sämtliche beim Einsatz neuer Telekommunikationstechniken und -dienste entstehenden Daten in den Geltungsbereich des Gesetzes fallen. Deshalb muß z. B. selbstverständlich sein, daß alle personenbezogenen Daten aus der Bild-, Sprach-, Text- und Datenübertragung geschützt werden. Die Regelung der Zulässigkeit der Verarbeitung personenbezogener Daten, deren Kontrolle und der erforderlichen technisch-organisatorischen Maßnahmen müssen an die neuen technischen Gegebenheiten angepaßt werden. Der bisher vorliegende Entwurf läßt die neuen Entwicklungen völlig außer Acht.

Die Länder sind wegen ihrer Zuständigkeit zum Erlaß von Regelungen zur *Nutzung der Telekommunikation* verpflichtet, auch die notwendigen Datenschutzvorschriften zu erlassen. Der Bildschirmtext-Staatsvertrag kann hierzu als Vorbild dienen. In einem derartigen Staatsvertrag müssen auch die materiellen Voraussetzungen zum Betrieb privater Telekommunikationsdienste und deren Zulassung geregelt werden. Ich werde die zuständigen Stellen in Berlin erneut auffordern, hier auch gegenüber den anderen Ländern aktiv zu werden.

Diese Überlegungen werden von der Konferenz der Datenschutzbeauftragten des Bundes und der Länder geteilt[1].

[1] vgl. Anlagen 4 und 5

3.2 Bildschirmtext

Entwicklung des Dienstes

Nach wie vor entwickeln sich die *Teilnehmerzahlen* bei Bildschirmtext nur schleppend. Allerdings überstieg Anfang 1988 die Zahl der Anschlüsse 100 000, doch die ursprünglichen Erwartungen sind schon von der Größenordnung her nicht annähernd erreicht worden. Die Ursachen sind sicher vielschichtig, vor allem aber ist davon auszugehen, daß sich bei Bildschirmtext ein Phänomen erkennen läßt, welches auch die optimistischen Prognosen für andere Dienste und Infrastrukturen der Telekommunikation widerlegen wird: Die Einführungsphase gestaltet sich zu lang und sehr teuer, da einerseits die potentiellen Teilnehmer abwarten, bis der Dienst wegen der attraktiven Angebote interessant wird und andererseits die potentiellen und bestehenden Anbieter zögern, attraktive Programme zu gestalten, solange noch nicht genügend Teilnehmer sie empfangen können. Erneut ist aber festzuhalten, daß sicher nicht Datenschutzmängel die Akzeptanz von Bildschirmtext beeinträchtigen.

Auffällig ist der Anstieg der *Geschlossenen Benutzergruppen* (GBG), was darauf hindeutet, daß Bildschirmtext vorrangig als preisgünstiges Medium zur Information und Kommunikation innerhalb abgeschlossener Personenkreise, z. B. bei Unternehmen zwischen Zentrale und Außendienst oder zwischen Abnehmern und Zulieferern gesehen wird.

Es sind folgende Systemänderungen in der letzten Zeit hervorzuheben:

Die bisher in Listenform angebotene *Seitenabrufstatistik* für Anbieter ist durch ein Statistikprogramm im Bildschirmtextdienst ersetzt worden. Erfaßt werden wie bisher die Seitenabrufe über direkte Seitenanwahl, Querverweise und Weiterblättern. Die Abrufe können pro Seite für den letzten Tag, die letzten 14 Tage und für mehrere Seiten des letzten Tages erfolgen.

Die *GBG-Verwaltung* ist neu organisiert worden. Beim Eröffnen oder Ergänzen einer GBG-Liste können bis zu 10 neue GBG-Einträge auf einer Seite eingegeben werden. Gibt man zusätzlich ein Zeichen in das Feld „Auswahl" ein, wird der Eintrag markiert. Nach Wahl der Anzeigefunktion im Feld „Eingabe" werden die Teilnehmerdaten zu den markierten Einträgen fortlaufend angezeigt. Der Teilnehmername und der Zusatz zum Namen wird nur angezeigt, wenn der Mitteilungsempfang des Mitgliedes nicht gesperrt ist.

Eine Neuerung im Berichtsjahr bietet die Möglichkeit, im Btx-System *Telex-Mitteilungen* zu übermitteln. Der Btx-Telex-Dienst wird von der Deutschen Bundespost im Rahmen eines Betriebsversuches angeboten. Er ermöglicht allen Btx-Teilnehmern mit Gebührenberechtigung, vom Btx-Gerät aus Mitteilungen an Telex-Teilnehmer im In- und Ausland abzusenden und von diesen zu empfangen. Telex-Mitteilungen werden über eine Eingabeseite abgeschickt. Die Übertragung erfolgt zeitversetzt und wird danach durch eine Btx-Mitteilung bestätigt. Die Btx-Nummer wird bei jedem Zugang zum Btx-Telex-Dienst der Deutschen Bundespost erfaßt. Außer zur aktuellen Auftragsbearbeitung (sie wird dem Telex-Empfänger mitgeteilt) wird sie ausschließlich für die Gebührenabrechnung und zur Prüfung der Empfangsbereitschaft bei ankommenden Telex-Mitteilungen gespeichert. Die Registrierung geschieht automatisch bei jedem Zugang zum Bildschirmtext-Telex-Dienst für die nächsten 60 Tage. Auf eingegangene Telex-Mitteilungen wird der Btx-Teilnehmer durch eine Btx-Mitteilung hingewiesen. Telex-Mitteilungen, die nicht innerhalb von 30 Tagen abgerufen werden, werden danach automatisch gelöscht.

Bildschirmtext in der Berliner Verwaltung

Zahlreiche öffentliche Stellen Berlins sind als Anbieter bei Bildschirmtext bereits seit längerem beteiligt. Bemerkenswert ist, daß die oben erwähnte Nutzung des Dienstes als günstiges Datenbereitstellungsmedium im Rahmen einer GBG ebenfalls in der Planung verschiedener ADV-Verfahren der Berliner Verwaltung berücksichtigt wird.

Im Rahmen des Projektes Senatsinformationssystem/Abgeordnetenhaus-Dokumentations- und Informationssystem (SIS/ADIS)[1] ist vorgesehen, den Mitgliedern des Abgeordnetenhauses als geschlossener Benutzergruppe über Bildschirmtext den Zugriff auf gespeicherte Dokumente im Dokumentenrechner zu ermöglichen. Dabei ist der Dokumentenrechner als externer Rechner an das Btx-System angeschlossen.

Nach mehrjähriger Vor- und Hauptuntersuchung beabsichtigt der Senator für Inneres nunmehr aufgrund eines Beschlusses des Rats der Bürgermeister den Einsatz eines Bildschirmtext-Informationssytems für Zwecke der *Bürgerberatung*. Das Btx-Inhouse-System soll die Bürgerberater - vornehmlich in den Bezirken - in die Lage versetzen, aktuell und individuell Auskünfte zu erteilen und bei Bedarf Ausdrucke dem ratsuchenden Bürger mitzugeben. Hierbei werden auch personenbezogene Daten, die im Btx-System gespeichert sind, abgefragt und übermittelt.

Zukünftig sollen weiteren Beratungseinrichtungen der Berliner Verwaltung und privaten Nutzern Informationen aus verschiedenen Bereichen des Senats, der Bezirksverwaltungen und teilweise auch aus Bundesverwaltungen angeboten werden.

Bei dem geplanten Ausbau des Verfahrens kommt der Rolle des Rechners des Landesamtes für Elektronische Datenverarbeitung, der als externer Rechner dienen soll, besondere Bedeutung zu. Aufgrund der künftigen technischen Lösung (Verbindung des externen Rechners mit der Btx-Zentrale über Datex-P-Leitung) sehe ich vor allem Risiken für die Speicher- und Zugriffskontrolle, zumal auf dem externen Rechner auch andere datenschutzrelevante DV-Anwendungen ablaufen.

Unter dem Schlagwort *Schule und Btx* soll ein Modellversuch für die Berliner Schulen anlaufen. Mit Hilfe eines externen Rechners will der Senator für Schulwesen, Berufsausbildung und Sport ein Btx-Programm zur Verfügung stellen, daß es den Schulen ermöglichen soll, schnell Unterrichtsmaterial (z. B. Filme, Videocassetten, Schulbücher, Zeitschriften) bei der Landesbildstelle und dem Pädagogischen Zentrum abzufordern.

Daneben können im System auch Beratungshinweise für die Lehrer zu bestimmten rechtlichen Problemen (z. B. Schulwechsel, Täuschungsversuche) abgefragt werden. Zur Zeit existiert beim Senator für Schulwesen, Berufsausbildung und Sport bereits ein funktionsfähiges Inhouse-System. Noch in diesem Jahr soll die Deutsche Bundespost eine Datex-P-Verbindung für dieses Verfahren herstellen, so daß der Versuch auf die Berliner Schulen ausgedehnt werden kann.

Längerfristig ist davon auszugehen, daß verstärkt Btx dafür eingesetzt wird, den Bürgern den Zugang zu behördlichen Datenbanken zu ermöglichen. Dabei sind die datenschutzrechtlichen Grenzen zu beachten.

Anbieterprüfungen

Insbesondere aufgrund von Hinweisen von Btx-Teilnehmern habe ich erneut eine Reihe von Btx-Angeboten im Rahmen meiner Kontroll- und Beobachtungsaufgaben untersucht und dabei verschiedene Verstöße gegen den Btx-Staatsvertrag festgestellt. Dabei handelt es sich im wesentlichen um zwei Probleme:

Verschiedene Anbieter fragen über Antwortseiten *Teilnehmerdaten* ab, ohne daß dafür eine Rechtsgrundlage gem. Art. 9 Abs. 6 Btx-Staatsvertrag vorliegt. Danach dürfen Daten nur abgefragt und gespeichert werden, soweit dies für das Erbringen der Leistung, den Abschluß oder die Abwicklung eines Vertragsverhältnisses erforderlich ist. Dies ist sicher dann nicht der Fall, wenn die Absendung der Antwortseite Voraussetzung für das Erreichen eines Angebotes ist, bei dem der Teilnehmer sich nur unterrichten, nicht aber entsprechende weitergehende Leistungen erbitten will. Im Falle privater Anbieter habe ich den Vorgang stets an den Senator für Inneres oder an andere Aufsichtsbehörden zur Weiterverfolgung abgegeben. Im Falle einer öffentlichen Stelle des Landes Berlin, der Technischen Universität Berlin, habe ich eine Beanstandung ausgesprochen, die zur sofortigen Korrektur des Programmes führte.

Gravierender wird es, wenn diese unzulässigen Datenabfragen für den Teilnehmer *versteckt* durchgeführt werden, weil die

[1] vgl. Ziff. 4.1

Dateneinblendungen in den Antwortseiten in der Hintergrundfarbe ausgeführt werden. In diesem Fall liegt zusätzlich ein Verstoß gegen Art. 9 Abs. 8 Nr. 2 Btx-Staatsvertrag vor. Dieser Verstoß mußte bei mehreren Anbietern festgestellt werden.

In den Stellungnahmen gegenüber der Aufsichtsbehörde wird von Anbietern gelegentlich die Auffassung vertreten, die Abfrage der Teilnehmerdaten sei notwendig, weil ohne diese Angaben Ansprüche auf *Vergütung von gebührenpflichtigen Seiten* nicht vor Gericht durchgesetzt werden können, da nicht die erforderlichen Angaben zum gebührenerzeugenden Vorgang gemacht werden können. Dem ist entgegenzuhalten, daß die Deutsche Bundespost auf Grund der 2. Vorordnung zur Änderung der Telekommunikationsordnung von den Anbietern die von Gerichten als erforderlich angesehene Angabe des Zeitpunktes des gebührenpflichtigen Vorgangs zusätzlich bereitstellt. Darüber hinaus ist jedoch davon auszugehen, daß das bisherige Verfahren zwar nicht alle Wünsche der Anbieter, die Probleme haben, ihre Entgelte von den Teilnehmern einzutragen, befriedigen kann, daß diesen berechtigten Interessen jedoch das datenschutzrechtliche Interesse gegenübersteht, daß möglichst nur wenige und dann nur kurzzeitig Daten über das Teilnehmerverhalten aufgezeichnet und gespeichert werden. Das von der Deutschen Bundespost durchgeführte Verfahren stößt an die Grenze dessen, was nach dem Btx-Staatsvertrag zulässig ist. Ein gerechter Interessenausgleich wird nur zu erreichen sein, wenn zumindest alternativ die Möglichkeit einer anonymen Nutzung z. B. durch Einführung einer abbuchbaren Chipkarte ähnlich dem Kartentelefon geschaffen wird.

3.3 Kabelpilotprojekt

Mittlerweile ist ein Drittel der Berliner Haushalte (370 000) verkabelt und nimmt mittels Kabelfernsehen am Berliner Kabelpilotprojekt teil.

Neben diesem quantitativen Fortschritt sind auch rechtliche und technische Weiterentwicklungen erfolgt, die den Datenschutz beim Kabelpilotprojekt berühren:

Nach einer Änderung des Kabelpilotprojektgesetzes (KPPG) wird es auch in den nächsten Phasen des Kabelpilotprojektes keine landesspezifischen Teilnehmerentgelte geben. Daher werden die Teilnehmer kein *Teilnehmerverhältnis* mit der Projektgesellschaft Kabelkommunikation Berlin (PK Berlin) begründen müssen, so daß die Speicherung von Teilnehmerdaten bei der PK Berlin auch in Zukunft nicht erforderlich sein wird.

Die im letzten Jahresbericht lobend erwähnte Technik zum Betrieb entgeltpflichtiger Fernsehprogramme *(Pay-TV)*, welche auf dem Prinzip des Verbrauchs eines bezahlten und voreingestellten Guthabens beruhte, wird voraussichtlich nicht in den Einsatz kommen, da sie als zu teuer gilt und sich deshalb Anbieter nicht haben finden lassen. Die Hoffnung beruht jetzt darauf, daß im Zuge der neuen Satelliten-Fernsehnorm D 2 - Mac mit billigeren Verschlüsselungstechniken gerechnet wird.

Davon abgesehen will ein Anbieter aus Niedersachsen auch über Kabel ein bundesweites Pay-TV-Programm anbieten. Dabei soll in vereinfachter Verschlüsselungstechnik gearbeitet werden. Der Teilnehmer soll gegen Entgelt einen Decoder ausgeliefert erhalten, mit dem er das Pay-TV-Programm empfangen kann. Wenn die Gebühr nicht mehr bezahlt wird, wird der Decoder wieder eingezogen. Bei einer solchen Technik fallen zwar keine Nutzungsdaten an, jedoch wird der Anbieter Teilnehmerstammdatenbestände aufbauen müssen.

Fraglich ist, ob angesichts der Regelung, daß die Projektgesellschaft nach § 50 Abs. 3 KPPG die Gebühren einzuziehen hat, der Anbieter Teilnehmerverhältnisse in Berlin begründen und entsprechende Daten der Teilnehmer verarbeiten darf.

Mit technischer Unterstützung der PK Berlin werden von verschiedenen Anbietern *Videotextprogramme* angeboten. So verbreitet u. a. der Anbieter TD 1 Kleinanzeigen, darunter auch Kontaktanzeigen über Videotext. Im Rahmen meiner Zuständigkeit nach dem KPPG werde ich die Rechtmäßigkeit der Verarbeitung entsprechender Daten prüfen.

Mittlerweile hat auf dem vermittlungsfähigen Glasfasernetz BERKOM ein begrenzter Feldversuch „Stadtinformationssystem" bzw. *Breitbandinformationssystem - BIS* begonnen. Von 14 öffentlich zugänglichen Terminals kann der kostenlose Abruf von Text-, Standbild- und Videofilmmaterial nach einem dem Bildschirmtext nachempfundenen Verfahren erfolgen. Die Anbieter kommen bisher ausnahmslos aus dem öffentlichen Bereich, insbesondere Museen, Theater, aber auch die Technische Universität Berlin.

Im BIS kann auch ein Mitteilungsdienst stattfinden, mit dem der Teilnehmer z. B. Wünsche an die Anbieter übermitteln kann. Diese Wünsche kommen bei der PK Berlin an und werden von dort aus über Telefax oder Briefpost an die Anbieter weitergereicht. Für die Rechtmäßigkeit der Abwicklung ist § 52 Abs. 5 KPPG heranzuziehen, dessen Einhaltung ich ebenfalls überprüfen werde.

3.4 Neue Telekommunikationsdienste

Unter den neuen Telekommunikationsdiensten sind die *Fernwirkdienste* von besonderer datenschutzrechtlicher Bedeutung. Ihrer Entwicklung habe ich in der Vergangenheit besondere Aufmerksamkeit gewidmet, zumal in Berlin im KPPG ausdrückliche Regelungen zur Abwicklung dieser Dienste enthalten sind.

Nach den Wasserwerken, deren Versuche mit fernablesbaren Wasserzählern im Rahmen des von der Bundespost betriebenen TEMEX-Dienstes ebenfalls bereits dargestellt worden sind, kommen in Berlin nun auch andere Dienste innerhalb und außerhalb der öffentlichen Verwaltung in den Blick:

So stellt das Universitätsklinikum Steglitz Überlegungen an, mit TEMEX Fernelektrocardiogramme durchzuführen. Den Probebetrieb hat eine Gesellschaft aufgenommen, die die Vermittlung von Taxis an Hotels mittels Fernwirken übernimmt. Daneben stehen Dienste, die zwar nicht personenbezogen abgewickelt werden, deren Funktionen jedoch ebenfalls in die grundsätzliche Bewertung einbezogen werden müssen: So die Kontrolle des Füllstandes von Briefmarkenautomaten durch die Landespostdirektion oder die Überwachung des Schaltzustandes von Alarmanlagen durch eine Wachgesellschaft.

4. Weitere Fragen aus der Kontroll- und Beratungspraxis

4.1 Abgeordnetenhaus und Senatskanzlei

Unter den Arbeitsbegriffen *„Senatsinformationssystem (SIS)"* und *„Abgeordnetenhaus-Dokumentations- und Informationssystem (ADIS)"* werden Informationssysteme für die Berliner Verwaltung und das Berliner Abgeordnetenhaus vorbereitet, die miteinander verknüpft werden sollen. Dahinter steht die politische Absicht, moderne Informations- und Kommunikationstechniken (IuK) für die Arbeit der Legislative und der Exekutive zu erschließen und eine flexible Infrastruktur zu schaffen. Im Verwaltungsbereich ist der Einsatz moderner IuK-Technik für den Aufbau von Dateien und Archiven und die schnelle Wiedergewinnung und Verarbeitung von Informalionen in der Leitungsebene der Verwaltung vorgesehen.

Nach den Aussagen des Senats ist vorgesehen, die Struktur eines übergreifenden, herstellerunabhängigen und zukunftsoffenen IuK-Systems mit den notwendigen Schnittstellen und Standards zu schaffen. Entsprechend dieser Vorgabe hat eine private Beratungsfirma ein Pflichtenheft erstellt, welches die Vorgaben des Senats im hohen Maße erfüllt.

Das Konzept SIS/ADIS läßt Parallelen zum Landessystemkonzept Baden-Württemberg erkennen, das sich allerdings nicht auf Führungsinformationen beschränkt. Gleichwohl teile ich die Auffassung der baden-württembergischen Landesbeauftragten für den Datenschutz, daß ein Landessystemkonzept, welches auf der Grundlage moderner IuK-Systeme den flexiblen und offenen Austausch von Informationen zwischen den verschiedenen Verwaltungsteilen fördern soll, von der Vorstellung der Verwaltung als Informationseinheit geleitet wird. Diese Vorstellung mag zwar den technischen Entwicklungstendenzen angepaßt sein, vernachlässigt jedoch das verfassungsrechtliche Gebot der informationel-

len Gewaltenteilung. Die staatlichen Organe treten dem Bürger als „allwissend" gegenüber, der seinerseits in der Ausübung seines informationellen Selbstbestimmungsrechts gehindert ist.

Aus diesen verfassungsrechtlichen Erwägungen heraus habe ich empfohlen, daß

- die *Beschränkung auf Führungsinformationen*, die im System bereitgehalten und übertragen werden, durch eine restriktive, eindeutige Definition des Begriffs oder eine abschließende Auflistung der darunter verstandenen Dokumentarten abgesichert wird,
- sichergestellt wird, daß die Überschreitung des Rahmens der Führungsinformationen durch *technische und organisatorische* Maßnahmen wirksam verhindert wird,
- für die Bereithaltung von Dokumenten mit Personenbezug im Dokumentenrechner und für den Austausch solcher Dokumente mittels des Mailbox-Rechners die notwendigen *Rechtsgrundlagen* geschaffen werden.

Die Nutzung des Verwaltungsnetzes ist nur dann zulässig, wenn sichergestellt ist, daß für die übrigen ADV-Verfahren, die im Verwaltungsnetz abgewickelt werden, keine zusätzlichen Risiken entstehen.

Während für den Dokumentenrechner eine Auflistung der zu speichernden Dokumente im Hauptuntersuchungsbericht enthalten ist, fehlt eine entsprechende Auflistung für den Dokumenten- und Datenverkehr über den *Mailbox-Rechner*. Gerade hier jedoch schätze ich die Mißbrauchsrisiken hoch ein, zumal die datenschutzrechtliche Kontrolle der Mailbox-Nutzung außergewöhnlich schwierig ist. Unmöglich wird sie jedoch, wenn der ordnungsgemäße Gebrauch und der Mißbrauch aufgrund unklarer Begriffe nicht unterschieden werden können. Der Austausch elektronisch geführter „Personalakten" aus den in der Berliner Verwaltung entstehenden Personalinformations- und -verwaltungssystemen könnte im Fall einer Personalentscheidung ebenso als Führungsangelegenheit angesehen werden wie etwa die Abstimmung über ein Sitzungsprotokoll des Rates der Bürgermeister. Es bedarf daher einer konkreten und verbindlichen Festlegung, welche Daten in welcher Form in welchen Zusammenhängen über die SIS/ADIS-Mailbox versandt werden dürfen.

Die Einrichtung eines Mailbox-Rechners im Rahmen von SIS und ADIS wirft überdies grundsätzliche Fragen des Datenschutzes bezüglich solcher Systeme im Land Berlin auf. Das Mailbox-System sieht vor, daß für jeden Teilnehmer ein persönliches elektronisches Postfach eingerichtet wird. Es ist darüber hinaus denkbar, daß es daneben Postfächer für ganze Benutzergruppen gibt. Ein Verzeichnis über die eingerichteten Postfächer soll dann die einzelnen Anwender in die Lage versetzen, in die entsprechenden Fächer ihre Nachricht abzusetzen. Die Nachrichten können nur abgerufen werden, wenn ein individuelles oder ein Gruppen-Paßwort eingegeben wird.

In diese Postfächer sollen ganze Dokumente abgelegt werden können; damit ist die Übertragung von Teildateien oder ganzen Dateien möglich. Auf diesem Weg könnten auch sensible personenbezogene Daten in Postfächern abgelegt werden, deren Besitzer für einen Zugriff auf diese Daten keine Berechtigung haben. Ohne besondere Maßnahmen würde eine derartige Datenübertragung nicht zu kontrollieren oder zu unterbinden sein.

Ich habe daher folgende Einschränkungen gefordert:

Die am Verwaltungsnetz angeschlossenen Kopfstellenrechner (Abteilungsrechner, PCs) sind mit einer Software auszustatten, die verhindert, daß der jeweilige Benutzer Systembefehle absetzt. Alle dafür eingesetzten Programme müssen abgenommen, geprüft und ordnungsgemäß dokumentiert sein. Änderungen an dieser Software sollten nur durch einzusetzende Systemverwalter erlaubt werden. Das Einspielen von geänderten Software-Versionen ist voll zu dokumentieren und zu kontrollieren. Das Verfahren ist in schriftlichen und verbindlichen Anweisungen festzulegen.

Um den Postverkehr sowohl in eingehender als auch in abgehender Richtung überwachen zu können, muß der gesamte externe Postverkehr in jedem dedizierten Rechner besonders aufgezeichnet werden. Die Aufzeichnung sollte so gestaltet werden, daß der gesamte Postverkehr kontrolliert und ausgewertet werden kann. Die Aufbewahrungsfrist für diese Protokolle wäre durch die zu bildende Projektgruppe festzulegen. Die mit einer solchen Protokollierung verbundenen Mißbrauchsrisiken wären durch begleitende Regelungen und Maßnahmen (Zugriffsrechte, Mitbestimmung) auszuschließen.

Der Dokumentenrechner soll allen beteiligten Stellen, über Bildschirmtext auch der Öffentlichkeit, die darin gespeicherten Dokumente zur Verfügung stellen. Über den Mailbox-Rechner soll ein flexibler Austausch von Dokumenten zwischen den beteiligten Stellen ermöglicht werden.

Es ist davon auszugehen, daß die Dokumente zum erheblichen Teil personenbezogene Daten enthalten (in erster Linie im Hinblick auf die beteiligten Funktionsträger: Verfasser, Redner, kritisierte Politiker usw.). Da das System Auswertungs- und Retrievalfunktionen vorsieht (z. B. Suche nach bestimmten Reden eines Politikers aus einem bestimten Zeitraum), ist sogar der herkömmliche Dateibegriff erfüllt.

Als Voraussetzung für die Einführung eines solchen Systems sollte daher eine angemessene Rechtsgrundlage geschaffen werden, die im übrigen auch eine befriedigende Lösung bisheriger Konfliktpunkte enthalten könnte (z. B. personenbezogene Daten in Kleinen Anfragen oder Untersuchungsausschußberichten).

Gegen die Einführung des *Berliner Verwaltungsnetzes* hatte ich nur unter der Voraussetzung keine Einwände erhoben, daß an das Verwaltungsnetz keine „multifunktionalen Terminals" mit Zugriffen auf verschiedene Verfahren angeschlossen werden.

Wenn das Verwaltungsnetz als Transportmedium für die Anschlüsse der Senats- und Bezirksdienststellen an SIS/ADIS dienen soll, würde dies bedeuten, daß diese Dienststellen Zugriffsmöglichkeiten zum zentralen Dokumentenrechner, zum systemeigenen Mailbox-Rechner und über eine Datex-P-Schnittstelle zu externen Datenbanken wie z. B. JURIS haben sollen.

Dies bedeutet, daß mindestens drei festgeschaltete Netzübergänge (Ports) für jeden Rechner oder jedes intelligente Terminal eingerichtet werden müßten. Ein solcher Netzaufbau würde eine wirtschaftliche Ankopplung an das Verwaltungsnetz unmöglich machen. Darüber hinaus wäre bei einer derartigen Konzeption ein Datenaustausch der einzelnen Dienststellen untereinander in keinem Fall möglich. Im Hauptuntersuchungsbericht ist daher von diesen Geräten ein wahlfreier Zugang zum Dokumentenrechner, zum Mailbox-Rechner, zur Datex-P-Schnittstelle und für den freien Datenaustausch untereinander vorgesehen.

Ein solcher Verbindungsaufbau ist allerdings aus datenschutzrechtlicher Sicht nur dann unbedenklich, wenn die Datenströme der fest vordefinierten Verbindungen (Geräte, die auf die zentralen Online-Verfahren [z. B. EWW, ASTA usw.] zugreifen), eindeutig von den Datenströmen des freien Verbindungsaufbaus für SIS und ADIS getrennt werden. Es muß also ausgeschlossen sein, daß Geräte, die auf die Verfahren SIS und ADIS zugreifen können, selbst wenn sie vorsätzlich manipuliert worden sind, eine solche Verbindung aufbauen können.

Diese eindeutige Trennung ist in dem jetzt in Aufbau befindlichen Verwaltungsnetz möglich, da es hier einen sog. synchronen Verbindungsaufbau (gleichbedeutend mit fest vordefinierten Verbindungen) und einen asynchronen Verbindungsaufbau (eingeschränkter wahlfreier Zugriff über Verbindungsaufbautabellen) gibt. Unter den Voraussetzungen, daß Geräte, die an asynchronen Eingangsports angeschlossen sind, keine physikalische Verbindung mit synchronen Ausgangsports aufnehmen können, und daß kein Datenendgerät, das für die Zugriffe auf die zentralen LED-Verfahren bestimmt ist, über asynchrone Ports angeschaltet wird, wäre die Verwendung des Verwaltungsnetzes als Transportmedium für SIS und ADIS hinnehmbar.

Im übrigen habe ich auf folgende Aspekte der beabsichtigten Infrastruktur hingewiesen:

- Zwar sollen durch SIS/ADIS auch die Möglichkeiten der Parlamentarier zur Gewinnung von Informationen verbessert werden. Allerdings wird zu beobachten sein, wie weit die beabsichtigte Verbesserung der Effizienz der Informations- und Kommunikationsbeziehungen zwischen den Verwaltungsgliederungen Auswirkungen auf das Gleichgewicht zwischen Regierung und Parlament hat und ob speziell Aus-

wirkungen auf die Kontrollmöglichkeiten des Parlaments über die Verwaltung zu erwarten sind (vgl. § 21 Abs. 2 BlnDSG).

- Wichtige Komponenten von SIS sind die Kopfstellenrechner in den Ressorts der Hauptverwaltung und in den Bezirken. Aufgrund der im Hauptuntersuchungsbericht dargestellten technischen Merkmale (Mehrplatzsysteme unter UNIX) ist davon auszugehen, daß es sich dabei um Büroinformations- und -kommunikationssysteme auf Abteilungsrechnerbasis für die Leitungsebene der Behörden handeln soll.

Da zu erwarten ist, daß auch unterhalb der Führungsebene solche oder kleinere Systeme eingesetzt werden, ist die Verknüpfbarkeit dieser Systeme mit dem der Führungsebene zu berücksichtigen. Einerseits können die Systeme des Verwaltungsvollzugs Daten für den Austausch über SIS zum Abruf bereithalten, so daß die Begrenzung auf Führungsinformationen aufgehoben wird, andererseits werden durch den mittelbaren Zugriff der Leitungsebene auf die Vollzugsdaten neue Einwirkungs- und Kontrollmöglichkeiten geschaffen. Für die datenschutzrechtliche Beurteilung von SIS/ADIS kommt es also entscheidend auf die Konzeption der Kopfstellenrechner und deren Einbettung in den jeweiligen Verwaltungen an.

4.2 Bau- und Wohnungswesen

Zur Vorbereitung von wohnungsmarktpolitischen Entscheidungen oder zur nachträglichen Überprüfung ihrer Effektivität wird zunehmend wissenschaftlicher Sachverstand herangezogen, um möglichst objektive Entscheidungsgrundlagen zu erhalten.

Der Senator für Bau- und Wohnungswesen gewährte aufgrund der Richtlinien über die *Förderung der Freimachung und der familiengerechten Belegung von großen Wohnungen* Umzugsprämien an Mieter sowie Prämien für Vermieter von Altbauwohnungen, falls auf diese Weise Wohnungen einer bestimmten Größe für kinderreiche Familien freigemacht wurden. Um zu überprüfen, was nach dem Außerkrafttreten dieser Richtlinien an die Stelle der Zuschußregelung treten soll, beauftragte die Senatsbauverwaltung das private Meinungsforschungsinstitut GEWOS mit einer Untersuchung, ob und von wem die Zuschüsse in Anspruch genommen wurden. Hierzu wollte die GEWOS Antragsunterlagen einschließlich der Einkommensnachweise bei der Wohnungsbau-Kreditanstalt einsehen und auswerten, die die Zuschüsse auszahlt.

Mit dem internen Datenschutzbeauftragten der Wohnungsbau-Kreditanstalt bin ich der Auffassung, daß diese Form der Auswertung von Antragsunterlagen durch Private unzulässig gewesen wäre. Die Antragsunterlagen hätten in personenbezogener Form nur mit Einwilligung der Antragsteller oder in anonymisierter Form an die GEWOS übermittelt werden dürfen. Aus diesem Grund hat die Wohnungsbau-Kreditanstalt entsprechend meinen Empfehlungen der GEWOS ausschließlich anonymisierte Daten aus den Zuschußanträgen übermittelt. Zur ergänzenden vollständigen Auswertung der Antragsunterlagen in personenbezogener Form versandte die Wohnungsbau-Kreditanstalt entsprechende Schreiben, in dem sie ausgewählte Mieter und Vermieter um ihre Einwilligung bat.

Bei der Erstellung des geltenden *Berliner Mietspiegels* für Altbauwohnungen wurden die erforderlichen Daten von den Mieter- und Vermieterverbänden erhoben. Für Zwecke der Plausibilitätskontrolle sind sie mit anonymisierten Daten der Wohngeldstatistik und des Mikrozensus 1985 verglichen worden.

Der gegenwärtige Mietspiegel für Altbauwohnungen soll Anfang 1990 durch einen neuen, auf der Grundlage einer repräsentativen Stichprobe erhobenen, Mietspiegel ersetzt werden. Der Senator für Bau- und Wohnungswesen hat hiermit wiederum die GEWOS beauftragt. An den Vorbereitungen der Erhebung, die voraussichtlich im Frühjahr 1989 stattfinden wird, wurde ich frühzeitig beteiligt. Meinen Empfehlungen zur datenschutzgerechten Stichprobengewinnung und Durchführung der Erhebung ist der Senator für Bau- und Wohnungswesen durchweg gefolgt.

Zur Erstellung einer Datei mietspiegelrelevanter Wohnungen, mit deren Hilfe die Befragung von Mietern und Vermietern durch Interviewer staltfinden soll, müssen zahlreiche Dateien und Register herangezogen werden. Die GEWOS plante ursprünglich, die *Zählerdatei der BEWAG* einschließlich der Namen der Wohnungsinhaber ohne deren Einwilligung hierfür auszuwerten. Dies läßt das Bundesdatenschutzgesetz nicht zu, worauf ich den Senator für Bau- und Wohnungswesen bereits anläßlich der Wohnungsmarktanalyse Berlin, die ebenfalls von der GEWOS durchgeführt wurde, im Jahre 1980 hingewiesen hatte. Die BEWAG wird der GEWOS nunmehr lediglich die Adressen der Gebäude mit mehr als zwei Zählern mitteilen, in denen Haushaltsstrom verbraucht wird.

Auch das *Regionale Bezugssystem* des Statistischen Landesamtes, in dem jede Berliner Adresse in Form eines digitalisierten Stadtplans enthalten ist, soll für die Erstellung der Datei genutzt werden. Ich habe dem wie auch in anderen vergleichbaren Fällen (z. B. Ärztlicher Notfalldienst, Berliner Stadtreinigung) nur unter der Voraussetzung zugestimmt, daß in den Vertrag zwischen dem Senator für Bau- und Wohnungswesen und der GEWOS detaillierte Sicherungsvorschriften und Vorkehrungen gegen Zweckentfremdung aufgenommen werden, bei deren Übertretung eine Vertragsstrafe fällig wird. Eine normenklare Regelung der Nutzung des Regionalen Bezugssystems steht erst im Landesstatistikgesetz in Aussicht.

Personenbezogene Daten, insbesondere Namen von zu befragenden Personen, kann die GEWOS nur aus dem *Melderegister* im Wege der *Gruppenauskunft* nach § 28 Abs. 3 Meldegesetz erhalten. Dies setzt voraus, daß die GEWOS die Merkmale der Gruppe bestimmt, deren Daten sie als Grundgesamtheit zur Ziehung einer repräsentativen Stichprobe benötigt. Die Abgrenzungskriterien sind im Meldegesetz abschließend aufgezählt. Bei der Auskunft selbst dürfen außer der Tatsache der Zugehörigkeit zu einer mit Hilfe dieser Kriterien abgegrenzten Gruppe nur Vor- und Familiennamen, akademische Grade sowie Anschriften, bei minderjährigen Kindern auch die entsprechenden Daten des gesetzlichen Vertreters mitgeteilt werden.

Eine Übermittlung der gewünschten Meldedaten an den Senator für Bau- und Wohnungswesen zur Weiterleitung an die GEWOS ist dagegen rechtlich nicht zulässig. Sie würde voraussetzen, daß der Senator für Bau- und Wohnungswesen als speichernde Stelle die Daten durch die GEWOS als Auftragnehmerin im Sinne des § 2 BlnDSG erheben und verarbeiten ließe. Die Voraussetzung einer solchen Auftragsdatenverarbeitung liegen hier jedoch nicht vor, weil es sich um einen Forschungsauftrag handelt, bei dem die GEWOS selbständig über den Umfang der Datenerhebung und die einzelnen Datenverarbeitungsschritte entscheidet. Vielmehr verarbeitet die GEWOS personenbezogene Daten zum Zwecke der Übermittlung in anonymisierter Form nach § 36 Bundesdatenschutzgesetz. Daraus ergibt sich zugleich, daß die GEWOS das Adreßmaterial nach Abschluß der Interviewer- bzw. Rücklaufkontrolle zum frühestmöglichen Zeitpunkt zu vernichten hat und dem Senator für Bau- und Wohnungswesen keine personenbezogenen Einzelangaben zugänglich machen darf. Eine entsprechende Verpflichtung ist in den Rahmenvertrag aufgenommen worden.

Ursprünglich hatte die GEWOS das Statistische Landesamt auch um Übermittlung von *Anstaltsadressen aus der Volkszählung 1987* gebeten, um diese Gebäude aus der Datei mietspiegelrelevanter Wohnungen aussondern zu können. Diese Angaben unterliegen jedoch dem Statistikgeheimnis und dürfen nach dem Volkszählungsgesetzes nur auf Blockseitenbasis, d. h. ohne Hausnummer, übermittelt werden. Auch Informationen über das Baualter bestimmter Gebäude dürfen aus der Gebäudevorerhebung zur Volkszählung 1987 nur blockseitenbezogen an die GEWOS weitergegeben werden.

Die von der GEWOS geplante Nutzung der Hauseigentümer- und Hausverwalterdatei der *Oberfinanzdirektion* scheidet aus, weil die in ihr enthaltenen personenenbezogenen Daten dem Steuergeheimnis unterliegen. Eine gesetzliche Offenbarungsbefugnis, wie sie z. B. speziell für die Volkszählung 1987 bestand, greift hier nicht ein.

Ich werde im Rahmen der „Arbeitsgruppe Mietspiegel 1990" den Senator für Bau- und Wohnungswesen auch bei der Gestaltung der Erhebungsunterlagen beraten, soweit dies aus datenschutzrechtlicher Sicht notwendig ist. Dabei ist insbesondere auf die Freiwilligkeit der Teilnahme an der Befragung hinzuweisen.

Bei der Durchführung der Erhebung werde ich das private Forschungsinstitut im Zusammenwirken mit dem Senator für Inneres kontrollieren.

4.3 Finanzwesen

Steuerverwaltung

Der vom Bundesminister der Finanzen vorgelegte Entwurf einer *Steuerdaten-Abruf-Verordnung* ist inzwischen aufgrund der Empfehlungen der Datenschutzbeauftragten des Bundes und der Länder in einigen Punkten datenschutzrechtlich verbessert worden. Die Konferenz der Datenschutzbeauftragten hat allerdings ernste Bedenken gegen die weiterhin vorgesehene Einrichtung von automatisierten Datenabrufverfahren für die obersten Finanzbehörden und die Oberfinanzdirektionen erhoben. Die Einrichtung derartiger Online-Anschlüsse ist datenschutzrechtlich gleichbedeutend mit der Übermittlung des gesamten Datenbestandes an den Anschlußinhaber. Ein unmittelbarer automatisierter Zugriff auf sämtliche Steuerdaten der Finanzämter ihres Zuständigkeitsbereiches ist jedoch für die Aufgabenerfüllung der Oberfinanzdirektionen, der Länderfinanzminister und des Bundesfinanzministers nicht erforderlich.

In Berlin soll der *automatisierte Abruf von Steuerdaten* durch die Finanzämter mit Hilfe eines neuen ADV-Verfahrens ermöglicht werden. Dabei wird unter Federführung der Oberfinanzdirektion ein Sternnetz aufgebaut, in dem auf HfD-Leitungen der Post Datenverkehr mit eigenem Datex-P-Protokoll durchgeführt wird. Zur Zeit sind fünf Finanzämter an dieses neue Verfahren angeschlossen. Eine Anbindung der restlichen Finanzämter ist für 1989 vorgesehen. Das Datenabrufverfahren ist die erste Stufe einer Entwicklung, die sich schließlich auf das gesamte Besteuerungsverfahren erstrecken soll.

Ich habe die Oberfinanzdirektion auf die Risiken, die dieses Netz mit sich bringt, in mehreren Informationsgesprächen hingewiesen. Dabei standen in erster Linie Fragen des Netzkonzeptes und der vorgesehenen Sicherungsmaßnahmen (z. B. Zugriffsberechtigungen der Benutzer) im Vordergrund. Eine Überprüfung des Verfahrens war mir bisher nicht möglich, da seine Einführung sich verzögert hat.

In einer Frage von grundsätzlicher Bedeutung bat mich der Senator für Finanzen um Beratung. Aufgrund eines Senatsbeschlusses sollten alle gesetzlichen Möglichkeiten ausgeschöpft werden, um in der gesamten Berliner Verwaltung Beschäftigungen für arbeitsfähige *Sozialhilfeempfänger* anbieten zu können. Bisher hatte die Oberfinanzdirektion derartige Möglichkeiten lediglich in den Bereichen Haus- und Hofarbeiten, Poststelle, Zentralkartei, Aktenverwaltung, Materialverwaltung, Botendienst und Druckerei gesehen. Auf Initiative des Senators für Gesundheit und Soziales sollten jedoch auch Tätigkeiten in der eigentlichen Steuerverwaltung geprüft werden. Dabei stellt sich vor allem die Frage der Wahrung des Steuergeheimnisses.

Nach § 30 Abs. 1 Abgabenordnung (AO) haben Amtsträger das Steuergeheimnis zu wahren. Den Amtsträgern gleichgestellt sind zwar die für den öffentlichen Dienst besonders Verpflichteten im Sinne des § 30 Abs. 3 Nr. 1 AO i. V. m. § 11 Abs. 1 Ziff. 4 StGB. Nach dieser Regelung ist für den öffentlichen Dienst besonders Verpflichteter, wer, ohne Amtsträger zu sein, bei einer Behörde oder sonstigen Stelle, die Aufgaben der öffentlichen Verwaltung wahrnimmt, beschäftigt oder für sie tätig und auf die gewissenhafte Erfüllung seiner Obliegenheiten aufgrund des Verpflichtungsgesetzes förmlich verpflichtet ist. Zweck dieser Regelung ist es, den Schutz der Steuerpflichtigen vor unbefugter Offenbarung gegenüber Dritten durch alle im Bereich der Steuerverwaltung tätigen Personen zu sichern. Diese Vorschriften treffen jedoch keine Regelung darüber, welche Personen mit der Bearbeitung von Steuerdaten befaßt werden sollen. Aus ihm kann daher nicht abgeleitet werden, daß der mit der Bearbeitung von Steuerdaten befaßte Personenkreis beliebig erweitert werden kann, indem er bei der Aufnahme der Tätigkeit auf das Steuergeheimnis verpflichtet wird.

Vielmehr ist vorab zu klären, für welche Personen die Befassung mit Steuerdaten unerläßlich ist. Die Streuung der sensiblen Steuerdaten ist im Hinblick auf eine Minimierung des Risikos einer unbefugten Offenbarung von vornherein auf das unbedingt Notwendige zu beschränken. Dabei hat die zuständige Behörde zunächst zu klären, wie groß der Kreis der Amtsträger oder diesen gleichgestellten Personen sein darf, der Steuerdaten bearbeiten soll.

Dagegen bestehen gegen die Beschäftigung von arbeitslosen Sozialhilfeempfängern aus datenschutzrechtlicher Sicht keine Einwände, wenn deren Tätigkeit nicht im Zusammenhang mit personenbezogenen Daten steht.

Haushaltswesen

Die Neukonzeption des *Automatisierten Haushaltswesens (AHW)* befindet sich weiterhin in der Entwicklung. Durch das Verfahren sollen sämtliche mit dem Haushaltswesen befaßten Dienststellen des Landes Berlin über mehrplatzfähige Arbeitsplatzcomputer Zugriff auf einen Großrechner im Landesamt für Elektronische Datenverarbeitung haben. Die Einführung dieser Dialoganwendung soll dem Sachbearbeiter eine durchgängige Vorgangsbearbeitung ermöglichen. Dies trifft für Direkteingaben, -änderungen und -löschungen zu, wobei die Dateien unmittelbar fortgeschrieben werden.

In verschiedenen Arbeitskreisen beim Senator für Finanzen soll den künftigen Anwendern die Möglichkeit gegeben werden, ihre Vorstellungen in das Projekt miteinzubringen. Ich bin im Arbeitskreis Technik an diesen Vorüberlegungen beteiligt.

Aus datenschutzrechtlicher Sicht birgt das geplante Verfahren Risiken, die sich an folgendem Beispiel verdeutlichen lassen: Im automatisierten Haushaltswesen soll jeder einzelne Zahlungs- und Buchungsvorgang, den ein Bediensteter des Landes Berlin veranlaßt, erfaßt werden. Dies bedeutet, daß z. B. Informationen darüber gespeichert werden, welcher Sachbearbeiter wie viele Bleistifte bestellt hat, aber auch, welcher Beihilfebetrag einem Bediensteten für eine Zahnbehandlung ausgezahlt werden soll. Bei der Zahl der beteiligten Dienststellen wird unmittelbar deutlich, welche gravierenden Probleme sich bei der Sicherung dieser sensiblen Angaben ergeben.

Ein besonderes Problem ergibt sich daraus, daß beim Zugriff vom Arbeitsplatzcomputer zum Zentralrechner das geplante Verwaltungsnetz genutzt werden soll. Bisher ist noch unklar, wie die Datenübertragung und die damit verbundene Verantwortlichkeit für die Datensicherheit im Netz realisiert werden soll.

Offen ist auch noch, ob die Arbeitsplatzcomputer programmierfähig sein werden. Da sie nicht ständig für das AHW-Verfahren genutzt werden, ist die Abwicklung sonstiger Aufgaben geplant. Von der Verfahrensentwicklung sollen dem Benutzer dafür Programme zur Verfügung gestellt werden, die er ausführen, aber nicht ändern kann. Ein Zugriff der Benutzer auf die Betriebssystemebene muß in jedem Fall ausgeschlossen werden.

4.4 Gesundheit und Soziales

Datenverarbeitung im Gesundheitswesen

Im Vorjahr habe ich ausführlich über eine Überprüfung der Datenverarbeitung in den Berliner Krankenhausbetrieben berichtet und dabei auf erhebliche datenschutzrechtliche Probleme hingewiesen, vor allem hinsichlich der Vertragslage zwischen den Krankenhäusern und der *Gesellschaft für Systemforschung und Dienstleistungen im Gesundheitswesen mbH (GSD)*, die die Datenverarbeitung entwickelt und weitgehend im Auftrag der Krankenhäuser durchführt, hinsichtlich des Zugriffs auf medizinische Daten, durch krankenhausfremdes Personal hinsichtlich der Vernetzung der Krankenhäuser untereinander und mit der GSD und hinsichtlich des Netzübergangs zum Dialogsystem Süd der Freien Universität.

In seiner Stellungnahme zu meinem Jahresbericht hat der Senat einem Teil meiner Feststellungen widersprochen oder diese anders bewertet. Gleichzeitig kündigte der Senator für Gesundheit und Soziales eine gutachterliche Untersuchung der Datenverarbeitung im Rahmen des von mir in erster Linie geprüften KRW-2-Verfahrens an, die sich vor allem mit meinen Prüffeststellungen auseinandersetzen sollte. Dieses Gutachten bestätigte in den wesentlichen Ergebnissen und Empfehlungen meinen Prüfbericht.

In der Stellungnahme des Senators für Gesundheit und Soziales zu meinem Gesamtprüfbericht wurde daraufhin die Umsetzung folgender Empfehlungen angekündigt:

- Die Netzverbindung zum Dialogsystem Süd wird aufgehoben.
- Die Verwaltung der Benutzerprofile für den Zugriff auf die personenbezogenen Datenbestände der Krankenhäuser geht auf die jeweilige Krankenhausverwaltung über. GSD-Mitarbeiter erhalten nur noch begrenzte Zugriffsrechte für Schulungs- und Wartungsarbeiten.
- Die Eigenverantwortlichkeit der Krankenhausbetriebe wird durch die Benennung und Ausbildung von System- und Datenschutzbeauftragten und deren Vertretern verstärkt. Es soll sichergestellt werden, daß die KRW-2-Programme von den Krankenhäusern vor deren Einsatz abgenommen werden.
- Für Testzwecke werden keine personenbezogenen Echtdaten mehr verwendet.
- Die Datenträgerverwaltung wird verbessert.
- Der Teilnehmerbetrieb wird durch den Einsatz eines Transaktionsmonitors auf den Teilhaberbetrieb umgestellt.
- Die Handhabung von Paßwörtern wird verbessert, u. a. werden die Terminals nach mehrmaliger Falscheingabe gesperrt.
- Die Zahl der prädialogfähigen Terminals wird reduziert.
- Durch organisatorische und bauliche Maßnahmen soll die Vertraulichkeit der Gespräche im Patientenaufnahmebereich verbessert werden.

Allerdings bleiben noch Defizite festzustellen:

- Das Verhältnis zwischen der GSD und den Krankenhausbetrieben wird zwar durch neue Vertragswerke zugunsten höherer Eigenverantwortlichkeit der Krankenhäuser verändert, jedoch sind die Vertragswerke weiterhin verbesserungsbedürftig.

  Als grundsätzlicher Mangel wurde im Prüfbericht angesehen, daß die Regelungen zwar auf datenschutzrechtliche Pflichten hinweisen, die Verantwortlichkeiten jedoch nicht klar verteilen. Insbesondere war nicht geregelt, in welchem Umfang von welchen Stellen eigene Daten verarbeitet werden und wo eine auftragsweise Datenverarbeitung stattfindet.

  Das Gutachten kommt zu dem Schluß, daß „von einer begrenzten auftragsweisen Datenverarbeitung durch die GSD" auszugehen ist, ohne deutlich werden zu lassen, wo diese Grenze genau verläuft.

  Die hierfür erforderlichen Klarstellungen enthalten die neuen Verträge ebensowenig wie die bisherigen. Insoweit sind demnach weitere Nachbesserungen erforderlich.

- Die Netzstruktur wird dahingehend bereinigt, daß nur noch ein sternförmiger Zugriff von allen Rechnern in den Krankenhaus-Betrieben auf das GSD-Rechenzentrum möglich ist, ein Verbindungsaufbau untereinander jedoch nicht mehr. Dies ist zwar eine einschränkende Maßnahme, läßt aber die Möglichkeit des File-Transfers von der GSD-Zentrale zu einem Krankenhausbetrieb und umgekehrt weiterhin zu. Trotz der Feststellung des Gutachers, daß bisher keine Daten mit Personenbezug übertragen wurden und die Möglichkeit des Datentransfers nur zur Übertragung von administrativen Daten und Programmen durch einen eng begrenzten Personenkreis genutzt wurde, schließt die Technik einen eventuellen Mißbrauch nicht aus. Gerade dies war aber von mir bemängelt worden. Nach wie vor halte ich die Netzverbindung zwischen dem GSD-Rechner und den Rechnern in den Krankenhausbetrieben im Gegensatz zum Gutachter nicht für erforderlich. Die angeführten organisatorischen und wirtschaftlichen Gründe sind nicht ausreichend mit entsprechendem Zahlenmaterial belegt worden.
- Auch bei einer Privatisierung der GSD muß sichergestellt werden, daß sowohl das Regelungsniveau des BlnDSG als auch der Umfang der Kontrolle durch den Berliner Datenschutzbeauftragten sichergestellt werden.

In einer Erörterung dieser ausstehenden Punkte im Unterausschuß Datenschutz des Innenausschusses hat der Senator für Gesundheit und Soziales die Änderung der Verträge sowie die Unterwerfung der GSD unter meine Kontrollkompetenz für den Fall der Privatisierung zugesagt. Über die weitere Reduzierung der Netzverbindungen sollen Verhandlungen geführt werden.

Zusammengefaßt läßt sich jedoch feststellen, daß aufgrund meiner Prüfung wesentliche Verbesserungen des Datenschutzes vorgenommen wurden.

AIDS

Datenschutzrechtliche Fragen im Zusammenhang mit der Immunschwächekrankheit AIDS bildeten in diesem Jahr erneut einen Schwerpunkt.

So habe ich beim Berliner Tropeninstitut, beim Institut für Virologie und bei dem Klinikum Steglitz der Freien Universität sowie in der AIDS-Beratungsstelle eines bezirklichen Gesundheitsamtes Überprüfungen durchgeführt. Mängel bei der Verarbeitung personenbezogener Daten von AIDS-Patienten oder bei der Gestaltung der Therapie und Beratungsverfahren habe ich dabei nicht festgestellt.

Obwohl AIDS als Erkrankung im Sinne des § 1 Bundesseuchengesetz gilt, wird die Einführung einer personenbezogenen Meldepflicht auch in Berlin weiterhin abgelehnt. Ein generelles Melderecht des behandelnden Arztes - etwa im Hinblick auf ein vermeintlich überwiegendes öffentliches Interesse - und ein damit korrespondierendes Anfragerecht der zuständigen Gesundheitsämter ist ebenfalls zu verneinen, weil dies gegen das informationelle Selbstbestimmungsrecht HIV-Infizierter verstoßen würde.

Ein grundsätzliches Problem stellt die Frage dar, in welchem Umfang *HIV-Tests bei Stellenbewerbern* vorgenommen werden dürfen.

Bemerkenswert ist ein Runderlaß des nordrhein-westfälischen Ministers für Arbeit, Gesundheit und Soziales vom Mai 1988[1]. Dort wird klargestellt, daß bei einem symptomlosen HIV-infizierten Beamtenanwärter lediglich eine Aussage zur statistischen Wahrscheinlichkeit des Ausbruchs der Erkrankung gemacht werden kann, die jedoch nicht bewerberbezogen, sondern ausschließlich allgemeiner Art ist. Im Hinblick auf

- die Seltenheit von Angehörigen sogenannter Risikogruppen unter den Beamtenbewerbern,
- den Aufwand für einen allgemeinen Test und
- die Signalwirkung eines solchen obligatorischen Tests für andere Bereiche des Erwerbslebens wird ein allgemeiner HIV-Test aller Beamtenbewerber und die daraus folgende Verarbeitung von Daten als unverhältnismäßig abgelehnt. Der öffentliche Dienstherr soll nicht als Vorreiter einer allgemeinen Diskriminierung von HIV-Infizierten im Erwerbsleben angesehen werden. Ich gehe davon aus, daß in Berlin entsprechend verfahren wird.

Demgegenüber werden in den „Gemeinsamen Hinweisen und Empfehlungen der Bundesärztekammer und der Deutschen Krankenhausgesellschaft zur HIV-Infektion" vom Januar 1988 routinemäßige HIV-Tests bei Stellenbewerbern im Krankenhausbereich, bestimmten Krankenhausbediensteten und Patienten befürwortet. Sowohl die Ärztekammer Berlin und die Berliner Krankenhausgesellschaft in ihrer gemeinsamen Stellungnahme als auch der Nationale AIDS-Beirat haben sich entschieden gegen diese Tendenz zu routinemäßigen HIV-Tests ausgesprochen. Derartige Tests seien aus medizinischer Sicht nicht erforderlich. Auch der mit der Erhebung von HIV-Testdaten verbundene Eingriff in das informationelle Selbstbestimmungsrecht ist nur dann zulässig, wenn die Erforderlichkeit der Datenerhebung im Einzelfall medizinwissenschaftlich nachgewiesen wird.

Schließlich waren mehrere *sozialempirische Erhebungen* zum Thema AIDS zu beurteilen. Dabei konnte ich mit mehreren Empfehlungen zum Ablauf der Studie zur Verbesserung des

[1] Ministerialblatt für das Land Nordrhein-Westfalen Nr. 45 vom 7. 7. 1988

Datenschutzes z. B. bei der „Multizentrischen Studie zur Langzeitbetreuung HIV-infizierter und HIV-exponierter Kinder" beitragen, die neben der Erhebung eine Studie zur Erprobung von Behandlungsmethoden umfaßt, die eng mit den Betroffenen durchgeführt werden muß und ohne ein enges Vertrauensverhältnis zwischen Arzt und Patient nicht realisiert werden kann.

Forschung und Planung mit Patientendaten

Im Auftrag des Bundesministeriums für Arbeit und Sozialordnung wird an einem Universitätsklinikum ein Forschungsprojekt durchgeführt, dessen Ziel es ist, Zusammenhänge zwischen medizinischen, sozialen und biographischen Gegebenheiten und der Art der Unterbringung und Betreuung *hochbetagter chronisch Kranker* in Berlin sowie Versorgungslücken aufzuzeigen. Zur Durchführung dieser Studie wurden aus dem Zentralen Bettennachweis beim Senator für Gesundheit und Soziales patientenbezogene Daten offenbart. Ich habe dies beanstandet, denn auch die vom Zentralen Bettennachweis verarbeiteten Patientendaten dürfen in personenbezogener Form nur mit Einwilligung der betroffenen Patienten an Wissenschaftler für Forschungszwecke weitergegeben werden.

Der Kontakt zu den Patienten, die sich in Akutkrankenhäusern befinden, darf ausschließlich über die ärztliche Leitung dieser Krankenhäuser bzw. die Stationsärzte hergestellt werden, die die Bereitschaft der Patienten zu einem Gespräch vorab festzustellen haben. Im Rahmen dieses Gesprächs müssen die Patienten in verständlicher Form über den Zweck der Untersuchung aufgeklärt und ihr Einverständnis zur Befragung auch des behandelnden Arztes, des Pflegepersonals und der Angehörigen eingeholt werden. Bei Patienten, die zu Hause oder außerhalb eines Krankenhauses gepflegt werden und befragt werden sollen, habe ich empfohlen, daß der Zentrale Bettennachweis entsprechende Ankündigungsschreiben an die Patienten adressiert und versendet. Der Senator für Gesundheit und Soziales und das Universitätsklinikum sind meinen Empfehlungen gefolgt.

Die von mir empfohlenen Maßnahmen zur Anonymisierung der *Diagnosestatistik* nach der Bundespflegesatzverordnung wurden in denjenigen Krankenhäusern, die am automatisierten Krankenhausrechnungswesen (Krw 2) teilnehmen, verwirklicht. In diesen Krankenhäusern ist damit ein Anonymisierungsgrad erreicht, der nicht nur der Voraussetzung des § 16 Bundespflegesatzverordnung entspricht, sondern sogar über den von der „Deutschen Gesellschaft für medizinische Dokumentation, Informatik und Statistik" empfohlenen Standard hinausgeht. Meine Bemühungen waren von Anfang an darauf gerichtet, die Anonymität auch in Bezug auf das Basismaterial zu einem möglichst frühen Zeitpunkt herzustellen.

Im Rahmen der Gesundheitsreform wird geplant, die Diagnosestatistik durch eine bundesweite *Krankenhausstatistik* unter Mitwirkung der Statistischen Landesämter zu ersetzen, die in wesentlichen Punkten der jetzt geführten Diagnosestatistik entsprechen soll. Nach dem Referentenentwurf einer Krankenhausstatistikverordnung sollen dabei Daten entlassener Patienten (einschl. Sterbefälle), deren Pflegetage sowie die Angabe, ob im Zusammenhang mit der Hauptdiagnose operiert worden ist, jeweils gegliedert nach der Hauptdiagnose, nach Alter, Geschlecht und Wohnsitz des Patienten den Statistischen Landesämtern übermittelt werden. Ob die nach dem Entwurf zu übermittelnden Daten hinreichend anonymisiert sind oder das Reindividualisierungsrisiko zu hoch ist, bedarf speziell für Berlin einer besonderen Prüfung. Ob die als Ermächtigungsnorm vorgesehene Änderung des § 28 Krankenhausfinanzierungsgesetz normenklar genug ist, begegnet Zweifeln, weil die Anonymität der erhobenen Daten nicht ausdrücklich festgelegt ist.

Transparenz im Gesundheitswesen - nur nicht für den Patienten?

Im Zusammenhang mit der Diskussion über die Reform des Gesundheitswesens waren zwei Fälle von Interesse, in denen Versicherte von einer Berliner Krankenkasse *Einsicht in ihre Versicherungsunterlagen* verlangten, um zu überprüfen, ob der Arzt ordnungsgemäß abgerechnet hatte. Die Krankenkasse lehnte diese Einsicht unter Inkaufnahme eines gerichtlichen Verfahrens ab, auch nachdem ich nach eingehender datenschutzrechtlicher Analyse den Anspruch des Betroffenen bejaht hatte. Die Entscheidung der Kasse ist mir insbesondere deshalb unverständlich, weil in anderen Bundesländern einige Krankenkassenverbände dazu übergegangen sind, ihren Patienten regelmäßig einen Abrechnungskontoauszug über die Leistungen des Arztes und der Krankenkasse zur Kontrolle zu übersenden.

Eine Berliner Krankenkasse hatte eine *Haftpflichtversicherung* (Rückversicherung) abgeschlossen, um dadurch Vermögensschäden abzudecken, die durch fahrlässiges Verhalten ihrer Mitarbeiter entstehen. Um die Berechtigung der Regulierungsansprüche prüfen zu können, hat die Haftpflichtversicherung um Übersendung solcher Unterlagen gebeten, aus denen der Krankheitsverlauf und die Diagnosen betroffener Versicherter hervorgehen (z. B. bei Schadensfällen aus überzahltem Krankengeld). Nach § 76 Abs. 1 Sozialgesetzbuch X (SGB X) ist auf die Offenbarungsbefugnis des behandelnden Arztes abzustellen, so daß Angaben über den Krankheitsverlauf und über die Diagnose einer vom Arzt behandelten Krankheit ohne Einwilligung des Patienten nicht dem Rückversicherer ffenbart werden dürfen. Wenn bei Schadensfällen jedoch überbezahltes Krankengeld beim Rückversicherer eingefordert werden soll, kann es sich um Daten handeln, die nicht der ärztlichen Schweigepflicht unterliegen, weil „der überbezahlte Zeitraum" gerade eben nicht der ärztlichen Behandlung und Verordnung unterlag. Die betreffende Krankenkasse stimmte dieser Auffassung zu.

Bei der Frage der Übernahme von Krankenhauskosten durch den Träger der *Sozialhilfe* bestehen seit Jahren Differenzen, in welchem Umfang Angaben über die Diagnose sowie sonstige relevante Hinweise zur Erkrankung offenbart werden dürfen. Ich begrüße die Absicht der Senatsverwaltung für Gesundheit und Soziales, in den Fällen, in denen die Einschaltung eines vertrauensärztlichen Dienstes bei den Krankenkassen angezeigt wäre, für den Träger der Sozialhilfe den Amtsarzt der Gesundheitsämter entscheiden zu lassen. Da die Gesundheitsämter bei der Gewährung der Behindertenhilfe nach dem Bundessozialhilfegesetz mit den Jugend- und Sozialämtern zusammenwirken, ist es sinnvoll, ihnen auch diese vertrauensärztliche Funktion zu übertragen. Das geplante Verfahren würde auch zu einer Verringerung medizinischer Daten in den Sozialhilfeakten führen.

Sozialversicherungsausweis und Rentenversicherungsnummer

Neben dem Gesundheitsreformgesetz ist das Gesetz zur Einführung eines Sozialversicherungsausweises von höchster Bedeutung für den Datenschutz im Sozialwesen:

Auch dieser Entwurf sieht keinen ausreichenden Schutz der personenbezogenen Daten vor, sondern beschleunigt im Gegenteil die Gefahr der Einführung eines allgemeinen Personenkennzeichens und begünstigt vorhandene Trends in diese Richtung. Ein allgemeines Personenkennzeichen wurde jedoch vom Bundestag und vom Bundesverfassungsgericht für verfassungswidrig gehalten.

Die Diskussion um den maschinenlesbaren Personalausweis kann uneingeschränkt auch auf den maschinenlesbaren Sozialversicherungsausweis übertragen werden. Die darauf gedruckte, lebenslang unveränderliche Sozialversicherungsnummer hat alle Voraussetzungen, sich zum allgemeinen Personenkennzeichen weiterzuentwickeln. Während die Personalausweisnummer lediglich eine sehr begrenzt nutzbare inhaltsleere Seriennummer enthält, lassen sich über die Sozialversicherungsnummer, die selbst eine „sprechende Zahl" ist, eine Fülle von Dateien und Informationssammlungen bei Arbeitgebern, bei Rentenversicherungen, bei Sozialämtern und anderen öffentlichen und privaten Stellen erschließen. Auch wenn die Krankenkassen die Rentenversicherungsnummer nicht für eingene Zwecke nutzen, erhalten sie doch über die üblichen Meldewege Kenntnis von ihr. Die Möglichkeiten, diese Informationssammlungen miteinander zu verbinden, werden entscheidend erleichtert und die Risiken für das informationelle Selbstbestimmungsrecht unkontrollierbar.

Ein inzwischen verabschiedeter Gesetzentwurf, der die Verwendung der Rentenversicherungsnummer einschränken sollte, hat trotz der wiederholten Kritik der Datenschutzbeauftragten des Bundes und der Länder zu einer Festschreibung der heutigen

- schon zu weit gehenden - Verwendungsformen geführt und darüber hinaus neue Wege für weitere Verwendungsformen eröffnet.

Amtshilfe zwischen Polizei und Sozialamt?

Nach wie vor erreichen mich Beschwerden von Sozialämtern, die das Verhältnis der Polizei zum Sozialdatenschutz betrafen. Im wesentlichen gingen die Beschwerden dahin, daß die Polizeibediensteten nicht nur die Offenbarung von mehr Daten verlangten, als das Gesetz es zuläßt, sondern sogar mit Strafanzeigen drohten, wenn die zuständigen Sachbearbeiter unter Hinweis auf die Rechtslage die Auskünfte verweigerten.

In einem Fall wurde ein Hilfeempfänger aufgrund einer unzulässigerweise erteilten Auskunft vorläufig festgenommen. Es konnte nicht ermittelt werden, wer die unzulässige Auskunft erteilt hatte. Fest steht jedoch, daß die Offenbarungsvoraussetzungen nicht vorlagen und daß darüber hinaus ein Grund für die Verhaftung des Sozialhilfeempfängers nicht gegeben war. Die Voraussetzungen eines Haftbefehls wurden von der Polizei nur irrtümlich angenommen.

Dies zeigt unmißverständlich, wie wichtig der Sozialdatenschutz ist, und daß seitens der Polizeibehörde die Richtlinien, die in Gesprächen zwischen den Senatsverwaltungen für Gesundheit und Soziales sowie Inneres in einem gemeinsamen Rundschreiben entwickelt wurden, künftig beachtet werden müssen.

In dem damaligen Rundschreiben ist ausdrücklich festgelegt, daß unter dem Begriff der Anschrift in § 68 SGB X nicht jeder „gegenwärtige" Aufenthaltsort, sondern vielmehr nur der Aufenthaltsort des tatsächlichen Wohnens zu verstehen sei. Im Widerspruch dazu wird jedoch immer wieder von der Polizei versucht, im Wege der Amtshilfe Auskunft über den „gegenwärtigen" aktuellen Aufenthalt eines Sozialhilfeempfängers zu erhalten. Dies ist unzulässig. Auch die im Rundschreiben geforderte Protokollierung der Auskünfte wird nicht in hinreichendem Umfang vorgenommen.

Forschung in der Sozialverwaltung

Die Zahl der Forschungsprojekte, die sich mit Sozialleistungsempfängern befassen, nimmt ständig zu. Trotz der detaillierten Regelung der damit verbundenen datenschutzrechtlichen Fragen im Sozialgesetzbuch treten auch hier immer wieder Probleme auf.

So beschwerten sich mehrere Versicherte einer Berliner Krankenkasse bei mir darüber, daß die Krankenkasse ihre Adressen und den Umstand, daß sie eine *zahnärztliche Vollprothese* erhalten haben, mit Genehmigung des Senators für Gesundheit und Soziales an eine Universitätszahnklinik zur Durchführung eines Forschungsvorhabens weitergegeben hatte. In zwei mir bekannt gewordenen Fällen erhielten zudem die betroffenen Versicherten im Rahmen dieses Forschungsvorhabens einen Fragebogen zu ihren Erfahrungen mit der Vollprothese im offenen Briefumschlag zugesandt.

Die Offenbarung der Versichertenadressen war zur Durchführung des Forschungsprojekts nicht erforderlich und daher unzulässig. Das Projekt hätte durchgeführt werden können, indem die Forscher ein Adreßmittlungsverfahren angewandt hätten. Dazu hätten sie die Fragebogen mit einem aufklärenden Anschreiben in frankierten Umschlägen der Krankenkasse mit der Bitte zuleiten können, daß die Krankenkasse diese Umschläge adressiert und versendet. Auf diese Weise hätte die Krankenkasse den Forschern keine Adressen von Prothesenträgern offenbart.

Der Genehmigungsbescheid des Senators für Gesundheit und Soziales nach § 75 SGB X hatte keinen Einfluß auf die datenschutzrechtliche Verantwortlichkeit der Krankenkasse als speichernde Stelle. Ich habe deshalb die Offenbarung der Versichertenadressen gegenüber der Krankenkasse beanstandet und den versehentlichen offenen Versand der Fragebogen gegenüber der Hochschule bemängelt. Die Krankenkasse hat mir daraufhin mitgeteilt, sie habe sich entschlossen, bei künftigen Forschungsvorhaben dieser Art die Schreiben an die Versicherten gegen volle Kostenerstattung durch den jeweiligen Forschungsbetrieb selbst zu verschicken.

Der Senator für Gesundheit und Soziales plant die Vergabe eines Forschungsauftrags an ein privates Sozialforschungsinstitut zum Thema *Wege aus der Sozialhilfe*. Dabei sollen ehemalige und gegenwärtige Sozialhilfeempfänger von Interviewern befragt werden. Auch hier besteht das entscheidende datenschutzrechtliche Problem darin, wie das Forschungsinstitut Kontakt mit den zu befragenden Personen aufnehmen kann, ohne daß das Sozialgeheimnis verletzt wird. Ich habe den Senator für Gesundheit und Soziales darauf hingewiesen, daß die Offenbarung der Adressen der Sozialhilfeempfänger ohne ihre Einwilligung unzulässig ist und auch nicht gem. § 75 SGB X genehmigt werden kann. Eine solche Genehmigung käme nur in Frage, wenn die Einholung der Einwilligung unzumutbar wäre. Die Versendung der Fragebogen durch die Sozialämter oder die Einholung der Einwilligung durch Bedienstete des Sozialamts bedeutet zwar einen erhöhten Verwaltungsaufwand. Dadurch wird die Einholung der Einwilligung - gemessen an der Sensibilität des Datums „gegenwärtiger oder ehemaliger Sozialhilfeempfänger" - jedoch nicht unzumutbar. Sollte die Zahl der Sozialleistungsempfänger, die zu einer Beteiligung an der Studie bereit sind, nicht ausreichen, um repräsentative Ergebnisse zu ermöglichen, müßten zusätzliche Sozialleistungsempfänger um ihre Einwilligung gebeten werden. Falls die Hilfeempfänger von einem Sachbearbeiter oder Sozialarbeiter des Sozialamts mündlich um ihre Einwilligung gebeten werden, ist es wesentlich, daß ihnen unter ausdrücklichem Hinweis auf die Freiwilligkeit der Teilnahme verdeutlicht wird, daß sie mit keinen Nachteilen zu rechnen haben, wenn sie nicht teilnehmen.

Durch eine Eingabe wurde ich auf eine *Telefonumfrage* zum Thema „Integration von jungen Türken und Jugoslawen in Berlin" aufmerksam gemacht, die im Auftrag der Ausländerbeauftragten des Senats von Berlin von einer privaten Firma durchgeführt worden war. Die Petentin beschwerte sich darüber, daß sie erst durch mehrmalige Rückfragen den Zweck des Anrufs und die auftraggebende Stelle erfahren habe.

Meine Überprüfung dieser Umfrage ergab, daß die Ausländerbeauftragte das Landeseinwohneramt um die Erteilung einer Gruppenauskunft aus dem Melderegister gebeten hatte, da sie die Namen, Adressen und Geburtsjahre der türkischen und jugoslawischen Jugendlichen im Alter von 16 bis 25 Jahren in Berlin für repräsentative Stichprobe benötigte. Die vom Landeseinwohneramt erhaltenen Daten gab die Ausländerbeauftragte dann an das private Umfrageinstitut weiter.

Meldedaten können auf drei verschiedenen Wegen für die Zwecke einer Umfrage oder wissenschaftlichen Erhebung genutzt werden:

Zum einen kann die Meldebehörde personenbezogene Daten aus dem Melderegister nach § 25 Abs. 1 Meldegesetz einer anderen Behörde übermitteln, die damit die Umfrage selbst durchführt. In der Praxis häufiger sind jedoch zwei andere Möglichkeiten der Nutzung von Meldedaten. In der einen Fallkonstellation beantragt ein Forschungsinstitut, das mit der Durchführung der Erhebung beauftragt wird, selbst eine Gruppenauskunft bei der Meldebehörde nach § 28 Abs. 3 Meldegesetz. Wenn der Senator für Inneres das Vorliegen eines öffentlichen Interesses an der Gruppenauskunft bestätigt, übermittelt die Meldebehörde die Gruppenauskunft direkt dem Forschungsinstitut. Im anderen Fall schreibt die auftraggebende öffentliche Stelle dem beauftragten Institut genau definierte Datenverarbeitungsvorgänge vor. So soll etwa ein von der Behörde entwickelter Fragebogen von Interviewern des privaten Instituts mit den Daten der befragten Personen ausgefüllt werden. In diesem Fall handelt es sich um Datenverarbeitung im Auftrag (§ 2 Abs. 1 BlnDSG), bei der die Auftragnehmerin datenschutzrechtlich als Teil der speichernden Stelle angesehen wird.

Im Fall der Telefonumfrage unter jungen Ausländern wurde keiner dieser zulässigen Wege gewählt. Die Firma beantragte nicht selbst die Gruppenauskunft, sondern erhielt die Adressen von der Ausländerbeauftragten, ohne daß der Senator für Inneres das Vorliegen des öffentlichen Interesses geprüft hätte. Auch lagen die Voraussetzungen einer Datenverarbeitung im Auftrag der Ausländerbeauftragten nicht vor, da der Fragebogen und die Konzeption der computergestützten Befragung nicht von ihr, sondern von dem privaten Forschungsinstitut entwickelt worden waren. Unter diesen Bedingungen hätten die Meldedaten an ein

privates Institut nur mit Einwilligung der Betroffenen weitergegeben werden dürfen (§ 11 Abs. 1 Satz 1 BlnDSG). Neben die Vorschriften des Meldegesetzes, die diese Fragen nicht regeln, treten insofern ergänzend die Regelungen des Berliner Datenschutzgesetzes.

Die Eingabe hat ein weiteres, für Telefonumfragen typisches Problem verdeutlicht:

Wenn die angerufene Person nicht vor dem Telefonanruf in einem vorbereitenden Brief über den Zweck der Umfrage aufgeklärt worden ist, besteht die Gefahr, daß die erforderliche Aufklärung und der zwingend notwendige Hinweis auf die Freiwilligkeit der Teilnahme zu Beginn des Telefongesprächs entweder unterbleibt, unzureichend erfolgt oder vom Angerufenen aufgrund der überraschenden Situation häufig nicht hinreichend wahrgenommen wird. Dies wird auch die amtliche Statistik zu berücksichtigen haben, wenn sie - wie vorgesehen - zukünftig verstärkt telefonisch Daten erhebt.

Technisch-organisatorische Maßnahmen

Ein kurioser Fall menschlichen Versagens ging durch die Berliner Presse, weil eine begründete Warnmeldung eines Bezirksamtes an andere Bezirksämter wegen eines betrügerischen Sozialhilfeempfängers mit dem *Telekopierer* statt an die Bezirksämter versehentlich an die Berliner Tageszeitungen versandt wurde. Der Vorfall hat mich veranlaßt, einmal mehr auf die Gefahren *nachlässiger Bedienung moderner Technik* hinzuweisen und außerdem zu verdeutlichen, daß der Sozialdatenschutz nicht gewährleistet ist, wenn per Telekopierer Sozialdaten übermittelt werden und das Empfangsgerät nicht beim zuständigen Sozialamt als Empfänger steht.

Eine Universitätszahnklinik plante, ihre Krankenakten von einem privaten Unternehmen mikroverfilmen zu lassen. Dies läßt die geltende Krankengeschichtenverordnung nicht zu. Sie sieht eine *Mikroverfilmung von Krankenakten* ausschließlich im jeweiligen Krankenhaus vor. Bei ihrem Erlaß ging man offenbar davon aus, daß die Krankenhäuser mit eigenen Mikroverfilmungsanlagen ausgestattet werden. Zwischenzeitlich hat sich jedoch herausgestellt, daß die Vergabe derartiger Arbeiten an private Spezialfirmen wesentlich kostengünstiger ist. Dies läßt sich nur dann mit dem geltenden Recht vereinbaren, wenn der private Auftragnehmer mit einer mobilen Mikroverfilmungsanlage im Krankenhaus und unter dessen Kontrolle arbeitet.

Erneut erwiesen sich *Unzulänglichkeiten bei der Aufbewahrung von Unterlagen.* So war es im Künstlerhaus Bethanien spielenden Kindern gelungen, durch die Vergitterung eines geöffneten Fensters in den Archivkeller zu gelangen und von dort Karteikarten mit Sozialdaten zum Spielen auf die Straße mitzunehmen.

In einem weiteren Fall lagen in einem geräumten und abrißbereiten Pavillon des Klinikums Rudolf Virchow - Standort Wedding - Patientenunterlagen offen herum. Ich habe dies als gravierenden Verstoß gegen die Pflicht zur Geheimhaltung von Patientendaten beanstandet. Der ärztliche Leiter einer Klinikabteilung muß vor dem Umzug in ein anderes Gebäude dafür Sorge tragen, daß patientenbezogene Unterlagen vollständig und unter Verschluß transportiert werden, so daß weder Speditions-, Bauarbeiter noch Dritte sie einsehen können.

Bei der Überprüfung einer Abteilung für Sozialwesen hat sich erneut bestätigt, daß die derzeitige *Aktenführung* im Sozialhilfebereich dringend einer Reform bedarf. Das Bezirksamt beklagte sich einerseits über mangelnden Platz, um alle Akten in Schränken unterzubringen (sie lagen daher teilweise auf Stühlen und Tischen), andererseits fand ich jedoch einen Vorgang über einen Sozialhilfeempfänger, der zwar vollständig in einem verschließbaren Schrank hing, jedoch lückenlos sämtliche Vorgänge seit etwa Mitte der 50iger Jahre dokumentierte und in der Zwischenzeit auf ein Volumen von ca. 18 Bänden angewachsen war. Eine Begründung für die ständige Verfügbarkeit des gesamten Aktenbestandes konnte nicht gegeben werden. Eine Differenzierung nach erledigten und unerledigten Teilen sowie nach Daten, die einem besonderen Schutz nach § 203 Strafgesetzbuch unterliegen (z. B. medizinische Daten), oder nach beteiligten Personen wäre angesichts des Umfangs dieses Vorganges sicherlich angebracht gewesen.

4.5 Inneres

Amtliche Statistik

Der Senat hat den Entwurf eines *Landesstatistikgesetzes* beschlossen und in das Abgeordnetenhaus eingebracht. Damit ist ein wichtiger erster Schritt zur Schaffung der erforderlichen normenklaren Rechtsgrundlage für die amtliche Statistik in Berlin getan worden, auf dessen Notwendigkeit ich seit Jahren hinweise. Der Entwurf berücksichtigt in einigen wichtigen Punkten meine Empfehlungen, wenngleich er in anderen Punkten noch verbesserungsbedürftig ist.

Insbesondere enthält der Entwurf eine ausführliche Regelung für die Nutzung personenbezogener Daten aus dem Verwaltungsvollzug für statistische Zwecke und für den Betrieb des *Statistischen Informationssystems* (STATIS). Entsprechend ist eine Ermächtigung zum Erlaß einer Rechtsverordnung vorgesehen, in der festzulegen ist, welche Daten aus welchen Bereichen der Vollzugsverwaltung zu welchem Verwendungszweck an das Statistische Landesamt übermittelt werden dürfen. Vor Erlaß dieser Rechtsverordnung räumt der Gesetzentwurf den Datenschutzbeauftragen ein Anhörungsrecht ein. Dabei werde ich im einzelnen zu prüfen haben, in welchem Umfang dem Statistischen Landesamt der Zugriff auf personenbezogene Daten aus der Vollzugsverwaltung eröffnet werden soll. Auch im Rahmen des Statistischen Informationssystems gilt das Gebot der frühestmöglichen Trennung der Hilfs- von den Erhebungsmerkmalen und der Löschung der Hilfsmerkmale nach Abschluß der Plausibilitätskontrolle. Die Struktur und Verwendung des Statistischen Informationsssytems wird sich daran zu orientieren haben, daß das Bundesverfassungsgericht die Verknüpfung von Datensammlungen des Verwaltungsvollzugs bezogen auf eine bestimmte Person als verfassungswidrigen Schritt zur Registrierung und Katalogisierung des einzelnen Bürgers in seiner ganzen Persönlichkeit bezeichnet hat.

Der Entwurf enthält erstmals auch eine Regelung für die Nutzung und Weitergabe des *Regionalen Bezugssystems.* Dabei handelt es sich um einen Stadtplan in digitalisierter Form, der jedes Grundstück in Berlin mit Straße und Hausnummer enthält. Auch wenn man dieser Datensammlung den Personenbezug abspricht, so eröffnet sie doch die Möglichkeit, andere statistische und nicht statistische Daten kleinräumig zu gliedern und damit die Gefahr der Herstellung eines Personenbezugs für diese Daten beträchtlich zu erhöhen. Ich begrüße es daher, daß der Senat entsprechend meiner Empfehlung die Nutzung und Weitergabe dieses Systems an gesetzliche Voraussetzungen knüpfen will.

Im Statistischen Informationssystem dürfen Erhebungsmerkmale wie z. B. Volkszählungsdaten, die aufgrund eines *Bundesgesetzes* erhoben worden sind, nicht verwendet oder mit Daten aus Landesstatistiken oder dem Verwaltungsvollzug verknüpft werden, weil der Bundesgesetzgeber die Verwendung dieser Daten abschließend geregelt hat. Dem trägt der Entwurf Rechnung.

Entgegen meinen Empfehlungen sieht der Entwurf lediglich vor, daß der Gesetzgeber zu entscheiden hat, ob landesstatistische Erhebungen beim Bürger mit oder ohne Auskunftspflicht durchgeführt werden. Ich würde es demgegenüber begrüßen, wenn im Landesstatistikgesetz ähnlich wie im Hessischen Landesstatistikgesetz der *Grundsatz der Freiwilligkeit* festgelegt würde, von dem nur der Gesetzgeber ausnahmsweise abweichen kann.

Die Einbringung des Entwurfs für ein Landesstatistikgesetz hat sich so weit verzögert, daß zu befürchten ist, daß der Entwurf vor der Neuwahl des Abgeordnetenhauses nicht mehr verabschiedet werden kann. Jedenfalls muß der Gesetzentwurf in der kommenden Legislaturperiode möglichst frühzeitig beraten und verabschiedet werden. Dem steht auch nicht der vom Abgeordnetenhaus am 20. Oktober 1988 beschlossene Berichtsauftrag an den Senat über Aufgabenstellung, Kostenentwicklung und Organisation des Statistischen Landesamtes entgegen. Die Schaffung einer gesetzlichen Grundlage für die amtliche Statistik im Land Berlin duldet keinen weiteren Aufschub. Soweit als Konsequenz des Senatsberichts über die Organisation des Statistischen Landesamtes eine teilweise Privatisierung seiner Aufgaben erwogen wer-

den sollte, weise ich bereits jetzt darauf hin, daß das Statistikgeheimnis auch eine auftragsweise Nutzung und Verarbeitung von staatlich erhobenen Einzelangaben durch Private ausschließt.

Das Statistische Landesamt setzt zunehmend *PCs für die Erstellung und Nutzung von Statistiken* ein. Diese Geräte sollen teilweise als intelligente Terminals an Großrechner (auch an das speziell für die Volkszählung eingerichtete Rechenzentrum) angeschlossen, teilweise untereinander vernetzt werden. Dabei muß sichergestellt werden, daß nur ein eng begrenzter Personenkreis auf statistische Einzelangaben zugreifen kann. Ein solcher Zugriff wird ohnehin - wenn überhaupt - nur in seltenen Fällen erforderlich sein, während der Fachstatistiker im Normalfall lediglich bestimmte Auswertungen im Großrechner zu veranlassen braucht, ohne auf die Einzelangaben zuzugreifen. Ein Vergleich von Einzelangaben aus verschiedenen Statistiken ist jedenfalls nur zulässig, soweit die jeweiligen Einzelstatistikgesetze dies zulassen. Dementsprechend muß die Verarbeitung statistischer Mikrodaten auf PCs denselben Anforderungen an die Datensicherung und Zugriffsdifferenzierung genügen, wie sie auch für den Großrechnerbetrieb gelten. Das Statistische Landesamt hat mir zugesichert, daß eine Verarbeitung von Einzelangaben auf PCs erst einsetzen wird, wenn die erforderlichen Maßnahmen zur Datensicherung getroffen sind.

In zwei Entscheidungen hat es das Bundesverfassungsgericht abgelehnt, Verfassungsbeschwerden von auskunftspflichtigen Bürgern gegen die Mikrozensuserhebung zur Entscheidung anzunehmen[1]. Die Anordnung einer Auskunftspflicht bei dieser Stichprobenerhebung hält das Gericht ebenso für verfassungsmäßig wie bei der Volkszählung. Dem weitergehenden Fragenkatalog beim Mikrozensus stehe die Schutzwirkung der Stichprobe gegenüber, die allenfalls einem kleinen Kreis privater Interessenten die Kenntnis ermögliche, daß der gesuchte Haushalt im Datensatz enthalten sei.

Ich habe die Aufbereitung der beim Mikrozensus 1988 erhobenen Daten im Statistischen Landesamt überprüft und dabei festgestellt, daß die Rücklaufkontrolle auf einem PC durchgeführt wurde, der keinerlei Schutz gegen den Zugriff Unbefugter aufwies. Diesen Mangel hat das Statistische Landesamt umgehend behoben.

Der Bundesminister des Innern plant die Einführung eines *Informationstechnischen Systems zur Unterstützung bei Kostenrechnungen im Dienstrechtsbereich (ISKD),* bei dem die zentralen Arbeiten dem Statistischen Bundesamt zufallen werden. Aufgabe dieses Systems soll es sein, die Auswirkungen besoldungsrechtlicher Maßnahmen zu berechnen.

Die Besoldungsdaten, die dem Statistischen Bundesamt dafür übermittelt werden sollen, sind zumindest teilweise personenbeziehbar. Eine Aggregation soll erst beim Statistischen Bundesamt erfolgen. Die aggregierten Daten werden in einem von den Statistikdaten abgeschotteten Teil des Statistischen Informationssystems des Bundes (STATIS-Bund) eingespeichert, auf den mehrere Bundesministerien und die Bundesländer online zugreifen können.

Eine Übermittlung von Berliner Personalstrukturdaten an das Statistische Bundesamt ist nur zulässig, wenn sie bereits vor der Übermittlung aggregiert werden oder wenn das Statistische Bundesamt die Daten unmittelbar im Auftrag des Berliner Senators für Inneres verarbeitet.

Mehrfach hatte ich grundsätzliche Fragen des Statistikgeheimnisses im Zusammenhang mit der Einsicht in den vertraulichen Teil der *Leichenschauscheine* zu prüfen. Dabei ging es zum einen um eine Auswertung zu Forschungszwecken, zum anderen um einen Zugriff der Strafverfolgungsbehörden.

Der vertrauliche Teil des Leichenschauscheins enthält in seinen drei Ausfertigungen teilweise identische Angaben des obduzierenden Arztes über die Todesursache und andere wesentliche Krankheiten des Verstorbenen zur Zeit des Todes. Ergeben sich bei der Leichenschau Anhaltspunkte dafür, daß der Verstorbene nicht eines natürlichen Todes gestorben ist, so hat der Arzt diese Feststellung nach dem Bestattungsgesetz unverzüglich der Polizeibehörde mitzuteilen. Ergeben sich solche Anhaltspunkte nicht, so übersendet der Arzt im Regelfall alle drei Ausfertigungen des vertraulichen Teils des Leichenschauscheins dem bezirklichen Gesundheitsamt. Dieses prüft die Vollständigkeit der medizinischen Angaben und leitet im Regelfall alle drei Ausfertigungen des Scheins mit Name und Anschrift des Verstorbenen an das Statistische Landesamt weiter, das ihn mindestens drei Monate aufzubewahren hat. Dort wird er für Zwecke der bundesweiten Todesursachenstatistik genutzt, indem die Todesursache in das Sterbefallzählblatt übertragen wird, das der Standesbeamte dem Statistischen Landesamt zugeleitet hat. Grundlage hierfür ist das Gesetz über die Statistik der Bevölkerungsbewegung und die Fortschreibung des Bevölkerungsstandes.

Der Senator für Gesundheit und Soziales plante für Zwecke der epidemiologischen Forschung zur Häufigkeit der *Asbestose* eine Auswertung des vertraulichen Teils der Leichenschauscheine im Statistischen Landesamt. Ich habe darauf hingewiesen, daß dies nur in anonymisierter Form zulässig ist. Die im Leichenschauschein enthaltenen Informationen unterliegen der statistischen Geheimhaltung, sobald der Schein das Statistische Landesamt erreicht. Auch vorher würde im Ergebnis nichts anderes gelten, da die Gesundheitsämter Daten verstorbener Personen nur in anonymisierter Form zu Forschungszwecken weitergeben dürfen.

Bereits zu Beginn des Jahres habe ich den Senator für Inneres darauf hingewiesen, daß die gegenwärtige Verwendung des Leichenschauscheins in Berlin nicht den Anforderungen des Bundesverfassungsgerichts an eine strikte Abschottung zwischen Verwaltungsvollzug und Statistik genügt. Dieses Abschottungsgebot gilt nicht nur gegenüber der amtlichen Statistik, die keine Einzelangaben an Stellen des Verwaltungsvollzugs weitergeben darf; es bedeutet umgekehrt auch, daß die amtliche Statistik, soweit sie Daten aus dem Verwaltungsvollzug nutzt, sich auf anonymisierte Daten beschränken muß. Erst recht darf das Statistische Landesamt nicht - wie beim Leichenschauschein - als „Endlager" für personenbezogene Unterlagen des Verwaltungsvollzugs dienen, nur weil sie ein einziges Merkmal enthalten, das für eine Statistik (der Todesursachen) benötigt wird.

Überdies fehlt für die personenbezogene Übermittlung der Todesursache im vertraulichen Teil des Leichenschauscheins auch die erforderliche gesetzliche Grundlage. Lediglich die Durchführungsverordnung zum Berliner Bestattungsgesetz enthält eine entsprechende Regelung.

Die personenbezogene Übermittlung von Todesursachen ist aus meiner Sicht - auch zu Zwecken der Plausibilitätskontrolle - nicht erforderlich und damit unverhältnismäßig. Eine Zusammenführung der Angaben zur Todesursache mit dem vom Standesbeamten ausgefüllten Sterbefallzählblatt kann auch aufgrund der Sterbebuchnummer erfolgen. Die Übermittlung aller über die Todesursache hinausgehenden Angaben im vertraulichen Teil des Leichenschauscheins an das Statistische Landesamt ist deshalb verfassungsrechtlich problematisch.

Der Bundesminister des Innern erarbeitet gegenwärtig einen Entwurf für ein neues, den Vorgaben des Bundesverfassungsgerichts angepaßtes Gesetz über die Statistik der Bevölkerungsbewegung und die Fortschreibung des Bevölkerungsstandes. Bei den Beratungen werde ich auf die Notwendigkeit einer datenschutzgerechten Regelung der Todesursachenstatistik hinweisen. Unabhängig davon habe ich dem Senator für Inneres empfohlen, die Durchführungsverordnung zum Bestattungsgesetz bereits vor einer Änderung des Bevölkerungsstatistikgesetzes den datenschutzrechtlichen Erfordernissen anzupassen. Sie müßte insbesondere vorsehen, daß die Angaben zur Todesursache dem Statistischen Landesamt nur in anonymisierter Form übermittelt werden. Gegebenenfalls könnte im Vorgriff bereits das Formular des Leichenschauscheins entspechend modifiziert werden.

Der Senator für Inneres ist meiner Empfehlung bisher nicht gefolgt, da nach seiner Auffassung der Novellierung des Bevölkerungsstatistikgesetzes nicht vorgegriffen werden sollte.

Welch gravierende Folgen die Aufrechterhaltung dieser verfassungswidrigen Gemengelage zwischen Verwaltungsvollzug und Statistik im Fall des Leichenschauscheins haben kann, wurde

[1] Beschlüsse vom 1. 3. 1988 (1 BvR 93/88) und vom 15. 4. 1988 (1 BvR 222/88)

wenig später deutlich: die Staatsanwaltschaft verlangte im Rahmen eines *Ermittlungsverfahrens* Auskunft über die Todesursache aus dem vertraulichen Teil dreier im Statistischen Landesamt aufbewahrter Leichenschauscheine. Sie ging dabei dem Verdacht nach, daß das Personal eines Altenpflegeheims den später verstorbenen Personen ärztliche Hilfe verweigert habe. Das Statistische Landesamt lehnte die Erteilung der Auskunft unter Berufung auf das Statistikgeheimnis ab.

Tatsächlich wird der Auskunftsanspruch der Strafverfolgungsbehörden durch das Statistikgeheimnis beschränkt. Das Bundesstatistikgesetz enthält im Gegensatz zur AO und zum SGB X keine Regelungen darüber, daß und in welchen Fällen (z. B. bei schweren Straftaten) Statistikdaten für Zwecke der Strafverfolgung verwendet werden dürfen. Es trägt damit der grundsätzlichen Forderung des Bundesverfassungsgerichts nach einem amtshilfefesten Schutz der Daten gegen Zweckentfremdung durch Weitergabe- und Verwertungsverbote Rechnung. Auch das Berliner Bestattungsgesetz geht davon aus, daß die Angaben über die Todesursache mit dem Eintreffen des Leichenschauscheins im Statistischen Landesamt ausschließlich statistischen Zwecken dienen und nicht einmal für Strafverfolgungszwecke offenbart werden dürfen (§ 19 Abs. 3).

Demgegenüber hat das Amtsgericht Tiergarten seinerseits das Statistische Landesamt gemäß § 95 StPO zur Auskunft über die Todesursache in den drei Fällen aufgefordert. Diese richterliche Entscheidung unterliegt nicht meiner Kontrollkompetenz (§ 21 Abs. 1 S. 1 BlnDSG). Nach einer entsprechenden Weisung des Senators für Inneres erteilte das Statistische Landesamt der Staatsanwaltschaft die gewünschten Auskünfte.

Ich werde mich gegenüber dem Senator für Inneres weiterhin für eine umgehende Änderung des Berichtsweges in der Todesursachenstatistik in der Weise einsetzen, daß das Statistische Landesamt Angaben über die Todesursache nicht mehr mit Name und Anschrift des Verstorbenen erhält. Damit wäre eine Auskunft des Statistischen Landesamtes an die Strafverfolgungsbehörden in Zukunft nicht mehr möglich.

Dem staatlichen Strafverfolgungsinteresse kann nur dadurch Rechnung getragen werden, daß die Unterlagen aus dem Verwaltungsvollzug, die bei Ermittlungen von Bedeutung sein könnten, auch bei den Stellen des Verwaltungsvollzuges verbleiben und der amtlichen Statistik nur in anonymisierter Form zugänglich gemacht werden.

Personalwesen

Der Petitionsausschuß des Deutschen Bundestages hatte 1986 einen Auftrag des Innenausschusses aus dem Jahre 1984 aufgegriffen und die Bundesregierung aufgefordert, zu Beginn des Jahres 1988 einen Bericht über den Sachstand der Neuordnung des Personalaktenwesens vorzulegen. Eine zu diesem Zweck beauftragte *„Interministerielle Arbeitsgruppe zur strukturellen Fortentwicklung des Personalaktenrechts im öffentlichen Dienst"* unter Leitung des Bundesministers des Innern legte im Juli ihren Bericht vor. Er kommt in wesentlichen Punkten meinen seit Jahren vertretenen Feststellungen nahe.

Die Arbeitsgruppe stellt nicht nur fest, daß eine Neustrukturierung des Personaldatenrechts wegen der erhöhten rechtsstaatlichen Anforderungen unter Berücksichtigung von Literatur und Rechtsprechung geboten ist. Insgesamt habe die Entwicklung einen Punkt erreicht, an welchem der Umgang mit dem Personaldatenrecht für alle Beteiligten zu immer größeren Schwierigkeiten führe - wie die Vielzahl der Rechtsstreitigkeiten und der heftigen Diskussionen zeige -, und an dem rechtsstaatlich vorrangige Ziele wie Rechtsklarheit und Rechtssicherheit auf Dauer verloren zu gehen drohten. Daraus schließt die Arbeitsgruppe unmißverständlich, daß dies den Gesetzgeber in seiner Absicht bestärken muß, das Personalaktenrecht insgesamt auf eine tragfähige Grundlage zu stellen.

Allerdings stellt die Arbeitsgruppe dabei überwiegend auf die Grundlagen des Beamtenrechts ab, wohingegen die datenschutzfreundlicheren Entscheidungen des Bundesarbeitsgerichts geringere Berücksichtigung finden.

Zwar werden - besonders bei der Akteneinsicht - die Persönlichkeitsrechte Betroffener hervorgehoben. Jedoch wird spätestens bei den Vorlage- und Auskunftsrechten Dritter, also den Übermittlungen, deutlich, daß letztlich dem „dienstlichen Interesse" (das dem „öffentlichen Interesse" gleichgestellt wird) Vorrang eingeräumt bleiben soll. Nicht gefolgt ist die Arbeitsgruppe insbesondere der vom Bundesarbeitsgericht vertretenen, differenzierten Sicht des Prinzips der Aktenvollständigkeit.

Gleichwohl ist hier im Ansatz eine geeignete Grundlage für notwendige Diskussionen im Rahmen der Gesetzesvorbereitung zu erkennen.

Auch die *Eingaben und Anfragen zu Personaldatenproblemen* lassen erkennen, daß der Mangel an materiell-rechtlichen Spezialregelungen zu Inhalten von Personalakten, Einsichtsrechten und Auskunftsbefugnissen sowie Aufbewahrungsfristen nicht mehr länger vertretbar ist.

So hatte der Senator für Inneres in einem Schreiben an die Personalstellen des Landes Berlin empfohlen, Überhangkräfte bei der Aufnahme in die *Personalüberhangliste* lediglich pauschal darüber zu informieren, daß unter Umständen Personalstellen, in deren Bereich Stellen zu besetzen sind, ihre Personalakten zur Einsicht anfordern werden. Gleichzeitig wurde darauf hingewiesen, daß die Personalakte nicht immer sofort greifbar sei, da Überhangkräfte möglicherweise von mehreren Personalwirtschaftsstellen zugleich in Auswahlverfahren einbezogen würden.

Dies macht deutlich, daß dem dienstlichen Interesse am Abbau des Personalüberhangs ohne Abwägung im Einzelfall Vorrang vor dem informationellen Selbstbestimmungsrecht der Betroffenen eingeräumt wird. Im Gegensatz zu der in Bewerbungsverfahren üblichen Praxis werden hier Übermittlungen der Personalakte ohne Zustimmung der Betroffenen zugelassen.

Der Senator für Inneres führte zwar aus, daß die Selbstauskunft und das persönliche Gespräch wesentliches Informationsmittel für eine sachgerechte Personalauswahl sind. Jedoch hatte er den Personalstellen nicht empfohlen, beim Betroffenen zu klären, ob er überhaupt für die jeweilige Stelle in die Personalauswahl einzubeziehen ist. Die Fürsorgepflicht gebietet es jedoch, den Inhalt der Personalakte nicht ohne hinreichenden dienstlichen Grund anderen Beschäftigten und Stellen zugänglich zu machen. Sollte diese Vorabklärung mit dem Betroffenen bereits dazu führen, daß er für die Besetzung in Frage kommt, ist kein Grund mehr ersichtlich, ihn um die Einwilligung zur Versendung der Personalakte zu bitten. Auch wenn die beteiligten Dienststellen zuvor geprüft haben, ob die betreffende Dienstkraft tatsächlich in die Auswahl für die zu besetzende Stelle einbezogen werden kann, macht eine solche Prüfung die Zustimmung der Dienstkraft nicht entbehrlich.

Entgegen meinen Empfehlungen lehnt der Senator für Inneres es weiter ab, eine Übersendung der Personalakte von der Zustimmung der betroffenen Mitarbeiter abhängig zu machen, weil dies „im Konfliktfall die Übernahme der Überhangkraft in besetzbare stellen unmöglich machen oder sie in nicht vertretbarem Umfang verzögern würde". Allerdings wurden die Personalwirtschaftsstellen noch einmal ausdrücklich gebeten, Aktenanforderungen zum Zweck der Vorinformation tatsächlich nur auf die notwendigen Fälle zu beschränken. Die anfordernden Dienststellen sollten sich zunächst durch persönliche Kontaktaufnahme mit den entsprechenden Dienstkräften informieren.

Der Mangel an Normen führt auch zu einer Verunsicherung bei Bediensteten, so daß häufig die Rechtmäßigkeit einer Datenerhebung durch die Dienstbehörde von vornherein in Zweifel gezogen wird, selbst wenn eine ausreichende Rechtsgrundlage vorliegt.

So lehnte ein Beamter es ab, bei seinem Antrag auf Genehmigung einer *Nebentätigkeit* auch Angaben zum voraussichtlichen Verdienst und dem Namen sowie der Anschrift des Auftraggebers zu machen. Der Petent hielt die Frage nach Art der Tätigkeit mit „Handel" als hinreichend beantwortet und vertrat die Auffassung, daß die Fragen im übrigen lediglich für Finanzamt und Gewerbeamt von Bedeutung sein dürften.

Zwar war der Hinweis des Petenten korrekt, daß jedes erhobene Datum mit einem Hinweis auf die Rechtsgrundlage versehen sein muß. Jedoch war der Bescheid der Dienstbehörde, über den Antrag nur befinden zu können, wenn auch die in Frage stehenden

Angaben beigebracht werden, nicht zu bemängeln. Von der Dienstbehörde war zu überprüfen, ob Versagungsgründe nach § 29 Abs. 2 Landesbeamtengesetz vorliegen. Dabei war insbesondere festzustellen, ob mit einer Genehmigung dienstliche Beeinträchtigungen zu befürchten wären. Genaue Kriterien über Art und Umfang für diese Prüfung sind spezialgesetzlich allerdings nicht festgelegt, so daß die Dienstbehörde die für die gesetzliche Überprüfung *erforderlichen* Angaben anzufordern hatte. Das Erforderlichkeitsprinzip nach § 9 Abs. 1 BlnDSG war eingehalten, da sowohl die voraussichtliche Höhe des Verdienstes als auch Anschrift und Name des Gewerbebetriebes Rückschlüsse auf Art und Umfang der Nebentätigkeit zulassen, die für die Überprüfung einer möglichen Beeinträchtigung der dienstlichen Interessen notwendig sind.

Zu prüfen war die Frage, ob von einer Strafverfolgungsbehörde Informationen aus einem strafrechtlichen Ermittlungsverfahren schon dann intern über die *Disziplinarstelle* an die Personalstelle weitergegeben und von dieser ohne personalrechtliche Grundlage verwendet werden dürfen, wenn eine Mitteilung nach der Anordnung über Mitteilungen in Strafsachen noch nicht eingegangen ist.

Ein Polizeibeamter beklagte sich darüber, daß eine anstehende Beförderung trotz vorheriger positiver Beurteilung bis zum Abschluß des Strafermittlungsverfahrens zurückgestellt wurde. Das Verfahren war aufgrund einer Strafanzeige wegen Freiheitsberaubung und Sachbeschädigung von Personen eingeleitet worden, die der Beamte zuvor festgenommen und bei denen er eine Durchsuchung vorgenommen hatte.

Trotz meines Verständnisses für die persönliche Situation des Petenten mußte ich zu dem Ergebnis kommen, daß die Weitergabe und Verwertung der Information nicht rechtswidrig war, obwohl das Verfahren lediglich in einer internen Geschäftsanweisung des Polizeipräsidenten geregelt ist.

Mit den Interessen des einzelnen Polizeiangehörigen an der vertraulichen Behandlung seiner Daten im Ermittlungsverfahren ist das dienstliche Interesse an einer frühzeitigen Information über mögliches Fehlverhalten des Polizeibeamten abzuwägen. Mangels gesetzlicher Grundlage muß der Dienstbehörde auch hier der Übergangsbonus eingeräumt werden, wobei Regelungen der Geschäftsanweisung als Kriterien für die Grenzen des Übergangsbonus herangezogen werden können. Solange lediglich die Tatsache der Einleitung des Ermittlungsverfahrens ohne belastende Einzelheiten übermittelt wird, ist auch das Verhältnismäßigkeitsprinzip gewahrt. Eine sachliche Rechtfertigung für die Höherbewertung der behördlichen Interessen ergibt sich auch aus dem Aufgabencharakter der polizeilichen Gefahrenabwehr. Die Polizeibehörde muß zur Vermeidung von Konflikten und auch hinsichtlich ihrer Außendarstellung frühzeitig in der Lage sein, auf Ermittlungsverfahren gegen einzelne Beamte zu reagieren. Bereits die Einleitung eines Ermittlungsverfahrens kann ein Anlaß für die Behörde sein, ihre Aufgabenverteilung und den Personaleinsatz zu überdenken. Die Dienstbehörde verstößt auch nicht gegen ihre Fürsorge- und Schutzpflicht, wenn sie bei einem Ermittlungsverfahren von Zweifeln an der Eignung ausgeht und eine Beförderung deshalb zurückstellt.

Die *Frauenbeauftragten* in den Bezirksämtern drängen zunehmend darauf, hinreichende Instrumente für die Wahrnehmung ihrer Kompetenzen zu erhalten. Insbesondere wurde gefordert, Einsicht in Personalakten bei Bewerbungen zu erhalten. So sehr die Arbeit von Frauenbeauftragten zu begrüßen ist, ergeben sich allerdings auch Datenschutzprobleme, die auf Dauer gelöst werden müssen. Ein Bezirksamt versuchte die Arbeitsmöglichkeiten der Frauenbeauftragten dadurch zu verbessern, daß der bezirklichen Frauenbeauftragten zur Erleichterung ihrer Arbeit ein unmittelbares, ressortübergreifendes Informationsrecht (ohne unbedingte Einhaltung des Dienstweges) zugesprochen wurde.

Ein Bezirksamtsbeschluß kann nur insoweit verbindliche Regelungen treffen, als diese nicht der geltenden Rechtslage widersprechen. Jedes Informationsrecht bewirkt bei der befragten Stelle eine Übermittlungspflicht. Sofern es sich um personenbezogene Informationen handelt, ist eine Übermittlung personenbezogener Daten nur zulässig, wenn hierfür eine gesetzliche Grundlage vorliegt oder aber der Betroffene eingewilligt hat. Dabei ist davon auszugehen, daß eine Übermittlung immer dann vorliegt, wenn mit der Weitergabe der Daten die ursprüngliche Zweckbestimmung verändert wird.

Bislang sind die Aufgaben der Frauenbeauftragten nicht gesetzlich festgelegt. Damit ist derzeit auch keine Spezialnorm vorhanden, die eine aufgabenübergreifende Informationsweitergabe erlauben würde. Auch die allgemeinen Bestimmungen des BlnDSG (insbesondere § 10) bieten keine geeignete Grundlage für derartige Übermittlungen, da auch hier für die Rechtmäßigkeit der Aufgabenerfüllung eine gesetzliche Aufgabenzuweisung zu fordern ist. So bleibt im Einzelfall nur die Möglichkeit, die Zustimmung der Betroffenen einzuholen.

Zwar könnte der Bezirksbürgermeister selbst die Frauenbeauftragte unmittelbar seinem Geschäftsbereich, dem regelmäßig auch der Personalbereich zugeordnet ist, unterstellen; aber auch in diesem Fall wären die Einsichts- und Informationsrechte auf dessen Kompetenzen beschränkt (vgl. §§ 38, 39 Bezirksverwaltungsgesetz). Insbesondere können Frauenbeauftragte, da sie nicht Beteiligte im Sinne des Personalvertretungsgesetzes sind, an Personalauswahlverfahren nur nach Zustimmung der Bewerber(-innen) beteiligt werden.

Eine Einsicht in Vorgänge, die dem Sozialgeheimnis unterliegen, wäre selbst aufgrund einer landesrechtlichen Regelung nicht möglich, da hierzu ausschließlich die Offenbarungsbefugnisse nach dem Sozialgesetzbuch in den dort genannten Fällen ausschlaggebend sind (§ 35 SGB I, §§ 67 ff. SGB X). Die Übertragung einer Zuständigkeit der Frauenbeauftragten für Aufgaben in diesem Bereich würde zwar die Einsichtnahme in die diesbezüglichen Vorgänge der Sozial- oder Jugendverwaltung ermöglichen, jedoch wäre auch hier ein umfassendes Einsichtsrecht mit den §§ 67 ff. SGB X nicht vereinbar.

Sollen den Frauenbeauftragten über die politische Unterstützung hinaus Befugnisse übertragen werden, die die informationelle Selbstbestimmung berühren, hat daher der Gesetzgeber auch alle juristischen Voraussetzungen für die gewünschten Aufgaben zu schaffen.

Im Jahresbericht 1987 hatte ich meine Auffassung zur *Einsicht der Kriminalpolizei in Personalakten* im Rahmen eines Ermittlungsverfahrens dargelegt. Ich hatte darauf verwiesen, daß die Kriminalpolizei vor einer Einsichtnahme in Personalakten ohne Einwilligung des Betroffenen darzulegen hat, daß das Ermittlungsverfahren einen Bezug zum Dienstverhältnis hat, und daß sie darüber hinaus präzisieren müsse, an welchen Informationen, die möglicherweise in der Personalakte enthalten sind, sie interessiert sei. In anderen Fällen sei die Kriminalpolizei auf den Weg der Beschlagnahme zu verweisen. Einige Anfragen haben gezeigt, daß meine Ausführungen erläuterungsbedürftig sind.

§ 161 StPO verpflichtet zwar alle öffentlichen Behörden zur Amtshilfe gegenüber Staatsanwaltschaft und Polizeidienst. Insbesondere im Hinblick auf das Grundrecht auf informationelle Selbstbestimmung muß diese Verpflichtung jedoch entsprechend den allgemeinen Amtshilferegeln in den Fällen eingeschränkt werden, in denen die Behörde aus rechtlichen Gründen zur Amtshilfe nicht in der Lage ist, so z. B., wenn die herauszugebenden Daten einer besonderen Geheimhaltungspflicht unterliegen. Dies ist der Fall bei Personaldaten, die nach einhelliger Rechtsprechung der Bundesgerichte einer derartigen Geheimhaltungspflicht unterliegen, auch wenn sich dies - was die Datenschutzbeauftragten mehrfach bemängelt haben nicht ausdrücklich aus dem öffentlichen Dienstrecht ergibt. Einschränkungen des informationellen Selbstbestimmungsrechts müssen allerdings dann hingenommen werden, wenn die Offenbarung einen Bezug zum Dienstverhältnis aufweist, da insoweit der Zweckzusammenhang mit den Personaldaten noch gewahrt ist.

Wann ein derartiger Bezug zum Dienstverhältnis vorliegt, muß im Einzelfall von der Dienstbehörde entschieden werden. Auch wenn kein Dienststraftatbestand vorliegt, kann ein solcher Bezug z. B. auch dann vorliegen, wenn ein (ehemaliger) Bediensteter im Verdacht steht, im Dienstgebäude eine allgemeine Straftat begangen zu haben.

Die Verarbeitung von Personaldaten wird ohne Zweifel zu einem wichtigen Anwendungsgebiet für *Bürokommunikations-*

systeme werden. Neben der bereits früher angesprochenen Frage, in welchen Fällen nach dem Personalvertretungsrecht ein Mitbestimmungsrecht des Personalrats besteht, ist hier in erster Linie zu klären, welche Funktionsbereiche bei der Personaldatenverarbeitung bestehen und welche Zugriffe auf die jeweiligen Bestände zulässig sind. Auszugehen ist dabei davon, daß die Personaldatenverarbeitung nicht eine einheitliche Aufgabe darstellt, sondern in funktional voneinander abzugrenzende Einzelbereiche zerfällt.

Planungen der Berliner Feuerwehr, mit Hilfe eines neuen Bürokommunikationssystems alle Personaldatensätze zu verarbeiten, beleuchten dieses Problem auf markante Weise:

Im engeren Bereich der Personalverwaltung fallen einerseits Administrationsaufgaben, andererseits Aufgaben der Personalwirtschaft an. Da für die Arbeit der Personalwirtschaftsstellen ein Zugriff auf die gesamten Datensätze nicht erforderlich ist, sind bereits diese beiden Bereiche informationell zu trennen. Dies ist in der Regel bei der herkömmlichen Organisation auch der Fall: die Trennung darf durch Automation nicht aufgehoben werden. Wo sie - wie bei der Feuerwehr - bisher nicht klar durchgeführt wurde, bietet die Automation eine Gelegenheit, dies nachzuholen.

Neben diesen beiden Bereichen erfordern weitere Aufgaben die Verarbeitung von Personaldaten: einerseits die Einsatzleitung, andererseits die Ausbildung in der Feuerwehrschule. Auch hier wird nicht der gesamte Datensatz der Personalverwaltung benötigt, sondern jeweils nur Teile; andererseits kommen Daten hinzu, die für die Personalverwaltung nicht erforderlich sind. Bei der Automatisierung der Datenverarbeitung ist durch entsprechende Zugriffsregelungen sicherzustellen, daß diese Differenzierung aufrechterhalten bleibt und nicht von einzelnen Mitarbeitern aufgehoben werden darf.

Öffentliche Sicherheit

Die Polizeibehörden des Bundes und der Länder betreiben zur Verfolgung von Straftaten, die gegen die freiheitliche demokratische Grundordnung, den Bestand und die Sicherheit des Bundes oder eines Landes gerichtet sind oder die eine ungesetzliche Beeinträchtigung der Amtsführung von Mitgliedern verfassungsmäßiger Organe des Bundes oder eines Landes zum Ziel haben, die Verbunddatei *APIS* (Arbeitsdatei PIOS - Personen, Informationen, Objekte, Sachen - innere Sicherheit). Zugriffsberechtigt sind die mit Aufgaben des Polizeilichen Staatsschutzes betrauten Bediensteten. Es gab mehrere Anlässe, die Speicherung personenbezogener Daten in APIS zu kontrollieren.

So habe ich im Zusammenhang mit der Verfolgung von Straftaten bei der Volkszählung die Verarbeitung personenbezogener Daten von *Volkszählungsgegnern* in APIS mehrfach überprüft. Dabei ergab sich, daß in APIS 45 Vorgänge mit 75 Verdächtigen gespeichert waren. Daneben bestand eine größere Zahl von Vorgängen, in denen die Verdächtigen nicht bekannt waren. Bei den geprüften Vorgängen handelte es sich ausschließlich um den Verdacht von Straftaten. Dagegen waren nicht Daten von solchen Personen gespeichert, gegen die lediglich Bußgeldverfahren im Zusammenhang mit der Volkszählung durchgeführt wurden. Auch Daten von Bürgern, die lediglich ihren Volkszählungsbogen nicht abgegeben hatten und gegen die Zwangsgelder festgesetzt oder vollstreckt wurden, sind nicht in APIS gespeichert worden.

Die Überprüfung ergab, daß bei einigen Fällen keine datenschutzrechtlichen Bedenken bestanden. Es handelte sich dabei um schwerere Taten (Raub, Drohung mit einer Körperverletzung, Verunglimpfung von Verfassungsorganen sowie Diebstahl und Sachbeschädigung in einer schweren Form).

Die weit überwiegende Zahl der Vorgänge erfüllte dagegen die Voraussetzungen für die Einspeicherung in APIS nicht, so daß ich in diesen Fällen eine Beanstandung ausgesprochen habe. Dabei handelte es sich unter anderem um Vorgänge, die von vornherein nicht gegen die Volkszählung gerichtet waren. So wurde ein Tatverdächtiger notiert, der in einem Lokal einem Volkszähler seinen Aktenkoffer entwendet hatte, ohne zu wissen, daß sich darin - für ihn wertlose - Volkszählungsunterlagen befanden.

Bei den übrigen Fällen handelte es sich zum größten Teil um Vorgänge wie die Verteilung von Flugblättern, in denen durch bildliche Darstellung oder Schrift auf die Möglichkeit hingewiesen wurde, die Heftnummer abzuschneiden, den Bogen zu verbrennen oder durch ein Haustier auffressen zu lassen, ferner um das Bekleben von Fenstern und Wänden mit Plakaten sowie um das Besprühen mit Boykottparolen. Auch bei diesen Vorgängen handelte es sich unter Zugrundelegung der Rechtsauffassung des Amtsgerichts Tiergarten zur Beschädigung von Volkszählungsbögen um Straftaten.

Gegenüber dem Senator für Inneres habe ich empfohlen, die beanstandeten Datensätze in APIS zu löschen. Der Beanstandung lag folgende rechtliche Bewertung zugrunde: Die automatisierte Speicherung personenbezogener Daten durch die Polizei ist bisher nicht gesetzlich geregelt. In der der Polizei für eine beschränkte Zeit einzuräumenden Übergangszeit ist davon auszugehen, daß sich die Zulässigkeit nach allgemeinen verfassungsrechtlichen Grundsätzen richtet. Das bedeutet vor allem, daß sich die polizeiliche Datenverarbeitung im Einzelfall strikt am verfassungsrechtlichen Grundsatz der Verhältnismäßigkeit zu orientieren hat. Äußerste Grenze für die Zulässigkeit der Erfassung und Übermittlung personenbezogener Daten beim Polizeilichen Staatsschutz bilden die „Richtlinien für den kriminalpolizeilichen Meldedienst in Staatsschutzsachen (KPMD-S)" von 1982, da darüber hinaus selbst aus der Sicht der Polizei eine Datenverarbeitung offensichtlich nicht für erforderlich gehalten wird. Insbesondere verfassungsrechtliche Überlegungen können allerdings zu einer Einschränkung dieses Rahmens führen. So ist etwa eine Übermittlung personenbezogener Daten Verdächtiger an das Bundeskriminalamt und alle anderen Landeskriminalämter nur bei überörtlicher Bedeutung des konkreten Einzelfalls verhältnismäßig. Die von mir beanstandeten Vorgänge hielten sich nicht im Rahmen der geschilderten Zweckbestimmung von APIS und waren allenfalls regional bedeutsam. Gestützt wurde meine Auffassung dadurch, daß auch in anderen Bundesländern, z. B. in Rheinland-Pfalz und Bremen, Zweifel an der Rechtmäßigkeit bestanden und vergleichbare Speicherungen im Zusammenhang mit der Volkszählung entweder gar nicht vorgenommen wurden oder zwischenzeitlich gelöscht waren.

Der Senator für Inneres hat aufgrund meiner Beanstandungen zunächst die Daten über 55 Täter bzw. Tatverdächtige in APIS gelöscht. Nach einer nochmaligen Überprüfung der noch in APIS verbleibenden Einspeicherung sind im Ergebnis nur sieben der ursprünglich 75 Personen-Datensätze gespeichert. In diesen Fällen waren die obengenannten Voraussetzungen für eine weitere Speicherung allerdings gegeben.

Die Speicherung von Personen, die einer Straftat verdächtig sind, im regionalen Informationssystem Verbrechensbekämpfung des Polizeipräsidenten in Berlin (ISVB) ist dagegen zulässig, da es sich beim ISVB nicht nur um ein Ermittlungsinstrument, sondern auch um ein Dokumentationssystem für das Vorgehen der Polizei handelt. Anhaltspunkte für unzulässige Übermittlungen von Berlin aus an weitere Dienststellen (z. B. Verfassungsschutzämter) ergaben sich bei der Prüfung nicht.

Noch drastischer zeigte sich die Problematik von APIS bei der Überprüfung einer Beschwerde, die sich auf strafrechtliche Ermittlungen zu politischen Aktionen im Zusammenhang mit der Einführung des neuen *Personalausweises* Anfang 1987 bezog: Personenbezogene Daten mehrerer Betroffener, die behelfsmäßige Personalausweise dadurch beschädigten, daß sie die Ausweise öffentlich in einer Waschschüssel „wässerten", waren in APIS eingegeben und damit an alle berechtigten Polizeidienststellen übermittelt worden. Trotz der beabsichtigten politischen Wirkung (die gering gewesen sein dürfte), war eine Einspeicherung und Weiterverbreitung der Informationen über APIS sicherlich nicht gerechtfertigt. Die Staatsanwaltschaft stellte die Verfahren auch mangels Strafverfolgungsinteresse ein, wobei ohnehin fraglich war, ob angesichts des Fehlens eines bei der Sachbeschädigung erforderlichen Antrags überhaupt die Strafverfolgungsvoraussetzungen vorlagen. Auf meine Beanstandung hin wurden die Daten gelöscht.

Die Ereignisse rund um die *Tagung der Weltbank* im September beleuchteten weitere Aspekte der polizeilichen Datenverarbeitung auf dem Gebiet des Staatsschutzes. Die Strafverfolgungs-

behörden waren aufgrund verschiedener Hinweise davon ausgegangen, daß es in Zusammenhang mit dieser Tagung zu gewalttätigen Aktionen einzelner politisch motivierter Straftäter kommen würde. Vorsorglich wurde daher eine Reihe von Maßnahmen ergriffen, die bedeutsame datenschutzrechtliche Aspekte aufwiesen.

Bereits im Frühjahr hatte der Bundesgerichtshof aufgrund polizeilicher Erkenntnisse nach § 111 StPO die Einrichtung von Straßensperren gestattet, um gesuchte Terroristen aus dem RAF-Umfeld zu ergreifen. Dieser Beschluß wurde im Hinblick auf die Tagung der Weltbank im Juni erneuert. Er ermöglichte auch in Berlin, entsprechende Straßensperren einzurichten. Nach § 111 StPO durften dabei die angetroffenen Personen durchsucht und ihre Personalien festgestellt werden. Nicht ergangen war dagegen ein Beschluß nach der neuen Vorschrift des § 163 d StPO, die auch die Speicherung der Daten aller angetroffenen Personen ermöglicht hätte, unabhängig davon, ob gegen die Person polizeiliche Maßnahmen ergriffen werden können (z. B. Festnahme aufgrund einer Fahndungsausschreibung). Für die ohne einen derartigen Beschluß anfallenden Daten schreibt § 163 c Abs. 4 StPO eindeutig vor, daß die Unterlagen und damit auch die erhobenen personenbezogenen Daten zu vernichten sind. Trotz der ursprünglichen Auffassung des Polizeipräsidenten, die Aufbewahrung der Daten sei zu Dokumentationszwecken zulässig, wurden die ursprünglich erhobenen Daten vernichtet bzw. keine Daten mehr erhoben.

Hiervon zu unterscheiden sind Maßnahmen, die aufgrund § 15 ASOG ergriffen wurden. Danach ist die Feststellung der Identität einer Person zulässig, wenn diese sich in der Nähe von besonders gefährdeten Objekten aufhält und Tatsachen die Annahme rechtfertigen, daß hier Straftaten begangen werden sollen. Aufgrund verschiedener Ankündigungen ging der Polizeipräsident davon aus, daß bei der Weltbanktagung Anschläge insbesondere auf Firmengebäude internationaler Unternehmen geplant seien. Daher wurden aufgrund § 15 ASOG bei Personen, gegen die der Verdacht bestand, sie könnten derartige Anschläge vorbereiten, Identitätsfeststellungen durchgeführt, z. B. bei den Teilnehmern an „antiimperialistischen Stadtrundfahrten". Zur Gefahrenabwehr (§§ 14 ASOG, 9 BlnDSG) wurden diese Daten aufbewahrt und in die „Arbeitsdatei politisch motivierte Straftat" eingespeichert, die dem Berliner Polizeipräsidenten ausschließlich für Zwecke der Gefahrenabwehr und Strafverfolgung bei Staatsschutzdelikten zur Verfügung steht. Da im Laufe der IWF-Tagung keine Erkenntnisse anfielen, die Anlaß für weitere Ermittlungen boten, wurden diese Daten nach Beendigung der Gefahrenlage vernichtet. Einspeicherungen in APIS wurden nicht vorgenommen. Eine Überprüfung ergab hier keinen Anlaß für Beanstandungen.

Erneut wurde schließlich eine große Anzahl Sicherheitsüberprüfungen bei Personen vorgenommen, die mit Dienstleistungen während der Tagung beschäftigt waren. Die in der Regel von Arbeitgebern erhobenen Daten wurden sofort nach Beendigung der Tagung vernichtet. Für die Zulässigkeit der Datenerhebungen kann auch hier nur der Übergangsbonus in Anspruch genommen werden, der angesichts des überwiegenden Interesses an der Verhinderung von Straftaten während der Tagung einzuräumen war.

Aufgrund einer Bitte des Unterausschusses Datenschutz des Innenausschusses habe ich überprüft, ob die Vergabe von *personengebundenen Hinweisen* in ISVB und INPOL ordnungsgemäß erfolgte.

Das Ergebnis bestätigte, daß der Umgang mit diesen Merkmalen dringend verbessert werden muß. So war in der von mir herangezogenen Stichprobe nur in einem verschwindend kleinen Teil der Akten die Eingabe des Hinweises dokumentiert. Der Grund der Eingabe war in einem Viertel der Fälle überhaupt nicht erkennbar, in einem weiteren Viertel reichten die Erkenntnisse für eine Vergabe nicht aus. Von den ursprünglich zu recht eingegebenen Hinweisen hätte wiederum die Hälfte wegen Zeitablaufs oder des Verfahrensausgangs wieder gelöscht werden müssen.

Auf Veranlassung des Unterausschusses faßte das Abgeordnetenhaus einen Beschluß mit dem der Senat aufgefordert wurde, zu veranlassen, daß die Speicherung der Merkmale „geisteskrank, geistesschwach, Prostitution, häufig wechselnder Aufenthaltsort, Ansteckungsgefahr bzw. Vorsicht Blutkontakt, Land- und Stadtstreicher sowie Entmündigung unterbleibt und die bestehenden Datensätze zu löschen sind.

Ich erwarte von dem inzwischen ebenfalls erfolgten Beschluß der Innenministerkonferenz eine grundsätzliche Besserung der Situation. Für den Polizeipräsidenten ist eine Revision aller Akten geboten, zu denen personengebundene Hinweise vergeben sind. Die Durchführung der Revision werde ich überprüfen.

Meldewesen

Die folgenden Beispiele belegen, daß Inhalt und Durchführung des Meldegesetzes nach wie vor zu Beschwerden führen.

Ein Amtsvormund hatte die Mutter eines *nichtehelichen Kindes* überredet, den verheirateten Vater zu benennen. Die Zusage, die Angaben würden geheimgehalten und auch keiner dritten Behörde übermittelt, veranlaßte die Kindesmutter, den Namen des Kindesvaters, der die Vaterschaft auch anerkannt hatte, bekanntzugeben. Einige Monate später beantragte der Kindesvater einen neuen Personalausweis. Seine Ehefrau, die den Ausweis abholte, stellte erstaunt fest, daß nicht nur die gemeinsamen ehelichen Kinder, sondern auch das ihr noch unbekannte nichteheliche Kind eingetragen waren.

Bei meiner Überprüfung habe ich festgestellt, daß das Bezirksamt die Vaterschaftsanerkennung nach § 29 Personenstandsgesetz (PStG) dem Standesamt mitteilte, das seinerseits im Geburtenbuch einen entsprechenden Randvermerk eintrug. Diese Änderung im Geburtenbuch gab das Standesamt nach § 70 PStG in Verbindung mit § 98 Dienstanweisung für die Standesbeamten und ihre Aufsichtsbehörden der Meldebehörde bekannt. Nach § 2 Abs. 1 Nr. 15 Meldegesetz speichert die Meldebehörde im Datensatz der Eltern die Daten ihrer minderjährigen Kinder (Vor- und Familiennamen, Tag der Geburt, Sterbetag). Das Meldegesetz differenziert hier nicht zwischen ehelichen und nichtehelichen Kindern, stellt auch nicht auf die gemeinsame Wohnung ab.

Die in den behelfsmäßigen Personalausweis einzutragenden personenbezogenen Daten des Antragstellers sind dem Melderegister zu entnehmen (§ 2 Abs. 2 Verordnung zur Durchführung der BK/O (46) 61). Auf Antrag des Ausweisinhabers können die Namen und Geburtsdaten von Kindern unter sechs Jahren, die ihre Hauptwohnung in Berlin haben und für die dem Ausweisinhaber oder der Ausweisinhaberin als Vater oder Mutter das Personensorgerecht zusteht, eingetragen werden. Zur Ausstellung des neuen maschinenlesbaren Personalausweises wird der Antrag maschinell aus dem Bestand des Melderegisters ausgedruckt. Da es die Meldestelle entgegen der VO BK/O unterließ, das Sorgerecht zu prüfen, wurden in den Antrag nicht nur die Daten der ehelichen Kinder des Kindesvaters unter sechs Jahren, sondern auch des nichtehelichen Kindes eingedruckt, da auch diese in seinem Datensatz gespeichert sind. Da der Antrag ordnungsgemäß unterschrieben war, wurde der Ausweis auch so ausgestellt. Die pikante Situation entstand also deshalb, weil die Meldestelle eine notwendige Prüfung unterließ, aber andererseits auch der Kindesvater den Antrag nicht mit der gebotenen Sorgfalt durchgelesen hatte.

Um die korrekte Umsetzung der VO BK/O sicherzustellen, muß eine Programmänderung vorgenommen werden, damit nur noch die Kinder über das Ausweisprogramm im maschinell ausgedruckten Antrag erscheinen, für die der Antragsteller auch das Sorgerecht hat.

Grundsätzliche Zweifel habe ich an der Speicherung der Daten von nichtehelichen Kindern im Datensatz des nicht sorgeberechtigten Elternteils geäußert. Die Erforderlichkeit sehe ich nur für steuerliche Zwecke. In diesem Fall wäre aber eine strenge Zweckbindung geboten.

Mit dem in der Anlage zum Meldegesetz vorgeschriebenen Anmeldeformular werden beim Meldepflichtigen der Rufname und die Art des Mietverhältnisses erhoben und im Melderegister gespeichert, ohne daß das Meldegesetz dies ausdrücklich vorsieht.

Zwar ist der *Rufname* ein Vorname, der im Melderegister gespeichert werden darf (§ 2 Abs. 1 Nr. 3 Melderegister). Aber durch die Kennzeichnung wird aus einem von möglicherweise mehreren Vornamen ein neues Merkmal, der Rufname. Dieses zusätzliche Herkmal ist nicht im Katalog der Daten, die nach § 2 Meldegesetz gespeichert werden dürfen, enthalten. Für die Speicherung fehlt damit die Rechtsgrundlage. Auch in den einschlägigen Personalausweisbestimmungen wird nur vom Vornamen gesprochen (§ 5 VO BK/O, § 6 Paßgesetz). Ich habe den Senator für Inneres darauf hingewiesen, daß damit die Kennzeichnung des Rufnamens nur auf freiwilliger Basis zulässig ist. Der Senator für Inneres hält die Erhebung dagegen mit dem Meldegesetz für vereinbar.

Die bei der Anmeldung erhobenen Daten des *Wohnungsgebers* nach § 2 Abs. 2 Nr. 6 Meldegesetz dürfen nur für den dort genannten Zweck, nämlich die Feststellung der Mitwirkungspflichtigen nach § 13 Meldegesetz, erhoben und gespeichert werden. Dies geschieht durch die Angabe des Namens und der Anschrift sowie der Unterschrift durch den Wohnungsgeber. Die weitergehende Verwendung des Namens des Wohnungsgebers als Adressierungszusatz ist dagegen auch nicht durch § 2 Abs. 1 Nr. 11 Meldegesetz abgedeckt, da danach lediglich gegenwärtige und frühere Anschriften sowie die Haupt- und Nebenwohnung gespeichert werden dürfen, nicht aber, in welchem privatrechtlichen Verhältnis der Betroffene zum Wohnungsgeber steht, noch welche Namen der Wohnungsgeber hat. Auch hier muß es dem Meldepflichtigen selbst überlassen werden, unter welchem Namen er bei der entsprechenden Anschrift anzutreffen ist (eigener Name, Firmenname, Name des Wohnungsgebers usw.).

Der Senator für Inneres wendete ein, das Melderegister habe auch die ordnungsgemäße Postzustellung zu sichern.

Nach § 1 Meldegesetz hat die Meldebehörde die Aufgabe, die in dem jeweiligen Geltungsbereich wohnhaften Bürger nach Maßgabe der Vorschriften des Meldegesetzes zu registrieren, um ihre Identität und Wohnungen festzustellen und nachweisen zu können. In diesem Rahmen hat die Meldebehörde nur die Tatsachen festzuhalten und unter Umständen darüber Auskunft zu geben, daß eine bestimmte Wohnung zu einer bestimmten Person gemeldet ist. Es hat jedoch nicht sicherzustellen, daß der Betroffene auch unter der angegebenen Adresse postalisch zu erreichen ist.

Meiner Empfehlung, die Anlage zur DVO-Meldegesetz zu ändern, folgte der Senator für Inneres nicht. Er war lediglich bereit, in den Erläuterungen zu den Feldern des Meldescheines die Erhebung selbst näher zu erklären, ohne aber von der bisherigen Praxis des Erhebens und Speicherns der Merkmale Rufname und Adressenzusatz Abstand zu nehmen.

In Bußgeldverfahren bei der *Volkszählung* hatte das Statistische Landesamt das Landeseinwohneramt um Mitteilung der neuen bzw. vollständigen Anschrift solcher Personen gebeten, deren Anhörungsbogen mit der Post unter der bisherigen Anschrift nicht zugestellt werde konnte. Das Landeseinwohneramt erteilte die entsprechenden Auskünfte, ohne bei dem jeweiligen Datensatz zu protokollieren, daß er dem Statistischen Landesamt übermittelt worden war. Damit sollten das Risiko eines Melderegisterabgleichs und entsprechender melderechtlicher Maßnahmen gegen Personen ausgeschlossen werden, die ihre Meldepflicht verletzt hatten.

Durch dieses Vorgehen der Meldebehörde wurde die melderechtlich gebotene Übermittlungskontrolle umgangen. Das Meldegesetz enthält zwar ausdrücklich Vorschriften zur Protokollierung nur bei der Übermittlung von Meldedaten an Strafermittlungs-, Strafverfolgungs-, Strafvollzugs- und Strafvollstrekkungsbehörden sowie an Verfassungsschutzbehörden (§ 25 Abs. 4 Meldegesetz) sowie bei automatisierten Abrufverfahren (§ 26 Abs. 3 S. 3 Meldegesetz). Dies bedeutet jedoch nicht, daß in allen anderen Fällen, in denen Behörden Auskünfte bei der Meldebehörde einholen, eine Protokollierung des Datenempfängers unterbleiben kann. Anderenfalls würden in großem Umfang unkontrollierbare Datenflüsse entstehen, so daß der Forderung des Bundesverfassungsgerichts nicht entsprochen würde, daß der Bürger wissen können muß, wer was wann und bei welcher Gelegenheit über ihn weiß. Bereits nach allgemeinem Datenschutzrecht gehört die Übermittlungskontrolle zu den unabdingbaren technisch-organisatorischen Maßnahmen, die jede speichernde Stelle zur Datensicherung zu treffen hat. Der Gesetzgeber wollte die Meldebehörde hiervon auch bezüglich der einfachen Melderegisterauskünfte nicht ausnehmen.

Bei der parlamentarischen Beratung des Meldegesetzes bestand allerdings Einvernehmen darüber, daß private Empfänger einfacher Melderegisterauskünfte nicht in Protokolldateien gespeichert werden sollten, weil dadurch deren Persönlichkeitsrechte beeinträchtigt würden. In derartigen Fällen müßte sich die Protokollierung darauf beschränken, daß auf diesen Datensatz zugegriffen worden ist.

Da die Meldebehörde meine Auffassung in diesem Punkt nicht teilt, würde ich es begrüßen, wenn der Gesetzgeber so bald wie möglich eine entsprechende Klarstellung ins Meldegesetz aufnehmen würde.

4.6 Justiz

Automation bei der Staatsanwaltschaft

Im Jahr 1984 hat die Staatsanwaltschaft das *ADV-Verfahren ASTA* in Betrieb genommen. An der Planungsphase bin ich umfassend beteiligt worden. Mit diesem System sollen strafrechtliche Ermittlungen durch aktuelle und fehlerfreie Auskünfte über alle anhängigen und abgeschlossenen Verfahren gegen Beschuldigte erleichtert und beschleunigt werden. ASTA enthält neben den personenbezogenen Daten der betroffenen Personen die Angabe des jeweiligen Delikts und das Aktenzeichen des Verfahrens. Auf diese Weise rationalisiert das System die Arbeit der Geschäftsleitung, der Geschäftsstellen sowie der Schreibstellen und insbesondere die Führung der zentralen Namenskartei der Staatsanwaltschaft bei dem Landgericht. ASTA dient zudem der Überwachung der Haftverhältnisse, der Einhaltung der Hauptverhandlungstermine und der Erstellung von Statistiken.

Der Datenverarbeitung in ASTA kommt angesichts der Sensibilität der darin enthaltenen Informationen besondere Bedeutung zu. Eine gesetzliche Grundlage für ADV-Systeme ist nicht vorhanden. Aus Gründen der Praktikabilität halte ich zwar die Weiterführung derartiger Systeme im Hinblick auf die zu erwartende Regelung für zulässig, jedoch muß auch hier die Datenverarbeitung auf das für die Aufgabererfüllung der jeweiligen Stelle unumgänglich Erforderliche beschränkt werden.

Gemessen an diesen Anforderungen hält ASTA im wesentlichen den datenschutzrechtliche Kriterien stand. Dennoch waren einzelne Mängel festzustellen:

Als speichernde Stelle im Sinne § 4 Abs. 3 BlnDSG wurde für ASTA die Generalstaatsanwaltschaft bei dem Kammergericht eingesetzt. Bereits früher hatte ich darauf hingewiesen, daß ein Online-Zugriff auf den Gesamtbestand für die Erfüllung der Aufgaben der Staatsanwaltschaft bei dem Kammergericht nach meiner Auffassung nicht erforderlich ist. Dementsprechend hatte ich empfohlen, die Online-Verbindung zur Staatsanwaltschaft bei dem Kammergericht durch geeignete programmtechnische Maßnahmen auf den Zugriff auf diejenigen Vorgangsdaten zu beschränken, mit denen die Staatsanwaltschaft des Kammergerichts befaßt ist. Der Senat widersprach dieser Auffassung.

Allerdings kann auch die Einsetzung der Generalstaatsanwaltschaft bei dem Kammergericht als speichernde Stelle nicht die Möglichkeit des unmittelbaren Zugriffs auf den Gesamtbestand rechtfertigen. Speichernde Stelle ist gem. § 4 Abs. 3 Ziff. 1 BlnDSG jede Behörde oder sonstige öffentliche Stelle, die Daten für sich selbst speichert oder durch andere speichern läßt. Die Bestimmung der speichernden Stelle steht damit nicht zur Disposition, sondern ist davon abhängig, welche Stelle die Daten zur Erfüllung der gesetzlich zugewiesenen Aufgaben benötigt.

Da das System ASTA eine Datensammlung sowohl für die Generalstaatsanwaltschaft bei dem Kammergericht als auch für die Generalstaatsanwaltschaft bei dem Landgericht und die Amtsanwaltschaft darstellt, dient es der Aufgabenerfüllung für alle drei Strafverfolgungsbehörden. Daher ist eine Zuweisung als speichernde Stelle gem. § 4 Abs. 3 Ziff. 1 BlnDSG in der Weise geboten, daß eine dieser Strafverfolgungsbehörden Daten für sich selbst speichert und für die beiden anderen im Auftrag tätig wird.

Die Kompetenz der Generalstaatsanwaltschaft bei dem Kammergericht gem. § 147 Gerichtsverfassungsgesetz, an die nachgeordneten Staatsanwaltschaften fachliche Weisungen zu geben, wird durch die Benennung der speichernden Stelle nicht berührt. Diese Befugnis steht der Generalstaatsanwaltschaft bei dem Kammergericht im Rahmen der Weisungsstränge ohnehin zu.

Da es sich bei ASTA sowohl um ein Vorgangs- als auch um ein Dokumentationssystem handelt, werden sämtliche Personen, gegen die ermittelt wird, eingetragen. Daher werden auch Daten von Kindern im ASTA-System gespeichert, obwohl bei diesen aufgrund ihrer Schuldunfähigkeit (§ 19 StGB) ein Verfahrenshindernis vorliegt. Da aber gerade bei Kindern eine spätere Verwertung der Erkenntnisse zu unverhältnismäßigen Nachteilen führen kann, sollte die Speicherung von personenbezogenen Daten von Kindern auf das unerläßliche Ausmaß beschränkt werden. Dies kann zum einen erfolgen, indem der Zugriff auf die Daten von Kindern auf die bei der Staatsanwaltschaft zuständige Abteilung beschränkt wird. Zum anderen sollte die Speicherungsdauer auf eine kurze Zeit begrenzt werden, um die Verwertung von Bagatell-Delikten und lange zurückliegenden Vorfällen einzuschränken oder zu verhindern.

Mit ASTA werden auch betriebsinterne Statistiken erstellt. Dabei werden bestimmte Deliktgruppen erfaßt, z. B. Ladendiebstahl und Verkehrssachen. Bei einigen der Merkmale habe ich Zweifel an der Erforderlichkeit der statistischen Erfassung geltend gemacht, insbesondere wenn die Fallzahlen gering sind. So habe ich die gesonderte statistische Erfassung der Volkszählungsverfahren bemängelt. Es handelt sich hierbei im Regelfall um Verfahren aufgrund §§ 303, 304 StGB, d. h. um Sachbeschädigungen. Da diese Sachbeschädigungen von der Staatsanwaltschaft nicht anders behandelt werden als andere Sachbeschädigungen auch, ist ein Grund für die gesonderte Erfassung nicht ersichtlich. Zudem kann eine Statistik nur einen Sinn haben, wenn ihr entsprechende Vergleichszahlen gegenübergestellt werden können. Bei der Erfassung von Volkszählungsverfahren sind Vergleichszahlen weder vorhanden noch in absehbarer Zeit zu erwarten.

Bei der schon mehrfach geforderten Rückmeldung des Verfahrensausgangs an ASTA bzw. an ISVB zeichnet sich eine Lösung ab. Wenn ein Verfahren zu einer Anklageerhebung durch die Staatsanwaltschaft führt, wird bisher das Ergebnis des darauf folgenden Gerichtsverfahrens nicht eingetragen. Das kann, wenn das Gerichtsurteil von der staatsanwaltschaftlichen Bewertung abweicht, in der ASTA-Datei ein falsches Bild des Beschuldigten ergeben. Wie bereits früher ausgeführt, wird durch das Fehlen dieser Angabe die dem Benutzer vermittelte Information unvollständig und nicht mit der Realität übereinstimmend, also unrichtig. Die Staatsanwaltschaft hat hierfür ein automatisiertes Rückmeldeverfahren entwickelt. Jedoch ergeben sich Schwierigkeiten dann, wenn unterschiedliche Beurteilungen des Sachverhalts durch die Polizei, die Staatsanwaltschaft und die Gerichte vorgenommen werden sowie wenn Verfahren abgetrennt oder verbunden werden.

Die Überprüfung des ASTA-Verfahrens hinsichtlich der technisch-organisatorischen Maßnahmen zum Datenschutz und der Ordnungsmäßigkeit ergab, daß zwar die Dokumentation des Gesamtverfahrens und der einzelnen Programme, die mit technischer Unterstützung vorgehalten werden, einem sachverständigen Dritten ausreichend Transparenz verschafft, daß jedoch die vorhandenen Protokollierungen die ordnungsgemäße Anwendung von ASTA nicht vollständig nachvollziehbar machen und, insbesondere im Anwenderbereich, den Geschäftsstellen der Staatsanwaltschaft, häufig kein ausreichender Schutz gegen unbefugte Kenntnisnahme der Daten durch Dritte besteht.

Zwar werden Eingaben, Veränderungen, Löschungen und Auswertungen im Batch-Betrieb protokolliert, nicht jedoch die Online-Abfragen. Angesichts der hohen Schutzbedürftigkeit der programmbezogenen Daten in ASTA ist eine solche Protokollierung jedoch angemessen und zur Vermeidung mißbräuchlicher Zugriffe auch notwendig.

Die Aufstellung der Sachbearbeiterterminals wurde in zahlreichen Geschäftsstellen überprüft. Dabei wurde festgestellt, daß nur in wenigen Zimmern die Aufstellung der Terminals den Anforderungen des Datenschutzes voll entspricht. Zum Teil waren die Bildschirme so aufgestellt, daß eintretende Besucher unmittelbar Einblick auf Bildschirme erhalten; zum Teil können sich Besucher Einsicht verschaffen, ohne daß Mitarbeiter der Geschäftsstellen wirksam dagegen einschreiten können. Als Ursache dafür ist neben der häufig zweifellos beengten Raumsituation das Fehlen jeglicher organisatorischer Regelungen zur Aufstellung von Datensichtgeräten in den Geschäftsstellen zu sehen. Vielmehr wird es den jeweiligen Geschäftsstellenmitarbeitern freigestellt, die Datensichgeräte nach eigenem Gutdünken aufzustellen. Dabei sind Belange des Datenschutzes meist nicht einbezogen worden.

Ich habe daher empfohlen, in einer Dienstanweisung festzulegen, daß die ASTA-Datensichtstationen in den Geschäftsstellen so aufzustellen sind, daß die unbefugte Einsichtnahme durch Besucher vermieden wird.

Nebenbei habe ich festgestellt, daß die Unterbringung von Akten und Karteien in den Geschäftsstellen bei weitem nicht den Sicherheitsanforderungen entspricht, die an die Unterbringung solcher Unterlagen zu stellen sind: Handakten und dazugehörige Hefter lagen in offenen Regalen, in vielen Räumen stapelten sich Aktentürme auf Tischen, Beistelltheken und Konsolen, häufig frei zugänglich für Besucher und unbefugtes Personal, z. B. Reinigungskräfte, die außerhalb der Bürozeiten dort tätig werden.

Zentrales Handelsregister

Eine Firma in Frankfurt plant, ein zentrales Handelsregister zu erstellen. Dafür sollen die Amtsgerichte die Daten aus den örtlichen Handelsregistern übermitteln, die dann in automatisierter Form zusammengestellt und bundesweit gegen Entgelt angeboten werden sollen. Auch in Berlin ist diese Firma an die Amtsgerichte mit der Bitte um Überlassung der Handelsregisterdaten herangetreten.

Datenschutzrechtlich bestehen gegen eine solche Überlassung erhebliche Bedenken: Das Handelsregister enthält personenbezogene Daten, beispielsweise über Namen und Anschrift der Gesellschafter. Für die Übermittlung dieser und firmenbezogener Daten aus dem Handelsregister enthält § 9 Handelsgesetzbuch (HGB) eine bereichsspezifische Regelung, nach der die Einsicht in das Register jedermann ohne Nachweis eines berechtigten Interesses gestattet ist.

Diese Vorschrift kann eine Übermittlung des gesamten Datenbestandes im Wege der Verfilmung des Registers allerdings nicht rechtfertigen. Schon dem Wortsinn nach kann die Möglichkeit der Einsicht nicht die Abnahme des gesamten Registerinhalts beinhalten.

Es kommt hinzu, daß durch die Überlassung der Registerdaten die örtlichen Handelsregister praktisch in private Hand überführt und zentral zusammengefaßt werden. Diese zentrale Zusammenfassung und die Auswertungsmöglichkeiten nach unterschiedlichsten Gesichtspunkten bilden eine neue Qualität, die über die Vorschriften des HGB hinausgeht. Der Gesetzgeber hat zudem in § 8 HGB zum Ausdruck gebracht, daß das Handelsregister dezentral von den Gerichten geführt wird. Die Zulassung eines zentralen, privaten Nebenhandelsregisters ist damit nicht vereinbar. Auch der Justizsenator vertritt diese Auffassung und hat daher eine Überlassung des Handelsregisters an die Firma unterbunden.

Die Firma hat gegen diese Ablehnung beim Kammergericht Klage erhoben mit dem Ziel, Abschriften im Wege der Mikroverfilmung aus dem Handelsregister zu erhalten, um die Datenbank zu erstellen. Die Firma beruft sich insbesondere auf eine Richtlinie der EG, wonach es Dritten möglich sein muß, vollständige oder auszugsweise Abschriften von bei den Registern hinterlegten Unterlagen zu erhalten. Dies ist nach Auffassung der Firma nur bei einem zentralen Handelsregister möglich. Dem ist entgegenzuhalten, daß die Richtlinie keinen Staat der EG zur Errichtung von zentralen Handelsregistern verpflichtet und auch bei der vom HGB vorgeschriebenen Verfahrensweise die Auskunftsrechte nicht eingeschränkt werden. Das Kammergericht hat noch nicht entschieden.

Datenschutzdelikte

Die Justiz mußte sich auch mit Straftaten gegen datenschutzrechtliche Bestimmungen befassen. Ein Beispiel:

In der Tagespresse sind unter der Rubrik Heim- und Nebenverdienst Inserate von Detekteien erschienen, mit der Sozialversicherungs- und Arbeitsamtsangestellte für Auskünfte als Nebentätigkeit angeworben werden sollten. Mitarbeiter der Sozialleistungsträger sollten offenbar dazu angehalten werden, Kenntnisse über personenbezogene Daten, die sie im Rahmen ihrer dienstlichen Obliegenheiten erhalten haben, geschäftsmäßig für private Zwecke zu verwenden. Die Staatsanwaltschaft hat ermittelt, daß der Beschuldigte versucht hatte, Beamten und Angestellten verschiedener Behörden (darunter auch Stellen des Landes Berlin) Geld für die pflichtwidrige Übermittlung personenbezogener Daten aus den diesen Personen zugänglichen Datenbeständen anzubieten, und sich somit wegen Bestechung strafbar gemacht hat. Gegen den Beschuldigten ist ein Strafbefehl erlassen worden.

4.7 Kulturelle Angelegenheiten

Archivwesen

Vom Senator für Kulturelle Angelegenheiten wurde der Entwurf eines *Archivgesetzes* vom Januar 1985, der auf der Grundlage eines Musterentwurfs der Datenschutzbeauftragten des Bundes und der Länder erstellt worden war, wieder aufgegriffen, nachdem nach dem Inkrafttreten des Bundesarchivgesetzes eine gesetzliche Regelung angemahnt worden war.

Die neue Vorlage enthält die Regelung, daß zugunsten von Forschungsvorhaben „die Rechte Betroffener ganz zurücktreten": Auch ein Grundrecht (hier das Grundrecht auf Forschung) kann nicht derart ausgedehnt werden, daß das Persönlichkeitsrecht eines anderen völlig zurücktritt. Schon in einer früheren Stellungnahme hatte ich darauf hingewiesen, daß durch den Gesetzgeber selbst Entscheidungsmaßstäbe festgelegt werden müßten, unter welchen Voraussetzungen eine Verkürzung der Sperrfristen möglich sein soll. Wissenschaftliche Forschung ist angesichts ihres abstrakten Wertgehaltes für sich allein kein hinreichendes Entscheidungskriterium. Vielmehr hat der Gesetzgeber festzulegen, unter welchen konkreten Voraussetzungen Persönlichkeitsrechte gegenüber der wissenschaftlichen Forschung zurückzutreten haben. Ferner hat der Gesetzgeber das Entscheidungsverfahren festzulegen, insbesondere die zuständige Stelle zu benennen. Trotz dieser verbesserungsbedürftigen Punkte hätte ich es begrüßt, wenn der Entwurf noch in dieser Legislaturperiode ins Parlament eingebracht worden wäre.

Dem Abgeordnetenhaus liegt allerdings bereits ein Antrag der AL-Fraktion über ein Archivgesetz des Landes Berlin vom 6. November 1987[1] vor. In der parlamentarischen Erörterung des Gesetzentwurfs habe ich vor allem auf folgendes aufmerksam gemacht: Außer einer nicht wünschenswerten Tendenz zur Bürokratisierung der Archivnutzung erscheint mir vor allem die vollständige Freigabe von Daten aus den Archiven vor dem 8. Mai 1945 insbesondere derjenigen Personen bedenklich, die weder den Nationalsozialisten noch den Verfolgten zugerechnet werden können. Ohne Zweifel müssen auch die Daten von heute lebenden Bürger aus der Zeit vor dem 8. Mai 1945 weiter geschützt werden, soweit dies mit dem Zweck der Erforschung des Nationalsozialismus vereinbar ist.

Die Dringlichkeit einer archivrechtlichen Regelung zeigten mehrere *Forschungsprojekte:* Wegen der fehlenden gesetzlichen Regelung mußten dabei die verfassungsrechtlichen Grundsätze, die vom Bundesverfassungsgericht[2] entwickelt wurden, zugrundegelegt werden. Das Bundesverfassungsgericht hat entschieden, daß das Schutzbedürfnis und entsprechend die Schutzverpflichtung in dem Maße schwindet, in dem die Erinnerung an den Verstorbenen verblaßt und im Laufe der Zeit auch das Interesse an der Nichtverfälschung des Lebensbildes abnimmt. Angesichts dieses allgemeinen Grundsatzes habe ich die Nutzung des Archivmaterials zu Forschungszwecken nicht beanstandet, wenn der Todeszeitpunkt mehr als 30 Jahre zurücklag. In einem anderen Fall habe ich auch gegen den Einblick in Krankengeschichten für ein Forschungsprojekt über die Euthanasie keine Einwände erhoben.

Bibliotheken

Sehr unbeweglich zeigte sich die Kulturverwaltung bei der Frage einer datenschutzgerechten Regelung des Bibliothekswesen. Auch das inzwischen privatrechtlich ausgestaltete Benutzungsverhältnis enthebt die Einrichtung nicht der Verpflichtung, den Datenschutz zu gewährleisten und vor allem hinreichende Rechtsgrundlagen zu schaffen. Weder ist für das Ausleihverfahren eine Datenschutzregelung in die Benutzungsbedingungen aufgenommen worden, obwohl ich dies dringend angeraten hatte, noch ist die Absicht erkennbar, daß die Datenerhebung für den geplanten Datenverbund auf eine gesetzliche Grundlage gestellt wird. Die Einführung der automatischen Datenverarbeitung wäre zu beanstanden, wenn es nicht bis dahin gelungen ist, hinreichende Rechtsgrundlagen für den Umgang mit den personenbezogenen Daten zu schaffen.

4.8 Schulwesen

Die Senatsschulverwaltung hat die erforderliche *Ergänzung des Schulgesetzes* um bereichsspezifische Datenschutzregelungen bis zur Novellierung des Verwaltungsverfahrensgesetzes des Bundes zurückgestellt. Allerdings hat sich die Erwartung des Senats, daß auf Bundesebene bis Mitte des Jahres ein entsprechender Gesetzentwurf vorgelegt würde, nicht erfüllt.

Die Schulverwaltung hat mir nunmehr mitgeteilt, erst im Sommer 1989 sei die Einbringung eines entsprechenden Gesetzentwurfs in das neugewählte Abgeordnetenhaus beabsichtigt. Ich bedauere diese weitere Verzögerung: Auch im Schulbereich neigt sich der vom Bundesverfassungsgericht anerkannte Übergangsbonus für Maßnahmen ohne normenklare gesetzliche Grundlage dem Ende zu.

Auf Grund eines Beschlusses des Innenausschusses hat die Senatsverwaltung mir erstmals die Gründe dafür erläutert, daß ihr nach dem Entwurf zur Änderung der *Ausführungsvorschriften über die dienstliche Beurteilung der Beamten des Schul- und Schulaufsichtsdienstes* (AV-Lehrerbeurteilung) alle dienstlichen Beurteilungen vorgelegt werden sollen. Meine Einwände gegen dieses Vorhaben sind dadurch nicht ausgeräumt worden. Die Senatsschulverwaltung hat die Inkraftsetzung der AV-Lehrerbeurteilung bis zum Abschluß eines Rechtsstreits mit dem Hauptpersonalrat aufgeschoben. In zwei weiteren Fällen der Übermittlung von Lehrerpersonaldaten wurde meine Überprüfungstätigkeit erneut dadurch erschwert, daß die Senatsverwaltung mir entgegen einem Beschluß des Unterausschusses Datenschutz die Kontrollkompetenz im Bereich der Lehrerpersonalakten absprach. Dabei hat das Bundesverfassungsgericht[1] hervorgehoben, daß das Recht auf informationelle Selbstbestimmung sich nicht auf den jeweiligen Anwendungsbereich der Datenschutzgesetze des Bundes und der Länder oder datenschutzrelevanter gesetzlicher Sonderregelungen beschränkt.

Erst der Presse entnahm ich, daß der Erlaß von neuen *Ausführungsvorschriften über die Erziehungs- und Ordnungsmaßnahmen an der Berliner Schule* (AV-EOM) geplant sei. Er sah vor, daß bei Berufsschülern vor oder neben Erziehungs- und insbesondere Ordnungsmaßnahmen in der Regel „Kontakte" mit dem Ausbildungsbetrieb aufzunehmen seien. Ich habe darauf hingewiesen, daß diese unbestimmte Formulierung nicht ausschließt, daß dem Ausbildungsbetrieb auch geplante oder verhängte Erziehungs- und Ordnungsmaßnahmen mitgeteilt werden. Da es sich bei dem Ausbildungsbetrieb jedoch um eine nicht-öffentliche Stelle handelt, und das Berufsbildungsgesetz keine Übermittlungsbefugnis für diesen Fall enthält, würde dies die Einwilligung des betroffenen Schülers voraussetzen (vgl. § 11 Abs. 1 Satz 1 BlnDSG). Auch das Erfordernis einer vertrauensvollen Zusammenarbeit zwischen Berufsschule und Ausbildungsbetrieb, auf das sich die Schulverwaltung berufen hat, rechtfertigt so lange nicht die Weitergabe personenbezogener Informationen, wie keine normen-

[1] Abgeordnetenhaus Drs. 10/1837

[2] Insbesondere im „Mephisto-Urteil", vgl. BVerfGE 30, 173 (196)

[1] Beschluß v. 9. März 1988 (1 BvL 49/86)

klare und bereichsspezifische Regelung derartiger Datenübermittlungen besteht. Die Ausführungsvorschriften wurden nur mit einer geringfügigen Änderung in Kraft gesetzt, die die Kontaktaufnahme zwischen Berufsschule und Ausbildungsbetrieb „erforderlichenfalls" vorschreibt. Dadurch sind meine datenschutzrechtlichen Einwände nicht ausgeräumt worden.

Die Senatsschulverwaltung leitete mir den Entwurf von neuen *Ausführungsvorschriften über Noten und Zeugnisse* (AV-Noten und Zeugnisse) zu, der entsprechend den bisher geltenden Vorschriften festlegt, daß Abgangs- und Abschlußzeugnisse keine Angaben über Fehlzeiten, Verspätungen, Nichtversetzung oder Ordnungsmaßnahmen enthalten dürfen. Unter „Bemerkungen" dürfen auf Abgangs- und Abschlußzeugnissen Aussagen über das allgemeine Verhalten, den Bildungswillen und die Mitarbeit des Schülers nur dann getroffen werden, wenn diese seinem Fortkommen dienlich sind.

Dieser Regelung liegt der zutreffende Gedanke zugrunde, daß Abgangs- und Abschlußzeugnisse von dem betroffenen Schüler häufig im außerschulischen Bereich verwendet und insbesondere bei Bewerbungen vorgelegt werden müssen. Durch den mittelbaren Zwang, derartige Angaben zusammen mit den Zeugnisnoten zu offenbaren, würde das Fortkommen des Schülers in aller Regel beeinträchtigt.

Schüler bewerben sich ab einer bestimmten Klassenstufe häufig bereits um Ausbildungsplätze oder Stellen, bevor sie ein Abgangs- oder Abschlußzeugnis erhalten haben. Sie müssen dann ihr letztes Halbjahreszeugnis, auf Verlangen vieler Arbeitgeber sogar mehrere ältere Halbjahreszeugnisse vorlegen. Auf diese Weise würde die beabsichtigte Wirkung der differenzierten Regelung für Abgangs- und Abschlußzeugnisse einerseits und Halbjahreszeugnisse andererseits zunichte gemacht, weil der Schüler dadurch zur Offenlegung der auf seinem Halbjahreszeugnis getroffenen nachteiligen Bemerkungen oder dokumentierten Fehlzeiten und Verspätungen gegenüber privaten Arbeitgebern gezwungen würde. Ich habe deshalb den Verzicht auf die Aufnahme derartiger Informationen in die Halbjahreszeugnisse, zumindest aber ein Verfahren empfohlen, das es dem Schüler ermöglicht, sich während des laufenden Schuljahres bei außerschulischen Stellen zu bewerben, ohne automatisch mit seinen Noten belastende Angaben offenbaren zu müssen.

Die Senatsschulverwaltung ist meinen Empfehlungen nicht gefolgt. Sie hält die Aufnahme dieser Informationen in die Halbjahreszeugnisse aus pädagogischen Gründen für erforderlich und ist der Auffassung, daß dies auch datenschutzrechtlich unbedenklich sei, da die Zeugnise den Schülern und nicht unbefugten Dritten zugänglich gemacht werden. Demgegenüber kann den Erfordernissen einer Dokumentation des gesamten Bildungsganges auch auf andere Weise genügt werden als durch Eintragung in die Halbjahreszeugnisse. So können Fehlzeiten und Verspätungen den Eltern brieflich mitgeteilt und damit im Schülerbogen festgehalten werden. Es ist bemerkenswert, daß in mehreren Bundesländern (z. B. Baden-Württemberg, Niedersachsen und Bremen) Fehlzeiten und Verspätungen entweder überhaupt nicht oder ab einer bestimmten Klassenstufe nicht mehr in Zeugnisse aufgenommen werden oder der Schüler zumindest ein Zwischenzeugnis für Bewerbungszwecke erhalten kann, das derartige Vermerke nicht enthält.

Auch datenschutzrechtlich ist der Standpunkt der Senatsschulverwaltung nicht überzeugend. Die Vorlage von Zeugnissen bei Bewerbungen um Ausbildungs- und Arbeitsplätze ist allgemein üblich. Der Schüler oder Schulabgänger befindet sich bei Bewerbungen deshalb in einer Zwangslage und kann die Vorlage von Zeugnissen mit einem vorgegebenen Inhalt nicht verweigern, wenn er an der Stelle interessiert ist. Von einer freiwilligen Offenbarung durch den Betroffenen, die datenschutzrechtlich ohne Belang ist, kann deshalb keine Rede sein.

Durch die Eingabe des Leiters einer Privatschule bin ich darauf hingewiesen worden, daß sowohl öffentliche als auch private Schulen einmal jährlich klassenweise an das Gesundheitsamt einen ausgefüllten Vordruck *„Masern-Mumps/Röteln-Impfliste* des Gesundheitsamtes" mit Namen und Anschriften der Impflinge und ihrer Erziehungsberechtigten schicken müssen. Die Impfliste enthält auch eine Rubrik für Informationen darüber, daß und aus welchen Gründen die Impfung unterblieben ist (z. B. „Zurückstellung wegen aktiver Tbc, anderer Infektionskrankheiten" usw.). Der für den Vordruck verantwortliche Senator für Gesundheit und Soziales hat mir auf meine Anfrage mitgeteilt, daß es eine Rechtsgrundlage für die Erhebung der Impflistendaten nicht gebe. Schutzimpfungen seien zwar freiwillig und bedürften des Einverständnisses der Personensorgeberechtigten. Um zur Impfung schriftlich einladen und das Einverständnis der Eltern einholen zu können, müßten dem Gesundheitsamt aber Namen und Anschriften mitgeteilt werden. Wenn Eltern ihre Kinder nicht durch das Gesundheitsamt impfen lassen wollten, brauchten sie dies nur der Schule mitzuteilen. Eintragungen in die Impfliste unterblieben dann.

Die Weitergabe von Namen und Anschrift eines Impflings an das Gesundheitsamt bedarf ebenso der Einwilligung der Personensorgeberechtigten wie die Impfung selbst. Diese Einwilligung wird nicht schon dadurch erteilt, daß die betroffenen Eltern einer Weitergabe dieser Daten an das Gesundheitsamt nicht widersprechen. Zudem enthält die Rubrik zum Fernbleiben von der Impfung und den gesundheitlichen Gründen hierfür höchst sensible Daten, die entweder der ärztlichen Schweigepflicht unterliegen oder geeignet sind, den betreffenden Schüler und seine Eltern sozial zu diskriminieren („wegen Fernbleibens vom Impftermin").

Anläßlich einer Eingabe habe ich mehreren Schulen Empfehlungen zur datenschutzgerechten Führung von *Schülerunterlagen* gegeben. Schülerbezogene Informationen dürfen nach der AV Schülerunterlagen in den Schülerbogen aufgenommen werden, wenn sie in der Schule über einen längeren Zeitraum für die Unterrichts- und Erziehungsarbeit sowie für notwendige Verwaltungsarbeiten benötigt werden. Der Klassenlehrer, Kerngruppen- und Oberstufenleiter, der den Schülerbogen führt, sollte in regelmäßigen Abständen prüfen, ob diese Voraussetzungen für die in den Schülerbogen - evtl. auch von einer früheren Schule - aufgenommenen Informationen immer noch vorliegen. Kommt er dabei zu einem negativen Ergebnis, weil er z. B. die weitere Aufbewahrung der Information, daß ein Oberstufenschüler in der Grundschule „Bettnässer" war, nicht für erforderlich hält, so sollte er den Schülerbogen entsprechend bereinigen. Dies gilt nicht für Zeugnisdurchschriften. Außerdem habe ich eine einheitliche datenschutzgerechte Praxis bei der Aufbewahrung von Unfallanzeigen empfohlen, wie ich sie in einer Oberschule festgestellt habe. Dort werden Unfallanzeigen generell nicht zum Schülerbogen, sondern zu eigenen Sachakten genommen. In jedem Fall sollten vor Weitergabe des Schülerbogens bei einem Schulwechsel die Unfallanzeigen herausgenommen bzw. nach einem Schulwechsel erhaltene Schülerbogen von dieser Anzeige bereinigt werden.

4.9 Verkehr und Betriebe

Führerscheindatei

Ein wichtiges Automatisierungsvorhaben des Landeseinwohneramtes betrifft die Einrichtung einer automatisierten Führerscheindatei anstelle der bisher noch manuell geführten Führerscheinkartei. Dabei soll ein bereits in München eingesetztes Verfahren an Berliner Verhältnisse angepaßt werden, da dieses den Anforderungen der Anwender am besten entsprechen soll.

Da es sich bei dem Münchener Verfahren um ein Programmpaket handelt, welches modernen Anforderungen an Anwendungssoftware nicht mehr entspricht, habe ich darauf hingewiesen, daß

- bei ASSEMBLER-programmierten ADV-Verfahren eine sorgfältige und aktuelle schriftliche Verfahrens- und Programmdokumentation vorliegen muß, damit gem. § 16 Satz 2 Nr. 2 BlnDSG die ordnungsgemäße Anwendung der ADV-Programme überwacht werden kann und die Quellprogramme, die wegen der verwendeten Programmiersprache auch für sachverständige Dritte in der Regel kaum lesbar sind, durch die dazugehörige Dokumentation erschließbar sein müssen;

– in ASSEMBLER geschriebene ADV-Verfahren eines besonders hohen Wartungs-, Pflege- bzw. Programmieraufwandes bei gelegentlichen Ergänzungen bedürfen.

Diese Umstände haben erhebliche datenschutzrechtliche Bedeutung: Gegen gebotene Programmodifikationen wird gelegentlich geltend gemacht, daß eine Programmänderung wegen des bei veralteten Programmiermethoden höheren Aufwandes im Sinne von § 5 Abs. 1 Satz 2 BlnDSG unangemessen ist. Der Datenschutz darf bei neu einzuführenden Verfahren nicht durch die Entscheidung für solche Programme beeinträchtigt werden.

Die Datenbestände der Führerscheindatei sollten zunächst unter Verwendung von Datenauszügen des Melderegisters aufgebaut werden. Dabei sollten die aktuellen Adressen und das melderechtliche Ordnungsmerkmal in die Führerscheindatei übernommen werden. Nachdem ich dagegen rechtliche Bedenken geäußert hatte, weil die Adressen für das Führerscheinwesen nicht erforderlich sind und gegen die Übermittlung der Ordnungsmerkmale der Wortlaut des § 3 Abs. 2 Meldegesetz spricht, ist von der Übernahme dieser Daten Abstand genommen worden.

Auf Grund meiner Einwände ist ferner Abstand davon genommen worden, die Ersterfassung der Führerscheindatei mit Listen aus dem Melderegister zu vereinfachen. Vor allem versprach sich das Landeseinwohneramt, mit der Verwendung der Listen Fehler der alten manuellen Führerscheinkartei eliminieren zu können. Das Landeseinwohneramt hat sich von meinen Zweifeln überzeugen lassen, daß auf diese Weise das angestrebte Ziel erreicht werden kann, da die Führerscheinkartei nur die in Berlin ausgestellten Fahrerlaubnisse enthält. Viele dieser Führerscheininhaber leben nicht mehr in Berlin und sind daher nicht mehr im Melderegister verzeichnet. Andererseits enthält das Melderegister im großen Maße Personen, die entweder keinen Führerschein besitzen oder ihren Führerschein in einem anderen Bundesland gemacht haben. Daraus entstehen neue Fehlerquellen, so daß auf diese Weise die Datei nicht sinnvoll zu berichtigen ist. Die Ersterfassung der Führerscheindatei wird also in der Übernahme der bisher manuell in der Kartei erfaßten Daten bestehen.

Die laufende Aktualisierung soll mit Hilfe einer Bereitstellungsdatei vorgenommen werden, die bei der Antragstellung in der Meldestelle aus den Antragsdaten und den aus dem Melderegister abgerufenen Meldedaten täglich erzeugt wird und die dann in die Führerscheindatei eingespielt wird. Ich habe gegen dieses Vorgehen keine Bedenken erhoben, sofern sichergestellt ist, daß damit weder eine Ergänzung der Datengruppen des multifunktionalen ADV-Verfahrens Einwohnerwesen noch eine Online-Verknüpfung zwischen diesem Verfahren und der Führerscheindatei verbunden ist.

Neue Fahrkarten bei der BVG

Im Zuge der Tarifumstellung der BVG wurden auch die Zeitfahrkarten geändert, auf denen das Feld für Name und Anschrift nicht mehr - wie vorher - auf der Rückseite, sondern nunmehr auf der Vorderseite aufgedruckt war. Einige Fahrgäste machten sich Sorgen, daß diese Angaben, auch im Zusammenhang mit dem Foto, beim Vorzeigen von anderen Fahrgästen eingesehen werden und für Einbrüche oder unerwünschte Telefonate mißbraucht werden könnten.

Ich hatte daraufhin mit der BVG Einigkeit erzielt, daß künftig in die neuen Karten eine Passage eingefügt wird, die es dem Inhaber freistellt, die Adresse einzutragen. Auf die Eintragung des Namens kann jedoch nicht verzichtet werden, um bei Kontrollen zumindest eine Identitätsüberprüfung durchführen zu können. Wegen der kurzfristigen Rücknahme der Möglichkeit für den Fahrgast, auch in dem Bus ohne obligatorisches Vorweisen der Karte einsteigen zu können, ist eine wichtige Voraussetzung für das erzielte Einvernehmen entfallen.

Eine Ausnahme stellen allerdings die Jahresnetzkarten und die für ein Jahr im voraus ausgegebenen Monatskarten, die monatlich per Abbuchung bezahlt werden, dar. Hier ersetzt die BVG im Fall des Verlustes oder der Krankheit die Karte, wenn sie nicht genutzt wird. Ein Ersatz kommt nur in Frage, wenn die Identität geprüft wurde, um Doppelausstellungen zu vermeiden.

Entsprechend haben sich die Tarifbestimmungen der BVG geändert, die bisher vorschrieben, daß Name und Anschrift auf der Karte enthalten sein müssen.

4.10 Wirtschaft und Arbeit

Mitgliedererfassung durch die IHK

Die IHK überraschte zahlreiche Berliner mit der Aufforderung, ihren Mitgliederbeitrag zu bezahlen. Dagegen gab es Beschwerden von Personen, die kein Gewerbe (mehr) betrieben. Das Verfahren beruhte auf einer Automatisierung der Datenverarbeitung für die Mitgliedererfassung der IHK, wobei gleichzeitig eine Berichtigung und Bereinigung des Bestandes stattfinden sollte. Betroffen waren nur Kleingewerbetreibende, da von den größeren Gewerbetreibenden ein sicherer Datenbestand vorlag.

Die der IHK bekannten Daten der Gewerbetreibenden werden von den bezirklichen Wirtschaftsämtern, die eine Durchschrift der Gewerbeanmeldung übersenden, angeliefert. Sofern keine Änderungsmitteilung oder eine Abmeldung (beim Bezirk) erfolgte, wurden die Daten auch nicht verändert. Die IHK wies darauf hin, daß ein großer Teil der Personen, die ein Gewerbe nicht mehr weiter betreiben, dies nicht dem Bezirksamt mitteilen. Auch Adressenänderungen werden nicht immer mitgeteilt. Auf diese Weise veralten die Datenbestände. Allerdings kann hieraus der IHK kein Vorwurf gemacht werden, denn es ist grundsätzlich Pflicht der Gewerbetreibenden selbst, Änderungen oder Abmeldungen mitzuteilen. In sämtlichen mir bekannten Fällen ergab sich dann auch, daß die Betroffenen dieser Verpflichtung nicht nachgekommen waren.

Ich habe daher - im Zusammenwirken mit der IHK - empfohlen, die entsprechenden Angaben nachzuholen. Die IHK hat mittlerweile die Mitgliederdaten entsprechend gelöscht oder berichtigt.

Kreditwesen

Über die Automatisierungstendenzen im Kreditwesen, insbesondere im Zusammenhang mit dem automatisierten Zahlungsverkehr habe ich im Vorjahr ausführlich berichtet. Die Entwicklung wird von mir weiterhin aufmerksam beobachtet. Darüber hinaus befaßt sich ein Arbeitskreis der Konferenz der Datenschutzbeauftragten des Bundes und der Länder mit den rechtlichen und technischen Problemstellungen auf diesem sich besonders dynamisch entwickelnden Anwendungsbereich modernster technischer Entwicklungen.

Auch auf anderen, weniger technologisch geprägten Gebieten sind Fortschritte, diesmal eindeutig zugunsten des Datenschutzes, zu verzeichnen: Durch die Neugestaltung der Kassenschalter bei der Sparkasse - zunächst in der Zentrale - wird wesentlich besser als bisher die *Diskretion* der Abwicklung von Bankgeschäften an der Kasse sichergestellt. Der Sparkassenkunde, der an der Kasse Geschäfte abzuwickeln hat, muß für das Gespräch mit dem Kassierer in eine kleine Nische treten, in die eine weitere Person nicht mehr hinzutreten kann.

Weniger erfreulich ist dagegen nach wie vor, daß beim Zusammenwirken zwischen den Kreditinstituten und der *SCHUFA* die Wahrung der schutzwürdigen Belange der Betroffenen nicht immer die notwendige Beachtung findet:

Ein Petent beschwerte sich darüber, daß er von der Sparkasse die Mitteilung erhalten hatte, daß gegen ihn ein Haftbefehl zur Erzwingung einer eidesstattlichen Versicherung vorliegt. Bei der Nachprüfung stellte sich heraus, daß bei der SCHUFA entsprechende Hinweise zu einer anderen Person mit ähnlichem Namen gespeichert waren. Zwar wurde bei der Auskunft an die Sparkasse von der SCHUFA auf die Überprüfungsbedürftigkeit hingewiesen. Dieser Vermerk wurde aber offenbar von der Zweigstelle übersehen und so kam es zu der für den Petenten unangenehmen - weil falschen - Mitteilung.

Ich habe dieses Versäumnis gegenüber dem Kreditinstitut beanstandet und bezüglich der SCHUFA auch den Senator für Inneres als Aufsichtsbehörde für den privaten Bereich eingeschaltet.

Ursache des Mangels ist das Auskunftssystem der SCHUFA. Es arbeitete mit einem Phonetik-Programm, das bei einer Nachfrage auch solche Namen herausgab, die dem Namen der gesuchten Person ähnelten. Die Streuung ging dabei so weit, daß auch Namen gefunden wurden, die kaum noch Ähnlichkeit mit dem

ursprünglich gesuchten Namen hatten. Als Sofortmaßnahme wurde das Phonetik-Programm dahingehend modifiziert, daß Negativ-Meldungen nur noch dann erfolgen, wenn bei den ersten vier Stellen des Vornamens *und* des Zunamens Gleichheit besteht.

4.11 Wissenschaft und Forschung

Rasterfahndung in der Hochschule

Bereits im April 1982 erhielt ich einen Hinweis darauf, daß eine Hochschule auf Grund eines konkreten Falles, in dem ein Bediensteter der Hochschule dort zugleich als Student immatrikuliert war, einen regelmäßigen Abgleich der Personaldatei mit der Studentendatei plante. Auf diese Weise sollte die Einhaltung der Anzeigepflicht für das Studium von Beschäftigten der Hochschule regelmäßig überprüft werden. Diese Anzeigepflicht gilt nicht nur für die Aufnahme des Studiums an der Hochschule, die zugleich Dienstbehörde ist, sondern für jedes Hochschulstudium.

Ich hatte dem Präsidenten der Hochschule bereits vor dem Volkszählungsurteil des Bundesverfassungsgerichts von 1983 meine Zweifel an der Rechtmäßigkeit dieser Maßnahme mitgeteilt. Sie ist schon deshalb nicht geeignet, das angestrebte Ziel zu erreichen, weil durch diesen Datenabgleich nicht festgestellt werden kann, daß ein Hochschulmitarbeiter an einer anderen Hochschule studiert.

Insbesondere besteht keine ausreichende Rechtsgrundlage für die personenbezogene Weitergabe der Daten zum Zweck des Abgleichs. Studentendaten von Hochschulmitarbeitern sind lediglich zu Studienzwecken erhoben worden und nicht, um eine Kontrolle im Beschäftigungsbereich zu ermöglichen. Damit sind diese Daten aber ausschließlich zu Studien- und Prüfungszwekken zu verwenden. Hinzu kommt, daß jeder Beschäftigte, soweit es das Studienfach zuläßt, den Abgleich umgehen kann, in dem er die Hochschule wechselt. Damit stößt die Zusammenführung von Personal- und Studentendaten ins Leere und widerspricht dem Gebot der Verhältnismäßigkeit.

Ich habe deshalb den Datenabgleich gegenüber dem Präsidenten der Hochschule beanstandet. Dieser hat mir daraufhin mitgeteilt, daß er in Zukunft nicht mehr die Personal- mit der Studentendatei vergleichen wird. Gegen eine gezielte Abfrage aus beiden Dateien bei konkreten Verdachtsmomenten im Einzelfall habe ich keine Einwände.

Stellenbesetzungslisten

Der Personalrat einer Hochschule hat mich darauf hingewiesen, daß die Präsidenten der Kuratorialhochschulen regelmäßig etwa vierteljährlich sowie nach Verabschiedung eines Haushaltsplans oder Nachtragshaushaltes Stellenbesetzungslisten mit Angaben über das Geburtsdatum, den Namen, die Beschäftigungsstelle, die Besoldungs-, Vergütungs-, Lohngruppe sowie die Amts-, Dienst-, Tätigkeitsbezeichnung des Stelleninhabers dem Senator für Wissenschaft und Forschung übermitteln. Dieser ist zwar Vorsitzender der Personalkommission der jeweiligen Berufsschule, die nach dem Berliner Hochschulgesetz Dienstbehörde, oberste Dienstbehörde sowie Personalstelle und Personalwirtschaftsstellen an den Kuratorialhochschulen ist. Sie hat jedoch dem jeweiligen Hochschulpräsidenten die Befugnisse der Personalwirtschaftsstelle übertragen. Dieser bedarf nur für bestimmte Entscheidungen der vorherigen Zustimmung des Vorsitzenden der Personalkommission. Nach der Übertragungsanordnung ist der Präsident auch verpflichtet, dem Vorsitzenden der Personalkommission alle angeforderten personalwirtschaftlichen Auskünfte zu erteilen und angeforderte Unterlagen einschließlich der gespeicherten Daten vorzulegen oder zugänglich zu machen.

Die Rechtmäßigkeit einer regelmäßigen Übermittlung von Stellenbesetzungslisten mit personenbezogenen Daten an den Senator für Wissenschaft und Forschung ist zweifelhaft. Der Senator ist zwar in seiner Eigenschaft als Vorsitzender der Personalkommission Mitglied eines Hochschulorgans, seine Aufgaben und Zuständigkeiten in dieser Eigenschaft sind jedoch im Hochschulgesetz und in den jeweiligen Übertragungsanordnungen abschließend aufgezählt. Nach dem Grundsatz der informationellen Gewaltenteilung müssen auch die hochschulinternen Informationsflüsse datenschutzrechtlichen Anforderungen genügen.

Selbst wenn die jeweilige Übertragungsanordnung den Präsidenten verpflichten sollte, auch personenbezogene Daten dem Vorsitzenden der Personalkommission vorzulegen oder zugänglich zu machen - was sich aus dem Wortlaut dieser Vorschrift nicht ergibt -, so hätte eine solche Befugnis zur regelmäßigen Übermittlung aller Personaldaten einer Hochschule zumindest in den Grundzügen vom Gesetzgeber selbst geregelt werden müssen. Auch an dieser Stelle zeigt sich erneut ein entscheidender Mangel des Berliner Hochschulgesetzes, in das der Gesetzgeber entgegen meinen Empfehlungen keine bereichsspezifische Regelung der Erhebung und Verarbeitung von Personaldaten aufgenommen hat.

Ein Erfordernis der regelmäßigen Übermittlung vollständiger Stellenbesetzungslisten mit den Namen aller Stelleninhaber „zur Vorbereitung personalwirtschaftlicher Entscheidungen" kann ich nicht erkennen. Die Übertragungsanordnungen sind dahingehend zu verstehen, daß der Präsident verpflichtet ist, dem Vorsitzenden der Personalkommission alle im Zusammenhang mit dessen Zustimmungsvorbehalt bei bestimmten personalwirtschaftlichen Entscheidungen des Präsidenten angeforderten Auskünfte zu erteilen und Daten vorzulegen oder zugänglich zu machen. Nur in diesem Umfang, d. h. im Zusammenhang mit Einzelfallentscheidungen halte ich die Offenbarung personenbezogener Angaben gegenüber dem Senator für Wissenschaft und Forschung in seiner Eigenschaft als Vorsitzenden der Personalkommission datenschutzrechtlich für hinnehmbar, solange der Gesetzgeber keine abweichende normenklare Regelung in das Berliner Hochschulgesetz aufnimmt. Der Senator für Wissenschaft und Forschung und die Präsidenten der Freien Universität und der Technischen Universität haben meiner Auffassung widersprochen. Gegenwärtig ist diese Frage Gegenstand eines Rechtsstreits.

4.12 Organisation und Geschäftsordnung

Postaustausch in der Berliner Verwaltung

Ein Verwaltungsmitarbeiter hat gegenüber dem Prüfungsausschuß für das Verbesserungsvorschlagswesen beim Senator für Inneres angeregt, die eingehende Post dem Sachbearbeiter direkt zuzuleiten. Nur wenn sich der Empfänger anhand der Adressierung nicht sofort bestimmen läßt, wird sie geöffnet und entsprechend ausgezeichnet.

Die zuständige Fachabteilung des Senators für Inneres hat dafür plädiert, den Vorschlag abzulehnen, weil bei der innerbehördlichen Behandlung die Übermittlungsbestimmungen des § 10 BlnDSG nicht herangezogen werden könnten. Bereits jetzt könnten die Absender durch entsprechende Zusätze wie „vertraulich" oder „persönlich" verhindern, daß Postsendungen in den Verteilstellen geöffnet werden. Für die zur Verschwiegenheit verpflichteten Mitarbeiter in den Verteilstellen handele es sich um ein Massengeschäft, bei dem es praktisch unmöglich sei, in die Eingänge mehr als zur Weiterleitung notwendig Einblick zu nehmen. Hinzu kämen organisatorische Schwierigkeiten im Zusammenhang mit der Anbringung des Eingangsstempels und eine zusätzliche Belastung der Sachbearbeiter. Die Vorgesetzten könnten ihre Leitungsfunktionen nicht mehr wahrnehmen.

Ich habe demgegenüber festgestellt, daß der Verbesserungsvorschlag datenschutzfreundlich ist. Dm Hinblick auf den funktionalen Behördenbegriff muß ohnehin eine Organisation der Postverteilung gefunden werden, die sowohl datenschutzrechtliche Erfordernisse als auch dienstrechtliche Belange berücksichtigt.

Der Verbesserungsvorschlag zielt darauf ab, Sendungen, die an einen Sachbearbeiter unmittelbar adressiert sind, denen gleichzusetzen, die den Zusatz beispielsweise „verschlossen" oder „persönlich" enthalten und somit direkt ungeöffnet zugeleitet werden sollen. In der Regel wird demgegenüber die eingehende Post in der Hauptverteilungsstelle einer Verwaltung geöffnet und dann offen an die Poststelle der Fachverwaltung oder -abteilung weitergeleitet. Auch wenn man der Argumentation des Senators für Inneres insbesondere im Hinblick auf die Wahrnehmung der Leitungsfunktion zustimmt, und damit der Verbesserungsvorschlag in der Tat zu weit geht, muß der Möglichkeit der Kenntnis-

nahme durch einen unüberschaubaren Kreis von Mitarbeitern und unbefugten Dritten entgegengewirkt werden. Daher muß die Post so spät wie möglich geöffnet werden. Das bedeutet, daß darauf hingewirkt werden sollte, daß nicht mehr die zentrale Hauptverteilungsstelle, sondern vielmehr die jeweilige Poststelle der speichernden Stelle im Sinne des funktionalen Behördenbegriffs die Post öffnet.

Sofern Postsendungen ohne Zusätze an eine Behörde gerichtet sind, müssen sie selbstverständlich in der Hauptverteilungsstelle geöffnet werden, um eine Zuordnung zu der jeweiligen Verwaltungseinheit vornehmen zu können. Im Einzelfall, insbesondere bei besonderen Amtsgeheimnissen (z. B. Arzt-, Steuer-, Sozial- oder Statistikgeheimnis) kann das bedeuten, daß die Sendung wieder verschlossen und der jeweiligen Stelle zugeleitet wird.

Auf meine Anregung hin hat sich ein Bezirksamt mit zwei Abteilungen bereiterklärt, versuchsweise für einen bestimmten Zeitraum in der Postverteilung eine Umorganisation mit dem Ziel vorzunehmen, ob ungeachtet der bestehenden Rechtslage und unterschiedlichen Auffassungen eine Umsetzung meiner Vorstellungen praktikabel ist. Die Post dieser beiden Abteilungen wurde nicht in der zentralen Hauptverteilungsstelle des Bezirksamtes geöffnet, sondern erhielt den Eingangsstempel außen auf dem Umschlag. Nur wenn im Einzelfall die Sendung keinen Hinweis auf den Empfänger enthielt, wurde auch die Post dieser Abteilungen geöffnet.

Die Post wird vom Boten der Fachabteilungen abgeholt, die dann ihrerseits die Schriftstücke entnehmen, auf Vollständigkeit prüfen und auf dem Schriftstück den Eingangsstempel der Fachabteilung anbringen. Danach wird die Post in der Abteilung weiter verteilt. Dieses Verfahren hat während des Versuchs keinerlei Grund zu Beanstandungen gegeben. Es hat sich vielmehr gezeigt, daß eine Umsetzung datenschutzrechtlicher Anforderungen praktikabel ist.

Aktenaufbewahrung

Mehr Aufmerksamkeit ist auch der ordnungsgemäßen Aufbewahrung und Vernichtung von Akten zu widmen. So ist mir eine im Müllcontainer gefundene Liste mit Kundeninformationen zugeleitet worden, weil das Reinigungspersonal entgegen den Geschäftsanweisungen gehandelt hatte. In einem anderen Fall sind mehrere Arztbriefe und handschriftliche personenbezogene Aufzeichnungen über die Behandlung der Patienten einem Arzt aus dem Auto gefallen. Ein Standesamt hatte einen Teil einer nicht mehr benötigten Urkundenregisterkopie als Schmierpapier für Notizen auf der Rückseite an eine dritte Person weitergegeben. In einer Kindertagesstätte wurden die Fotokopien von vollstreckbaren Ausfertigungen von Unterhaltsanpassungsbeschlüssen mit detaillierten Angaben und Zahlen über den Kindesvater, das nichteheliche Kind und die Zahlungsverpflichtung ebenfalls als Schmierpapier verwandt. In einem Bezirksamt ist eine komplette Sozialhilfeakte aus einem während der Dienstzeit offen stehenden Dienstzimmer entwendet und später in einem Kino am Kurfürstendamm aufgefunden worden.

Diese Beispiele, insbesondere aber auch die teilweise reservierten Stellungnahmen der betroffenen Stellen lassen hier noch viel Problembewußtsein vermissen.

Mitschnitt von Telefonaten

Ein Bezirksamt beabsichtigt, in der Fernsprechvermittlung für jeden Vermittlungsplatz eine besondere Taste anbringen zu lassen, die ein Tonband auslöst, so daß bei Bombendrohungen usw. der Wortlaut mitgeschnitten und das Band dem polizeilichen Erkennungsdienst zugeleitet werden kann. Von der Polizei sollte dann in kurzer Zeit die Ernsthaftigkeit oder gar der Anrufer ermittelt werden.

Meine Überprüfung hat ergeben, daß in den letzten Jahren telefonisch mehrere Bombendrohungen bei dem Bezirksamt eingegangen sind, aber auch sexuelle Belästigungen der Mitarbeiterinnen in der Telefonzentrale. Ein Mitschneiden sollte nur in diesen Fällen erfolgen, wäre aber praktisch bei jedem eingehenden Telefonat möglich.

Die Frage, ob das Mitschneiden von Telefonaten zulässig ist, stellt sich nicht nur bei Bezirksämtern, sondern bei allen Stellen, die Sicherheitsgründe dafür geltend machen. Eine datenschutzrechtliche Bewertung ergibt folgendes:

Gemäß § 201 Abs. 1 StGB macht sich strafbar, wer unbefugt das nicht öffentlich gesprochene Wort eines anderen auf einen Tonträger aufnimmt oder eine so hergestellte Aufnahme gebraucht oder einem Dritten zugänglich macht. Nicht öffentlich ist ein Wort, wenn es nicht an die Allgemeinheit gerichtet ist. Das ist bei Gesprächen mit dem Bezirksamt oder sonstigen öffentlichen Stellen üblicherweise der Fall.

Eine Befugnis kann sich daraus ergeben, daß eine gesetzliche Erlaubnis vorliegt. Eine solche ist nach einer ersten Überprüfung nicht ersichtlich (wie z. B. §§ 100 a, 100 b StPO).

Auch die Einwilligung des Sprechenden, der über die Mitschneidemöglichkeit nicht informiert ist, kann nicht angenommen werden.

Gegenüber einem Bombendroher, Erpresser usw. kommt allerdings eine Notwehrhandlung in Betracht. Ein Mitschneiden dürfte hier jedoch nur im konkreten Einzelfall zulässig sein. Anderenfalls könnten jeder potentiell bedrohte Privatbetrieb und praktisch alle öffentlichen Stellen eingehende Anrufe mitschneiden, da nicht auszuschließen ist, daß darunter auch Drohungen und Erpressungen sein können. Die vorsorgliche Installation von Aufnahmegeräten kann also nur dann gerechtfertigt sein, wenn ganz konkrete Anhaltspunkte dafür bestehen, daß es tatsächlich zu einer Erpressung, Bombendrohung kommt.

Eine Mitschneideeinrichtung kann daher erst dann eingeschaltet werden, wenn festgestellt wird, daß die Drohung zumindest ernstgemeint sein könnte. Diese Feststellung kann das Bezirksamt selbst oder auch unter Zuhilfeziehung der Polizei treffen. Bei dem geschilderten Sachverhalt wird jedoch umgekehrt vorgegangen, indem zunächst mitgeschnitten wird und sodann die Polizei anhand des Mitschnitts entscheidet, ob die Drohung ernstzunehmen ist oder nicht.

Ich habe erhebliche Zweifel, ob dieser mögliche Zugewinn an Sicherheit das Risiko von Mitschnitten rechtfertigen kann.

5. Nachträge zu Feststellungen aus den Vorjahren

Arbeitsunfähigkeitsbescheinigung (Jahresbericht 1986, Ziff. 5.3)

Meiner Bewertung eines Rundschreibens des Präsidenten der Technischen Universität Berlin, in dem die Beschäftigten aller Bereiche verpflichtet wurden, ihre Arbeitsunfähigkeitsbescheinigung mit der Angabe der Fachrichtung des behandelnden Arztes (z. B. „Psychiater") nicht unmittelbar der Personalstelle, sondern zunächst der jeweiligen Beschäftigungsstelle vorzulegen, hat der Senat in seiner Stellungnahme zu meinem Jahresbericht 1986 nicht widersprochen. Gleichwohl hat der Präsident der Technischen Universität das Verfahren nicht geändert.

Vordrucke (Jahresbericht 1987, Ziff. 5.7)

Bei der Anzeige eines Gewerbes wurde bisher von den bezirklichen Wirtschaftsämtern ohne Kenntnis des Gewerbetreibenden ein Führungszeugnis für Behörden vom Bundeszentralregister eingeholt. Dazu hatte ich empfohlen, dem Betroffenen die Wahl zu lassen, ob er selbst ein Führungszeugnis beibringen wolle oder ob er mit der Einholung durch die Behörde einverstanden ist. Der Senator für Wirtschaft und Arbeit hat sich dem zwar nicht angeschlossen, aber inzwischen das Formular zur Gewerbeanzeige durch einen Hinweis ergänzt, daß über den Gewerbetreibenden ein Führungszeugnis und ein Auszug aus dem Gewerbezentralregister von der Behörde angefordert wird. Damit ist gewährleistet, daß der Betroffene über das Verfahren Bescheid weiß. Mein ursprünglich weitergehender Vorschlag befindet sich noch in der Diskussion mit dem Bundesminister für Wirtschaft und den Wirtschaftsministern bzw. -senatoren der Länder.

Vordrucke (Jahresbericht 1985, Ziff. 4.5)

Auf meine Empfehlungen zur datenschutzgerechten Gestaltung von Vordrucken, mit denen personenbezogene Daten erhoben werden, hat der Senator für Inneres nochmals in einem Rundschreiben hingewiesen. Darüber hinaus wird auch in den

vom Senat erlassenen Vordruckgrundsätzen ausdrücklich auf diese Anforderungen hingewiesen.

Bezirksämter - Führung der Grundstückseigentümerkartei (Jahresbericht 1985, Ziff. 4.1)

Zehn Bezirke haben zwischenzeitlich die bei ihnen geführte Grundstückseigentümerkartei vernichtet. Die übrigen zwei Bezirke werden die Kartei im kommenden Jahr vernichten.

Schulpsychologischer Dienst (Jahresbericht 1987, Ziff. 5.5)

Im Amtsblatt für Berlin wurden im September 1988 die Ausführungsvorschriften für den schulpsychologischen Dienst in Kraft gesetzt und veröffentlicht, die mit nur geringfügigen Veränderungen meine Empfehlungen zum Umgang mit den personenbezogenen Daten enthalten (vgl. Anlage 6).

6. Zusammenarbeit mit anderen Stellen

Konferenz der Datenschutzbeauftragten

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat in drei Sitzungen unter Vorsitz der Datenschutzkommission Rheinland-Pfalz beraten:

33. Konferenz am 14./15. März 1988
- Beschluß über die polizeiliche Datenverarbeitung bis zum Erlaß bereichsspezifischer gesetzlicher Regelungen
- Beschluß zur Änderung und Ergänzung des Personenstandsgesetzes

34. Konferenz am 4. Juni 1988
- Entschließung zur Neufassung des Bundesdatenschutzgesetzes
- Beschluß zum Entwurf eines Gesetzes zur Strukturreform im Gesundheitswesen

35. Konferenz am 10./11. Oktober 1988
- Beschluß über Datensicherheit beim Einsatz kleinerer DV-Anlagen
- Beschluß zum Entwurf einer Steuerdaten-Abruf-Verordnung
- Beschluß über die Sicherstellung des Datenschutzes bei der Poststrukturreform
- Beschluß über aktuelle Probleme des Datenschutzes in der Telekommunikation

Der Konferenzvorsitz wird mit dem Jahreswechsel turnusgemäß auf den Landesbeauftragten für Datenschutz des Saarlandes übergehen.

Abgeordnetenhaus

Datenschutzprobleme wurden in bewährter Weise vor allem in den Ausschüssen des Abgeordnetenhauses sowie in Gesprächen mit Fraktionen und einzelnen Abgeordneten erörtert.

Der *Unterausschuß Datenschutz* des Ausschusses für Inneres, Sicherheit und Ordnung hat in mehreren Sitzungen den Jahresbericht 1987 und andere datenschutzrelevante Fragen beraten.

Ein Schwerpunkt aus dem Bereich Gesundheitswesen war die Frage des Einsichtsrechts der Patienten in die eigenen Krankenakten und die regelmäßige Krankendatenweitergabe an die Krankenversicherungsträger. Der Unterausschuß vertrat die Ansicht, daß die gesetzliche Regelung forciert werden müsse und ist daher an den Ausschuß für Gesundheit und Soziales herangetreten. Dieser hat die Frage ebenfalls erörtert. Eine gesetzliche Regelung zu Beginn der neuen Legislaturperiode wurde ins Auge gefaßt.

Weiter wurde eingehend das Ergebnis meiner Überprüfung der Datenverarbeitung in den Berliner Krankenhausbetrieben erörtert. In diesem Rahmen wurde auch das vom Senator für Gesundheit und Soziales in Auftrag gegebene Gutachten diskutiert. Der Gutachter wurde im Ausschuß angehört. Der Ausschuß billigte die von mir erzielten Ergebnisse[1].

Für die Hochschule hat der Unterausschuß vorgeschlagen, das Berliner Hochschulgesetz zu ändern und den § 6 (Erhebung und Verarbeitung von Daten) zu streichen, da die Bestimmung ohnehin nicht angewendet wird. Die Sachprobleme könnten entsprechend dem Landesstatistikgesetz geregelt werden. Weiter sah der Ausschuß einen Handlungsbedarf im Bereich Schule hinsichtlich der AV-Lehrerbeurteilung und AV-Schülerunterlagen. Der Unterausschuß vermochte nicht nachzuvollziehen, warum jede einzelne Beurteilung eines Lehrers grundsätzlich an die Hauptverwaltung geht und von dort kontrolliert wird. Da es sich hierbei um die Bewertung von Beförderungsvorgängen handeln soll, ist nicht einzusehen, daß eine automatische Übersendung aller Beurteilungen notwendig ist. Weiterhin hat der Unterausschuß um Überprüfung gebeten, ob das Einsichtsrecht von Schülern, die das 14. Lebensjahr vollendet haben, in ihre Schülerunterlagen tatsächlich von der Zustimmung der jeweiligen Erziehungsberechtigten abhängig gemacht werden muß.

Ferner wurden im Ausschuß die Problematik der personengebundenen Hinweise in der polizeilichen Datenverarbeitung sowie die Erhebung und Löschung von Daten anläßlich der IWF-Tagung behandelt[2].

Schließlich habe ich in der letzten Sitzung des Unterausschusses eine Stellungnahme zum Änderungsentwurf der FDP zum ASOG sowie zum Entwurf eines Berliner Datenschutzgesetzes der SPD-Fraktion abgegeben.

Mit der *Parlamentarischen Kontrollkommission* (PKK), die die Tätigkeit des Landesamtes für Verfassungsschutz kontrolliert, wurden zahlreiche Fragen erörtert. So habe ich einen Überblick über die insgesamt in diesem Bereich angefallenen Vorgänge gegeben. Die Vorgänge wurden detailliert behandelt.

Im *Unterausschuß Datenverarbeitung* des Hauptausschusses wurden Fragen des Datenschutzes bei vernetzten Computern im Statistischen Landesamt erörtert mit dem Ziel, in jedem Fall den Datenschutz auch bei einem Inhouse-System sicherzustellen.

Aufsichtsbehörde nach dem Bundesdatenschutzgesetz

Die gute Zusammenarbeit mit der Aufsichtsbehörde für den Datenschutz beim Senator für Inneres wurde fortgesetzt. Gegenstand der Abstimmung waren vor allem: Die Volkszählung, das Vorhaben, erstmals ein Landesstatistikgesetz zu schaffen, die Novellierung des Bundesdatenschutzgesetzes, die rechtzeitige Übersendung von Gesetzentwürfen des Bundes an den Berliner Datenschutzbeauftragten sowie Datenschutzprobleme beim automatisierten Zahlungsverkehr. Ferner wurden Datenschutzfragen der GGO II, Fragen der datenschutzgerechten Postbearbeitung in den Behörden sowie der Zugriff der Strafverfolgungsbehörden auf statistische Daten erörtert.

Meldungen zum Dateienregister

Das von mir zu führende Dateienregister enthält nunmehr 1 726 (Stand 30. September 1988) Dateien (Vorjahr: 1 598) von 372 (333) Stellen. Für interessierte Bürger und öffentliche Stellen steht eine Zusammenfassung des Dateienregisters zur Verfügung.

---

[1] Vgl. oben Ziff. 4.4

[2] Vgl. oben Ziff. 4.5

Berlin, den 14. Dezember 1988

Der Berliner Datenschutzbeauftragte

Dr. Kerkau

Anlagen

1. Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 6. Juni 1988 zur Neufassung des Bundesdatenschutzgesetzes.
2. Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 6. Juni 1988 zum Entwurf eines Gesetzes zur Strukturreform im Gesundheitswesen.
3. Beschluß der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 14. März 1988 betr. Polizeiliche Datenverarbeitung bis zum Erlaß bereichsspezifischer gesetzlicher Regelungen.
4. Beschluß der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 10. Oktober 1988 zur Sicherstellung des Datenschutzes bei der Poststrukturreform.
5. Beschluß der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 10. Oktober 1988 über aktuelle Probleme des Datenschutzes in der Telekommunikation.
6. Ausführungsvorschriften über den Schulpsychologischen Dienst vom 18. August 1988.
7. Beschluß der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 10. Oktober 1988 über Datensicherheit beim Einsatz kleinerer Datenverarbeitungsanlagen.
8. Informationen zur Datenträgervernichtung.

Anlage 1

Entschließung
der Konferenz der Datenschutzbeauftragten
des Bundes und der Länder
sowie der Datenschutzkommission Rheinland-Pfalz
vom 6. Juni 1988
zur Neufassung des Bundesdatenschutzgesetzes

Die Datenschutzbeauftragten stellen mit Bedauern fest, daß der vorliegende Entwurf einer Neufassung des Bundesdatenschutzgesetzes im wesentlichen die gleichen Mängel aufweist wie der entsprechende Entwurf der 10. Legislaturperiode des Deutschen Bundestages. Diese Mängel haben die Datenschutzbeauftragten bereits in ihrer Entschließung vom 14. März 1986 aufgezeigt.

Die Datenschutzbeauftragten halten es insbesondere für verfehlt, das allgemeine Datenschutzrecht aufzusplittern in ein streng auf die Datenverarbeitung in Dateien bezogenes Bundesdatenschutzgesetz und ein den Datenschutz in Akten regelndes Verwaltungsverfahrensgesetz, das weite und wichtige Verwaltungsbereiche (z. B. Finanzverwaltung und Sozialverwaltung) ebensowenig erfaßt wie die Strafverfolgung, und dessen Einhaltung sich überdies weitgehend der Datenschutzkontrolle entzieht.

Die Datenschutzbeauftragten stellen ferner fest, daß bei der Vorbereitung des Entwurfs ihre Empfehlungen sowie die zwischenzeitlich von einigen Bundesländern erlassenen, in wesentlichen Punkten vorbildlichen Neuregelungen des Datenschutzes nahezu unberücksichtigt geblieben sind.

Die Datenschutzbeauftragten verkennen nicht, daß auch der jetzige Entwurf einige Verbesserungen gegenüber dem geltenden Recht aufweist. Insgesamt jedoch werden die in der Begründung des Entwurfs genannten Ziele der beabsichtigten Weiterentwicklung des Bundesdatenschutzgesetzes nicht erreicht:

- Die Anpassung an die Grundsätze des Urteils des Bundesverfassungsgerichts vom 15. Dezember 1983 zum Volkszählungsgesetz ist in mehrfacher Hinsicht nicht gelungen: so enthält der Entwurf keine ausdrückliche Regelung der Datenerhebung, obwohl gerade diese den Bürger unmittelbar belastet; die geplante Regelung im Verwaltungsverfahrensgesetz reicht nicht aus. Auch erfährt der Grundsatz der Zweckbindung zu weitgehende Ausnahmen und die Transparenz der Datenverarbeitung, insbesondere das Recht des Betroffenen auf Auskunft, bleibt hinter verfassungsrechtlichen Anforderungen zurück.
- Dem technologischen Fortschritt auf dem Gebiet der Informations- und Kommunikationstechnik (z. B. Arbeitsplatzcomputer, neue optische Speichermedien, Videoaufzeichnungen, Telekommunikation und Vernetzung) wird der Entwurf nicht gerecht. Der im Entwurf verwandte Dateibegriff und die Beibehaltung des bisherigen Katalogs technischer und organisatorischer Datensicherungsmaßnahmen vernachlässigen die technische Entwicklung.
- Die Kontrollbefugnis des Bundesbeauftragten für den Datenschutz wird insgesamt eingeschränkt, insbesondere durch den Ausschluß systematischer Kontrollen bei der Erhebung und Verwendung personenbezogener Informationen außerhalb von Dateien. Keinesfalls kann eine Einschränkung der Kompetenz der Landesbeauftragten durch den Bundesgesetzgeber hingenommen werden.
- Die Datenschutzvorschriften für den nichtöffentlichen Bereich orientieren sich nicht an dem Grundsatz der Zweckbindung und räumen unvertretbare Verarbeitungsprivilegien ein.

Der Entwurf entspricht daher nicht den Erwartungen an ein zeitgemäßes Datenschutzrecht als Ausprägung des verfassungsrechtlich garantierten Rechts des Bürgers auf informationelle Selbstbestimmung. Dieses Recht ist erst jüngst durch das Bundesverfassungsgericht in seiner Entscheidung vom 9. März 1988 bestätigt worden. Dort heißt es: „In dieses Recht wird nicht nur dann eingegriffen, wenn der Staat vom einzelnen die Bekanntgabe persönlicher Daten verlangt oder diese der automatisierten Datenverarbeitung zuführt ... Das Recht auf informationelle Selbstbestimmung schützt vielmehr wegen seiner persönlichkeitsrechtlichen Grundlage generell vor staatlicher Erhebung und Verarbeitung personenbezogener Daten und ist nicht auf den jeweiligen Anwendungsbereich der Datenschutzgesetze des Bundes und der Länder oder datenschutzrelevanter Sonderregelungen bechränkt."

Die Konsequenz daraus muß eine möglichst lückenlose und präzise Regelung des Datenschutzes sein, um Rechtssicherheit für Bürger und Verwaltung herzustellen.

Anlage 2

Entschließung
der Konferenz der Datenschutzbeauftragten
des Bundes und der Länder
sowie der Datenschutzkommission Rheinland-Pfalz
vom 6. Juni 1988
zum Entwurf eines Gesetzes zur Strukturreform
im Gesundheitswesen
(Gesundheits-Reformgesetz - GRG)

Die Konferenz der Datenschutzbeauftragten stellt fest, daß es in Verhandlungen zwischen dem Bundesbeauftragten für den Datenschutz und dem Bundesminister für Arbeit und Sozialordnung gelungen ist, eine Reihe von Forderungen des Datenschutzes im Regierungsentwurf gegenüber den Vorentwürfen zu verwirklichen.

Gleichwohl halten die Datenschutzbeauftragten eine Verbesserung des Persönlichkeitsschutzes der Krankenversicherten im weiteren Gesetzgebungsverfahren vor allem in den folgenden Punkten für notwendig:

1. **Erfassung medizinischer Daten und Grundsatz des geringstmöglichen Eingriffs**

   Die im Zusammenhang mit Leistungen der gesetzlichen Krankenversicherung vorgesehene automatisierte Verarbeitung von Daten der Versicherten, Ärzte und Zahnärzte darf der Gesetzgeber wegen des damit verbundenen gravierenden Eingriffs in das Selbstbestimmungsrecht der Versicherten nur zulassen, wenn damit tatsächlich auch die erklärten Ziele des Gesetzgebungsvorhabens gefördert, namentlich ein wesentlichen Beitrag zur Kostendämpfung geleistet werden kann, und sich dies nicht auch durch weniger einschneidende Maßnahmen erreichen läßt. So würde es für die Erstellung von Statistiken, die für die Bewertung und Beeinflussung des Leistungsgeschehens wichtig sind, genügen, einen anonymisierten Transparenzbestand zu bilden. Darüber hinaus wäre zu fragen, ob es nicht ausreicht, statt der vorgesehenen versichertenbezogenenen umfassenden Datenspeicherung nur die rechtlichen und organisatorischen Voraussetzungen zur Überprüfung von Einzelfällen festzulegen.

2. **Festlegung des Verwendungszwecks personenbezogener Daten**

   Gegen die Nutzung personenbezogener Daten, soweit sie für die Überprüfung der Abrechnung medizinischer Leistungen und zur Kontrolle der Wirtschaftlichkeit erforderlich ist, bestehen keine grundsätzlichen Bedenken. Nach der Rechtsprechung des Bundesverfassungsgerichts muß der Verwendungszweck erhobener Daten vom Gesetzgeber normenklar festgelegt werden. Für kassenärztliche Vereinigungen und für den Medizinischen Dienst fehlt es im Gesetzentwurf an einer Festlegung des Verwendungszwecks. Der Gesetzentwurf stellt außerdem nicht sicher, daß Daten der Krankenkassen nur für deren Zwecke verwendet werden. Eine Verwendung medizinischer Daten über den eigentlichen Aufgabenbereich der Krankenkassen, der Kassenärztlichen Vereinigungen und des Medizinischen Dienstes hinaus darf wegen der besonderen Sensibilität der Daten nur für eng umschriebene Ausnahmefälle zugelassen werden. Die allgemeinen Offenbarungsvorschriften des SGB X lassen eine zu weitgehende Nutzung durch Dritte zu.

   Dies gilt um so mehr, als die im Entwurf bereits einbezogene technische Entwicklung (maschinenlesbare Datenträger, Krankenversicherungskarte) immer mehr dazu führen wird, daß die versicherungsbezogenen Krankheitsdaten in maschinenlesbarer Form und damit vielfältig verwertbar vorliegen werden.

   Die Konferenz begrüßt die Verbesserungsvorschläge der Ausschüsse des Bundesrates.

3. **Vereinbarungen der Verbände**

   Der Gesetzentwurf überläßt die Regelung der Abrechnung der kassenärztlichen Versorgung einschließlich der dafür erforderlichen Datenübermittlung den Vereinbarungen der Verbände der Krankenkassen und Kassenärztlichen Vereinigungen. Verschiedene Vereinbarungen greifen nachhaltig in das informationelle Selbstbestimmungsrecht der Versicherten ein, ohne daß diese - insbesondere als Pflichtversicherte - eine Wahlmöglichkeit hätten. Das betrifft z. B. Festlegungen über den Inhalt von Rezepten und Krankenscheinen, die Einbeziehung Dritter zur Prüfzwecken, Meldung von Behinderungen an die Krankenkassen.

   Da der Gesetzgeber nach der Rechtsprechung des Bundesverfassungsgerichts alles Wesentliche selbst regeln muß, reicht es nicht aus, die Regelungsbefugnis an die Verbände zu delegieren. Vielmehr müßte der Umfang der Eingriffe in das informationelle Selbstbestimmungsrecht und der Mindestinhalt der datenschutzrechtlichen Regelungen konkreter als bisher gesetzlich festgelegt werden. Das gilt auch für die Voraussetzungen zur Einführung maschinenlesbarer Krankenversicherungskarten. Darüber hinaus wäre klarzustellen, daß die Verarbeitung und Nutzung personenbezogener Daten für andere als die im Gesetz genannten Fälle nicht durch Vereinbarung vorgesehen werden kann. Der Gesetzgeber sollte überdies ein Verfahren vorsehen, in dem die Wahrung der Rechte der Patienten bei Erlaß solcher Vereinbarungen überprüft wird (z. B. Genehmigungsvorbehalt; eine Genehmigung dürfte nur erteilt werden, wenn in den Vereinbarungen die Forderungen des Datenschutzes der Versicherten angemessen berücksichtigt sind).

   Der Inhalt der Vereinbarungen ist dem Betroffenen auf Verlangen zugänglich zu machen.

4. **Medizinischer Dienst**

   Im Hinblick auf die Schutzwürdigkeit der beim Medizinischen Dienst anfallenden Krankheitsdaten sind gesetzliche Regelungen erforderlich über

   - Art und Umfang der zu verarbeitenden Daten
   - Zweckbestimmung und Verwendungsmöglichkeit (etwa im Bereich des Sozialmedizinischen Dienstes der Rentenversicherungsträger)
   - Vermeidung einer med. Zentraldatei
   - Informationsrechte der Betroffenen
   - Einschränkung der Offenbarungsbefugnisse gegenüber Dritten
   - Löschungszeitpunkte.

   Die Konferenz begrüßt auch hier die in diese Richtung zielenden Vorschläge der Ausschüsse des Bundesrates.

5. **Auskunftsanspruch**

   Wegen der zentralen Bedeutung des Auskunftsanspruchs ist im Gesetzestext deutlich klarzustellen, daß auf Verlangen des Versicherten Auskunft über Leistungen und Kosten sowie nach Maßgabe des § 83 SGB X auch über die Diagnose zu erteilen ist. Der Auskunftsanspruch darf nicht durch Satzung beschränkt werden. Der Anspruch muß auch gegenüber dem Medizinischen Dienst bestehen.

6. **Aufbewahrungsfristen**

   Der verfassungsrechtliche Verhältnismäßigkeitsgrundsatz gebietet, die Speicherungsdauer personenbezogener Daten auf das erforderliche Maß zu begrenzen. Hierzu sind konkret bestimmte Aufbewahrungsfristen unerläßlich.

   Im Gesetzentwurf ist bisher nur bei den Krankenkassen eine nach Jahren festgelegte Frist für die Aufbewahrung von Daten über Leistungsvoraussetzungen (z. B. Art der Erkrankung, Arbeitsunfähigkeitszeiten) vorgesehen. Die Speicherungsdauer für andere Daten bei Krankenkassen und Kassenärztlichen Vereinigungen (z. B. verordnete Medikamente, ärztliche Leistungen, Überweisungen, Abrechnungsunterlagen) ist im Gesetzentwurf nicht konkret befristet. Nach dem Grundsatz der Normenklarheit und dem Wesentlichkeitsgebot des Bundesverfassungsgerichts hat der Gesetzgeber hier selbst eine bestimmte Aufbewahrungsfrist festzulegen.

Die Konferenz begrüßt auch hier die in diese Richtung zielenden Vorschläge der Ausschüsse des Bundesrates. Sie weist jedoch darauf hin, daß die Aufbewahrungsfrist jeweils am Tage der jeweiligen Leistungsgewährung beginnen muß.

7. **Zentrale Krankheitsdatei der Unfallversicherungsträger**

Der Gesetzentwurf räumt den Unfallversicherungsträgern die Möglichkeit ein, eine zentrale Krankheitsdatei einzurichten.

Angesichts der schon früher diskutierten vielfältigen datenschutzrechtlichen Probleme zentraler Krankheits- und Gefährdungsregister muß der Gesetzgeber jedoch gleichzeitig mit der Erlaubnis zur Einrichtung dafür sorgen, daß für solche Register ausreichende rechtliche und organisatorische Schutzvorkehrungen wirksam werden. Vorzusehen ist insbesondere eine Einwilligung des Betroffenen in die Speicherung seiner Daten.

Sicherzustellen ist ferner:

- die Verantwortlichkeit für die gespeicherten Daten (speichernde Stelle)
- Art und Umfang der zu speichernden Daten
- die konkrete Zweckbestimmung der Daten in dem betreffenden Register
- Zugriffsrechte.

Sicherzustellen ist schließlich, daß die Patientendaten nicht aus dem durch § 35 SGB I geschützten Bereich (Sozialgeheimnis) herausgelöst werden.

Anlage 3

Beschluß
der Konferenz der Datenschutzbeauftragten
des Bundes und der Länder
vom 14. März 1988
betr. Polizeiliche Datenverarbeitung bis zum Erlaß bereichsspezifischer gesetzlicher Regelungen

Beschluß der Konferenz der Datenschutzbeauftragten des Bundes und der Länder und der Datenschutzkommission Rheinland-Pfalz vom 14./15. März 1988 in Mainz.

Eines der dringendsten datenschutzrechtlichen Anliegen ist die Schaffung bereichsspezifischer Grundlagen für die Datenverarbeitung der Sicherheitsbehörden. Dies gilt ebenso für die Nachrichtendienste. Schon seit Jahren haben die Datenschutzbeauftragten entsprechende Forderungen erhoben. Spätestens seit dem „Volkszählungsurteil" des Bundesverfassungsgerichts vom 15. Dezember 1983 ist das gesetzliche Regelungsdefizit offenbar. So hat der Bayerische Verfassungsgerichtshof in einer Entscheidung vom 9. Juli 1985 bezogen auf die polizeiliche Datenverarbeitung hervorgehoben, es sei geboten, daß der Gesetzgeber die Materie regele, die bisher Gegenstand der „Richtlinien für die Führung kriminalpolizeilicher personenbezogener Sammlungen (KpS)" ist.

Mit der Erhebung, Speicherung und Weitergabe personenbezogener Daten greift die Polizei in die Grundrechte der Betroffenen ein, ohne daß dafür immer die verfassungsrechtlich gebotenen gesetzlichen Grundlagen vorhanden sind. So haben schon einige Gerichte die polizeiliche Datenverarbeitung zum Zwecke vorbeugender Straftatenbekämpfung bis zum Erlaß bereichsspezifischer gesetzlicher Grundlagen für unzulässig erklärt. Gleichwohl kommen die gesetzgeberischen Initiativen zur Behebung dieses Zustandes nur äußerst schleppend voran.

Allerdings hat das Bundesverfassungsgericht dem Gesetzgeber in der Vergangenheit Übergangsfristen zur Beseitigung von Regelungsdefiziten zugebilligt, wenn damit eine sonst eintretende Funktionsfähigkeit staatlicher Einrichtungen vermieden werden kann, die der verfassungsmäßigen Ordnung noch ferner stünde als der bisherige Zustand.

Dabei ist auf folgendes hinzuweisen:

1. Übergangsfristen können ihrer Natur nach nicht unbegrenzt in Anspruch genommen werden. Das Bundesverfassungsgericht hat ausdrücklich darauf hingewiesen, daß sie dann nicht mehr anerkannt werden können, wenn der Gesetzgeber eine Neuregelung ungebührlich verzögert.

2. Während der Übergangsfrist reduziert sich die Befugnis zu Eingriffen auf das, was für die geordnete Weiterführung eines „funktionsfähigen Betriebes" unerläßlich ist. Es ist mithin unzulässig und mit den vom Bundesverfassungsgericht festgestellten reduzierten Befugnissen unvereinbar, bereits bestehende Datenverarbeitungsabläufe noch auszuweiten, etwa durch den Aufbau neuer Datenbanken oder die Ausschöpfung neuer technischer Möglichkeiten, soweit die Eingriffe in die Rechte der Betroffenen damit eine neue Qualität erreichen.

3. Besondere Zurückhaltung hat sich die Polizei dort aufzuerlegen, wo Eingriffe in das informationelle Selbstbestimmungsrecht noch weitere Grundrechte betreffen.

   3.1 Die Feststellungen von Personalien, damit verbundene Datenabgleiche und Speicherungen sowie Film- und Videoaufnahmen sind anläßlich von öffentlichen Versammlungen während der Übergangszeit nur dann als zulässig anzusehen, wenn Anhaltspunkte dafür vorliegen, daß strafbare Handlungen begangen werden.

   3.2 Die Nutzung technischer Hilfsmittel zur verdeckten Datenerhebung durch Lauschangriffe in Wohnungen muß grundsätzlich ausgeschlossen sein.

4. Der Einsatz von verdeckten Ermittlern und V-Leuten sowie langfristige Observationen und polizeiliche Beobachtung dürfen nur zugelassen werden, wenn konkrete Anhaltspunkte für bestimmte schwere Straftaten bestehen. Es muß festgelegt werden, wer diese Maßnahmen anordnen darf, wie die anfallenden Erkenntnisse verwertet werden dürfen und wann die Betroffenen zu unterrichten sind.

5. Im Hinblick auf die von den Verfassungsgerichten für die Übergangszeit geforderte Beschränkung auf das, was für die geordnete Weiterführung eines „funktionsfähigen Betriebs" unerläßlich ist, erinnern die Datenschutzbeauftragten an ihre früheren Beschlüsse zur polizeilichen Datenverarbeitung. Danach sind künftig insbesondere folgende Datenverarbeitungsvorgänge zu unterlassen:

   - Speicherung diskriminierender personenbezogener Hinweise in polizeilichen Informationssystemen;
   - Speicherung (ehemals) verdächtiger Personen zu Zwekken vorbeugender Straftatenbekämpfung ohne verantwortbare kriminologische Prognose;
   - Speicherung von Daten über Personen, bei denen eine Anklageerhebung mangels öffentlichen Interesses abgelehnt wurde;
   - Speicherung von Daten über Kinder, die der Begehung einer Staftat verdächtigt werden;
   - Weitergabe von Informationen, die mit speziellen polizeilichen Befugnissen erhoben wurden, an andere als Polizeidienststellen.

Anlage 4

Beschluß
der Konferenz der Datenschutzbeauftragten
des Bundes und der Länder
sowie der Datenschutzkommission Rheinland-Pfalz
vom 10. Oktober 1988
Sicherstellung des Datenschutzes bei der Poststrukturreform

Die Bundesregierung hat dem Parlament den Entwurf eines Poststrukturgesetzes vorgelegt, in dem eine teilweise Privatisierung des Fernmeldewesens vorgesehen ist. Eine Verwirklichung dieses Entwurfs hätte zur Folge, daß für die künftigen privaten Telekommunikationsanbieter weniger strenge Datenschutzregelungen gelten als im Bereich der Bundespost.

Das Poststrukturgesetz muß deshalb über die bisherigen Regelungen hinaus sicherstellen, daß auch in den Bereichen, in denen Endeinrichtungen durch Private betrieben oder sonstige Netzfunktionen durch Private wahrgenommen werden, ebenso strenge Datenschutzregelungen gelten, wie sie im Bereich der Bundespost notwendig sind.

Hierzu reicht die Verordnungsermächtigung, die die Bundesregierung nur unzureichend zum Tätigwerden verpflichtet, nicht aus. Außerdem könnte der Datenschutz durch private Geschäftsbedingungen unterlaufen werden. Notwendig ist eine abschließende gesetzliche Regelung, die den Umfang der Daten auf das unerläßliche Ausmaß beschränkt, eine strenge Zweckbindung vorsieht und für den Bürger die Datenflüsse offenlegt. Dies gilt auch für personenbezogene Daten, die beim Betrieb privater Telekommunikationsdienstleistungen (§ 1 Abs. 4 Entwurf Fernmeldeanlagengesetz) anfallen. Solche Dienstleistungen dürfen nur zugelassen werden, wenn sie den gesetzlichen Anforderungen entsprechen.

Die gesetzliche Regelung sollte von den Unternehmen der Deutschen Bundespost und von den privaten Unternehmen auch verlangen, daß diese technische und organisatorische Maßnahmen durchführen, um eine datenschutzgerechte und sichere Telekommunikation zu gewährleisten. Schließlich muß auch für die privaten TK-Anbieter eine angemessene Kontrolle vorgesehen werden.

Anlage 5

Beschluß
der Konferenz der Datenschutzbeauftragten
des Bundes und der Länder
sowie der Datenschutzkommission Rheinland-Pfalz
vom 10. Oktober 1988
Aktuelle Probleme des Datenschutzes
in der Telekommunikation

Mit Inkrafttreten der Telekommunikationsordnung am 1. Januar 1988 hat die Deutsche Bundespost den Übergang von bisher getrennten Fernmeldenetzen zu einem einzigen, diensteintegrierten digitalen Telekommunikationsnetz für die Übermittlung aller Nachrichtenarten eingeleitet; künftig fallen an zentralen Stellen erheblich mehr und leichter auswertbare personenbezogene Daten an als bisher, die je nach Dienstart mehr oder weniger präzise Rückschlüsse auf das Verhalten der Teilnehmer erlauben. In der Telekommunikationsordnung wurden die Empfehlungen der Konferenz der Datenschutzbeauftragten des Bundes und der Länder zur Verbeserung des Datenschutzes und zur Beherrschung der möglichen Risiken bisher leider nur zum Teil befolgt.

Auch das Bundesdatenschutzgesetz kann mit seinen allgemeinen Vorschriften die Risiken nicht auffangen; dies gilt auch für die bisher bekanntgewordenen Novellierungsentwürfe. Hier bedarf es weiterer spezieller Regelungen. Bei der Novellierung des Bundesdatenschutzgesetzes muß vor allem sichergestellt werden, daß sämtliche beim Einsatz neuer Telekommunikationstechniken und -dienste anfallenden Daten in den Geltungsbereich des Gesetzes fallen. Deshalb muß z. B. selbstverständlich sein, daß alle personenbezogenen Daten aus der Bild-, Sprach-, Text- und Datenübertragung geschützt werden. Die Regelung der Zulässigkeit der Verarbeitung personenbezogener Daten, deren Kontrolle und der erforderlichen technisch-organisatorischen Maßnahmen müssen an die neuen technischen Gegebenheiten angepaßt werden.

Das Grünbuch der europäischen Gemeinschaften über die Entwicklung des gemeinsamen Marktes für Telekommunikationsdienstleistungen und Telekommunikationsgeräte zeigt, daß der Datenschutz bei der geplanten Liberalisierung des Angebots von Dienstleistungen und Geräten nur unzureichend berücksichtigt wird. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder weist nachdrücklich darauf hin, daß das nationale Datenschutzrecht nicht durch ein Gemeinschaftsrecht überlagert werden darf, das im Ergebnis zu weniger Datenschutz führt als das nationale Recht. Die frühzeitige Einbindung des Datenschutzes in die jetzt folgenden Beratungen - auch auf EG-Ebene - ist daher dringend erforderlich.

Die Länder sind im Rahmen ihrer Zuständigkeit zum Erlaß vom Regelungen zur Nutzung der Telekommunikation verpflichtet, auch die notwendigen Datenschutzvorschriften zu erlassen. Der Bildschirmtext-Staatsvertrag kann hierzu als Vorbild dienen. In einem derartigen Staatsvertrag müssen auch die materiellen Voraussetzungen zum Betrieb privater Telekommunikationsdienste und deren Zulassung geregelt werden.

Anlage 6

Ausführungsvorschriften über den Schulpsychologischen Dienst

Vom 18. August 1988

SchuBSport V A 22

Tel.: 30 32 - 5 68 oder 30 32 - 1, intern 9 87 - 5 68

Auf Grund des § 59 Satz 1 des Schulgesetzes für Berlin (SchulG) in der Fassung vom 20. August 1980 (GVBl. S. 2103), zuletzt geändert durch Gesetz vom 24. Juni 1988 (GVBl. S. 953), wird bestimmt: ...

IV. Behandlung vertraulicher Unterlagen und Informationen; Einsichtsrecht

13. (1) Die bei der schulpsychologischen Tätigkeit anfallenden personenbezogenen Daten unterliegen besonderer Vertraulichkeit.

(2) Insbesondere sind die Dienstkräfte des Schulpsychologischen Dienstes zur Verschwiegenheit und zur Wahrung des Persönlichkeitsschutzes der Betroffenen verpflichtet. Diese Verpflichtung gilt sowohl für persönliche Mitteilungen als auch für Daten, die im Rahmen von Tests erhoben werden. Von ihrer Schweigepflicht, die auch gegenüber anderen Personen und Stellen außerhalb der Schule und des Schulaufsichtsdienstes besteht, können die Berater nur durch denjenigen befreit werden, der die zu schützenden Informationen gegeben hat. Erteilt ein minderjähriger Schüler die Befreiung von der Schweigepflicht, so bedarf dies der Zustimmung der Erziehungsberechtigten. Dies gilt nicht hinsichtlich der erforderlichen Informationen gegenüber der Schule, dem Schulamt und der Schulaufsicht in den Fällen des § 21 Abs. 2 SchulG. Die Dienstkräfte sind auf die strafrechtlichen Folgen einer unbefugten Offenbarung von persönlichen Geheimnissen nach § 203 des Strafgesetzbuches hinzuweisen. Über die besonderen Offenbarungsbefugnisse bei Gefahren für Leib, Leben und persönliche Freiheit der am Beratungsvorgang beteiligten Personen (§ 34 StGB) sind sie zu belehren.

14. (1) Bei allen Untersuchungen des Schulpsychologischen Dienstes sind nur die zur Erfüllung der Aufgabe erforderlichen Informationen zu erheben. Ihre Verwendung ist auf den durch Gesetz oder durch das Ersuchen bestimmten Zweck zu beschränken. Eine Weitergabe an Stellen und Personen außerhalb der Schule und des Schulaufsichtsdienstes ist nur mit Zustimmung der Erziehungsberechtigten bzw. des volljährigen Schülers zulässig, es sei denn, daß die Informationen auf eine schwerwiegende Gefährdung des Schülers im Sinne des § 34 Strafgesetzbuch hindeuten und unverzügliche Maßnahmen des Jugendamtes oder der Strafverfolgungsbehörden zum Schutze des Schülers erforderlich machen.

(2) Über das Ergebnis von Untersuchungen nach Nummer 10 Abs. 1 Buchstabe a werden die Erziehungsberechtigten oder die volljährigen Schüler im Rahmen der Begründung der schulbehördlichen Entscheidung in Kenntnis gesetzt. Bei Untersuchungen nach Nummer 10 Abs. 1 Buchstabe b ist die ersuchende Stelle über das Ergebnis der Untersuchung mündlich oder schriftlich zu informieren und entsprechend zu beraten. Die Erziehungsberechtigten oder der volljährige Schüler sind von dem Ergebnis auf Verlangen zu unterrichten. Die Erziehungsberechtigten oder der volljährige Schüler sind vom Ergebnis der Untersuchungen nach Nummer 10 Abs. 1 Buchstabe c und Nummer 10 Abs. 3 zu informieren; die Information anderer Stellen und Personen, auch der Schule oder des Schulaufsichtsdienstes, bedarf ihrer Zustimmung. Würde die Unterrichtung der Erziehungsberechtigten das Wohl der Minderjährigen nachhaltig gefährden, gilt die Schweigepflicht auch gegenüber den Erziehungsberechtigten.

(3) Schriftliche Berichte an die Schulen sind als besonders vertraulich zu kennzeichnen und in einem verschlossenen Umschlag zum Schülerbogen zu nehmen. Die Einsichtnahme ist nur mit Zustimmung des Schulleiters zulässig. Sie sind auf Antrag der Betroffenen drei Jahre nach Entstehen dem Schülerbogen zu entnehmen und zu vernichten.

15. (1) Erziehungsberechtigte, volljährige Schüler und minderjährige einsichtsfähige Schüler haben das Recht auf Einsicht in die Unterlagen des Schulpsychologischen Dienstes. Dies gilt ohne Einschränkung, wenn jeder Betroffene mit der Einsichtnahme durch alle anderen Betroffenen einverstanden ist und Rechte Dritter nicht beeinträchtigt werden. Anderenfalls können Betroffene nur in diejenigen Unterlagen Einsicht nehmen, die sich auf sie selbst beziehen oder von anderen Betroffenen zur Einsichtnahme freigegeben sind. Läßt die Gestaltung der Akten die so begrenzte Einsichtnahme nicht zu, oder würde die Einsichtnahme den Erfolg der Untersuchung in Frage stellen oder sonst das Wohl eines Beteiligten gefährden, so entscheidet der Leiter der Schulpsychologischen Beratungsstelle, in welcher Weise die Einsichtnahme durch eine Information über den Akteninhalt ersetzt werden kann. Von der Einsichtnahme minderjähriger Schüler können die Erziehungsberechtigten informiert werden, es sei denn, daß schutzwürdige Interessen der Schüler entgegenstehen. In Fällen der Nummer 10 Abs. 1 Buchstabe a ist § 29 des Verwaltungsverfahrensgesetzes zu beachten.

(2) Einsichtsberechtigte Schüler und Erziehungsberechtigte noch nicht volljähriger Schüler können die Berichtigung falscher tatsächlicher Angaben verlangen.

(3) Die Akten des Schulpsychologischen Dienstes sind so zu führen, daß die differenzierte Einsichtnahme in die Akten (Nummer 14 Abs. 1) möglich ist.

16. Akten des Schulpsychologischen Dienstes sind bis zum Ablauf von 2 Jahren nach Beendigung des Schulverhältnisses aufzubewahren. Danach sind diese als Vorgänge vertraulichen Inhalts zu vernichten.

Anlage 7

Beschluß
der Konferenz der Datenschutzbeauftragten
des Bundes und der Länder
sowie der Datenschutzkommission Rheinland-Pfalz
vom 10. Oktober 1988
Datensicherheit beim Einsatz kleinerer
Datenverarbeitungsanlagen

Beim Einsatz kleinerer Datenverarbeitungsanlagen, vor allem von persönlichen Computern (PC), bereiten die Datensicherheit und die Ordnungsmäßigkeit der Verarbeitung personenbezogener Daten besondere Probleme. Im Hinblick auf diese Probleme geben die Datenschutzbeauftragten des Bundes und der Länder folgende Empfehlungen:

1. Vor jeder Entscheidung, ob für die Arbeiten eines Aufgabengebiets ein PC oder eine sonstige kleinere Datenverarbeitungsanlage eingesetzt werden kann, muß geprüft werden, ob die dabei erzielbare Datensicherheit ausreichend ist. Bei dieser Prüfung müssen insbesondere die Empfindlichkeit der Daten und der Grad der Verbindlichkeit der Verarbeitungslogik berücksichtigt werden. Die Verarbeitung personenbezogener Daten mit einem automatisierten Verfahren, das keine angemessene Datensicherheit bietet, verstößt gegen die Datenschutzgesetze.
2. Eine speichernde Stelle hat auch bei der Verarbeitung personenbezogener Daten auf einem PC oder einer sonstigen kleineren Datenverarbeitungsanlage die technischen und organisatorischen Maßnahmen zu treffen, die je nach Art der zu schützenden Daten geeignet sind, die Datensicherheit zu gewährleisten. Sofern die Datensicherheit mit den verfügbaren Maßnahmen nicht in dem erforderlichen Umfang gewährleistet werden kann, muß auf den Einsatz des PC oder der kleineren Datenverarbeitungsanlage verzichtet werden.

   Um die Datensicherheit zu gewährleisten, sind insbesondere die dem neuesten Stand entsprechenden technischen Maßnahmen zu treffen. Weisungen sollten schriftlich erfolgen und in einer Dienstanweisung zusammengefaßt werden. Durch Kontrollen der Arbeitsdurchführung ist sicherzustellen, daß alle Vorschriften und Weisungen befolgt werden.
3. Die Hersteller von Hard- und Software werden aufgefordert, für kleinere Datenverarbeitungsanlagen einschließlich der persönlichen Computer Verfahren zu entwickeln und bereitzustellen, die einen Betrieb dieser Geräte mit einem Maß an Datensicherheit ermöglichen, das demjenigen großer Rechenzentren entspricht. Vor allem müssen Hilfsmittel verfügbar gemacht werden, die es einer datenverarbeitenden Stelle ermöglichen,
   - ohne organisatorisch strukturiertes Rechenzentrum und damit auch ohne Funktionstrennungen bei der Arbeitsabwicklung,
   - ohne organisatorische Trennung zwischen Anwendung und Durchführung der automatisierten Datenverarbeitung und
   - trotz Verzichts auf Detailkenntnisse der automatisierten Datenverarbeitung bei Vorgesetzten und der für die Revision zuständigen Organisationseinheit

   sicherzustellen, daß bei der Verarbeitung auf der eingesetzten Datenverarbeitungsanlage eine verbindlich vorgeschriebene Verarbeitungslogik eingehalten wird. Dazu ist es unter anderem erforderlich, Verfahren bereitzustellen, die gewährleisten, daß Programme ausschließlich in der freigegebenen Fassung zum Ablauf kommen. Systemprogramme und Anwendungsprogramme könnten dazu mit einem geeigneten kryptografischen Verfahren versiegelt werden, wodurch Manipulationen erkennbar würden.

   Für persönliche Computer und sonstige kleinere Datenverarbeitungsanlagen sollten zur Datensicherheit Systemprogramme und systemnahe Programme mit einem an der Ausstattung großer Anlagen orientierten Leistungsumfang zur Verfügung gestellt werden. Wesentliche der Datensicherheit dienende Komponenten sollten in das Betriebssystem integriert werden, um Manipulationen und Umgehungsmöglichkeiten zu erschweren.

Anlage 8

Informationen zur Datenträgervernichtung
(Auch als Faltblatt vom Berliner Datenschutzbeauftragten erhältlich)

Zerreißen und „ab in den Papierkorb", damit wird dem **Datenschutz** nicht entsprochen. So wurden einst und gelegentlich auch heute in Behörden und Betrieben Schriftstücke mit personenbezogenen und/oder vertraulichen Inhalten vernichtet.

Nicht mehr benötigtes Papier mit personenbezogenen Daten darf nicht einfach achtlos in den Papierkorb gelangen. Dies gilt für z. B. Altakten, vertippte Briefe, überzählige Durchschläge, Fotokopien. Häufig sind Akten und Listen an allgemein zugänglichen Stellen gefunden worden, weil der Verantwortliche nicht die Chance hatte, eine der Sensibilität des **Datenträgers** gemäße **Vernichtungsart** zu nutzen.

Bei zu vernichtenden Datenträgern kann es sich um Carbon-Farbbandkassetten, Magnetbänder, Filmmaterial, Disketten und ähnliches handeln. Das Löschen von Daten stellt nach § 1 Abs. 1 Bundesdatenschutzgesetz[1] und § 4 Abs. 2 Berliner Datenschutzgesetz[1] eine Phase der Datenverarbeitung dar. Die Gesetze stellen darauf ab, daß das Löschen ein Unkenntlichmachen (Vernichten) zum Ziel hat. Dabei ist das Verfahren bzw. die Mittel gleichgültig, entscheidend ist allein der Erfolg.

Im Herbst 1985 trat die neue **DIN-Norm 32757** über die Vernichtung von Informationsträgern in Kraft. Dort wird in Bezug auf Partikelgrößen in 5 Sicherheitsstufen unterschieden. In der öffentlichen Verwaltung[2] sind Informationsträger mit personenbezogenen Daten mindestens der Sicherheitsstufe 3 zuzuordnen, während im privaten Bereich überwiegend die Sicherheitsstufe 2 ausreicht. Die Sicherheitsstufe 3 fordert, daß die Informatonsträger so vernichtet werden, daß die Reproduktion der auf ihnen wiedergegebenen Informationen nur unter erheblichem Aufwand möglich ist. Für Papier ist dies bei einer Materialteilchenbreite von ≦ 4 mm und Materialteilchenlänge von ≦ 60 mm oder einer Streifenbreite von ≦ 2 mm gegeben. Bei der Sicherheitsstufe 2 darf die Materialteilchenfläche des Papiers bis zu 400 mm² groß sein.

Wie sollte nun vernichtet werden? Als erstes sollte eine Bestandsaufnahme für alle regelmäßig wie unregelmäßig anfallenden Datenträger erfolgen. Je nach Art des Datenträgers kommen unterschiedliche Vernichtungsverfahren in Frage. Danach stellt sich die Frage, ob die **Vernichtung zentral oder dezentral** erfolgen

[1] Das Berliner Datenschutzgesetz regelt einen wesentlichen Bereich des Datenschutzes öffentlicher Stellen des Landes Berlin. Nach § 21 BlnDSG ist der Berliner Datenschutzbeauftragte für die Kontrolle der Einhaltung dieser Vorschriften verantwortlich. Das Bundesdatenschutzgesetz gilt auch in Berlin und regelt den Datenschutz bei öffentlichen Stellen des Bundes, die in Berlin ihren Sitz oder Dienststellen haben. Es regelt ferner die Verarbeitung personenbezogener Daten durch nicht-öffentliche Stellen und damit im gesamten Bereich der Privatwirtschaft. Die Kontrolle des Datenschutzes wird bei Stellen des Bundes vom Bundesbeauftragten für den Datenschutz, bei nicht-öffentlichen Stellen von der Aufsichtsbehörde für den Datenschutz, in Berlin der Senator für Inneres, wahrgenommen.

[2] Entsprechendes ist in § 88 der Gemeinsamen Geschäftsordnung für die Berliner Verwaltung (GGO I) geregelt.

soll. Die Art des Datenträgers, die örtlichen Gegebenheiten, der mengenmäßige und zeitliche Anfall des zu vernichtenden Schriftgutes bestimmen die individuelle Lösung.

Nach unseren Erfahrungen ist eine getrennte Sammlung von geheim- und nichtgeheimzuhaltendem Material und sonstigen Abfällen in der täglichen Praxis so gut wie nicht durchführbar. Ist eine getrennte Sammlung geschützter Informationsträger nicht sichergestellt, müssen alle Informationsträger ohne Rücksicht auf ihre Schutzwürdigkeit wie geheimzuhaltendes Material behandelt werden.

Informationsträger sofort und **vor Ort** zu **vernichten,** ist die sicherste Lösung. Dafür gibt es sogenannte Schreibtisch- oder Büroaktenvernichter, z. B. für eine Abteilung. Nach Zerkleinerung kann das Papier der Altpapierverwertung zugeführt werden.

Bei der dezentralen **Entsorgung** ist zu beachten, daß jede Weitergabe an andere Personen und lange Wege zum Aktenvernichter zusätzliche Sicherheitsrisiken schaffen, die nicht unterschätzt werden dürfen. So sind z. B. Altakten während des Tansportes auf einem nur mit Plane abgedeckten Lkw verloren gegangen. Die Sicherheit der Zwischenlagerung und der Transportwege, die die Datenträger zurücklegen müssen, ist daher zu prüfen. Werden Sammelbehälter eingesetzt, muß sichergestellt werden, daß Unbefugte keine Datenträger entnehmen können.

In Fällen, in denen die Datenverarbeitung nicht selbst durchgeführt wird, also andere beauftragt werden, handelt es sich um **Auftragsdatenverarbeitung.** Die auftraggebende Stelle kann sich bei Pannen nicht aus der Verantwortung ziehen, da die gesetzlichen Regelungen (§ 8 Abs. 1 BDSG und § 2 Abs. 1 BlnDSG) den Auftraggeber im besonderen Maße verpflichten. So ist das Unternehmen unter besonderer Berücksichtigung der Eignung der von ihm getroffenen technischen und organisatorischen Maßnahmen zur Datensicherung sorgfältig auszuwählen.

Dem Auftraggeber ist anzuraten, die Pflichten des Auftragnehmers in einem **Vertrag** festzulegen, der unter anderem die Ausstellung eines Vernichtungsprotokolls einschließt. Der Auftragnehmer soll dem Auftraggeber das Recht auf jederzeit durchführbare Stichproben für die Zeit einräumen, in denen sich das zu vernichtende Material in den Geschäftsräumen oder Fahrzeugen des Auftragnehmers befindet. Der Auftragnehmer soll der Aufsichtsbehörde für Datenschutz gemeldet sein, und die bei der Vertragserfüllung beteiligten Personen sind gemäß Bundesdatenschutzgesetz und entsprechender Landesdatenschutzgesetze auf das Datengeheimnis zu verpflichten. Weiterhin sollte bei Bedarf festgelegt werden, daß die abgeholten Unterlagen am gleichen Tag vernichtet und der Transport nur in geschlossenen Fahrzeugen durchgeführt werden darf.

Im Berliner Stadtgebiet gibt es mehrere **Privatunternehmen,** die über allgemein zu nutzende Reißwölfe und technische Einrichtungen **zur Vernichtung von Datenträgern** verfügen und entsprechende Dienstleistungen anbieten. Der Senator für Inneres führt eine Liste der bei ihm zum Register nach § 39 BDSG angemeldeten Unternehmen, die gewerbsmäßig Datenträger vernichten. Sie kann unter der Anschrift Senator für Inneres - I B -, Fehrbelliner Platz 2, 1000 Berlin 31, Telefon: 8 67 44 89, angefordert werden. Auch dem Branchenfernsprechbuch können unter den Stichwörtern „Aktenvernichtung" und „Recycling" Anschriften entnommen werden.

Als weitere Möglichkeit können Altakten und Papiere mit personenbezogenen Daten mit einem Lkw zur Müllverbrennungsanlage der Berliner Stadtreinigungs-Betriebe in Ruhleben gefahren und dort unter Aufsicht eines Mitarbeiters der jeweiligen Dienststelle gegen das übliche Abnahmeentgelt der **Verbrennung** zugeführt werden. Ob die BSR zusätzlich eine stationäre oder mobile Aktenvernichtung betreiben wird, ist derzeit noch nicht entschieden.

Carbonfarbband-Kassetten sind im Gegensatz zu Gewebefarbbändern einseitig eingefärbt. Beim Schreiben wird der Farbstoff vollständig vom Farbband auf das Papier übertragen. Dadurch ist der abgedruckte Buchstabe deutlich zu erkennen. Wegen der guten Nachlesbarkeit müssen solche Farbbänder mit geeigneten Geräten vernichtet oder unter Aufsicht verbrannt werden. Die nach der DIN-Norm 32757, Teil I, zugelassenen Materialteilchengrößen entsprechen den Papierteilchengrößen, da es sich um Informationsdarstellung in Originalgröße handelt.

Besonders informationshaltig sind **Mikrofilme,** auf deren sachgerechte Beseitigung deshalb genau geachtet werden muß. Bereits eine Materialteilchengröße von 6 mm × 10 mm kann ausreichen, um eine komplette Seite des Formats DIN A 4 zu reproduzieren. In der DIN-Norm 32757 wird deshalb für Filmmaterial aus Polyester mit verkleinerter Informationsdarstellung in der Sicherheitsstufe 3 eine Materialteilchenfläche von $\leq$ 1 mm² gefordert. Auch chemische und thermische Vernichtungsmethoden sind möglich.

Magnetdatenträger können nach Demagnetisierung wie Hausmüll behandelt werden.

Stichwortverzeichnis

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