



Bericht

**des Berliner Datenschutzbeauftragten
zum 31. Oktober 1989**

Der Berliner Datenschutzbeauftragte gibt zu Beginn des Jahresberichts¹⁾ einen Überblick über die Situation des Datenschutzes. Im Vordergrund steht in diesem Jahr die Entwicklung der Informationstechnologie auf internationaler Ebene, die entscheidender Anstrengungen sowohl gesetzgeberischer als auch organisatorischer Art bedarf, um das informationelle Selbstbestimmungsrecht der Bürger auch bei grenzüberschreitendem Datenverkehr sicherzustellen. In den folgenden Abschnitten 1 - 4 werden die Ergebnisse der Datenschutzkontrolle und Beratung dargelegt. Dabei wird unter 3 - entsprechend den gesetzlichen Vorschriften²⁾ - über 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.

Inhaltsverzeichnis

1. Zur Situation

Ausbau des Datenschutzes dringend nötig:
Der Gesetzgeber ist mehr denn je gefordert

2. Brennpunkte des Datenschutzes

- 2.1 Die zunehmende internationale Verflechtung
- 2.2 Vom Sammeltrieb eines Nachrichtendienstes
- 2.3 Gentechnik
- 2.4 ISDN und ISDN-fähige Nebenstellenanlagen
- 2.5 Bürokommunikation
- 2.6 Erfahrungen mit Personalcomputern

3. Neue Medien

- 3.1 Telekommunikationsrecht
- 3.2 Bildschirmtext
- 3.3 Kabelpilotprojektgesetz

4. Weitere Fragen aus der Kontroll- und Beratungspraxis

- 4.1 Bau- und Wohnungswesen
- 4.2 Finanzen
- 4.3 Gesundheit und Soziales
- 4.4 Inneres
- 4.5 Justiz
- 4.6 Kulturelle Angelegenheiten
- 4.7 Schule, Berufsbildung und Sport
- 4.8 Wissenschaft und Forschung
- 4.9 Organisation und Geschäftsordnung
- 4.10 Bezirksämter

5. Nachträge zu Feststellungen aus den Vorjahren

6. Zusammenarbeit mit anderen Stellen

Anlagen

- 1. Entschließungen der Konferenz der Datenschutzbeauftragten des Bundes und der Länder sowie der Datenschutzkommission Rheinland-Pfalz
 - 1.1 Entschliebung vom 5./6. April 1989 zum Strafverfahrensänderungsgesetz vom 3. November 1988
 - 1.2 Entschliebung zur Neuregelung des Bundesdatenschutzgesetzes vom 5./6. April 1989
 - 1.3 Entschliebung zum Entwurf eines Rentenreformgesetzes vom 5./6. April 1989
 - 1.4 Entschliebung zu § 100 a StPO vom 5./6. Mai 1989
 - 1.5 Entschliebung zu den Entwürfen eines Bundesverfassungsschutzgesetzes, eines MAD-Gesetzes und eines BND-Gesetzes vom 30. Mai 1989
- 2. Beschlüsse der Internationalen Konferenz der Datenschutzbeauftragten
 - 2.1 Berliner Resolution der 11. Internationalen Konferenz der Datenschutzbeauftragten vom 30. August 1989
 - 2.2 Zusatzklärung der Datenschutzbeauftragten der EG-Länder
 - 2.3 Entschliebung der 11. Internationalen Konferenz der Datenschutzbeauftragten vom 30. August 1989 über die Arbeitsgruppe Telekommunikation und Medien
 - 2.4 Beschluß der 11. Internationalen Konferenz der Datenschutzbeauftragten vom 30. August 1989 zu ISDN auf Vorschlag der Arbeitsgruppe Telekommunikation und Medien
- 3. Empfehlungen für den datenschutzgerechten Einsatz von UNIX-Systemen

Stichwortregister

für alle seit 1979 veröffentlichten Jahresberichte

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

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

1. Zur Situation

Ausbau des Datenschutzes dringend nötig: Der Gesetzgeber ist mehr denn je gefordert

Als vor zehn Jahren, am 1. November 1979, der Berliner Datenschutzbeauftragte seine Tätigkeit aufnahm, hätte wohl niemand zu hoffen gewagt, daß der Datenschutz eine so weitgehende Anerkennung finden würde, wie sie in dem berühmten Volkszählungsurteil des Bundesverfassungsgerichts zum Ausdruck gekommen ist. Umso paradoxer erscheint die Feststellung, daß wir heute weiter von der Verwirklichung des Datenschutzes entfernt sind als vor zehn Jahren. Ursache hierfür ist vor allem der fundamentale Wandel der Informationstechnik vom isolierten Großrechenzentrum hin zur vernetzten Datenverarbeitung, in der Großrechner mit vor zehn Jahren kaum vorstellbarer Leistungsfähigkeit und Kleinrechner mit der Kapazität früherer Großrechner zusammenarbeiten. Dieser Phase der informationstechnischen Revolution muß der Datenschutz mit radikalen Maßnahmen zum Schutz der Rechte des Bürgers begegnen. Das bisher errichtete Datenschutzgebäude reicht dazu nicht aus. Auch die bisher unter dem Stichwort Novellierung erörterten Punkte sind kaum mehr als ein Kurieren an Symptomen. Angesichts der folgenden Entwicklungen sind der Berliner wie auch andere Gesetzgeber zu einschneidenden über die bisherige Novellierungsdiskussion hinausgehenden Gesetzesänderungen aufgerufen.

Allein die durch die Vernetzung ermöglichte Internationalisierung und Europäisierung der Datenverarbeitung führt zu bedenklichen Erscheinungen:

- Firmen und die öffentliche Verwaltung haben die Tendenz, die Datenverarbeitung in Länder zu verlegen, die kein Datenschutzgesetz aufweisen und daher als Datenoasen gelten.

Ein Beispiel hierfür ist die Möglichkeit, das im Schengener Abkommen zum Ausgleich des Grenzabbaus vorgesehene Polizeifahndungssystem nach Belgien zu verlegen.

- Zum anderen mehrten sich selbst in Berlin Fälle, in denen Bürger Schwierigkeiten haben, wenn ihre Daten ins Ausland übermittelt wurden. Bekanntester Fall ist die Festnahme einer Reisenden in Indien unter Terrorismusverdacht, über den ich bereits früher berichtet hatte. Grundlage war eine zehn Jahre zurückliegende Fahndungsausschreibung, die zwar über das BKA und Interpol Paris in alle Welt verteilt worden war. Die längst erfolgte Rücknahme der Ausschreibung war jedoch nicht nachvollzogen worden.

Der grenzüberschreitenden Datenverarbeitung muß daher ein Konzept des grenzüberschreitenden Datenschutzes gegenübergestellt werden, wie es auch von der 11. Internationalen Konferenz der Datenschutzbeauftragten im August in Berlin gefordert worden ist. Die Abgeordneten sind dazu aufgerufen, die Rechte des Datenschutzbeauftragten zu stärken, ihm die Möglichkeit des Verbots der Datenübermittlung in Länder zu geben, in denen die Datenschutzrechte der Bürger nicht ausreichen. Zudem sollte das „Verursacherprinzip“ gesetzlich verankert werden, d. h. der Grundsatz, daß eine Behörde, die ein Datum in ein Netz gibt, für die Aktualität und Richtigkeit dieses Datums verantwortlich und zur Korrektur verpflichtet ist.

Noch weitreichender sind die Probleme, die sich aus der Verwandlung unserer Gesellschaft in eine Informationsgesellschaft und damit aus der zunehmenden Abhängigkeit von der Informationstechnik ergeben. Die Situation ist zur Zeit ähnlich wie früher beim Umweltschutz: Fachleute sehen die Probleme deutlich, der Bürger spürt sie jedoch nur in Ausnahmefällen. Aber in wenigen Jahren hat er elektronische Meßgeräte für Gas, Wasser, Strom, elektronischen Einbruchschutz, Geräte für die Überwachung Kranker und Alter neben dem Homecomputer und Btx in seinem Haus. Damit entstehen heute unvorstellbare Überwachungsmöglichkeiten in dem von der Verfassung besonders geschützten privaten Bereich. Daneben wird das Konsum- und Reiseprofil der Bürger durch die Umstellung des Zahlungsverkehrs vom anonymen Geld zur Kreditkarte oder Scheckkarte ermittelbar, die er bei jedem Zahlvorgang in elektronische Kassen eingeben muß.

Diese revolutionäre Entwicklung erfordert ein Weiterdenken über die rechtlichen Kategorien hinaus. Wir müssen, was ich seit

längerem tue, mit den Herstellern von Computern, Betriebssystemen und Endgeräten in Verbindung treten und von ihnen fordern, daß bei der Konzeption ihrer Systeme der Datenschutz einbezogen wird.

- So ist es z. B. gelungen, für die Versuche des elektronischen Fernablesens durch die Berliner Wasserwerke eine datenschutzgerechte Wasseruhr zu konstruieren. Sie ist ein Beispiel für die Ausgestaltung zukünftiger Meßgeräte, deren zunehmender Einsatz im Privatbereich der Bürger erwartet wird.
- Ein Gegenbeispiel ist das ISDN-Netz der Post. Die Post hat noch immer nicht der Forderung zugestimmt, den neuen Möglichkeiten der offenen Netze durch mehr Sicherheit, etwa einen Verschlüsselungsdienst zu begegnen, sowie die Speicherung von Verbindungsdaten mengenmäßig und zeitlich zu beschränken.
- Auch sind praktisch keine Datenverarbeitungsanlagen und Betriebssysteme auf dem Markt, bei deren Konzeption der Datenschutz eine entscheidende Rolle gespielt hat. Dies wird sich allerdings in Zukunft ändern.

Der Gesetzgeber ist daher aufgefordert, diese wichtige Aufgabe gesetzlich zu umschreiben und sie zu einem Schwerpunkt der künftigen Arbeit der Datenschutzbeauftragten zu erklären. Eine denkbare Alternative wäre, diese Aufgabe auch einer neu zu gründenden oder vorhandenen Institution zuzuschreiben, die mit dem Datenschutzbeauftragten zusammenarbeitet. Hierbei könnte auch an eine europäische Institution gedacht werden, für die sich Berlin anbietet.

Gleichgewichtig mit diesen Fragen des Einbaus des Datenschutzes in die Gerätekonzeption und -konstruktion ist die frühzeitige Beteiligung des Datenschutzes bei neuen Datenverarbeitungssystemen.

Ein Beispiel ist der Vergleich des österreichischen mit dem deutschen Bildschirmtextsystem. In Österreich werden kostenpflichtige Seiten anonym mit einer elektronischen Zahlkarte bezahlt, bei uns werden alle Daten minutiös erfaßt. Das Beispiel zeigt, daß der Einsatz anonymer elektronischer Zahlkarten auf allen Ebenen gefordert werden muß, um den gewaltigen Anfall von privaten Daten zurückzudrängen. Es zeigt zugleich, daß die Elektronik durchaus zum Schutz des Bürgers eingesetzt werden kann, wenn man es nur richtig macht. Der Druck in diese Richtung sollte verstärkt werden, indem man den Datenschützern ein gesetzliches Vetorecht gegen Verfahren einräumt, die zu einem unnötigen Datenanfall führen. Auf diese Weise könnte sichergestellt werden, daß der Datenschutz nicht lediglich ein Reparaturbetrieb, sondern konzeptioneller Teil der Verfahrensentwicklung ist und unter dem Gesichtspunkt der Datensparsamkeit in die Verfahrensentwicklung eingreifen kann.

Darüber hinaus ist der Ausbau der Rechte des Datenschutzbeauftragten gegenüber der Legislative erforderlich. Denn die Verzögerung der Vorbereitung wichtiger Gesetzesvorhaben, die ich z. B. in Berlin seit 1983 ständig annehme, wie das Statistikgesetz, Polizeigesetz, Regelung der Personaldatenverarbeitung, das Archivgesetz, wiegt außerordentlich schwer. Die Gründe der Verwaltung für dieses Verhalten überzeugen nicht. Dieses Problem könnte gelöst werden, wenn man dem Datenschutzbeauftragten in Zukunft selbst unter bestimmten Bedingungen das Recht gibt, dem Parlament Gesetzesvorschläge vorzulegen, die auf die gleiche Weise wie Gesetzesinitiativen der Regierung oder des Parlaments zu behandeln wären.

Nicht zuletzt sind die hauseigenen Berliner Probleme durch gesetzgeberisches Handeln zu lösen.

Die Umstände der Neuwahl des Datenschutzbeauftragten zeigen, daß nach der Gesetzeslage eine kontinuierliche Leitung der obersten Landesbehörde „BlnDSB“ nicht gewährleistet ist. So erschien es weniger als zwei Wochen vor Ablauf der Amtszeit des bisherigen Datenschutzbeauftragten möglich, daß der derzeitige Amtsinhaber mit Ablauf seiner Amtszeit die Geschäfte nicht ordnungsgemäß einem Nachfolger übergeben kann. Die Parlamentarier aller Parteien sind daher aufgefordert, eine Wiederholung dieser Situation durch eine Gesetzesänderung auszuschließen.

Einer Regelung bedürfen weiter die Datenschutzprobleme, die sich aus der bezirklichen Datenverarbeitung ergeben. Denn einerseits werden diesen Bezirken Aufgaben de jure übertragen, wie etwa Wohngeld oder Sozialhilfe. Die Programmerstellung und Datenhaltung erfolgt in der Regel aber zentral bei Senatsdienststellen. Dieses Auseinanderklaffen von Programmerstellung und Datenhaltung auf der einen und Programm- und Datenverarbeitung auf der anderen Seite hat erhebliche negative Folgen. Das in diesem Bericht geschilderte Beispiel eines Betrugs von über 100 000,- DM durch einen Bediensteten einer Wohngeldstelle spricht für sich. Datenverantwortung und juristische Verantwortung für die Daten müssen in jedem Falle bei einer Stelle liegen.

Ein weiteres bezirkliches Problem bildet der Umgang mit Sozialdaten. Die Behörden sind angeblich so überlastet, daß sie nicht einmal notieren können, an wen Auskünfte aus Sozialakten gegeben werden, wozu sie gesetzlich verpflichtet sind. Hier wäre es dringend erforderlich, etwa durch den Einsatz der Datenverarbeitung für Abhilfe zu sorgen.

In dem Jahresbericht ist daher einmal gründlich auf die Probleme der bezirklichen Datenverarbeitung eingegangen worden. Probleme, die sich nicht zuletzt aus dem Fehlen eines Datenverarbeitungskonzeptes erklären, aber nicht zu billigen sind.

2. Brennpunkte des Datenschutzes

2.1 Die zunehmende internationale Verflechtung

Die Datenschutzdiskussion hat sich in den vergangenen zehn Jahren darauf konzentriert, die in den Bundes- und Landesdatenschutzgesetzen vorgegebenen Grundlinien für die Gewährleistung des informationellen Selbstbestimmungsrechts zu konkretisieren und in angemessene Handlungskonzepte für die öffentliche Verwaltung einerseits, für die Privatwirtschaft andererseits umzusetzen.

Diese Konzentration auf nationale Probleme verstellt leicht den Blick auf eine Entwicklung, die in den nächsten Jahren sowohl die öffentliche als auch die private Datenverarbeitung zunehmend prägen wird: Auf der technischen Seite wird die Datenverarbeitung mehr und mehr eingebunden in Netze, die international verknüpft sind und die einen grenzüberschreitenden *Datenaustausch* („transborder data flow“) ermöglichen. Ein typisches Beispiel ist die Ankündigung einer großen Auskunftsfrei sowie einer Kreditversicherung, gemeinsam ein europäisches Datennetz aufzubauen – die Auskunftsfrei will ihre Daten, die Versicherung EDV-know-how und internationale Verbindungen einbringen. Neben der Datenübermittlung an ausländische Stellen liegen damit auch die Voraussetzungen dafür vor, daß die Datenverarbeitung selbst ins Ausland verlagert wird; ein Beispiel hierfür bietet ein deutscher Automobilhersteller, der alle Personaldaten von einer privaten, in den USA beheimateten EDV-Firma verarbeiten lassen will.

Zwischen den Industriestaaten besteht ein erhebliches Gefälle bei der Datenschutzgesetzgebung. Selbst von den zwölf Staaten der Europäischen Gemeinschaften verfügen fünf nicht über ein umfassendes Datenschutzgesetz, darunter Belgien, ein Land, in dem sich seit Jahren große internationale Datenverarbeitungszentren etabliert haben (z. B. die Zentrale des internationalen Bankeninformationssystems SWIFT oder des Flugreservierungssystems SITA), und in dem gleichwohl ein Datenschutzgesetz noch nicht über das Entwurfstadium hinauskommen ist – ganz zu schweigen von den USA, in denen sich einerseits international genutzte Datenverarbeitungskapazitäten ballen, andererseits – abgesehen von bereichsspezifischen Regelungen wie dem Kreditwesen – nur für die öffentliche Verwaltung des Bundes und einiger Einzelstaaten ein Datenschutzgesetz existiert.

Auch die internationale Rechtsentwicklung hat bisher nicht angemessen auf diese Entwicklung reagiert: Zwar werden in der *Europaratskonvention Nr. 108* zum Schutz von Personen im Bereich personenbezogener automatischer Datenverarbeitung vom 28. Januar 1981 materielle und verfahrensmäßige Anforderungen an die Datenschutzgesetzgebung der Unterzeichnerstaaten gestellt. Die Konvention ist allerdings erst von acht Ländern

ratifiziert worden. Auf der Ebene der Europäischen Gemeinschaften wird bislang der Datenschutz eher als Hemmnis für die Realisierung des Binnenmarktes auf dem Gebiet der Informationsverarbeitung (Europäischer Informationsmarkt) denn als konkrete Aufgabe für die Schaffung eines angemessenen Gemeinschaftsrechtes gesehen.

In dieser Situation drohen für die Gewährleistung des informationellen Selbstbestimmungsrechts erhebliche Einbußen. Einerseits ist zu befürchten, daß eine Tendenz dahin entsteht, die Datenverarbeitung in „Datenoasen“ zu verlagern. Andererseits verliert der Bürger auch die im innerstaatlichen Recht eingeräumten Möglichkeiten, Auskunft über seine Daten zu erhalten, Berichtigungen und Aktualisierungen zu verlangen oder eine effektive Datenschutzinstanz anzurufen.

Diesen Fragen widmete sich die *11. Internationale Konferenz der Datenschutzbeauftragten*, die in diesem Jahr erstmals in Berlin zusammentrat. An der Konferenz, zu der der Bundesbeauftragte für den Datenschutz eingeladen und deren organisatorische Betreuung ich übernommen hatte, nahmen über 120 Personen teil. Es handelte sich dabei einerseits um Vertreter der bestehenden Datenschutzinstitutionen und von Regierungen aus Ländern, in denen eine Datenschutzgesetzgebung ansteht, andererseits aber auch um Vertreter der Wissenschaft und einschlägiger Publikationsorgane. Besondere Bedeutung hatte die Teilnahme von zwei Datenschutzexperten aus Ungarn, in deren Augen die Gewährleistung des Datenschutzes einen wichtigen Schritt zur Demokratisierung darstellt.

Zum Abschluß ihrer Beratungen verabschiedete die Konferenz zwei Resolutionen, die die Bedeutung des Datenschutzes für den internationalen Datenverkehr in besonderem Maße unterstreichen.

In der *„Berliner Resolution der Internationalen Konferenz der Datenschutzbeauftragten vom 30. August 1989“*¹⁾ verweisen die Teilnehmer insbesondere darauf, daß verschiedene internationale Organisationen Empfehlungen und Leitlinien zum Datenschutz verabschiedet haben, die einen gemeinsamen Bestand von Grundsätzen für eine faire Praxis in der Datenverarbeitung formulieren. Eine besondere Rolle spielt dabei die Konvention Nr. 108 des Europarates, in der materielle und verfahrensmäßige Anforderungen an die Datenschutzgesetzgebung in den Unterzeichnerländern gestellt werden. Die Konferenz bedauerte, daß sich bisher nur acht Staaten durch ihren Beitritt international verpflichtet haben, den in der Konvention vorgesehenen Datenschutzstandard einzuhalten.

In dieser Situation könne der einzelne Bürger nicht mehr sicher sein, daß nach der Übermittlung von Daten ins Ausland ein hinreichender Schutz seiner personenbezogenen Daten gewährleistet ist; sein Recht, einen Datenschutzbeauftragten anzurufen, könne er nicht mehr wahrnehmen.

Die Konferenz forderte, daß dem Datenschutz bei der Entwicklung und Nutzung internationaler Datendienste gleiche Priorität gegeben würde wie der Förderung der Datenverarbeitung und der Telekommunikation. Dies bedeute einerseits gesetzliche Sicherungen des Datenschutzes, andererseits aber auch die Verpflichtung der Datenverarbeiter, die Beachtung der Rechte der Betroffenen auch nach der Übermittlung über die Grenzen hinweg sicherzustellen. Als Maßnahmen werden außer der Ratifizierung der Europaratskonvention sowie der Beachtung der OECD-Leitlinien eine bürgerfreundliche Gestaltung internationaler Datenverarbeitungssysteme, die Sicherstellung von Berichtigungen, Aktualisierungen und Löschungen von Daten auch im Ausland sowie eine verstärkte internationale Zusammenarbeit der Datenschutzbeauftragten gefordert.

Ein konkreter Schritt insbesondere zur Realisierung der letzten Forderung wird die Einrichtung eines ständigen Sekretariats der Internationalen Konferenz der Datenschutzbeauftragten sein, für dessen Sitz sich die französische Datenschutzkommission beworben hat.

¹⁾ vgl. Anlage 2.1

Eine *Zusatzklärung der Datenschutzbeauftragten der EG-Länder*²⁾ verweist insbesondere darauf, daß der für Ende 1992 angestrebte EG-Binnenmarkt auch auf den freien Austausch personenbezogener Informationen etwa in den Bereichen Direkt-Marketing/Adressenhandel und Kreditinformationen gerichtet sei; zunehmend würden auf europäischer Ebene statistische Daten erhoben, einige Länder planten ein Pilotprojekt für ein gemeinsames polizeiliches Fahndungssystem („Schengener Informationssystem“), die Einrichtungen der EG selbst führten zunehmend personenbezogene Datenbanken, die keinem Datenschutzgesetz unterlägen, da die Europäischen Gemeinschaften selbst weder eine interne Datenschutzregelung besitzen noch sich der Europaratskonvention angeschlossen haben.

Für „Europa 1992“ wird ein umfassender und konsistenter Ansatz zur Verwirklichung der Grundsätze des Datenschutzes in den Mitgliedsländern gefordert. Im einzelnen schlägt die Konferenz vor, durch entsprechende Rechtsakte der Gemeinschaft die Grundsätze der Europaratskonvention Nr. 108 nicht nur für die Mitgliedsstaaten, sondern auch für die Institutionen der EG selbst verbindlich zu machen, sowie eine unabhängige Datenschutzkontrollinstanz einzurichten, die die Institutionen der EG in Datenschutzfragen berät und die Verarbeitung personenbezogener Daten in der EG kontrolliert.

Ich erhoffe mir von diesen bedeutsamen, in Berlin gefaßten Beschlüssen einen deutlichen Impuls zur Verbesserung des Datenschutzes im internationalen Datenverkehr einerseits, im europäischen Informationsmarkt andererseits.

Neben den umfassenden Problemen des internationalen Datenaustausches hat sich die Konferenz auch den *technischen Problemen der Telekommunikation* zugewandt. Hierzu fanden bereits seit Jahren regelmäßige Sitzungen des Arbeitskreises Medien der Internationalen Konferenz in Berlin statt, der für die Konferenz bereits mehrere Beschlüsse erarbeitet hat.

In diesem Jahr hatte der Arbeitskreis der Konferenz einen Beschlüßentwurf zu ISDN, der künftigen Netzstruktur für öffentliche, aber auch lokale Telekommunikationssysteme vorgelegt³⁾. Er wurde von der Konferenz begrüßt; die Teilnehmer wurden aufgefordert, die Forderungen in den einzelnen Staaten durchzusetzen⁴⁾.

Auch auf diesem Spezialgebiet, für das sich der Berliner Datenschutzbeauftragte national und international engagiert hatte, wird ein ständiges Sekretariat für sinnvoll gehalten. Unter der neuen Bezeichnung „Arbeitsgruppe Telekommunikation und Medien“ wird sich der interessierte Teil der Datenschutzbeauftragten künftig regelmäßig in Berlin mit den aktuellen Problemen der Fortentwicklung der Telekommunikation befassen.

2.2 Vom Sammeltrieb eines Nachrichtendienstes

Im Berichtszeitraum trat mit dem Landesamt für Verfassungsschutz, in Berlin als Abteilung IV der Senatsverwaltung für Inneres eingegliedert, eine Behörde in das Rampenlicht des öffentlichen Interesses, die zuvor in besonderem Maße als Teil der staatlichen Geheimsphäre erschien. Vor allem im Zusammenhang mit der Diskussion über die Verfassungstreueprüfungen im öffentlichen Dienst („Berufsverbote“) war die Rolle dieser Dienststelle in der Öffentlichkeit stets kritisch betrachtet worden, ohne daß jedoch Transparenz über ihre Aktivitäten hergestellt worden wäre.

Im Gegenteil, unter – allgemein für verfassungswidrig gehalten – Berufung auf eine Bestimmung in den Datenschutzgesetzen weigerte sich das Amt bis in die jüngste Zeit, den betroffenen Bürgern selbst in den Fällen Auskunft geben, in denen die vom Amt gesammelten Daten von diesem selbst stammten oder in denen nichts anderes als öffentlich zugängliche Informationen vorlagen.

Die Kontrolle des Landesamtes gehört zu den Aufgaben des Berliner Datenschutzbeauftragten. Im Laufe der vergangenen Jahre hatte ich in einer Vielzahl von Einzelvorgängen Überprü-

fungen vorgenommen, die auch zur Feststellung von Mängeln und zu Beanstandungen führten. Diese Mängel waren auch Gegenstand von Berichten, die ich gegenüber der im Jahre 1987 eingerichteten Parlamentarischen Kontrollkommission (PKK) abgegeben habe.

Der taz-Komplex

Ende November 1988 wurde im Zusammenhang mit der Tätigkeit der PKK öffentlich die Frage erörtert, ob das Landesamt für Verfassungsschutz jahrelang unbefugt Erkenntnisse über Journalisten und ganze Zeitungen, insbesondere über die alternative „Tageszeitung“ (taz) gesammelt habe. In der folgenden Zeit gingen beim Datenschutzbeauftragten eine Reihe von Eingaben ein, in denen Journalisten die Befürchtungen äußerten, sie seien vom Landesamt in ihren Rechten verletzt worden. Diese Ereignisse nahmen ich zum Anlaß, von Amts wegen eine breit angelegte Prüfung vorzunehmen, ob der Verdacht, das Landesamt verarbeitet generell personenbezogene Daten über Journalisten, gerechtfertigt war.

Über die Ergebnisse der Prüfung berichtete ich sowohl in dem am 9. Dezember 1988 eingesetzten Untersuchungsausschuß zur „Aufklärung von möglichen Fehlentwicklungen beim Landesamt für Verfassungsschutz“ am 10. Januar 1989 als auch – nach weiteren Untersuchungen – dem Senator für Inneres in einem Prüfbericht vom 10. März 1989.

Darin kam ich zu folgenden Feststellungen:

Im November 1977 erschien in der vom Berliner Landesamt für Verfassungsschutz als „linksterroristisches Agitationsblatt“ eingeordneten Schrift „radikal“ ein „Aufruf zur Gründung einer überregionalen Tageszeitung“. Aus diesem Anlaß wurde vom Landesamt eine *Sachakte* unter dem Arbeitstitel „Neue überregionale linksradikale Tageszeitung“ angelegt. In diesem Vorgang, der zum Zeitpunkt der Einsichtnahme vierzehn Bände umfaßte, wurden bis in die Gegenwart beim Landesamt eingehende Materialien gesammelt, die aus der Sicht des Amtes einen Bezug zur taz aufwiesen. Hierzu gehörten anfangs Berichte und Unterlagen zur Gründungsphase der taz, später Materialien und Erkenntnisse zu einzelnen Mitarbeitern der Zeitung. Nach den Erkenntnissen aus einzelnen Aufklärungsmaßnahmen in den Jahren 1981 bis 1983 (Umfragen bei Bundesamt und Landesämtern, Einholung von Informationen bei verschiedenen Behörden und Personen) nimmt der Anteil der in der taz veröffentlichten Artikel stark zu.

Noch im August 1988 wird die Einstufung der taz als Verdachtsfall gerechtfertigt, jedoch darauf hingewiesen, daß sich im Jahr 1984 abzuzeichnen begann, daß sich „die Tageszeitung immer mehr zu einem reinen Alternativblatt zur bürgerlichen Presse entwickelt habe“. Niedergelegt wurde ferner, daß diese Entwicklung den zuständigen Sachbearbeiter hätte veranlassen müssen, einen entsprechenden zusammenfassenden Auswertungsvermerk zu fertigen und das weitere Sammeln von Materialien zum taz-Komplex einzustellen. Dies unterblieb „aus Gründen der Arbeitsüberlastung“.

Seit Beginn der Datenerhebung im Zusammenhang mit der taz wurden zu Personen, die in diesem Zusammenhang auffällig wurden, Aktenzeichen mit Hinweis auf die taz-Akte in *Nachrichtendienstlichen Informationssystemen (NADIS)* eingespeichert bzw. vorhandenen Aktenzeichen zugespeichert. Erst im November 1987 wurde vom Gruppenleiter die Anweisung gegeben, die Datensätze aller Personen zu löschen, die nur mit einer taz-Fundstelle gespeichert waren. Bei einer meiner Überprüfungen am 13. Dezember 1988 wurde allerdings in zwei Fällen nach wie vor ein derartiges Aktenzeichen in NADIS gefunden.

Als weitere Strukturierungshilfe wurde eine nach Personen geordnete „Strukturkartei“ angelegt. Diese Karteikarten enthielten (entsprechend der allgemeinen Übung) kurze Beschreibungen der einzelnen Sachverhalte, die im Zusammenhang mit den betroffenen Personen festgestellt worden waren. Diese Strukturkartei, die nach Aussage der Mitarbeiter ca. 50 Datensätze enthielt, wurde Anfang 1988 aufgelöst. Zu einzelnen Personen wurden darüber hinaus auch Personenakten angelegt.

²⁾ vgl. Anlage 2.2

³⁾ vgl. Anlage 2.3

⁴⁾ vgl. unten unter 2.4

Ich kam in meinem Prüfbericht zu folgenden Bewertungen:

Rechtsgrundlage für das Berliner Landesamt für Verfassungsschutz ist das Gesetz über das Landesamt für Verfassungsschutz (VerfSchG) vom 21. Februar 1952, das zwischenzeitlich mehrfach geändert wurde.

Dieses Gesetz enthält zur Verarbeitung personenbezogener Daten lediglich Vorschriften über das Recht des Landesamtes, über alle Angelegenheiten, deren Aufklärung es zur Durchführung seiner Aufgaben für erforderlich hält, von allen öffentlichen Stellen des Landes Auskünfte zu erlangen (Befugnis zur Datenerhebung, § 3 Abs. 1) sowie über die entsprechende Pflicht dieser Stellen, auch unaufgefordert alles mitzuteilen, was ihnen über Bestrebungen bekannt wird, die die freiheitliche demokratische Grundordnung bedrohen (Pflicht zur spontanen Datenübermittlung, § 3 Abs. 2). Im übrigen ist die Verarbeitung personenbezogener Daten spezialrechtlich nicht geregelt.

Entsprechende Regelungen sind seit dem Urteil des Bundesverfassungsgerichts zum Volkszählungsurteil angemahnt. Ich habe mehrfach auf die Notwendigkeit einer Regelung hingewiesen⁵⁾ und einen Forderungskatalog für ein Verfassungsschutzgesetz vorgelegt⁶⁾.

Es kam bereits mehrfach zu Novellierungsentwürfen. Zuletzt hat die Bundesregierung am 20. Dezember 1988 im Rahmen eines Gesetzes zur Fortentwicklung der Datenverarbeitung und des Datenschutzes auch den Entwurf eines Gesetzes über die Zusammenarbeit des Bundes und der Länder in Angelegenheiten des Verfassungsschutzes und über das Bundesamt für Verfassungsschutz beschlossen, die derzeit im Innenausschuß des Bundestages beraten werden.

Auch untergesetzliche Regelungen, die eine bundeseinheitliche Handhabung garantieren könnten, fehlen, obwohl gerade bei den Verfassungsschutzämtern der Zusammenarbeit größte Bedeutung zukommt. Jedenfalls im Berliner Landesamt bestehen keine Richtlinien für die Aktenführung. Auch die Erfassung personenbezogener Daten auf sortierbaren und auswertbaren Datenträgern („Verkartungspläne“) ist formal nicht geregelt. Damit kann bei der rechtlichen Bewertung von Informationssammlungen nur auf die Grundsatznormen des Berliner Datenschutzgesetzes (BlnDSG) i. V. m. den Aufgabenzuweisungen in § 2 VerfSchG zurückgegriffen werden. Hier spielt der Begriff der „Erforderlichkeit zur rechtmäßigen Erfüllung der in der Zuständigkeit der speichernden Stelle liegenden Aufgaben“ (§§ 9, 10 BlnDSG) die zentrale Rolle. Diese im Lichte der Verfassungsrechtsprechung nicht hinreichend normenklare Generalklausel muß im Hinblick auf das Grundrecht auf informationelle Selbstbestimmung sowie das daraus abzuleitende Zweckbindungsgebot restriktiv interpretiert werden. Die höchstrichterliche Rechtsprechung legt insbesondere nahe, den Begriff der Erforderlichkeit im Sinne einer strengen Anwendung des verfassungsrechtlichen Verhältnismäßigkeitsgebotes auszulegen: Die Verarbeitung personenbezogener Daten muß danach für die gesetzlichen Zwecke geeignet sein, unter verschiedenen zur Wahl stehenden Maßnahmen den geringstmöglichen Eingriff bewirken und insgesamt bei einer Abwägung zwischen Verwaltungszweck und informationeller Selbstbestimmung des Betroffenen angemessen sein.

An Hand dieser Maßstäbe wurden die vorgefundenen Informationssammlungen bewertet.

Die Sachakte

Zweifel waren bereits an der Geeignetheit der Sachakte anzubringen. Bezugspunkt für die Güterabwägung war hier unbestritten die Aufgabe, Auskünfte, Nachrichten und sonstige Unterlagen über Bestrebungen zu sammeln, die gegen die freiheitliche demokratische Grundordnung gerichtet sind (§ 2 Abs. 1 Nr. 1 VerfSchG). Diesem Zweck dienen die Unterlagen nur dann, wenn sich die Zuordnung der Daten zu einer extremistischen Zielsetzung belegen läßt (vgl. auch Art. 87 Abs. 1 GG). Dies schließt zwar nicht aus, daß Unterlagen in bloßen Verdachtsfällen

gespeichert werden. Erhärtet sich der Verdacht jedoch nicht, so läßt sich auch die Geeignetheit nicht mehr begründen. Die Unterlagen sind dann zumindest dem Verwaltungsvollzug zu entziehen (zu „sperrern“), nach dem Rechtsgedanken des BlnDSG sogar zu löschen, wenn nicht schutzwürdige Belange des Betroffenen (z. B. Beweissicherung) dem entgegenstehen (§ 14 Abs. 3 BlnDSG). Der Verdacht, daß es sich bei der taz um ein Unternehmen mit extremistischer Zielsetzung handelt, war selbst für den Verfassungsschutz spätestens 1984 ausgeräumt; meine Überprüfung der Akte legt darüber hinaus die Vermutung nahe, daß man bei einer kritischen Prüfung bereits erheblich früher zu dieser Bewertung hätte kommen können. In diesem Licht erscheinen die zahlreichen, zwischen 1981 und 1983 vorgenommenen Erhebungsmaßnahmen schon im Hinblick auf die Geeignetheit der Maßnahme als problematisch.

Soweit die Geeignetheit die Sammlung der Informationen trägt, war zu prüfen, ob diese auch erforderlich in dem Sinne waren, daß sie die für den Verwaltungszweck am wenigsten belastende Maßnahme darstellten. Zwar kann davon ausgegangen werden, daß eine Sachakte, also eine auf einen Sachzusammenhang orientierte Akte, weniger belastend ist als eine Personenakte, die die Erkenntnisse zu einer Person bündelt: Daß dem Amt bekannte Persönlichkeitsbild erschließt sich nicht auf den ersten Blick, dies setzt vielmehr erst einen mehr oder weniger aufwendigen Such- und Ordnungsprozeß voraus. Dennoch können aus einer Sachakte mit einem mehr oder weniger großen Aufwand jederzeit die zu einer Person vorhandenen Daten wieder herausgesucht und zusammengestellt werden; dies zumal dann, wenn hierzu in Form von automatischen oder manuellen Dateien Hilfsmittel vorhanden sind.

Auch bei einer Sachakte ist damit die Erforderlichkeit im Hinblick auf den geringstmöglichen Eingriff zu prüfen. Berücksichtigt man, daß die Aufgabe des Verfassungsschutzes primär die Beobachtung von Bestrebungen, also Organisationen, und nicht von Einzelpersonen ist, ist die Verarbeitung personenbezogener Daten nur in dem Umfang zulässig, in dem sie für die Beurteilung der Organisation unerlässlich ist. Dies führt unter dem Blickwinkel der Erforderlichkeit zu der Forderung, in institutionsbezogenen Sachakten den Anteil personenbezogener Daten auf das unerlässliche Ausmaß zu beschränken. Das Studium der taz-Akte zeigte demgegenüber das Gegenteil: Zeitweise (insbesondere zwischen 1981 und 1983) konzentrieren sich die Unterlagen auf eine für die Beurteilung des Unternehmens taz in der Regel irrelevante Erhebung persönlicher Daten einzelner Journalisten.

Schließlich sind auch geeignete und erforderliche Maßnahmen daraufhin zu prüfen, ob sie im Verhältnis zum Verwaltungszweck nicht in unangemessener Weise in die Rechte der Betroffenen eingreifen. Diese Prüfung muß bei jeder Information vorgenommen werden, die in eine Sammlung aufgenommen wird; besonders strenge Kriterien sind naturgemäß da anzulegen, wo die Daten wegen ihrer Intimität oder aber wegen ihrer möglichen Folgewirkungen besonders sensibel sind.

Die Prüfung der taz-Akte hat ergeben, daß auch unter diesem Gesichtspunkt nicht hinreichend zurückhaltend vorgegangen wurde. So wären z. B. vorgefundene Informationen über die nichteheliche Abstammung einer Journalistin, eine gemeinsame Reise von drei Journalisten nach Westdeutschland oder Angaben über „Schlafplätze“ der Mitarbeiter auch dann problematisch, wenn sie – wovon hier nicht einmal auszugehen ist – einen Beitrag zur Einschätzung der Betroffenen leisten würden.

Somit wurde bei der Führung der taz-Unterlagen auch das Gebot der Angemessenheit nicht immer hinreichend berücksichtigt.

Diese Feststellungen haben nicht nur für sich Bedeutung. Sie deuten vielmehr auf einen grundsätzlichen Mangel hin, der allem Anschein nach über den vorliegenden Komplex hinaus für die gesamte Arbeit des Berliner Landesamtes bei der Beobachtung des Extremismus kennzeichnend war: Die Einhaltung der genannten Kriterien kann nur dann gewährleistet werden, wenn die Führung derartiger Sachakten durch Richtlinien geregelt ist und durch regelmäßige Revision auch kontrolliert wird. Nur wenn gewisse Grundsätze ordnungsgemäßer Aktenführung eingehalten werden, kann die Balance zwischen der Realisierung des

⁵⁾ vgl. u. a. Stellungnahme des Berliner Datenschutzbeauftragten zum Urteil des Bundesverfassungsgerichts zum Volkszählungsgesetz 1983 vom 15. Dezember 1983 Abghs.Drs. 9/1711 S. 21 ff. Jahresbericht 1985, Ziff. 2.3

⁶⁾ Jahresbericht 1986, Anlage 2

Verwaltungszwecks einerseits und der gebotenen Zurückhaltung andererseits eingehalten werden. Das Fehlen von Richtlinien zur Aktenführung und das Fehlen einer entsprechenden internen und externen Revision stellen den eigentlichen beanstandeten Mangel dar. *

Strukturkartei

Die zur Erschließung der Sachakte angelegte „Strukturkartei“ stellte ein Hilfsmittel dar, das den Inhalt von Sachakten auf Personen hin konzentriert darstellte, ohne daß eine Personenakte angelegt werden mußte. Es ist davon auszugehen, daß schnell zu erledigende Auskünfte unmittelbar aus dieser Kartei erteilt werden, so daß die Geltung des BlnDSG außer Frage steht. Die darin enthaltenen personenbezogenen Daten sind gem. § 9 Abs. 1 BlnDSG auf ihre Erforderlichkeit zu untersuchen.

Zu unterscheiden ist dabei die Entscheidung, eine Kartei als solche anzulegen, von der Frage, welche Einzeldaten in die Kartei einzutragen sind. Die Anlage einer auf eine Sachakte bezogenen Strukturkartei, die nach Personen geordnet ist, ist nur dann gerechtfertigt, wenn die entsprechenden personenbezogenen Daten für die Beobachtung der Bestrebung unerlässlich sind. Aus der Bewertung der Sachakte ergibt sich, daß bereits die Rechtmäßigkeit der Anlage der Strukturdatei (bzw. ihre weitere Führung, wenn sie vor Inkrafttreten des BlnDSG angelegt worden sein sollte) fragwürdig war, daß aber jedenfalls nach Wegfall des Verdachts die Weiterführung der Datei rechtswidrig war und damit einen Verstoß gegen § 9 Abs. 1 BlnDSG darstellte.

NADIS

Die Eintragung personenbezogener Daten in NADIS wirft über die angesprochenen Probleme hinaus die Frage auf, ob die Übermittlung der Daten an das Bundesamt und die anderen Landesämter rechtmäßig ist. Bei der Einrichtung eines Online-Anschlusses gilt der Gesamtbestand der Daten, auf die der Zugriff ermöglicht wird, als übermittelt (§ 4 Abs. 2 Nr. 2 BlnDSG). Das bedeutet, daß bei jedem einzelnen eingegebenen Datum die Erforderlichkeit der Kenntnis durch alle Ämter bestehen muß.

Dieses Erfordernis besteht von vornherein nicht bei den Daten, die bereits aus den oben genannten Gründen nicht in die Akte aufgenommen werden durften; da NADIS nur personenbezogene Globalverweise auf Aktenfundstellen enthält, heißt dies präziser:

Der Hinweis auf die taz-Akte durfte nicht in NADIS aufgenommen werden, wenn die entsprechenden Daten über den Betroffenen zur Beurteilung der taz keinen Beitrag leisten konnten. War der taz-Hinweis in diesen Fällen das einzige in NADIS eingegebene Aktenzeichen, so war auch die Einspeicherung der Personalia nicht rechtmäßig.

Differenziert zu beurteilen sind die Fälle, in denen die Aufnahme personenbezogener Daten in die Akte unerlässlich war. Die langjährige Philosophie des Landesamtes ging dahin, daß jede in einer Akte auftauchende Person in NADIS zu speichern ist, da NADIS als (einziger) umfassender Personennachweis geführt wird. Unter der Voraussetzung, daß alle Ämter so verfahren, und eine strenge Prüfung der Erforderlichkeit der Speicherung erfolgt, wurde dies vom Berliner Datenschutzbeauftragten zuvor nicht beanstandet.

Dieses Verfahren hatte auch gegensätzliche Effekte: Im Amt war es üblich, von der „Löschung personenbezogener Daten“ zu sprechen, wenn die Personalia in NADIS gelöscht sowie die zugehörigen Karteikarten vernichtet waren. Gleichwohl blieben die Unterlagen selbst in den Sachakten erhalten: Ein Umstand, der bei der Arbeit des Untersuchungsausschusses in diesem Fall für erhebliche Verwirrung sorgte.

Die Ergebnisse der Prüfung zeigen, daß die Philosophie des Landesamtes revisionsbedürftig ist. Dies gilt umso mehr, weil ich über verschiedene Erkenntnisse verfüge, die deutlich auf eine nicht bundeseinheitliche Handhabung hinweisen. Zudem muß die Erforderlichkeit der Übermittlung aller Daten an die anderen Ämter über NADIS stark bezweifelt werden.

Die Beanstandungen

Im einzelnen stellte ich u. a. folgende Mängel fest:

1. Die Sammlung personenbezogener Daten ging in Quantität und Qualität über das im Hinblick auf das Verhältnismäßigkeitsprinzip vertretbare Maß hinaus. Es wurden auch ungeeignete Daten gesammelt, es wurden nicht immer die am wenigsten belastenden Verarbeitungsformen gewählt und es wurden Daten gespeichert, die die informationelle Selbstbestimmung auf unangemessene Weise beeinträchtigen. In Einzelfällen stellt die Hereinnahme personenbezogener Unterlagen in die Sachakte für sich genommen bereits einen Mangel dar.
2. Durch die Einspeicherung in das Nachrichtendienstliche Informationssystem NADIS wurden Daten an das Bundesamt und die Landesämter für Verfassungsschutz übermittelt, die für die Aufgaben nicht erforderlich waren.
3. Ursprünglich für die Aufgabenerfüllung geeignete Daten wurden nicht rechtzeitig gelöscht. Die gesamte Sachakte wurde aufbewahrt und über NADIS und Karteien erschließbar gehalten, auch nachdem eine Behandlung der taz als Verdachtsfall nicht mehr geboten war.
4. Durchführungsvorschriften oder Arbeitsanweisungen, die die Ordnungsmäßigkeit der Führung von Informationssammlungen sicherstellen könnten, fehlen. Die Akten wurden nicht einmal nach eindeutigen, vorher festgesetzten, aus den Vorgängen erkennbaren Prinzipien geführt. Hierin ist ein Mangel an Ordnungsmäßigkeit zu sehen, die auch bei manuellen Datensammlungen geboten ist.
5. Regelmäßige Prüfvermerke, die eine interne oder externe Kontrolle hätten ermöglichen können, fehlen ebenso wie konkrete Berichts- und Vorlagepflichten weitgehend. Eine Fachaufsicht ist nicht eingerichtet; die Institution eines Staatssekretärs erscheint als Aufsichtsorgan nicht ausreichend, um die festgestellten Mängel zu beheben.

Ich verwies darauf, daß die Beseitigung der Mängel auf Dauer ein Verfassungsschutzgesetz voraussetze, das das Recht auf informationelle Selbstbestimmung in angemessener Weise berücksichtigt. Die beim Landesamt für Verfassungsschutz angewandten Formen der Informationsverarbeitung können – auch soweit ich sie nicht beanstandet habe – derzeit nur im Rahmen des sogenannten Übergangsbonus gerechtfertigt werden.

Vertiefung der Prüfung

Mit dem Ende der Legislaturperiode stellte der Untersuchungsausschuß seine Arbeit ein. In der neuen Legislaturperiode wurde kein Untersuchungsausschuß zu dieser Thematik eingerichtet, allerdings benannte der Senator für Inneres eine Projektgruppe, die die Sachverhalte und Fragestellungen, für die das Abgeordnetenhaus den Untersuchungsausschuß eingesetzt hatte, umfassend klären sollte; hinzu kamen weitere, zum Teil öffentlich diskutierte Einzelfälle, die ebenfalls das Arbeitsverfahren des Landesamtes für Verfassungsschutz betrafen.

Zugleich wurde ich gebeten, den Senator für Inneres und die Projektgruppe durch weitere Einzelfallüberprüfungen zu Problembereichen zu unterstützen, die im Untersuchungsausschuß nicht mehr erörtert werden konnten (Verarbeitung personenbezogener Daten von Abgeordneten, Journalisten, Richtern, Staatsanwälten, Rechtsanwälten und Pfarrern). Dabei sollten Empfehlungen zur Ausgestaltung von Arbeitsanweisungen vorgelegt werden, die die künftige Arbeit des Landesamtes für Verfassungsschutz festlegen.

Diese Prüfungen, die im Juli 1989 abgeschlossen wurden, bestätigten auf allgemeinerer Ebene die im taz-Komplex gewonnenen Ergebnisse.

Im Hinblick auf diese Feststellungen war der weitaus größte Teil der aufgrund von Stichproben in die Prüfung einbezogenen Vorgänge zu beanstanden. Das Landesamt sagte in allen Fällen auch die Löschung der Daten zu, wobei der Vollzug derzeit aufgrund einer Weisung des Senators für Inneres (noch) nicht möglich ist.

Die eklatantesten Mängel stellte ich bei einer über viele Jahre geführten Sachakte zum Thema „Infiltration der Alternativen Liste“ mit den zugehörigen Erschließungsdateien fest. Unabhängig von der Frage der ursprünglichen Zulässigkeit der Sammlungen lagen die rechtlichen Voraussetzungen für die Speicherung von Daten von Personen, von denen lediglich AL-Aktivitäten bekannt gewesen seien, nicht mehr vor; so war spätestens seit Ende 1987 die AL vom Landesamt selbst nicht mehr als verfassungsfeindliche Bestrebung eingestuft worden. Die Dateien waren zur ordnungsgemäßen Aufgabenerfüllung des Landesamtes nicht mehr erforderlich; sie wurden auch nach der Erkenntnis, daß dies der Fall sei, fortgeschrieben; die Unterlagen wurden selbst dann nicht vernichtet, als bei zahlreichen Anfragen von AL-Mitgliedern und -Mandatsträgern gegen Ende 1987 die Unzulässigkeit der Sammlung offensichtlich geworden sein mußte.

Beanstandet wurde ferner, daß das Landesamt Ende 1987/Anfang 1988 Auskünfte gegeben hat, die die Empfänger irreleiten mußten. Dies betraf in erster Linie die Auskunftersuchen der Betroffenen, aber auch der Datenschutzbeauftragte wurde über die Verarbeitung dieser Daten nicht korrekt informiert. Ich betonte, daß dies nicht hingenommen werden könne und beanstandete die irreführenden Auskünfte mit Nachdruck.

Nicht bestätigt hat sich dagegen, daß bestimmte Berufsgruppen als solche gezielt beobachtet würden; auch von Journalisten werden personenbezogene Daten nur dann gesammelt, wenn zusätzliche extremistische Erkenntnisse angefallen sind.

Zur Beseitigung der Vollzugsmängel schlug ich eine Reihe von organisatorischen Maßnahmen vor; insbesondere halte ich den Erlaß entsprechender Verwaltungsvorschriften für sinnvoll, die im Gegensatz zum Bundesamt und anderen Landesämtern nur in sehr geringem Umfang vorliegen.

Empfehlungen

Die zentrale, inzwischen auch vom Landesamt nicht mehr bestrittene Beanstandung geht dahin, daß auch über Einzelsvorgänge hinaus im Landesamt eine erhebliche Anzahl nicht oder nicht mehr erforderlicher Akten aufbewahrt und entsprechende Daten in Datensammlungen gespeichert werden. Der große Umfang dieser nicht (mehr) rechtmäßig geführten Unterlagen kann nur durch eine umfassende Bereinigungsaktion beseitigt werden. Diese sollte einer eigens hierfür eingesetzten Arbeitsgruppe anvertraut werden.

Von entscheidender Bedeutung für die künftige Arbeit des Landesamtes ist eine präzise Regelung des Umgangs mit personenbezogenen Daten. Arbeitsanweisungen sollten entwickelt werden, die alle Phasen der Verarbeitung der Daten von der Entscheidung zur Aufbewahrung bis zur Vernichtung umfassen. Großes Gewicht sollten dabei die fortlaufenden Bewertungen der erhobenen und gespeicherten Informationen haben, die auch in die Akten aufgenommen werden müßten und in regelmäßigen Abständen der Überprüfung dienen, ob die Akte noch weiter geführt werden sollte.

Auch die Protokollierung des Zugriffs auf die Daten bzw. der Herausgabe von Daten innerhalb und außerhalb des Amtes muß umfassender vorgenommen werden.

Eine regelmäßige Überprüfung der Datenbestände sollte künftig verhindern, daß zu lange zu viele Daten aufbewahrt werden. Dabei müssen auch Verfahren gefunden werden, die verhindern, daß sich nach der Löschung der Daten in den Erschließungssystemen die Unterlagen an anderer Stelle wiederfinden. Der Umstand, daß dies derzeit nicht gewährleistet ist, hat in den Auseinandersetzungen im Untersuchungsausschuß eine wichtige Rolle gespielt.

Bereits im Prüfbericht zur taz wurde einer der Gründe für die Mängel im Landesamt im Fehlen einer Aufsicht gesehen. Die Einrichtung einer Fachaufsicht bei der Senatsverwaltung für Inneres und die Umwandlung des Landesamtes in eine nachgeordnete Behörde ist ein geeigneter Weg zur Verbesserung der Situation.

Daneben sollte eine innere Revision im Verfassungsschutz eingeführt werden, die gleichzeitig Aufgaben des behördlichen Datenschutzbeauftragten übernimmt. Hierdurch könnte nicht

nur eine gleichmäßige Umsetzung der zu erarbeitenden Arbeitsanweisungen sichergestellt, sondern auch die Kooperation mit dem Datenschutzbeauftragten verbessert werden.

Wesentliche Bedeutung für die Rückgewinnung des Vertrauens in der Bevölkerung dürfte sein, in welchem Ausmaß und auf welche Weise das Landesamt künftig auf Auskunftersuchen von Bürgern antwortet. Die Kriterien hierfür sollten ebenfalls in Arbeitsanweisungen niedergelegt werden.

Zwar ist davon auszugehen, daß die künftigen Verfassungsschutzgesetze den Auskunftsanspruch des Bürgers inhaltlich ausgestalten werden. Absehbar ist allerdings, daß auch dort Generalklauseln zur Abwägung zwischen dem informationellen Selbstbestimmungsrecht der Betroffenen und dem Geheimhaltungsinteresse des Amtes verwendet werden.

Unumstößlich ist insbesondere, daß das Landesamt künftig nicht mehr pauschal die Auskunft über die gespeicherten Daten verweigern kann. Die Tatsache, daß den Betroffenen nach den Datenschutzgesetzen kein Anspruch gegen den Verfassungsschutz zusteht, führt nicht zu einem Ausschluß der Auskunft, sondern zu der Verpflichtung zu einer ermessensfehlerfreien Entscheidung. Dabei ist dem Geheimhaltungsinteresse des Amtes nicht mehr der absolute Vorrang über das informationelle Selbstbestimmungsrecht der Betroffenen einzuräumen. Vielmehr ist eine Abwägung zu treffen, inwieweit die Interessen des Amtes die schutzwürdigen Belange der Bürger überwiegen. Dem modernen Grundrechtsverständnis entspricht es, wenn hierfür das Amt begründungspflichtig ist.

Auch kann dem Bürger nicht ausschließlich die Darlegungslast für sein Interesse an der Auskunftserteilung aufgebürdet werden. Sein Recht auf Auskunft besteht als Konsequenz des informationellen Selbstbestimmungsrechts, ohne daß ein zusätzliches Interesse (etwa zur Rechtsverfolgung) hinzutreten müßte. Auch das schlichte Interesse an Kenntnis über die gespeicherten Daten ist ein zu beachtendes Rechtsgut.

Die Mängelfeststellungen führten im Landesamt zu verschiedenen Aktivitäten. Insbesondere wurde damit begonnen, Arbeitsanweisungen für die verschiedenen Bereiche zu konzipieren.

Als erstes Ergebnis liegt inzwischen der Entwurf für eine Arbeitsanweisung zur Auskunftserteilung durch das Landesamt vor, die dem Bürger im Vorgriff auf die künftigen gesetzlichen Regelungen einen Anspruch auf Auskunftserteilung einräumt, wenn die Interessen des Amtes nicht überwiegen. Die Auskunftsverweigerung muß künftig - entsprechend der höchstgerichtlichen Rechtsprechung - in der Regel begründet werden.

Die Ausarbeitung weiterer Arbeitsanweisungen, insbesondere zur Aktenführung, wird folgen.

Ich gehe davon aus, daß auch der nunmehr eingerichtete Ausschuß für Verfassungsschutz des Abgeordnetenhauses den datenschutzrechtlichen Problemen beim Verfassungsschutz große Bedeutung beimessen wird. Eine der wesentlichen Aufgaben wird dabei die Schaffung eines Landesverfassungsschutzgesetzes sein, das den nunmehr erreichten, rechtsstaatlichen Stand an Transparenz auch bei dieser Behörde rechtlich festschreibt.

Verfassungsschutzgesetz

Ohne daß diese grundsätzlichen Probleme gelöst worden wären, trat Anfang Juli dieses Jahres das Fünfte Gesetz zur Änderung des Gesetzes über das Landesamt für Verfassungsschutz in Kraft, das auf einen Antrag der Koalitionsfraktionen zurückging⁷⁾. Damit wurde die bisherige parlamentarische Kontrollkommission durch den Ausschuß für Verfassungsschutz ersetzt, in dem alle Fraktionen des Abgeordnetenhauses vertreten sind. Eine umfassende Anpassung der materiellen Vorschriften des Gesetzes über das Landesamt für Verfassungsschutz wurde zunächst zurückgestellt. Aber auch das Fünfte Gesetz zur Änderung des Verfassungsschutzgesetzes enthält datenschutzrechtlich relevante Bestimmungen. Das Gesetz sieht vor, daß Eingaben einzelner Bürger oder einzelner Dienstkräfte des Landesamtes für Verfassungsschutz dem Ausschuß für Verfassungsschutz zur Kenntnis

⁷⁾ GBVl. 1989 S. 1237

zu geben sind. Der Ausschuß hat auf Antrag von zwei Mitgliedern Petenten oder einzelne Dienstkräfte des Landesamtes zu hören (§ 5 Abs. 4).

Ich hatte bei den Beratungen im Rechtsausschuß des Abgeordnetenhauses darauf hingewiesen, daß diese Vorschrift zur Folge hat, daß jede Beschwerde eines Petenten über das Landesamt ausnahmslos dem Ausschuß zur Kenntnis gegeben würde. Der Wortlaut der Vorschrift schließt es auch nicht aus, daß Anträge von Bürgern, die Auskunft über ihre beim Landesamt gespeicherten Daten verlangen und dies häufig mit einer Beschwerde verbinden, an den Verfassungsschutzausschuß weitergeleitet werden. Soweit dies ohne Einwilligung der Betroffenen geschieht, wie es das inzwischen verabschiedete Gesetz vorsieht, bestehen hiergegen erhebliche verfassungsrechtliche Bedenken. Das Bundesverfassungsgericht hat in seinem Volkszählungsurteil ausdrücklich darauf hingewiesen, daß kein Bürger durch die staatliche Erhebung und Weitergabe von personenbezogenen Informationen davon abgehalten werden darf, von seinen Grundrechten Gebrauch zu machen. Eben diese Gefahr wird durch das Gesetz über den Ausschuß für Verfassungsschutz jedoch heraufbeschworen. Ein Bürger, der sich mit einer Eingabe an das Landesamt wenden will, ohne daß diese Eingabe automatisch dem Ausschuß zur Kenntnis gegeben wird, ist gezwungen, von der Eingabe ganz abzusehen.

Der Senator für Inneres hat bei den Beratungen im Rechtsausschuß zu meinen Einwänden erklärt, die Regelung des Gesetzentwurfs beziehe sich nicht auf Auskunftsansprüche Betroffener über die zu ihrer Person gespeicherten Daten. Er hat außerdem zugesichert, meine Empfehlungen bei der Novellierung des Berliner Datenschutzgesetzes oder bei der noch bevorstehenden Anpassung des Verfassungsschutzgesetzes an die Vorgaben des Volkszählungsurteils zu berücksichtigen.

Zu berücksichtigen ist bei dieser Problematik auch ein Beschluß des Oberverwaltungsgerichts Berlin vom 10. Januar 1989⁸⁾, in dem das Gericht im Zusammenhang mit dem Untersuchungsausschuß das Recht des betroffenen Antragstellers betont hatte, vor der abschließenden Beratung eines Berichtes über die ihn betreffenden Tatsachen zum Untersuchungsthema informiert zu werden. Dieses Recht ist nach Auffassung des Oberverwaltungsgerichts Bestandteil des Grundrechts auf rechtliches Gehör. Den weitergehenden Antrag, dem Betroffenen die Teilnahme an den nicht-öffentlichen Sitzungen des Untersuchungsausschusses zu gestatten, lehnte das Oberverwaltungsgericht mangels eines einfachgesetzlichen Anhörungsrechtes ab. Aus diesem Beschluß ergibt sich, daß der Gesetzgeber durchaus die Möglichkeit gehabt hätte, ein entsprechendes Anhörungsrecht Betroffener nicht nur in einem Untersuchungsausschuß, sondern auch in einem ständigen Kontrollausschuß wie dem Verfassungsschutzausschuß durch einfaches Gesetz vorzuziehen. Dennoch verabschiedete der Rechtsausschuß den Entwurf mehrheitlich, ohne meine Einwände und Vorschläge zu berücksichtigen.

Ich werde bei der anstehenden Novellierung des Berliner Datenschutzgesetzes und des Gesetzes über das Landesamt für Verfassungsschutz darauf dringen, daß § 5 Abs. 4 des Gesetzes alsbald geändert wird.

2.3 Gentechnik

Allgemeines

Die Erhebung genetischer Informationen durch die Analyse der menschlichen Erbanlagen gewinnt immer stärkere Bedeutung. Die damit verbundenen datenschutzrechtlichen Probleme sind allerdings noch nicht gelöst. Ein Arbeitskreis der Datenschutzbeauftragten hat sich unter meiner Mitwirkung eingehend mit diesen Problemen auseinandergesetzt und für die Konferenz der Datenschutzbeauftragten ein Arbeitspapier vorbereitet, das Forderungen zu den wichtigsten Einsatzgebieten der Genomanalyse (Strafverfolgung, Arbeitsverhältnis, Versicherungswesen, pränatale Diagnostik und Neugeborenen-Screening) enthält.

Die folgenden Datenschutzüberlegungen gehen von dem derzeitigen wissenschaftlichen Erkenntnisstand aus, wonach

- durch Genomanalysen zwar genetische Dispositionen für bestimmte Krankheiten, nicht aber aktuell bestehende Erkrankungen - allenfalls deren Ursachen - feststellbar sind,
- die Vielfalt genomanalytischer Untersuchungsmethoden zu verlässliche Beschränkungen auf bestimmte Untersuchungsziele, insbesondere auf Feststellungen im nicht-codierenden Bereich des Genoms (Identitätsfeststellung) erlaubt,
- weder die Feststellung persönlicher oder charakterlicher Eigenschaften oder intellektueller Fähigkeiten möglich ist, noch Aussagen über das äußere Erscheinungsbild eines Menschen gewonnen werden können, die sich beispielsweise für Fahndungszwecke eignen.

Den erweiterten Möglichkeiten der Genomanalyse zur Früherkennung von Krankheitsanlagen, die zum Teil eine bessere medizinische Behandlung des Patienten oder zumindest eine Linderung seines Leidens ermöglichen, stehen schwerwiegende Risiken für die informationelle Selbstbestimmung des einzelnen gegenüber. Das Recht auf informationelle Selbstbestimmung als Teil des Grundrechts auf freie Entfaltung der Persönlichkeit umfaßt auch ein „Recht auf Nichtwissen“. Werden dem einzelnen bisher unbekannte Informationen über seine genetische Disposition etwa zu einer unheilbaren Krankheit aufgezwungen, die möglicherweise in der Zukunft ausbrechen kann, so wird dies in aller Regel zu schweren psychischen Belastungen führen, die in extremen Situationen auch die Gefahr eines Selbstmords begründen können. Zudem können genetische Informationen dazu beitragen, den Betroffenen sozial zu diskriminieren und auszugrenzen. Wegen der Vererbung genetischer Informationen betreffen diese in aller Regel mehrere Personen, z. B. Familienangehörige, die häufig über die Erhebung dieser Daten nicht informiert sein werden.

Die Bundesregierung hat zwar den Entwurf eines Gesetzes zur Regelung von Fragen der Gentechnik beschlossen, der jedoch Fragen der Humangenetik und damit auch der Genomanalyse bewußt ausklammert.

Genomanalyse für die Strafverfolgung und die Feststellung der Abstammung

Die Methode des sogenannten genetischen Fingerabdrucks (DNA-fingerprinting)⁹⁾ ist in diesem Jahr mehrfach in gerichtlichen Verfahren zum Einsatz gekommen. Das Landgericht Darmstadt hat auf der Grundlage dieses Beweismittels den Angeklagten in einem Vergewaltigungsprozeß freigesprochen, der zuvor von mehreren Zeuginnen belastet worden war. Das Oberlandesgericht Karlsruhe hat in einem Abstammungsprozeß die Vaterschaft eines Mannes aufgrund einer Genomanalyse festgestellt, dessen Vaterschaft sich bei Anwendung herkömmlicher Methoden der Blutuntersuchung nicht zweifelsfrei hatte bestätigen lassen. In beiden Fällen ist Revision zum Bundesgerichtshof eingelegt.

Die Anwendung dieser Methode bedarf allerdings unverzüglich eines klaren gesetzlichen Rahmens. Da es sich um ein qualitativ neues Verfahren handelt, ist für eine Berufung auf den sogenannten Übergangsbonus kein Raum. Deshalb hoffe ich, daß der Bundesminister der Justiz entsprechend seiner Ankündigung noch vor Jahresende den Entwurf einer entsprechenden Ergänzung zumindest der Strafprozeßordnung vorlegt. Diese wird sich unter dem Gesichtspunkt der informationellen Selbstbestimmung an folgenden Grundsätzen zu orientieren haben:

- Die Genomanalyse im Strafprozeß muß sich auf die Identitätsfeststellung und damit auf die sogenannten nicht-codierenden Abschnitte des Genoms beschränken, die aufgrund ihrer individuellen Struktur zuverlässig Auskunft darüber geben, ob eine bestimmte am Tatort gefundene Spur von einer Vergleichsperson stammt oder nicht. Das entscheidende Hilfsmittel bei dieser Untersuchung ist die sogenannte DNA-Sonde, eine künstlich hergestellte Erbsubstanz, mit

⁸⁾ Az. 8 S 449.88

⁹⁾ vgl. Jahresbericht 1988, Ziff. 2.2

deren Hilfe aus der untersuchten Erbinformation ein „menschliches Strickmuster“ unterschiedlich entwickelt wird. Diese DNA-Sonden müssen einem staatlichen Zulassungsverfahren unterworfen werden, bei dem zu prüfen ist, ob mit ihrer Hilfe ausschließlich die Informationen erhoben werden können, die der Hersteller der Sonde angegeben hat. Sonden, die über die Identität der untersuchten Person hinaus noch weitere Informationen sichtbar werden lassen, sind für die Verwendung im Strafprozeß nicht zuzulassen. Ihre Anwendung ist unter Strafandrohung zu stellen.

- Die Untersuchung darf nur in einem konkreten Strafverfahren an Vergleichspersonen oder an Spuren einer Straftat erfolgen.
- Die Untersuchung an Vergleichspersonen setzt eine richterliche Anordnung voraus, in der das Ziel, die anzuwendende Methode der Untersuchung und das ausführende Institut festzulegen sind.
- Nur besonders hierfür zugelassene Institute dürfen mit der Untersuchung beauftragt werden.
- Solange sonstige Beweismittel zur Überführung oder Entlastung eines Verdächtigen ausreichen, ist für die Anwendung der Genomanalyse kein Raum.
- Auch die Genomanalyse von Tatspuren darf nur der Identitätsfeststellung des Spurenlegers dienen und ist deshalb auf die nicht-codierenden Abschnitte des Genoms zu beschränken.
- § 81 b StPO und die Polizeigesetze der Länder lassen eine Anwendung genomanalytischer Methoden für präventiv-polizeiliche Zwecke nicht zu. Diese Rechtslage muß bestehen bleiben. Nach Abschluß eines Strafverfahrens darf die Polizei keine genomanalytischen Befunde weiter speichern oder für präventiv-polizeiliche Zwecke umwidmen. Der Senat hat in seiner Antwort auf eine Kleine Anfrage¹⁰⁾ im Abgeordnetenhaus erklärt, er beabsichtige nicht, die Nutzung „genetischer Fingerabdrücke“ zu Zwecken der Gefahrenabwehr zuzulassen. Daher werde auch das neu zu schaffende Polizeirecht keine Rechtsgrundlage dafür enthalten. Dies begrüße ich.
- Auch die Speicherung genomanalytischer Befunde bedarf einer zusätzlichen bereichsspezifischen Regelung in der Strafprozeßordnung, da § 81 b StPO hierfür ebensowenig ausreicht wie § 81 a StPO für die Datenerhebung. Eine Speicherung durch die Staatsanwaltschaft für Zwecke eines anderen, zukünftigen Strafverfahrens ist ausdrücklich zu untersagen. Sobald eine Vergleichsperson durch einen genomanalytischen Befund entlastet worden ist, muß dieser Befund gelöscht und aus den Akten entfernt werden.
- Die genomanalytische Untersuchung ist anonym durchzuführen. Den dafür zugelassenen Einrichtungen ist ausschließlich Zellmaterial mit einer Kennziffer, aber ohne Aktenzeichen des Verfahrens und ohne Namen des Beschuldigten zur Verfügung zu stellen. Nach Abschluß des Verfahrens ist die Kennziffer zu löschen.
- Genomanalytische Befunde müssen einer strengen Zweckbindung unterliegen. Für sie ist daher ein Beschlagnahmeverbot (unabhängig vom Ort der Aufbewahrung) vorzusehen, welches verhindert, daß für andere Zwecke zulässigerweise erhobene genetische Daten bei dritten Stellen (z. B. im Rahmen genetischer Beratung) für die Strafverfolgung genutzt werden können. Der herkömmliche Schutz von Patientendaten (§ 97 StPO) reicht hierfür nicht aus. Genomanalytische Befunde, die rechtswidrig erhoben worden sind, sollten im Strafprozeß einem Verwertungsverbot unterworfen werden.

Auch für die Anwendung der Genomanalyse im Verfahren der Abstammungsfeststellung ist eine bereichsspezifische Ergänzung der Zivilprozeßordnung erforderlich, die eine Beschränkung auf die nicht-codierenden Abschnitte des Genoms vorschreibt und die Untersuchung von einer richterlichen Anordnung abhängig macht.

Genomanalysen bei Einstellungs- und Vorsorgeuntersuchungen

Genomanalysen könnten auch im Arbeitsleben bei Einstellungsuntersuchungen für Stellenbewerber und bei Vorsorgeuntersuchungen an Bedeutung gewinnen. Sie geben keinen Aufschluß über den gegenwärtigen Gesundheitszustand, sondern nur über die genetische Disposition, möglicherweise über das Risiko, künftig einmal zu erkranken. Dieses Risiko hat der Arbeitgeber jedoch nach dem geltenden Arbeitsrecht mitzutragen; er darf es nicht auf einen Stellenbewerber abwälzen, indem er von ihm die Durchführung einer Genomanalyse verlangt. Auch für Vorsorgeuntersuchungen sind Genomanalysen kein taugliches Mittel, weil sie mit ihrer eingeschränkten Aussagekraft die hohen Anforderungen an einem wirksamen Vorsorgeschutz nicht ausreichend erfüllen.

Genomanalysen im Arbeitsleben sind deshalb gesetzlich zu verbieten. Nur so ist die informationelle Selbstbestimmung des Arbeitnehmers unter den Bedingungen der Privatautonomie des Arbeitgebers effektiv zu sichern, und nur so kann verhindert werden, daß Arbeitsschutz hinter Arbeitnehmerselektion zurücktritt. Dem Arbeitnehmer ist es unbenommen, außerhalb des Arbeitsverhältnisses bei einer zugelassenen Einrichtung oder Arztpraxis seiner Wahl, jedoch nicht beim Betriebsarzt, genomanalytische Untersuchungen durchzuführen. Arbeitgebern ist gesetzlich unter Strafandrohung zu untersagen, von Bewerbern oder Arbeitnehmern Bescheinigungen über genomanalytische Befunde zu fordern oder entgegenzunehmen, die der Betroffene auf eigene Initiative erstellen ließ. Für den öffentlichen Dienst gelten diese Forderungen entsprechend.

Genomanalyse beim Abschluß von Versicherungsverträgen

Auch beim Abschluß eines Versicherungsvertrages ist die Genomanalyse keine geeignete und verhältnismäßige Methode zur Feststellung des gegenwärtigen Gesundheitszustandes. Eine sichere Vorhersage, ob und wann eine genetisch bedingte Krankheit in der Zukunft beim Versicherungsnehmer ausbrechen wird, ist selbst mit Hilfe der Genomanalyse in aller Regel nicht möglich. Außerdem ist zu berücksichtigen, daß die Versicherungsunternehmen die Daten der Versicherten weitgehend automatisiert verarbeiten. Wenn auch genetische Informationen in dieser Weise verarbeitet werden dürften, so bestünde die Gefahr, daß prognostisch unsichere und interpretationsbedürftige genetische Daten ohne Kontext sich zu Scheinfakten verfestigen und über Wagnis-Dateien ganze Bevölkerungsgruppen als mögliche Versicherungsnehmer ausgrenzen würden.

Nur in ganz bestimmten Fällen, bei denen aufgrund bestimmter Gendefekte der Ausbruch einer schweren Erbkrankheit innerhalb überschaubarer Zeit sehr wahrscheinlich ist, muß der Versicherungsnehmer, der hiervon aufgrund einer freiwilligen Genomanalyse vor Abschluß des Versicherungsvertrages Kenntnis erhalten hat, dies dem Versicherer anzeigen. Im übrigen darf der Abschluß eines Versicherungsvertrages nicht von der Durchführung einer Genomanalyse abhängig gemacht werden.

Genomanalyse bei der pränatalen Diagnostik und beim Neugeborenen-Screening

Genomanalytische Methoden werden bereits heute bei der genetischen Beratung vor der Schwangerschaft, bei der pränatalen (vorgeburtlichen) Diagnostik und bei der Untersuchung Neugeborener („Screening“) angewandt. In der Praxis liegt der Schwerpunkt derzeit bei der pränatalen Diagnostik. Dabei kann Schwangeren, die – z. B. altersbedingt – einer Risikogruppe angehören, in mehr als 90 % der Fälle die Angst genommen werden, ihr Kind könne mit bestimmten genetischen Defekten geboren werden.

Diesen positiven Möglichkeiten der Genomanalyse stehen jedoch schwerwiegende Probleme gegenüber wie die Gefahr einer pränatalen Selektion oder die gesellschaftliche Diskriminierung Behinderter. Darüber hinaus ist die informationelle Selbstbestimmung Dritter gefährdet, die die Beratung nicht gesucht haben. Schließlich ist die Gewinnung von sensiblen Überschußinformationen in den humangenetischen Labors möglich und nur

¹⁰⁾ Nr. 397 v. 9.8.1989, LPD v. 13.9.1989, S. 4

schwer kontrollierbar. Gleichwohl erscheint ein Verbot der Genomanalyse im vorgeburtlichen Bereich angesichts der erweiterten Erkenntnismöglichkeiten für die einzelne Schwangere nicht gerechtfertigt. Zwar hat der Staat mit der Entscheidung für die Straflosigkeit des Schwangerschaftsabbruchs aufgrund kindlich-eugenischer Indikation keine Entscheidung darüber getroffen, ob Kinder mit unheilbaren Erbkrankheiten geboren werden sollen oder nicht. Dies bleibt die alleinige Entscheidung der Eltern. Wenn die Wissenschaft neue, für diese Entscheidung wesentliche Informationen erheben kann, darf der Staat sie jedoch den unmittelbar Betroffenen nicht vorenthalten.

Allerdings sollte der Gesetzgeber eine grundsätzliche Entscheidung über die Zulassung genomanalytischer Methoden vor und nach der Geburt fällen und angesichts der beschriebenen Risiken mit genauen Regelungen über Erhebung und Verwendung solcher genetischer Daten verbinden. Ärztliches Standesrecht oder Absprachen zwischen Kostenträgern reichen hierfür nicht aus. Eine gesetzliche Regelung sollte sich an folgenden Grundsätzen orientieren:

1. Im Rahmen der pränatalen Diagnostik dürfen nur Informationen über das Vorhandensein oder Fehlen von Erbanlagen erhoben werden, die zu einer so schwerwiegenden Gesundheitsschädigung des Kindes führen würden, daß ein Schwangerschaftsabbruch straffrei bliebe. Alle darüber hinaus bei der Untersuchung zwangsläufig anfallenden genetischen Informationen sind im Zeitpunkt ihrer Entstehung sofort wieder zu vernichten. Über das Geschlecht des Kindes darf die Schwangere erst nach Ablauf der 12. Schwangerschaftswoche informiert werden.
2. Das Neugeborenen-Screening ist auf Erbkrankheiten zu beschränken, die geheilt oder zumindest spürbar therapeutisch begleitet werden können. Auch beim Neugeborenen-Screening muß die informierte Einwilligung der Eltern vorliegen. Genomanalytische Untersuchungsmethoden dürfen nicht routinemäßig angewandt werden. Auch aus der Pflicht zur elterlichen Sorge und dem Kindeswohl kann nicht abgeleitet werden, daß die Eltern einem Neugeborenen-Screening zustimmen müssen, ohne daß Anzeichen für genetische Risiken vorliegen.
3. Die Erhebung genetischer Daten vor der Empfängnis bei pränataler Diagnostik und beim Neugeborenen-Screening setzt in jedem Einzelfall die informierte Einwilligung der Eltern voraus. Dies schließt ein, daß die Eltern zuvor darüber aufgeklärt worden sind, daß die Genomanalyse keine Gesundheitsgarantie für ihr Kind bieten kann und auch bei Anwendung genomanalytischer Methoden ein Basisrisiko für nicht erkennbare, unvorhersehbare Erkrankungen des Neugeborenen stets bestehen bleibt. Die Eltern sind eingehend über die möglichen Ergebnisse einer Genomanalyse und die sich daraus ergebenden schwerwiegenden Entscheidungen (z. B. für oder gegen eine Abtreibung) aufzuklären.
4. Die Freiwilligkeit der Entscheidung für oder gegen die Anwendung genomanalytischer Methoden darf auch nicht indirekt beeinträchtigt werden. Zwar ist der Arzt nach der Rechtsprechung des Bundesgerichtshofes verpflichtet, der Schwangeren die jeweils neuesten diagnostischen Methoden darzulegen, wenn sie einer Risikogruppe angehört. Dies darf jedoch in der Praxis nicht zu einer direktiven Beratung oder routinemäßigen Erhebung genetischer Daten (Embryonen-Screening) führen, der sich die Schwangere faktisch nicht entziehen kann. Jede Benachteiligung von Eltern, die sich gegen die Anwendung genomanalytischer Methoden vor der Geburt ihres Kindes entscheiden, z. B. durch Kürzung von Krankenversicherungs- oder anderen Sozialleistungen, ist unzulässig. Der Staat muß alles tun, um zu verhindern, daß die Möglichkeiten der Genomanalyse in der Gesellschaft der Einstellung zum Durchbruch verhelfen, die Geburt behinderter Kinder oder von Kindern mit hohem Gesundheitsrisiko sei „unnötig“ oder „unerwünscht“.
5. Das Recht auf informationelle Selbstbestimmung umfaßt auch ein „Recht auf Nichtwissen“. Deshalb darf der Arzt keine Beratung durchführen, bei der er Dritten (z. B. ein-eigenen Zwillingen oder anderen Familienangehörigen der beratenen Person), die nicht selbst an der Beratung teilgenommen haben, Informationen über genetische Risiken oder Defekte aufdrängt.
6. Das Untersuchungsmaterial sollte dem untersuchenden Institut nur mit einem verschlüsselten Identifikator ohne Name und Anschrift des Betroffenen zugänglich gemacht werden. Der behandelnde Arzt sollte den Untersuchungsauftrag an das Institut und damit den Umfang der Genomanalyse auf der Grundlage der erfüllten Einwilligung schriftlich festlegen. Das Institut darf Forschung nur mit anonymisierten genetischen Daten betreiben.
7. Die Dokumentation der vor und nach der Geburt erhobenen genetischen Daten des Kindes sollte den Eltern überlassen bleiben. Den Eltern ist die schwierige Entscheidung vorzubehalten, ob und wann ein Kind oder ein betroffener Dritter über das Risiko einer Erkrankung oder Weitervererbung eines genetischen Defekts aufgeklärt werden soll. Die Speicherung genetischer Daten in öffentlichen Dateien und Akten ist unzulässig.
8. Auf europäischer Ebene sind Maßnahmen zu treffen, die eine Umgehung von strikten nationalen Regeln zur Genomanalyse bei der genetischen Beratung, der pränatalen Diagnostik und beim Neugeborenen-Screening effektiv unterbinden. Den Vorarbeiten des Europarats auf diesem Gebiet kommt deshalb besondere Bedeutung zu¹¹⁾.

Forschungsprojekte im Bereich der Humangenetik

Im Rahmen des vom Umweltbundesamt finanzierten Forschungsprojektes „Population Monitoring von Chromosomenanomalien“ ist geplant, daß die 42 Humangenetischen Institute in der Bundesrepublik dem Humangenetischen Institut der Freien Universität Berlin, Universitätsklinikum Rudolf-Virchow, die Befunde der bei ihnen durchgeführten Untersuchungen des Fruchtwassers und der Eihautzellen (Chorionzotten) auf Datenträgern übermitteln. Die Fruchtwasseruntersuchungen selbst werden in den meisten Fällen von niedergelassenen Ärzten oder Frauenkliniken an Schwangeren durchgeführt, die das entnommene Fruchtwasser den Humangenetischen Instituten zur Untersuchung übermitteln. Die Entnahme von Chorionzotten erfolgt ausschließlich in Kliniken. Die Humangenetischen Institute führen mit dem entnommenen Zellmaterial Chromosomenanalysen durch, um numerische oder strukturelle Chromosomenanomalien wie z. B. Trisomie 21 (Mongolismus) in einem möglichst frühen Stadium der Schwangerschaft feststellen zu können. Gegenwärtig werden pro Bundesland ca. 2 000 derartige Untersuchungen pro Jahr durchgeführt. Zweck des Forschungsprojektes ist es, für die gesamte Bundesrepublik das Auftreten von Chromosomenanomalien statistisch zu erfassen und etwaige Zusammenhänge mit Umwelteinflüssen aufzudecken. Insbesondere seit der Reaktorkatastrophe von Tschernobyl ist die Notwendigkeit der Erforschung dieser Zusammenhänge allgemein anerkannt.

Das Institut für Humangenetik hat mich frühzeitig um Beratung bei der Durchführung dieses Forschungsprojektes gebeten. In zahlreichen Gesprächen habe ich eine Reihe von datenschutzrechtlichen Verbesserungen erreichen können.

In einem weiteren Forschungsprojekt, das am selben Institut durchgeführt wurde, sollten Daten über die „Beteiligung von schwangeren Frauen ab dem 35. Lebensjahr an Fruchtwasseruntersuchungen (Amniozentesen)“ erhoben und ausgewertet werden. Dazu sollten Mütter gesunder Kinder im Wochenbett von einer Forscherin befragt werden. Ich habe darauf hingewiesen, daß dies nur zulässig ist, wenn zuvor der behandelnde Arzt die Einwilligung der Mütter zur Kontaktaufnahme mit der Forscherin einholt. Auch während der Befragung muß die Patientin jederzeit die Möglichkeit haben, Antworten zu verweigern oder die Befragung insgesamt abzubrechen. Darüber hinaus beschränkte sich die Erhebung aufgrund meiner Empfehlung weitgehend auf anony-

¹¹⁾ Council of Europe, Ad Hoc Committee of Experts of Progress in the Biomedical Sciences, Draft Recommendation on Prenatal Genetic Screening, Prenatal Genetic Diagnosis and Associated Genetic Counselling and Draft Explanatory Memorandum, CAHBI (89) 6.

miserte Angaben. Die Daten, die auf einem PC des Instituts für Humangenetik gespeichert und verarbeitet wurden, sind zwischenzeitlich gelöscht worden.

In einem dritten Projekt soll mit Hilfe der Technik des „genetischen Fingerabdrucks“ die Zahl der *eineiigen oder zweieiigen gleichgeschlechtlichen Zwillinge* in Berlin bestimmt werden. Hierzu ist es notwendig, nach der Geburt von beiden Kindern ein Stück Nabelschnur zu entnehmen und im Institut einer DNA-Analyse zu unterziehen. Dies setzt die schriftliche Einwilligung der Mutter voraus. Entsprechend meinen Empfehlungen hat das Institut für Humangenetik ein Informations- und Einwilligungsblatt entwickelt, in dem die Mutter darüber aufgeklärt wird, daß diese Form der Analyse sich nach dem heutigen Kenntnisstand auf die nicht-codierenden Abschnitte der Erbsubstanz beschränkt und keine weiteren Rückschlüsse auf die genetische Konstitution der untersuchten Kinder, die über die Ein- bzw. Zweieiigkeit hinausgehen, zuläßt. Der Befund wird ausschließlich dem behandelnden Arzt mitgeteilt und kann von der Mutter ca. zwei Monate nach der Geburt dort erfragt werden. Nach Erhebung des Befundes wird das Untersuchungsmaterial verworfen; es werden keine weiteren Untersuchungen an der Erbsubstanz vorgenommen. Sämtliche Unterlagen können von der Mutter innerhalb von vier Wochen nach Übermittlung des Befundes vom Institut für Humangenetik angefordert werden. Anschließend werden sämtliche personenbezogenen Daten im Institut für Humangenetik gelöscht.

Derzeit führe ich eine technisch-organisatorische Überprüfung im Institut für Humangenetik des Klinikums Rudolf-Virchow der Freien Universität Berlin durch.

Zu kontroversen Diskussionen in der Öffentlichkeit führte ein Vorschlag der EG-Kommission für ein Forschungsprogramm „Prädiktive Medizin“. Ziel dieses Programms war es, die wissenschaftlichen Anstrengungen zur umfassenden Kartierung des menschlichen Genoms, die bisher vor allem in Japan und in den USA unternommen werden, auch in Europa zu koordinieren und zu fördern. Die Begründung des Vorschlags der EG-Kommission enthielt Formulierungen, die an den Gedanken der Zuchtauswahl (Eugenik) erinnerten. Vor allem aus diesem Grund wurden vielfältige Einwände gegen das Forschungsprogramm erhoben. Die Bundesregierung und das Europäische Parlament haben dem Vorschlag der Kommission nicht zugestimmt. Dies begrüße ich, zumal derartige Forschungsvorhaben jedenfalls in bestimmten Stadien nicht ohne die Erhebung von personenbezogenen Daten im großen Umfang auskommen. Bemerkenswert ist, daß das Europäische Parlament eine inhaltliche Überarbeitung des Kommissionsvorschlages und die Einsetzung eines beratenden Gremiums auf europäischer Ebene vorgeschlagen hat, das die Einhaltung der ethischen und rechtlichen Schranken bei der Realisierung eines solchen Programms überwachen soll. Dieses Gremium wird auch den Grundsatz der informationellen Selbstbestimmung der untersuchten Personen in seine Überlegungen mit-einzubeziehen haben.

2.4 ISDN und ISDN-fähige Nebenstellenanlagen

In diesem Jahr hat die Deutsche Bundespost nach früheren Vorarbeiten und Versuchen damit begonnen, das dienstintegrierende digitale Fernmeldenetz (ISDN-Integrated Services Digital Network) zu installieren. Dabei handelt es sich zunächst um die Installation auf der postinternen, vor allem überregionalen Netzebene. Ein Vordringen dieser Technologie auf die Ebene der Teilnehmer, also die Einrichtung von Schnittstellen für den Anschluß digitaler Endgeräte an das ISDN wird erst in nächster Zeit zu erwarten sein.

Dennoch ist es dringlich, daß sowohl national als auch international dem Datenschutz bei ISDN eine größere Rolle zugemessen wird als dies bisher der Fall war. Die Pläne der Deutschen Bundespost, für die Gebührenabrechnung erforderliche Verbindungsdaten auch für betriebsinterne Auswertungen zu speichern, machen deutlich, daß die Sorge um das informationelle Selbstbestimmungsrecht der Teilnehmer bei der Telekommunikation bei der Deutschen Bundespost noch unterentwickelt zu sein scheint.

Insgesamt ist zu bedauern, daß die Deutsche Bundespost sich noch nicht in der Lage gesehen hat, ein umfassendes Datenschutzkonzept für ISDN vorzulegen.

Auch die 11. Internationale Konferenz der Datenschutzbeauftragten hat zu ISDN für ein solches Konzept eine Reihe konkreter Anforderungen beschlossen. Im Mittelpunkt stehen die Forderungen nach einer Reduzierung der Erhebung und Verarbeitung personenbezogener Daten sowie nach einem dem hohen Gefahrenpotential entsprechenden Standard an Datensicherungsmaßnahmen.

Ein Schlaglicht auf die zu erwartenden Probleme wirft die bereits verbreitete Digitalisierung der hausinternen Telefonsysteme durch ISDN-fähige Nebenstellenanlagen bereits sehr verbreitet. Auch die Berliner Verwaltung greift zunehmend im Rahmen der Erneuerung der Telefon-Nebenstellenanlagen auf solche Anlagen (Inhouse-ISDN-Anlagen) zurück. Im Gegensatz zu herkömmlichen elektromechanischen Telefonvermittlungen sind digitale Nebenstellenanlagen u. a. durch folgende Merkmale gekennzeichnet:

- Die Signale werden in digitaler Darstellungsform übertragen.
- Die Vermittlung erfolgt programmgesteuert mittels digitaler Prozeßrechner, die auch über digitale Speichermedien zur Pufferung (Zwischenspeicherung) und Dokumentation (Dauerspeicherung) verfügen.
- Es existiert mindestens eine potentielle Schnittstelle zum Post-ISDN (derzeit noch nicht flächendeckend eingeführt).

Diese Eigenschaften führen zu folgenden Konsequenzen:

- ISDN wie Inhouse-ISDN vereinheitlichen die Signaldarstellung und Nachrichtenvermittlung aller Dienste auf dem Netz, gleichgültig ob analoge Signale digital simuliert werden (Fernsprechen, Telefax, Bildübertragung), oder die Übertragung ausschließlich digital (z. B. im ASC II-Code) erfolgt. Aufgrund dieser Vereinheitlichung ist die Dienstintegration möglich.
- Wegen der digitalen Darstellung der Signale können in digital gespeichert und computergestützt ausgewertet werden. Das gleiche gilt für die Verbindungsdaten, die digital im Netz bewegt und gespeichert werden. Anders als bei der alten Drehwähltechnik bedarf es einer Löschaktivität, um die Verbindungsdaten, die nach dem Ende der Verbindung nicht mehr benötigt werden, zu eliminieren.

Datenschutzrechtliche Probleme sind vor allem mit folgenden Teilaspekten verbunden:

- die Speicherung von Inhaltsdaten (z. B. der Telefongespräche in Voiceboxes, aber auch der Inhalte der Datenkommunikation),
- die Speicherung von Verbindungsdaten (zwischen welchen Anschlüssen wurde mit welchem Dienst kommuniziert?),
- die Führung elektronischer Telefonverzeichnisse,
- die Nutzung zusätzlicher Leistungsmerkmale, die das Mit-hören, Umlenken und Verteilen von Kommunikationsvorgängen ermöglichen,
- die Nutzung von Datenübertragungsdiensten durch Einbindung von Rechnern bzw. Datenstationen, z. B. im Rahmen der Bürokommunikation,
- die Anzeige der Anschlußnummer beim angewählten Kommunikationspartner,
- die Freisprech- und Lauthöreinrichtungen,
- die Administration der Anlagen,
- die Wartung bzw. Fernwartung der Anlagen.

Dadurch entstehen datenschutzrechtlich bedeutsame Risiken:

- Telekommunikationsvorgänge können unbemerkt aufgezeichnet werden.
- Benutzerprofile können aufgrund der Verbindungsdatenprotokolle aufgestellt werden.
- Telefongespräche können unbemerkt mitgehört werden.

- In Räumen persönlich geführte Gespräche können mittels Freisprecheinrichtungen unbemerkt von außen mitgehört werden.
- Auf angeschlossene Rechner kann unbefugt zugegriffen werden, da diese über Wahlverbindungen im Netz erreicht werden können.
- Auf Überlaufplätze umgelenkte Druckausgaben können von Unbefugten eingesehen werden.
- Mittels Administration und Wartung/Fernwartung kann Einfluß auf die organisatorische Telekommunikationsinfrastruktur in einer Weise genommen werden, die diesen Instanzen nicht zukommt.

Bei einem Eigenbetrieb habe ich eine Überprüfung der dort eingesetzten digitalen Nebenstellenanlage vom Fabrikat HICOM 3000 der Fa. Siemens durchgeführt.

Die Prüfung umfaßte die Verarbeitung personenbezogener Daten im Rahmen des HICOM-Systems sowie Aspekte der Vertraulichkeit der im System übertragenen Daten, insbesondere des gesprochenen Wortes. Darüber hinaus wurden die Administration des Systems und der Kontrollierbarkeit seiner ordnungsgemäßen Anwendung geprüft.

Dabei stellte ich diverse Mängel fest, die ich beanstandet habe, und deren umfassende Beseitigung in den Stellungnahmen des Eigenbetriebes und der Senatsverwaltung für Arbeit, Verkehr und Betriebe zugesagt wurde. Unter anderem wurde folgendes festgestellt:

- Obwohl zwischen Personalrat und Geschäftsleitung vereinbart worden war, daß eine Aufzeichnung und Auswertung von Gebührendaten nur kostenstellenbezogen erfolgen sollte, wurden auf einem abgesetzten Drucker anschußbezogene Aufzeichnungen von Gebührendaten ausgegeben.
- Die Administration des HICOM-Systems über das HICOM-Betriebsterminal ist grundsätzlich mit weitgehenden Kompetenzen für die Vergabe der differenzierten Berechtigungen, für den Zugriff auf und die Veränderung von personenbezogenen Daten, für die Steuerung und Wartung des Gesamtsystems, für die Kopplung mit anderen Rechnern, so auch bei der Fernwartung, verbunden.

Wegen der Bedeutung einer leistungsfähigen Kommunikationsinfrastruktur ist die Administration der digitalen Nebenstellenanlage mit einer besonderen Verantwortung verbunden.

Es wurde jedoch festgestellt, daß die Administration durch einen Mitarbeiter des Herstellers erfolgte, ohne daß praktisch eine Kontrolle durch den Eigenbetrieb stattfand.

Dies bedeutete, daß der Eigenbetrieb nicht selbst die Einhaltung der datenschutzrechtlichen Bestimmungen im eigenen Hause sicherstellen konnte, und daß Sie die ordnungsgemäße Anwendung der Datenverarbeitungsprogramme, mit deren Hilfe personenbezogene Daten verarbeitet werden können, nicht überwachen konnte. Dies verstieß gegen § 16 BlnDSG.

Gegen diese Vorschrift verstieß auch, daß die Verwaltung von Programm- und Gebührendaten sowie alle vom Eigenbetrieb anzustoßenden Aktivitäten der Fernwartung in der Hand des vom Hersteller gestellten Systemadministrators lagen.

Ich habe empfohlen, unverzüglich die Administration des HICOM-Systems von eigenen Kräften durchführen zu lassen. Es sollten entsprechende Anstrengungen zur Qualifizierung des eigenen Personals gemacht werden. Soweit für eine begrenzte Übergangszeit auf die Administrationsleistungen des Herstellers noch nicht verzichtet werden kann, sollte durch geeignete vertragliche Absprache und ihre Kontrolle durch den Eigenbetrieb dessen Hoheit über den HICOM-Einsatz im eigenen Hause hergestellt werden.

Grundsätzlich ergab sich aus dieser Prüfung sowie aus anderen Beratungsvorgängen zu solchen digitalen Nebenstellenanlagen die Erkenntnis, daß mit der Zusammenführung von Fernmelde- und Datenverarbeitungstechnik, zweier Technikbereiche also, die traditionell unterschiedlicher Zuständigkeit zugeordnet werden, organisatorische Probleme auftreten, die zu Zuständigkeits- und Verantwortungslücken führen können. So konnte bei dem Eigen-

betrieb in vielen Fällen nicht eindeutig geklärt werden, wer die Beantwortung unserer Prüffragen übernehmen sollte, teilweise auch mit dem Ergebnis, daß eine klare und eindeutige Beantwortung der Fragen im Rahmen des Gesprächs nicht möglich war. Ein solches Zuständigkeitsvakuum kann die Konsequenz haben, daß Dritte, nicht dafür vorgesehene Instanzen die Abwicklung solcher Aufgaben übernehmen, ohne dafür rechtlich Verantwortlich zu sein.

Bei der Einführung einer digitalen Nebenstellenanlage im Bereich des Rathauses Schöneberg war in Betracht gezogen worden, auch die Datenkommunikation des Abgeordnetenhaus-Dokumentations- und Informationssystems (ADIS) über diese Anlage laufen zu lassen. Ich habe darauf hingewiesen, daß ich es für verfehlt halte, ausgerechnet im Bereich der Legislative mit der Integration der Bürokommunikation in eine digitale Fernsprechnebenstellenanlage ein Technologiekonzept zu verfolgen, welches in seinen Auswirkungen hinsichtlich der Datensicherheit und der Veränderung von Kontrollstrukturen zumindest als wenig erprobt, wahrscheinlich aber als noch nicht voll beherrschbar bezeichnet werden muß.

Ich habe es für unerlässlich gehalten, daß

- die Abschottung der im Inhouse-Netz integrierten Systeme vor unbefugten Zugriffen aus den öffentlichen Telekommunikationsnetzen der Deutschen Bundespost sichergestellt wird;
- die datenschutzrechtlich gebotenen Abschottungen zwischen den im Rahmen von ADIS integrierten Bürokommunikationssystemen möglich gemacht werden;
- die entstehenden Protokollierungen von Verbindungs- und Inhaltsdaten nicht dazu verwendet werden können, personenbezogene Nutzungs- und Kommunikationsprofile der Teilnehmer, z. B. der Abgeordneten, zu erstellen;
- Gefahren für die Vertraulichkeit der Kommunikationsvorgänge ausgeschlossen werden.

Die Verwaltung des Abgeordnetenhauses hat sich schließlich aus verschiedenen Gründen dafür entschieden, für ADIS ein eigenes lokales Netz unabhängig vom digitalen Telefonnetz aufzubauen.

Aber auch dabei wurde in Beratungsgesprächen deutlich, daß die auseinanderklaffenden Zuständigkeiten für die technisch zusammenwachsenden Bereiche Fernmeldewesen einerseits und Datenfernübertragung/Datenverarbeitung andererseits zu Konfliktpotentialen oder Zuständigkeits- bzw. Verantwortungslücken führen können.

Ich habe deshalb in einer Stellungnahme zu einem Entwurf einer Senatsvorlage zur Neuordnung der Telekommunikation darauf hingewiesen, daß eine getrennte Zuständigkeit für das Fernmeldewesen einerseits und Datenfernübertragung/Datenverarbeitung andererseits angesichts der auf Integration zielenden technischen Entwicklung nicht mehr sachgerecht ist.

2.5 Bürokommunikation

Datenschutzrechtliche Probleme

Um die Verwaltung bürger näher und effizienter zu gestalten und die Arbeitssituation der Mitarbeiter zu verbessern, sollen in der Berliner Verwaltung verstärkt Bürokommunikationssysteme eingesetzt werden. Darunter werden Systeme verstanden, die Aufgaben der Texterstellung, der Büroorganisation (z. B. Wiederholungen, Terminkalenderführung und -überwachung, Telefonbücher, Handkarteien), der Vorgangsverwaltung und der Telekommunikation unterstützen und miteinander integrieren. Gleichzeitig kann die Datenhaltung mit Datenbanksystemen weiter automatisiert und in die Bürokommunikation einbezogen werden.

Sind Bürokommunikationssysteme einerseits Werkzeuge zur Integration verschiedener und auch an verschiedenen Stellen abgewickelter Bürovorgänge, so sind sie andererseits willkommen Instrumente der individuellen Datenverarbeitung, erlauben

also dem einzelnen Mitarbeiter in flexibler Weise und nach eigenem Ermessen die Unterstützung individueller Arbeitsabläufe durch automatische Verfahren.

Ferner bildet die Bürokommunikation das Bindeglied zwischen der Unterstützung der Büroarbeit und weiteren, teils schon vorhandenen und nur zu integrierenden Anwendungen der automatisierten Datenverarbeitung. Der Benutzer erhält die Möglichkeit, seine individuell organisierte Arbeitsunterstützung, die Textverarbeitung, die Unterstützung der Büroorganisation sowie interne und externe Kommunikationsvorgänge mit dem Zugang zu Verfahren der Massendatenverarbeitung, ob vorhanden oder erst anlässlich der Einführung der Büroautomation automatisiert, zu verbinden.

Dieses alles kann man mit Bürokommunikations-, oder richtiger Büroinformationssystemen erreichen, wenn sie gut an die gewohnten oder sinnvoll geänderten Organisationsabläufe angepaßt sind und eine hohe Akzeptanz bei den Mitarbeitern erreicht wurde. Allerdings zeigt die zögerliche Einführung solcher Systeme und die noch geringe Ausnutzung des Anwendungsspektrums (die Textverarbeitung spielt noch immer die mit Abstand überragende Rolle), daß die gern verbreitete Idee der Installation schlüsselfertiger und ohne vor Ort verhandender DV-Fachkompetenz einsetzbarer Systeme weitgehend noch nicht umgesetzt werden konnte und noch für absehbare Zeit unrealistisch erscheint.

Bei der Novellierung der Datenschutzgesetze sind diese Probleme einzubeziehen.

Die datenschutzrechtliche Gestaltung solcher Systeme wirft erhebliche Probleme auf:

- Wie schützt man vertrauliche Dokumente vor unbefugter Einsicht, z. B. vor Einsicht durch privilegierte Benutzer (Systemadministratoren)?
- Wie schützt man gespeicherte Dokumente, die verbindlich geworden sind, vor unbefugter nachträglicher Änderung - nicht nur durch den Verfasser, sondern auch durch privilegierte Benutzer?
- Wie realisiert man die bei der manuellen Vorgangsbearbeitung aus arbeitsorganisatorischen Gründen selbstverständlichen, aber durch die Verfügbarkeit im System aufgehobenen informationellen Abschottungen innerhalb von Organisationen wie z. B. Behörden?

Diese Fragen, die auf selbstverständliche Anforderungen abzielen, gewinnen erst durch die Bürokommunikation besondere Bedeutung. Wo vorher Lösungen in einfacher und wirksamer Weise durch den Verschluß der Dokumente oder den vielfältigen Nachweisen ihrer Echtheit realisiert waren, bedarf es mit der Einführung der Bürokommunikation einer genauen Planung und Umsetzung der Zugriffsdifferenzierung auf die gespeicherten Vorgänge. Mit dem Übergang vom Papier zur elektronischen Verarbeitung müssen Lösungen für Probleme gefunden werden, die so früher nicht bestanden. Die Sicherung der Dokumentenechtheit bei elektronischer Speicherung oder der Nachweis von Veränderungen in Mitzeichnungsverfahren sind typische Beispiele.

Die Anwendung der Datenschutzgesetze auf diese Form der Informationsverarbeitung bringt Probleme mit sich. Die gebotene strenge Auslegung führt unter anderem zu folgenden Konsequenzen:

- Die nach § 3 Abs. 3 Berliner Datenschutzgesetz bisher privilegierten und nur hinsichtlich ihrer sicheren Unterbringung datenschutzrechtlich beachtlichen internen manuellen Karten unterliegen nach ihrer Erfassung in einem Bürokommunikationssystem in vollem Umfang den datenschutzrechtlichen Bestimmungen einschließlich aller Nebenbestimmungen, wie etwa Verpflichtung zur Auskunftserteilung oder zur Dateiregistrierung.
- Auch Textmengen, die man mit Textretrieval- und analysesystemen in vergleichbarer Weise auswerten kann wie „klassische“ Dateien, unterliegen ungeachtet der Diskussion über diesen Terminus den Dateibegriff - damit fallen alle mit der Textverarbeitungskomponente geschriebenen Dokumente in den Geltungsbereich der Datenschutzgesetze.

- Insbesondere bei Dateien in relationalen Datenbanken ist die Erfüllung der formalen Pflichten wie Veröffentlichungen und Dateiregistrierungen in vollem Umfang kaum möglich, weil der Umfang der auf eine Person bezogenen Daten nicht genau bestimmbar ist.
- Bei der individuellen Datenverarbeitung (z. B. Telefonbücher, Terminkalender, Notizblockfunktionen) verschärfen sich die Probleme noch. Es ist davon auszugehen, daß die Kontrolle eines dienstlichen Computers nicht mit dem Hinweis abgeblockt werden kann, es handele sich um private Aufzeichnungen.

Probleme der Sicherheit von UNIX

Die Bürokommunikation wird mit Mehrplatzsystemen realisiert, wobei sich zwei Typen durchgesetzt haben: Personalcomputer-Netze mit Server und UNIX-Mehrplatzsysteme. Da PC-Netze in der Berliner Verwaltung zunehmend Verbreitung finden, habe ich die seit 1986 herausgegebenen Grundsätze zum Datenschutz bei Personalcomputern überarbeitet und auf vernetzte Personalcomputer erweitert.

Der Einsatz von Mehrplatzsystemen unter UNIX, insbesondere für die Bürokommunikation, bedarf ebenfalls der Aufmerksamkeit gegenüber Risiken, die sich aus den Besonderheiten des Betriebssystems ergeben. Dabei ist vorab allgemein festzustellen, daß das Datenschutzziel, in Hardware und Betriebssystemsoftware den Datenschutz von vornherein konzeptionell mit einzubauen, generell noch nicht befriedigend erreicht ist.

UNIX ist vor rund 20 Jahren mit dem Ziel entwickelt worden, den an bestimmten Maschinentypen und Prozessoren angepaßten Betriebssystemen ein auf verschiedenen Rechnern einsetzbares System entgegenzusetzen. Dies hat den Vorteil, daß Programme, die mit dem Betriebssystem arbeiten, auf verschiedene Rechner übertragbar sind. Ermöglicht wird die leichte Übertragbarkeit von UNIX dadurch, daß es überwiegend in der höheren maschinenunabhängigen Programmiersprache C geschrieben worden ist, die im Zusammenhang mit der UNIX-Entwicklung entstanden ist. Die Verwendung einer höheren Programmiersprache bewirkt auch, daß UNIX leichter variiert werden kann, ein Umstand, der einerseits viele zusätzliche Anregungen bei der Fortentwicklung ermöglicht hat, andererseits aber der angestrebten Standardisierung des Systems lange Zeit im Wege gestanden hat. Mittlerweile ist durch die sog. X/Open-Gruppe, ein Zusammenschluß bedeutender Herstellerfirmen, eine Standardisierung erreicht worden, die offensichtlich bei den Anwendern eine breite Akzeptanz findet. Auch in der Berliner Verwaltung wird in Ausschreibungen von UNIX-Systemen die Ausrichtung an diesem Standard verlangt.

Im Gegensatz zu dem zweiten weltweit verbreiteten Standard-Betriebssystem MS-DOS ist unter UNIX die gleichzeitige Bedienung mehrerer Benutzer möglich. Während MS-DOS als Betriebssystem für Einplatz-Personalcomputer überhaupt keine Instrumente zur Differenzierung berechtigter und unberechtigter Benutzer und zur Festlegung unterschiedlicher Zugriffsrechte bereithält, gibt es unter UNIX standardmäßig Paßwortverfahren zur Identifikation und Authentifikation von Benutzern, Möglichkeiten zur Definition differenzierter Zugriffsrechte auf Dateien und Programme sowie Verschlüsselungstechniken.

Trotz dieser Komponenten wird die Sicherheit von UNIX im Vergleich zu anderen Betriebssystemen für Großrechner bzw. Mehrplatzsysteme nicht sehr hoch eingeschätzt. Die Benutzer-, Speicher- und Zugriffskontrolle enthält bei anderen Systemen (gegebenenfalls unter Hinzufügung spezieller Ergänzungssoftware) wesentlich bessere Leistungsmerkmale. Aus diesem Grunde gibt es weltweit bei verschiedenen Herstellern Bemühungen, durch Modifizierungen bei UNIX höheren Sicherheitsanforderungen gerecht zu werden. Wie jüngeren Veröffentlichungen zu entnehmen ist, scheint dies auch erfolgreich zu sein, denn spezielle UNIX-Versionen sind mittlerweile nach den Kriterien der amerikanischen Evaluationsbehörde (Orange Book) beachtlich hoch eingestuft worden.

UNIX ist als ein streng hierarchisch in einer Baumstruktur angeordnetes Dateisystem organisiert. Die Zugriffsrechte auf die

einzelnen Dateien und Dateiverzeichnisse lassen sich differenzieren nach Lese-, Schreib- und Ausführrechten (bei Programmdateien) für die Besitzer allein, für Angehörige ihrer Gruppe und für die gesamte Benutzerschaft. Mit speziellen Möglichkeiten, die sich aus Mechanismen für den Besitzerwechsel bei Dateien und der Auswirkung verschiedener Zugriffsrechte auf Dateiverzeichnisse ergeben, lassen sich differenzierte und außerordentlich komplexe Zugriffsprofile implementieren. Diese Komplexität birgt auch Gefahren, da die Überwachung und Administration der Zugriffsprofile hohe Sorgfaltsanforderungen bei der Systeminstallation und an den Systemverwalter stellt. Wird diesen nicht genügt, können Lücken der Zugriffskontrolle entstehen, deren Mißbrauch die Sicherheit des Systems gefährden kann.

Die effiziente Verwaltung von UNIX-Systemen wird gewährleistet durch die Kumulierung aller Zugriffsrechte beim Systemverwalter, der deshalb auf alle Dateien und Dateiverzeichnisse lesend und ändernd zugreifen und in alle Prozesse eingreifen kann. Dies stellt aber gleichzeitig aus Sicht des Datenschutzes und der Verfahrenssicherheit einen entscheidenden Schwachpunkt dar. Zwar gibt es auch bei anderen komplexen Betriebssystemen vergleichbar mächtige Systemverantwortliche. Da anders als die meisten anderen Mehrbenutzer-Betriebssysteme UNIX-Systeme jedoch in sogenannte Büroumgebungen eingesetzt werden und dort auch die Administration stattfindet, entfällt der erhebliche Sicherheitsgewinn durch die Arbeitsteilung in Rechenzentren und die Anwendungsferne der Systemadministration. Die Ziele bei der datenschutzgerechten Gestaltung des Einsatzes von UNIX-Systemen in Büroumgebungen konzentrieren sich daher im wesentlichen auf die organisatorischen und technischen Maßnahmen zur Eindämmung der Risiken durch die weitreichenden Zugriffsrechte der Systemverwalter und zur Verhinderung, daß andere Benutzer sich die Zugriffsrechte des Systemverwalters aneignen können, in dem sie lückenhafte Zugriffsprofile dafür ausnutzen.

In der Anlage 3 dieses Jahresberichtes habe ich Empfehlungen für die datenschutzgerechte Gestaltung des Einsatzes von UNIX-Systemen formuliert, soweit sie sich auf Spezifika des Betriebssystems beziehen.

Sie gehen ein auf

- (1) organisatorische Maßnahmen zur Eindämmung der Risiken, die sich aus den weitreichenden Berechtigungen der Systemverwalter ergeben;
- (2) technische Maßnahmen zur Beschränkung der Benutzerkompetenzen, die nicht benötigt werden, z. B. die Verfügbarkeit von Betriebssystemkommandos;
- (3) den risikoarmen Umgang mit Dateizugriffsrechten;
- (4) den datenschutzgerechten Umgang mit Paßwörtern;
- (5) Schutz der Hardware typischer UNIX-Systeme;
- (6) die Lösungsverfahren;
- (7) die Protokollierung.

Diese Empfehlungen stellen ein erstes Konzept dar, das bei den bevorstehenden Einsatzformen von UNIX die Einhaltung der datenschutzrechtlichen Bestimmungen erleichtern soll. Zugleich bilden sie einen Maßstab für die Datenschutzprüfungen. Ich gehe davon aus, daß sie zu einem breiten Erfahrungsaustausch führen werden, bei dem allgemein anerkannte Prüfkriterien entwickelt werden sollten.

2.6 Erfahrungen mit Personalcomputern

Im Berichtsjahr habe ich damit begonnen, Personalcomputer-Anwendungen in verschiedenen Bereichen der Verwaltung systematischen Prüfungen zu unterziehen. Inhaltliche Grundlage dieser Überprüfungen sind grundsätzlich die von mir entwickelten und jetzt in überarbeiteter und ergänzter Form veröffentlichten „Grundsätze für organisatorische und technische Maßnahmen zum Datenschutz beim Einsatz von isolierten oder vernetzten Personalcomputer (PC-Grundsätze)“.

Wegen seiner breiten Einsatzmöglichkeiten im professionellen Anwendungsbereich, gepaart mit leichter Erlernbarkeit und flexi-

blen Gestaltungsmöglichkeiten erfreut sich der Personalcomputer in der Berliner Verwaltung immer größerer Beliebtheit. Dabei übernehmen die Einzelplatz-Systeme vermehrt Aufgaben, die noch vor wenigen Jahren Rechneranlagen mittlerer Größe vorbehalten waren. Wegen der Leistungsfähigkeit der Kleinrechner werden zudem Bereiche automatisiert, die man zuvor nicht für automationswürdig gehalten hat. So ist in den letzten Jahren ein sprunghafter Anstieg beim Einsatz von Arbeitsplatzcomputern auf allen Verwaltungsebenen zu verzeichnen.

Mit den vielfältigen technischen Möglichkeiten sind aber auch erhebliche Risiken mit dem Einsatz der Einzelplatzrechner verbunden.

Die Geräte erfordern zu ihrer Bedienung keine besonderen EDV-Kenntnisse. Sie sind frei programmierbar, erlauben jedem, Daten ohne den Nachweis einer Berechtigung zu verarbeiten, zeichnen Datei- und Systemzugriffe nicht auf und bieten keine Verschlüsselungsmechanismen. Die Speicherkapazitäten sind enorm angewachsen; die damit verbundene Miniaturisierung peripherer Speicher erleichtert den Mißbrauch gespeicherter personenbezogener Daten durch Diebstahl der Datenträger oder Kopie der Dateien. Für den Betrieb steht eine breite Palette leistungsfähiger Standardsoftware zur Verfügung.

Neben den beachtlichen Leistungsdaten geben oftmals rein ökonomische Gesichtspunkte den Ausschlag zur Anschaffung derartiger Insellösungen. Auf notwendige Sicherheitsmaßnahmen darf man jedoch nicht deshalb verzichten, weil diese den Einsatz vergleichsweise billiger Personalcomputer verteuern. Deshalb muß vor der Anschaffung von Arbeitsplatzcomputern ein vollständiges PC-spezifisches Datensicherungskonzept erstellt werden. Die Kosten der Umsetzung sind in die Kalkulation mit einzubeziehen.

Erfahrungen aus der Praxis

Da das zur Zeit auf dem PC-Sektor marktbeherrschende Betriebssystem MS-DOS als klassisches Single-user-System im Vergleich zu UNIX über keinerlei Datensicherungseinrichtungen verfügt, sind zusätzliche Maßnahmen zu treffen. Erfreulicherweise ist eine Weiterentwicklung und eine Verbreiterung des Angebots auf dem Markt befindlicher Sicherheitssoft- und -hardware-Komponenten zu verzeichnen. Fachzeitschriften berichten ausführlich in Form von Tests über die Produkte und tragen somit zu deren Popularität bei. Darüber hinaus werden Implementierung und Handbücher zunehmend anwendungsfreundlicher, obwohl hier noch vieles verbesserungswürdig ist.

Der Einsatz von Sicherheitssoft- und -hardware setzt voraus, daß man sich ausführlich über das Angebot informiert. Testberichte deuten an, daß nicht immer die bekanntesten Produkte die sichersten sind. Darüber hinaus ist es nicht schon alleine mit dem Kauf und der Installation solcher Produkte getan. Erfahrungen aus meiner Prüfpraxis haben gezeigt, daß vielfach die Möglichkeiten der Sicherheitstools nicht ausgeschöpft werden. So ist es in einzelnen Fällen als ausreichend empfunden worden, die systemimmanenten Paßwortverfahren einzusetzen; Verschlüsselungstechniken und Dateizugriffsbeschränkungen blieben dagegen ungenutzt. Daneben fehlt es vielfach an bereichsinternen Konzepten und entsprechendem Know-how für die Implementierung derartiger Programme. In einem Fall kam selbst der Systemverwalter weder auf die Installationsebene einer Sicherheitssoftware noch in das Betriebssystem. Daß hier eine optimale Einrichtung ausgeschlossen ist, erklärt sich von selbst.

Nur in einem Fall besaß eine von mir überprüfte Behörde eine Aufstellung über die Anzahl und Anwendungsbereiche der von ihr eingesetzten PC. Aus Gründen der Revisionsfähigkeit und um einen Wildwuchs zu vermeiden, ist es jedoch unentbehrlich, sich einen Überblick über die Geräte und deren Anwendungen zu verschaffen. Nur wer weiß, wo auf welchen Geräten welche Daten verarbeitet werden, kann Schwachstellen aufspüren und beseitigen, um so datenschutzrechtlichen Anforderungen Rechnung zu tragen.

Voraussetzung für die Überwachbarkeit der ordnungsgemäßen Programmanwendung ist eine formelle Freigabe des PC-unterstützten Verfahrens. Dem geht eine Prüfung des Abschlußtests

voraus, der nachweist, daß das einzusetzende Programm den dienstlichen Anforderungen genügt und so aufgebaut und dokumentiert ist, daß sachverständige Dritte in angemessener kurzer Zeit die Pflege des Programms voll verantwortlich übernehmen können. Die Funktionstrennung zwischen Anwendung und Freigabe ist dafür ebenso unabdingbar wie für die Revisionsfähigkeit und Ausfallsicherheit die Vollständigkeit der Programmunterlagen. Bei einer Prüfung bin ich auf folgende Fallkonstellationen gestoßen, die es einem Bezirksamt unmöglich macht, auf größere Störungen angemessen zu reagieren: Ein Programmierer einer Softwarefirma, der ein Programm für das Bezirksamt entwickelt hatte, schied aus; zudem hatte der eingearbeitete Sachbearbeiter des Bezirksamts den Arbeitsplatz gewechselt; die für die Anwendung erforderlichen Unterlagen sind nicht vollständig. Daß bisher das Programm reibungslos läuft, kann nicht als Argument für eine ordnungsgemäße Anwendung gelten.

Dem Einwand eines Anwenders, daß die Führung einer vollständigen Programmakte viel zu aufwendig sei, da die Aufnahme jeder Programmänderung mit einem enormen Zeitaufwand verbunden ist, ist zu entgegnen, daß für eine ordnungsgemäße Dokumentierung des Programms der Ausdruck eines, allerdings gut kommentierten Quellprogramms ausreichen kann.

Programmunterlagen sollten nach ihrer Anfertigung nicht in der Versenkung verschwinden und nur zum Einsatz kommen, wenn Programmstörungen auftreten. Anhand des vorhandenen Materials sollte auch stichprobenweise überprüft werden, ob laufende Anwendungen mit dem freigegebenen Verfahren noch übereinstimmen.

Nach wie vor scheitert der ordnungsgemäße Einsatz von Personalcomputern in Verwaltungsverfahren an der fehlenden technisch erzwungenen Funktionentrennung zwischen Benutzern und Gestaltern (Programmierern). Eine formelle Freigabe muß ihren Sinn verlieren, wenn der PC-kundige Sachbearbeiter als Benutzer die Möglichkeit hat, Programm- und Verfahrensänderungen unkontrolliert durchzuführen, gleichgültig, ob dies in guter oder böser Absicht erfolgt. Da geeignete Programmversiegelungstechniken noch nicht marktgängig sind, habe ich bei PC-Verfahren, die formelle Verwaltungsverfahren automatisieren, darauf gedrängt, daß den Anwendern ausschließlich ablauffähige, also bereits aus dem Quellcode übersetzte Programme zur Verfügung gestellt werden.

Als Schwachstelle erwiesen sich auch die Zuständigkeitsverteilungen hinsichtlich der Systemverantwortlichkeit. Zwar wurde der PC als „persönliches“ System konzipiert und auf die Wünsche eines einzelnen Anwenders zugeschnitten, dem als „Herr des Verfahrens“ alle technischen Möglichkeiten zur Verfügung gestellt werden sollten, jedoch werden diese Rechner überwiegend zur Abwicklung von Verfahren eingesetzt, bei denen mehrere Sachbearbeiter Zugriff auf das System haben. Aber nicht nur bei gewidmeten Systemen, sondern auch im personengebundenen Betrieb ist auf die für den Großrechnereinsatz fast schon selbstverständliche organisatorische und personelle Funktionstrennung zwischen Entwicklung, Anwendung und Aufsicht hinzuwirken. In der Praxis des PC-Einsatzes ist vielfach der am Rechner arbeitende Sachbearbeiter gleichzeitig Systemverwalter. Unabhängig von der Gefahr, daß sich die Behörde in den Fällen, in denen sich das gesamte Know-how auf eine Person konzentriert, in die Abhängigkeit von dem Wissen eines Einzelnen begibt, ist bei einer derartigen Konstellation der „zu Kontrollierende“ gleichzeitig sein „eigener Kontrolleur“. Zugunsten einer objektiven Revision und Kontrollmöglichkeit von Verfahren ist die Wahrnehmung von Systemverwalteraufgaben durch vom Verfahren betroffene Mitarbeiter ebenso abzulehnen wie die Personalunion von Systemverwalter und internem Datenschutzbeauftragten.

Aus anderen Gründen habe ich Bedenken gegen einen von der Organisationsabteilung der Senatsverwaltung für Inneres im Zusammenhang mit einem Gutachten über die Möglichkeit einer Übertragung des ADV-Verfahrens „Kosteneinziehung“ auf alle bezirklichen Sozialämter erarbeiteten Vorschlag geäußert. Dieser zielte darauf ab, einen für alle PC-unterstützten Kosteneinziehungsverfahren verantwortlichen überbezirklichen Systemverwalter einzusetzen, der organisatorisch entweder bei einem Bezirksamt oder der Fachaufsicht angesiedelt werden soll. Unab-

hängig von der Frage der örtlichen Zuständigkeit kann bei dieser Konstruktion bei Verfahrenstörungen eine schnellstmögliche Hilfestellung nicht geleistet werden. Ferner müßte ein übergeordneter Systemverwalter für eine ausreichende Pflege und Wartung und zur Gewährleistung des technischen Datenschutzes mit den individuellen Anpassungen aller Bezirksämter vertraut sein. Hier erweist sich die Ferne von der konkreten Anwendung als unpraktikable Lösung, so daß die Gefahr besteht, daß Systemmängel eigenmächtig und unabhängig von der für das Verfahren zuständigen Kontrollinstanz versuchsweise behoben werden. Demgegenüber habe ich vorgeschlagen, innerbezirkliche Systemverwalter einzusetzen, die – aus der Fachabteilung ausgegliedert – den bezirklichen Organisationsstellen unterstellt werden könnten. Somit wäre die Unabhängigkeit vom Verfahren garantiert, ohne den Nachteil der Systemferne und dem fehlenden Wissen über bezirksinterne Arbeitsabläufe in Kauf nehmen zu müssen. Um einer Überforderung der mit Systemverwalteraufgaben betrauten Mitarbeiter vorzubeugen, sollte sich die Zuständigkeit nicht auf die einzelnen Verfahren, sondern auf die dazu eingesetzte Hardware beziehen.

Von datenschutzrechtlicher Bedeutung ist nicht nur die vertikale Zuständigkeit bei PC-unterstützten Verfahren. In einem Einzelfall erwies sich die Aufgabenverteilung innerhalb eines Sachgebietes als so unstrukturiert, daß eine Fülle von übergreifenden, aber nicht notwendigerweise erforderlichen Dateizugriffen durchgeführt werden müssen, um das Verfahren ordnungsgemäß aufrecht zu erhalten. Auch hier liegt der Grund in einer fehlenden Systemkonzeption, die datenschutzrechtliche Belange bei der Automatisierung des Verfahrens berücksichtigt. Nach Nr. 10 der Anlage zu § 5 Berliner Datenschutzgesetz ist die innerbehördliche Organisation bei der automatisierten Datenverarbeitung so zu gestalten, daß sie dem besonderen Anforderungen an den Datenschutz gerecht wird (Organisationskontrolle). Die Vorschrift wird bei der Umsetzung bisher manuell durchgeführter Verfahren allzuleicht übersehen. Die Folge ist eine Mißachtung der informationellen Gewaltenteilung, nach der jeder Sachbearbeiter nur auf die Daten zugreifen darf, die für seine Aufgabenerfüllung unbedingt erforderlich sind. Unter Umständen setzt die Automatisierung neue Zuständigkeits- und Aufgabenzuweisungen voraus. Vielfach bietet gerade die Automation die Möglichkeit, Arbeitsabläufe datenschutzgerecht zu gestalten.

Ein verstärkter PC-Einsatz ist nur erfolgversprechend, wenn auf ausreichende Fachkenntnisse zurückgegriffen werden kann. Zwar ist die Bedienung von Personalcomputern im Vergleich zu Großrechenanlagen ungleich einfacher, es darf jedoch nicht übersehen werden, daß die größten Sicherheitsrisiken auf fehlendes Fachwissen, Irrtümer und Nachlässigkeit auf Seiten der Benutzer zurückzuführen sind. Aus diesem Grund sind auch oder gerade deshalb Sicherheitskonzepte zu entwickeln, die die Gefahr größerer Schäden minimieren. Dazu gehört, daß die Möglichkeit des Betriebssystemzugriffs nur privilegierten Benutzern (Systemverwaltern) offenstehen darf. Bei der Programmierung oder Installation von Sicherheitssystemen ist auch darauf zu achten, daß Sicherungsmaßnahmen nicht durch einen Systemstart über das Diskettenlaufwerk umgangen werden können: Bei einer Bezirksamtsüberprüfung konnte ein eigenprogrammiertes Paßwortverfahren durch das Laden einer Systemdiskette ausgeschaltet werden.

Zu einem ordnungsgemäßen Paßwortverfahren gehört auch eine datenschutzgerechte Paßwortverwaltung. Paßwörter sollten bei der Eingabe nicht auf dem Bildschirm erscheinen. Sie sollten eine Mindestlänge von acht Zeichen haben und in regelmäßigen Abständen geändert werden, wobei die Paßwortauswahl dem Benutzer übertragen werden sollte. Paßwörter dürfen nicht am Arbeitsplatz notiert und nicht aus dem privaten Umfeld ausgewählt werden. Darüber hinaus sollten Paßwörter verschlüsselt in einer gesonderten Datei hinterlegt werden, die besonders zu schützen ist. Paßwortverfahren sind nicht nur für eine generelle Authentifizierung gegenüber dem System sinnvoll, sondern auch zur Einrichtung gestaffelter Zugriffsberechtigungen innerhalb eines Dateiverzeichnisses. Zu einer sicheren Verwendung der Paßwörter gehört ferner, daß bei einer Protokollierung von Systemzugriffen diese nicht im Klartext im Login-Protokoll erscheinen.

Da trotz aller vorbeugender Sicherheitsmaßnahmen eine hundertprozentige Sicherheit beim Einsatz von Personalcomputern nicht erreicht werden kann, sind Systemaktivitäten zu protokollieren. Dafür ist nicht nur die nach Nr. 7 der Anlage zu § 5 Berliner Datenschutzgesetz erforderliche Eingabekontrolle sicherzustellen, sondern auch die Aufzeichnung sämtlicher Systemeingaben, um unbefugte Zugriffe oder Zugriffsversuche auch im nachhinein nachvollziehen zu können. Dabei ist darauf zu achten, daß die daraus resultierende Protokolldatei nur privilegierten Benutzern zugänglich sein darf und einem Zweckbindungsgebot unterliegt, denn bei der Aufzeichnung von Rechneraktivitäten können unter Umständen sensiblere Datensammlungen entstehen als sie die ursprünglich gespeicherten Daten darstellen.

Aussichten

Die technische Entwicklung stellt die Datenschutzbeauftragten vor immer neue Aufgaben. Dazu gehört die Ausweitung der Speicherkapazitäten auf Rechnern und beweglichen Datenträgern ebenso die Weiterentwicklung der Betriebssysteme und Standardprogramme. Die Ablösung der klassischen Single-user-Systeme durch Multi-tasking und multi-user-fähige Systeme zeichnet sich ab. Durch die anfallenden Datenmassen, ständig zunehmende Aufgabenteilung und dem damit einhergehenden Bedarf an Informationsaustausch führt der Trend zu einer Vernetzung und verstärkten Mobilität der Kleinrechner. Auch in der Verwaltung ist mit einer steigenden Zahl von *Laptops* - tragbare Kleincomputer mit aufklappbarem (lap) Bildschirm - zu rechnen. Diese können es zum Teil gemessen an ihrer Ausstattung und Leistungsfähigkeit mit den bisher eingesetzten Arbeitsplatzcomputern ohne weiteres aufnehmen und bieten zudem den Vorteil der Beweglichkeit. Dadurch entfällt die Möglichkeit, durch raumbezogene organisatorische Maßnahmen einen gewissen Sicherheitsstandard zu erreichen. Die Gefahr des unbefugten Zugriffs erhöht sich erheblich. Da der Einsatzort nicht einzugrenzen ist und sich der örtlichen Kontrollbefugnis des Datenschutzbeauftragten entziehen kann, z. B. durch Mitnahme und Einsatz in privaten Räumen, sind hier Vorkehrungen zu entwickeln, die eine jederzeitige datenschutzrechtliche Kontrolle sicherstellen.

Die mangelnde Sicherheit der PC erfordert umfangreiche technisch-organisatorische Maßnahmen, deren Umsetzung dem einzelnen Anwender widerstrebt. Waren es gerade noch die leichte Handhabung und die flexiblen Einsatzmöglichkeiten der Rechner, die für eine Anschaffung zur Entlastung von lästigen Routinearbeiten sprachen, so entstehen Bedenken hinsichtlich eines rentablen und einfachen Einsatzes, wenn es um die Erfüllung datenschutzrechtlicher Anforderungen geht. Eine für datenschutzrechtliche Belange hinreichende Sensibilität bei den für die PC-gesteuerten Verfahren verantwortlichen Stellen zu erzeugen, wird weiterhin zu den Hauptaufgaben der Datenschutzbeauftragten gehören.

3. Neue Medien

3.1 Telekommunikationsrecht

Auf bundesrechtlicher Ebene stand im Mittelpunkt der Erörterungen die Diskussion um das Poststrukturgesetz, in dem die Deutsche Bundespost nicht nur in drei Unternehmensbereiche aufgeteilt wurde, sondern mit dem auch für die Telekommunikation in der Bundesrepublik neue Weichen gestellt wurden.

Der Unternehmensbereich Telekom soll die Telekommunikationsdienstleistungen künftig verstärkt in Konkurrenz zur Privatwirtschaft in betriebswirtschaftlicher Form erbringen. Dies wird auch Konsequenzen haben für die datenschutzrechtliche Beurteilung der Verarbeitung von Teilnehmerdaten.

Auf dem Endgerätemarkt können künftig verstärkt private Betreiber tätig werden; da in einem bestimmten Umfang auch die Vermittlung in den Bereich der Endgeräte zählte, entstehen hier im nicht-öffentlichen Bereich alle datenschutzrechtlichen Probleme mit Nutzungsdaten, die bisher im wesentlichen Gegenstand der Erörterung mit der öffentlichen Bundespost waren.

Zwar wurde auf Drängen der Datenschutzbeauftragten die¹⁾ Verordnungsermächtigung zum Erlass von Verordnungen zur Sicherstellung des Datenschutzes auf private Betreiber ausgedehnt. Es muß jedoch sichergestellt werden, daß die entsprechenden Vorschriften das derzeit gewährleistete Niveau des Datenschutzes nicht unterschreiten. Insbesondere wird darauf zu achten sein, daß die noch ausstehenden Forderungen der Datenschutzbeauftragten insbesondere nach einer präziseren Festlegung der für die Abwicklung der einzelnen Dienste erforderlichen Daten eingelöst werden.

Auf dem Gebiet des Landesrechts sind neue Initiativen noch nicht sichtbar geworden, obwohl die Geltungsdauer des Kabelpilotprojektgesetzes (KPPG) im kommenden Jahr ausläuft. In das Landesmediengesetz, das an seine Stelle treten muß, sind in erheblichem Umfang auch datenschutzrechtliche Regelungen einzubeziehen, die den Regelungen des KPPG nicht nur entsprechen, sondern sie auch weiterentwickeln. Insbesondere kann die Erarbeitung eines Landesmediengesetzes Anlaß sein, die von den Datenschutzbeauftragten schon seit Jahren eingeforderte Beteiligung der Länder bei der Ausgestaltung der Nutzung neuer Telekommunikationsdienste sicherzustellen. Die bisher nur ansatzweise für den Bildschirmtextdienst und Fernwirkdienste bestehenden Bestimmungen müssen auf eine allgemeinere Grundlage gestellt werden. Mir ist von der Senatorin für Kulturelle Angelegenheiten eine frühzeitige Beteiligung zugesichert worden.

3.2 Bildschirmtext

Entwicklung des Dienstes

Im Berichtszeitraum konnte ich eine spürbare Zunahme der Kontaktaufnahme von Bürgern zu meiner Dienststelle über Bildschirmtext (Btx) feststellen. Sowohl beim Anwählen meines Btx-Angebots als auch bei der Bestellung von Informationsmaterial - wobei im letzteren Fall sogar eine Verdopplung gegenüber dem Vorjahr zu verzeichnen war - bedienten sich die „Besitzer“ von Btx-Anschlüssen immer mehr dieses elektronischen Dienstes.

Ich führe diese Zunahme auf die verstärkten Werbeaktivitäten der DBP zurück und die Tatsache, daß die Geräte bzw. Zusatzgeräte für eine Btx-Nutzung immer preiswerter werden.

Im Zuge der internationalen Datenvernetzung wird sich auch die Btx-Zukunft entscheidend verändern. Das Zusammenwachsen verschiedener Systeme findet im wesentlichen auf zwei Ebenen statt: Einmal auf der Ebene der Telekommunikationsdienste und zum anderen auf der Ebene der Staaten und deren unterschiedliche Btx-Systeme - die im internationalen Sprachgebrauch als „Videotex-Systeme“ bezeichnet werden. Die neue Software wird in der Lage sein, den Mitteilungsempfang und -versand über Btx, Telex, Telefax, Teletex und Mailbox automatisch abzuwickeln. Zwei dieser fünf Möglichkeiten bietet die Post bereits derzeit an - nämlich Btx und Telex. Vom deutschen Btx-System aus sind die Systeme verschiedener anderer Staaten, z. B. Frankreich und Österreich erreichbar.

Zur Erhöhung der Sicherheit beim Zugriff auf das Btx-System will die Bundespost zukünftig zwei Verfahren erproben, die auf der Anwendung von Verschlüsselungstechniken beruhen: zum einen die Verwendung einer Chipkarte, in der ein verschlüsseltes Kennwort zur Authentifizierung des Benutzers abgelegt ist, zum anderen den Einsatz von Zusatzgeräten zur Verschlüsselung von Nachrichten.

Unabhängig davon hat die Bundespost die Forderung der Datenschutzbeauftragten, den Anfall von Nutzungsdaten durch den Einsatz von Chipkarten auf Guthabenbasis zu minimieren, bislang nicht erfüllt.

Die Bundespost hat in letzter Zeit ihrerseits etwas für die zunehmende Akzeptanz des Btx-Dienstes getan und neben der zusätzlichen Installation öffentlicher Btx-Geräte u. a. folgende Systemänderungen vorgenommen:

Mit der Software-Erweiterung vom Januar 1989 ist auch ein anonymer Zugang („Gastzugang“), möglich. Hiermit wird Interessenten Gelegenheit gegeben, Btx auch ohne eigene Zugangsbe-

¹⁾ vgl. Anlage 4 des Jahresberichts 1988

rechti gung kennenzulernen. Technische Voraussetzungen hierfür sind: Modem oder Akustikkoppler und ein Btx-fähiges Endgerät. Es können alle vergütungsfreien Leistungen des Btx-Dienstes in Anspruch genommen werden. Der Gastzugang über die übliche Btx-Anschlußbox ist nicht möglich.

Einen neuen Service stellt auch die Funktion *Beenden der Btx-Verbindung mit Halten der Leitung* dar. Diese Funktion ermöglicht den Neuzugang zum System mit anderer Btx-Nummer, ohne die Telefonverbindung zum Btx-Rechner abzutrennen. Dafür ist die Schaltung der Anschlußfreizügigkeit des benutzten Btx-Anschlusses und der Teilnehmerfreizügigkeit der Btx-Nummer, die eingegeben werden soll, Voraussetzung.

Auf die Problematik der Freizügigkeitsschaltung habe ich schon mehrmals hingewiesen. Sie sollte so kurz wie möglich erfolgen, da in diesem Fall nur einfacher Kennwortschutz besteht und einem möglichen Mißbrauch der Kennungen Tür und Tor geöffnet wird.

Der erste Dienst, der bereits im Entstehen mit Btx gekoppelt wird, ist Cityruf. Zur Zeit wird das neue Kommunikationssystem im Betriebsversuch getestet. Btx-Teilnehmer können – vorläufig kostenlos – mitesten. Cityruf ist vergleichbar mit dem Europieper; die Empfangsgeräte sind ungefähr scheckkartengroß. Der Empfang von Cityruf-Botschaften ist allerdings auf die Rufzone beschränkt, für das der Empfänger angemeldet ist. Eingegeben werden die Informationen entweder per Telefon, per Telex/Teletex oder am Btx-Terminal. Jeder Cityruf-Teilnehmer kann so angesprochen werden, egal wo das Telefon, das Telex- oder Btx-Gerät steht und in welcher Stadt sich der Adressat befindet. Vor allem vom Anschluß an Btx versprechen sich die Cityruf-Befürworter eine rasche Durchsetzung des neuen Dienstes.

Es wird zu prüfen sein, ob dieser Dienst zur Verarbeitung von personenbezogenen Daten führt, die über das erforderliche Maß hinausgeht.

Anbieterprüfungen

Auch im abgelaufenen Berichtszeitraum habe ich Verstöße von Btx-Anbietern gegen Vorschriften des Btx-Staatsvertrages festgestellt:

Auf einer bestimmten Antwortseite wurde vom Teilnehmer die Eingabe eines Kennwortes verlangt, ohne die er das weitere Angebot nicht erreichen konnte. Dabei wurde nicht erläutert, um welche Art von Kennwort es sich handelt (z. B. Nutzungskennwort, GBG-Kennwort), so daß Btx-Teilnehmer durch diese Art der Abfrage veranlaßt werden, unbekannt persönliche Kennwörter preiszugeben.

Erneut habe ich den Fall einer verdeckten Abfrage von Teilnehmerdaten festgestellt. Derselbe Anbieter hatte bereits vor zwei Jahren einen ähnlichen Verstoß begangen. Die zuständige Aufsichtsbehörde will es nicht bei einer Ermahnung bewenden lassen, sondern ein angemessenes Bußgeld aussprechen.

Besonders schlaun kam sich ein Anbieter offenbar vor, der mit einer der Btx-Eingangsseite nachempfundenen Seite Teilnehmer auf den Leim führen wollte, um an ihre persönlichen Daten zu gelangen. Er bot an einer bestimmten Stelle in seinem Angebot plötzlich die täuschend ähnlich gestaltete blaue Seite mit den Eingabefeldern für die Zugangskennwörter an, so daß Teilnehmer meinen mußten, sie seien durch einen technischen Fehler wieder zur Post-Eingangsseite zurückgekommen. Sie gaben so erneut ihre Kennwörter ein, nicht ahnend, daß sie sich immer noch im Angebot des Anbieters befanden und nun ihre Kennwörter preisgegeben hatten.

Einmalig ist bisher die Untersagung der Abfrage personenbezogener Daten eines privaten Anbieters durch die zuständige Aufsichtsbehörde in Berlin. Der betreffende Anbieter fragte auf der Gateway-Seite zu seinem Btx-Programm personenbezogene Daten ab, um – wie er angab – den sinnlosen Verbrauch von Maschinenressourcen zu vermeiden und der Teilnehmer habhaft zu werden, um eventuellen Mißbräuchen nachgehen zu können.

Die in Berlin für private Anbieter zuständige Aufsichtsbehörde, die Senatsverwaltung für Inneres, bemängelte gegenüber dem Anbieter in mehreren Schriftwechseln die Praxis, beim Übergang vom Btx-Rechner in den externen Rechner des Anbieters Teilnehmerdaten wie Teilnehmernamen, -nummer und Adresse abzufragen.

Sie begründete ihre Auffassung damit, daß es unzulässig sei, bis zum Übergang zum externen Rechner Teilnehmerdaten abzufragen, da zu diesem Zeitpunkt der Btx-Nutzung noch kein die Kenntnis der Daten rechtfertigendes Vertragsverhältnis vorliegt.

Diese Abfrage steht im Widerspruch zur Regelung im Btx-StV, nach dem ein Anbieter personenbezogene Daten nur abfragen und speichern darf, soweit diese für das Erbringen einer Leistung, den Abschluß oder die Abwicklung eines Vertragsverhältnisses erforderlich sind.

Da der Anbieter keine Einsicht zeigte und nicht bereit war, von seiner Datenhaltungspraxis abzugehen, wurde die Untersagung im Einvernehmen mit der Senatsverwaltung für Kulturelle Angelegenheiten gem. Art. 12 Abs. 3 S. 1 i. V. m. Abs. 2 und Art. 9 Abs. 6 Btx-StV ausgesprochen.

Bei einem Angebot der Senatsverwaltung für Schule, Berufsbildung und Sport werden auf einer sog. Antwortseite ebenfalls die Systemdaten der Teilnehmer abgefragt. Um etwaigen Manipulationen bei zunehmender Verbreitung von Btx und dem Einsatz neuer, billigerer Software-Decoder zu begegnen, will die Senatsverwaltung in Zukunft die Teilnehmerdaten speichern. Manipulationen will sie so anhand der Nutzerdaten nachweisen können.

Aus datenschutzrechtlicher Sicht stellt diese Handhabung – wie im ersten Fall – einen Verstoß gegen Art. 9 Abs. 6 Satz 1 Btx-StV dar, denn die Speicherung dieser Daten ist für das Erbringen einer Leistung, den Abschluß oder die Abwicklung eines Vertragsverhältnisses ebenfalls nicht erforderlich.

In diesem Angebot werden auch die Namen von Schulleitern veröffentlicht. Dabei stellt sich die Frage, ob die Schulleiter aufgrund ihres Amtes zur Duldung der Veröffentlichung ihrer Namen verpflichtet sind oder ob hierfür die Einwilligung der Betroffenen erforderlich ist.

Ich vertrete die Auffassung, daß ersteres bei Inhabern von Ämtern mit Außenfunktionen der Fall ist. Da nur Namen aus öffentlichen Verzeichnissen (z. B. Berliner Schulverzeichnis) verwendet werden, sehe ich hierin keinen Verstoß gegen Datenschutzbestimmungen.

Bei der Abwicklung der Gebühren kostenpflichtiger Seiten zu Gunsten des Anbieters teilt die Post unter bestimmten Voraussetzungen den Anbietern die Daten der säumigen Zahler mit. Die Anbieter gehen verstärkt dazu über, solche Teilnehmer in *Negativlisten* aufzunehmen und sie vom Zugang zu ihrem Angebot zu sperren. Nach Art. 9 Abs. 1 i. V. m. § 23 BDSG ist die Speicherung in Zahlungsverzug geratener Teilnehmer zwecks Abweisung des Zugriffs zulässig; wenn hierbei ein berechtigtes Interesse geltend gemacht werden kann. Dagegen ist die Übermittlung solcher Listen – auch wenn sie schon anderweitig bekannt geworden sind – nicht erlaubt, da sie – auch durch Veröffentlichung in einem Btx-Angebot – schutzwürdige Belange beeinträchtigt (§ 24 BDSG).

3.3 Kabelpilotprojektgesetz

Nach vielfältigen Schwierigkeiten nahm in diesem Jahr der erste Pay-TV-Anbieter seinen Betrieb auf. Im Gegensatz zu früheren Planungen, bei denen auch datenschutzfreundliche, allerdings technisch aufwendige Verfahren diskutiert worden waren, verwendet der „Teleclub“ eine einfache Technologie. Vermittelt über den Rundfunk- und Fernsehhandel tritt der Teilnehmer dem Teleclub bei, der die Teilnehmerdaten über den Handel erhält und die Abrechnung nutzungsneutral vornimmt. Da auch die technische Abwicklung über die Bundespost und nicht über die Projektgesellschaft für Kabelkommunikation erfolgt, laufen die Daten nicht, wie im KPPG vorgesehen, über die Projektgesellschaft als neutrale Inkassostelle. Da ein Nutzungsprofil bei diesem Verfahren nicht entstehen kann, sind hier die datenschutzrechtlichen Gefahren als gering anzusehen.

Weiter entwickelt wurde das „Berlin-Info“ im Rahmen des Breitbandversuchsprojekts BERKOM. Hier wird die vierte Stufe des Kabelpilotprojektes verwirklicht, in der an einer beschränkten Teilnehmerzahl Versuche zur vermittelten Breitbandkommunikation unternommen werden sollen. Das Projekt, das noch bis 1991 läuft, wird auch einer eingehenden datenschutzrechtlichen Beurteilung zu unterziehen sein - die bisherigen Bemühungen konzentrieren sich auf die technischen Voraussetzungen dieser Kommunikationsform.

Die im KPPG ebenfalls geregelten und von den Datenschutzbeauftragten aufmerksam verfolgten Fernwirkdienste haben auch in diesem Jahr noch keinen Durchbruch erreicht. Das Interesse an einer Beteiligung scheint noch sehr gering. Nichtsdestoweniger halte ich an meiner Bewertung fest; daß mit derartigen Systemen erhebliche datenschutzrechtliche Risiken verbunden sind.

4. Weitere Fragen aus der Kontroll- und Beratungspraxis

4.1 Bau- und Wohnungswesen

Mietspiegel 1990

Zu einer umfangreichen Verarbeitung personenbezogener Daten führte die Erstellung des Mietspiegels 1990. Bei der Vorbereitung der Erhebung von Grundlagendaten wurden die Fragebogen und Merkblätter entsprechend meinen Empfehlungen¹⁾ datenschutzgerecht gestaltet. Während der Erhebungsphase erreichten mich nur vereinzelt Beschwerden und Anfragen betroffener Bürger. Unabhängig davon habe ich das private Forschungsinstitut, das die Erhebung im Auftrag der Senatsverwaltung für Bau- und Wohnungswesen durchführte, im Zusammenwirken mit der Senatsverwaltung für Inneres überprüft. Dabei habe ich festgestellt, daß die Interviewer mit einem mißverständlichen Formular auf die Geheimhaltung der erhobenen Daten verpflichtet worden waren. Das Institut, das in Berlin häufig Markt- und Meinungsforschungsaufträge durchführt, hat mir zugesichert, bei zukünftigen Erhebungen auf eine eindeutige Verpflichtung der Interviewer auf das Datengeheimnis zu achten. Ich habe außerdem Empfehlungen zur Verbesserung der Datensicherung gegeben.

Die Fragebogen sollen nach Abschluß der Untersuchung - voraussichtlich Mitte November - vernichtet werden. Lediglich die Anschriften, die für den Mietspiegel 1990 verwertet worden sind, bleiben bei der Senatsverwaltung für Bau- und Wohnungswesen gespeichert, um in zwei Jahren für die erforderliche Fortschreibung des Mietspiegels erneut genutzt zu werden. So wie die erstmalige Erhebung der Daten auf freiwilliger Basis erfolgte, ist auch bei zukünftigen Befragungen zur Fortschreibung des Mietspiegels kein Betroffener zur Mitwirkung verpflichtet. Jeder Wohnungsinhaber, der der Stichprobe angehört, kann außerdem bei der Senatsverwaltung für Bau- und Wohnungswesen die Löschung seiner Anschrift verlangen.

Computerkriminalität im Wohnungsamt

Aufgrund des Verdachts eines Computerbetruges habe ich zu Beginn des Jahres 1989 eine technisch-organisatorische Prüfung im Bezirksamt Neukölln durchgeführt, die zu einer Beanstandung führte.

Ein Mitarbeiter des Wohnungsamts hatte im Zusammenhang mit dem Mietausgleichsverfahren Überweisungen zu seinen Gunsten veranlaßt, indem er das an sich vorgesehene Vier-Augen-Prinzip außer Kraft gesetzt hatte. Dazu war es erforderlich, neben den Eingaben unter eigener Kennung auch Eingaben unter der Kennung eines anderen Mitarbeiters zu machen. Das Wohnungsamt gab an, daß der Täter, der von sich aus die Tat offenbarte und sofort kündigte, unter fremder Kennung am System arbeitete, wenn Kollegen kurzfristig den Bildschirmarbeitsplatz verließen, ohne sich vom System abzumelden. Das Schöffengericht legt diesen Fallhergang seinem - inzwischen rechtskräftigen - Urteil zugrunde.

Die Manipulationen waren nur möglich, indem durch geschicktes Handeln des Täters mehrere Sicherheitsbarrieren des Verfahrens durchbrochen wurden und menschliche Nachlässigkeit dieses Vorgehens zusätzlich unterstützte. Der Täter nutzte die Kennung eines anderen Kollegen und bearbeitete mehrere Fälle unter dessen Namen. Durch Erhöhung der Personalzahl bei Mietausgleichsanträgen änderte er bereits abgelehnte Mietausgleichsfälle, so daß nunmehr ein Anspruch auf Ausgleichszahlungen entstand. Als Empfänger dieser Zahlungen setzte er sich selbst ein. Die weitere Verarbeitung der Daten erfolgte im LED, wobei zum Abschluß der einzelnen Fälle sog. Protokollisten erstellt wurden. Diese Protokollisten, die im LED ausgedruckt und über die Hauptverteilungsstelle im Bezirksamt Neukölln an die Poststelle des Wohnungsamtes Neukölln gesandt wurden, holte der Täter bei der Poststelle selbst ab, um die vom Verfahren vorgesehene Gegenprüfung durch einen anderen Sachbearbeiter zu vermeiden. Er sonderte die Protokolle aus und versteckte sie in seinem Schreibtisch oder vernichtete sie. Somit konnten die eigentlich zuständigen Mitarbeiter den Betrug nicht erkennen. Aufgrund der bestehenden Vorschriften hat der Amtsleiter des Wohnungsamtes den Empfang der Protokolle zu bestätigen. Dies geschah bei den manipulierten Fällen nicht, und somit konnten die Listen auf dem Transportweg vom LED zum Wohnungsamt von einem Unbefugten gelesen, verändert oder gelöscht werden.

Neben diesem Mangel der Transportkontrolle bedeutete auch der Umstand, daß aufgrund der Beseitigung der Protokolle nicht mehr nachträglich überprüft und festgestellt werden konnte, welche personenbezogenen Daten wann und von wem in das System eingegeben worden sind, einen Mangel der Eingabekontrolle.

Bei Ablehnungen eines Antrags auf Mietausgleich erhält das Wohnungsamt von der Senatsverwaltung für Bau- und Wohnungswesen einen mikroverfilmten Bescheidtext, der ohne Kontrolle abgelegt wird. Vermutlich setzte der Täter hier an, um an die Fälle zu gelangen, die er später für seine Manipulationen präparierte.

Es ist weiterhin festzustellen, daß einige Mitarbeiter es - zumindest teilweise - zuließen, daß der Täter die für ihre Aufgabenerledigung zugeordneten Terminals benutzen konnte. Neben der Verpflichtung auf das Datengeheimnis sind diese Mitarbeiter vor Aufnahme ihrer Tätigkeit über die Einhaltung der Ordnungsmäßigkeit der Datenverarbeitung aufgeklärt worden. Da einige von ihnen offensichtlich die notwendige Sensibilität für die Sicherheit und den Schutz der Daten vermissen ließen, ist zu überlegen, ob in diesen Fällen nicht Maßnahmen zu treffen sind, die das Vier-Augen-Prinzip zusätzlich unterstützen. Hierbei könnte man eine generelle Verpflichtung zur Gegenzeichnung bei wichtigen Eingaben entweder auf manuelle Weise oder aber durch Software gesteuert in Erwägung ziehen.

Bezeichnend für die unzureichende Gewährleistung des Datenschutzes in diesem Wohnungsamt waren meine Feststellungen bei einem Rundgang anläßlich der Überprüfung. An drei unbesetzten Datensichtgeräten waren die Bildschirme noch eingeschaltet und die Arbeitsmasken eingabebereit. So wäre es Unbefugten möglich gewesen, das Datenverarbeitungssystem unbefugt zu nutzen oder Daten zu manipulieren. Dieser Mangel der Benutzerkontrolle sowie die zuvor aufgeführten Mängel haben in Verbindung mit dem Fehlen jeglicher Kontrolle die Manipulationen des Täters entscheidend begünstigt. Die innerbetriebliche Organisation konnte den Anforderungen des Datenschutzes, deren Beachtung die Vorfälle nicht möglich gemacht hätten, nicht gerecht werden. Hier liegen in besonders schwerwiegender Weise Mängel der Organisationskontrolle vor.

Daß der Täter über Jahre hinweg Manipulationen der festgestellten Art durchführen konnte, weist darauf hin, daß in diesem Wohnungsamt offenkundig die Ausführung des Berliner Datenschutzgesetzes nicht sichergestellt war. Andernfalls hätten die Organisationsmängel von der internen Datenschutzkontrolle bemerkt werden müssen.

Angesichts derart grundsätzlicher Mängel habe ich eine Beanstandung ausgesprochen. Das Bezirksamt muß daraus die Lehre ziehen und die internen Kontrollen sowohl des Datenschutzes als auch des Umgangs mit den ADV-Verfahren des Wohnungsamts

¹⁾ vgl. Jahresbericht 1988, Ziff. 4.2

wesentlich verstärken und effizienter gestalten. Dem entspricht die Feststellung des Schöffengerichts, „daß es dem Angeklagten infolge der unzureichenden Sicherungsmaßnahmen *sehr* leicht gemacht wurde.“

Generell sollte überlegt werden, ob nicht bei derartigen zentral erstellten Verfahren diese erst dann in den Wirkbetrieb übergehen dürfen, wenn vom Auftraggeber eine umfassende Abnahme erfolgt, z. B. mittels Durchführung von Funktionstests und eingehender Prüfung auf Schwachstellen. Erst wenn das Verfahren von der verantwortlichen Stelle freigegeben ist, darf es in der Praxis angewendet werden. Für diese Testverfahren ist natürlich der Einsatz qualifizierten Personals notwendig, was zur Zeit bei den meisten Stellen nicht vorhanden sein dürfte. Deshalb ist hier eine beschleunigte Aus- und Weiterbildung der vorhandenen DV-Kräfte bzw. Neueinstellung von geeignetem DV-Personal vonnöten.

Eine erste Stellungnahme des Bezirksamts läßt – unverständlicherweise – noch nicht unbedingt auf eine schnelle Bereitschaft zur Beseitigung der von mir aufgeführten Mängel schließen. Man stellt sich dort auf den Standpunkt, daß die Mehrzahl dieser Mängel dem System und seiner Struktur anzulasten sei und man eine Zuständigkeit hierfür nicht sehe; im übrigen werden die bisher durchgeführten Kontrollmaßnahmen als ausreichend angesehen. Das Wohnungsamt steht weiterhin auf dem Standpunkt, daß es nicht jedem Mitarbeiter kriminelle Neigungen unterstellen und auch nicht jeden überwachen könne. Die Programmsysteme würden in allen Wohnungsämtern der Bezirke verwendet, wobei nicht der einzelne Bezirk, sondern die Senatsverwaltung für Bau- und Wohnungswesen für die Programmerstellung und -betreuung zuständig sei.

Ein anläßlich einer Besprechung mit der Senatsverwaltung aufgestellter Kriterienkatalog zur Verhinderung oder Erschwerung von kriminellen Handlungen mit Hilfe der Datenverarbeitung ist jedoch schon ein erster Schritt in die richtige Richtung und sollte sukzessive um weitere Regelungen bezüglich des Datenschutzes und der Datensicherheit erweitert werden.

Nach dem Bekanntwerden der Straftat hat die Senatsverwaltung die Wohnungsdatei des Mietausgleichsverfahrens nach mehrfach auftretenden Bankkontonummern bei Geldinstituten ausgewertet. Dabei traten einige Fälle zutage, bei denen der Verdacht auf Unregelmäßigkeiten in der Bearbeitung bestand. Nach Auswertung der Stellungnahme der Wohnungsämter stellte sich jedoch heraus, daß es durch fehlerhafte Sachbearbeitungen zu diesen Mehrfacheinträgen bei Kontonummern kam. Letztlich konnte festgestellt werden, daß es keine Unregelmäßigkeiten in anderen Wohnungsämtern gab, die den Verdacht auf die Veruntreuung von Mietausgleichszahlungen zuließen. Die Senatsverwaltung will in unregelmäßigen Abständen diese Prüfungen fortsetzen, wobei die Rechtmäßigkeit dieses Verfahrens im Hinblick auf die Zuständigkeit der Bezirksamter noch zu prüfen ist²⁾.

4.2 Finanzen

Kirchensteuer

Nach dem Gesetz über die Erhebung von Steuern durch öffentlichrechtliche Religionsgemeinschaften im Land Berlin können Kirchen und andere Religionsgemeinschaften, die Körperschaften des öffentlichen Rechts sind, Steuern aufgrund eigener Steuerordnungen erheben. Zu diesem Zweck haben die Katholische und die Evangelische Kirche aufgrund einer Verwaltungsvereinbarung aus dem Jahr 1969 gemeinsame Kirchensteuerstellen bei den Finanzämtern Berlins eingerichtet, welche die Kirchenzugehörigkeit der Steuerpflichtigen überprüfen. Die Berechnung der Kirchensteuer bei Kirchenmitgliedern erfolgt durch die Finanzämter, also nicht durch die Kirchensteuerstellen.

Um der Kirchensteuerstelle die Überprüfung der Kirchenzugehörigkeit der Steuerpflichtigen zu ermöglichen, übermitteln die Berliner Finanzämter sämtliche eingehenden Einkommensteuerklärungen zunächst der Kirchensteuerstelle. Anträge auf Lohnsteuerjahresausgleich werden der Kirchensteuerstelle dann

übermittelt, wenn der Steuerpflichtige im Besteuerungszeitraum aus der Kirche ausgetreten ist. Teilweise wurde auch der Steuerbescheid mitsamt den Unterlagen nach Berechnung des Steuerbetrags nochmals der Kirchensteuerstelle zur Kontrolle weitergegeben.

Dieses Verfahren führte in der Vergangenheit mehrfach zu Beschwerden: Zum einen wurden auch die Einkommensteuerklärungen solcher Bürger an die Kirchensteuerstelle weitergeleitet, die aus der Kirche ausgetreten waren. Zum anderen wurden auch von Kirchenmitgliedern die vollständigen Einkommensteuerklärungen mit sämtlichen Belegen und Nachweisen weitergereicht, darunter auch Unterlagen, die für die Feststellung der Kirchensteuerpflicht bzw. der Höhe der Kirchensteuer nicht erforderlich waren.

Ich habe der Senatsverwaltung für Finanzen mitgeteilt, daß eine Offenbarung des Inhalts der Steuerklärungen gegenüber den Kirchensteuerstellen gemäß § 30 Abs. 4 Abgabenordnung nur dann zulässig ist, wenn es durch Gesetz ausdrücklich zugelassen ist bzw. wenn es der Durchführung eines Steuerverfahrens dient. Die Befugnis zur Offenbarung erfaßt dabei nur solche Daten, die für die Aufgabenerfüllung der empfangenden Stelle erforderlich sind. Das in Berlin eingeführte Verfahren erfüllt diese Kriterien nicht.

Es ging dabei nicht darum, den Kirchen die Ausübung des Rechts auf Steuererhebungen bei ihren Mitgliedern zu erschweren oder dieses Recht selbst zu bestreiten, sondern die Belange des Datenschutzes im Lichte des informationellen Selbstbestimmungsrechts stärker zu berücksichtigen.

Für eine Änderung des Verfahrens sprach auch, daß in anderen Bundesländern datenschutzfreundliche Lösungen bei der Erhebung der Kirchensteuer gefunden wurden: So wird teilweise von den Finanzämtern an die Kirchen ein Pauschalbetrag abgeführt, ohne daß die Kirchen Kenntnis über finanzielle Angaben von bestimmten Personen erhalten. In anderen Bundesländern wird nur ein Grunddatensatz der Steuerpflichtigen an die Kirchen übermittelt, die damit in der Lage sind, die subjektive Kirchensteuerpflicht zu prüfen, ohne jedoch darüber hinausgehende Einzelangaben zu erhalten.

Die Senatsverwaltung für Finanzen schaltete auf meine Bitte um Stellungnahme hin die betroffenen Kirchen ein. Diese vertraten die Auffassung, daß die Weiterleitung der Steuerklärungen von den Finanzämtern an die Kirchensteuerstellen keine Übermittlung im datenschutzrechtlichen Sinn darstellten, da die Kirchen selbst Steuergläubiger seien. Zudem hätten die Kirchen nach Artikel 140 GG in Verbindung mit Artikel 137 Weimarer Reichsverfassung seit jeher das Recht, Einsicht in die „Bürgerlichen Steuerlisten“ zu nehmen. Da Steuerlisten nicht mehr angelegt werden, richtet sich der Anspruch auf die entsprechenden Ersatzunterlagen.

Die Kirchen wiesen weiter darauf hin, daß ihre Mitarbeiter in den Kirchensteuerstellen auf die Einhaltung des Steuergeheimnisses verpflichtet seien.

Dem ist entgegenzuhalten, daß nach dem funktionalen Behördenbegriff die Kirchensteuerstellen organisatorisch der Kirche angehören, auch wenn sie räumlich in den Finanzämtern untergebracht sind. Insoweit liegt eine Übermittlung zwischen unterschiedlichen Stellen vor, wobei auch das Recht auf die Einsicht in „Bürgerliche Steuerlisten“ nur im Rahmen des Erforderlichen zulässig ist.

Auch der Umstand, daß die Mitarbeiter der Kirchensteuerstellen auf das Steuergeheimnis verpflichtet sind, kann nichts daran ändern, daß diese nur über solche Daten Kenntnis erhalten dürfen, die für die Aufgabenerfüllung benötigt werden.

Ich habe daher das Verfahren gegenüber der Senatsverwaltung für Finanzen wegen eines Verstoßes gegen § 30 Abgabenordnung förmlich beanstandet und empfohlen, künftig den Kirchensteuerstellen nur noch solche Daten zuzuleiten, die für die Feststellung der Kirchenzugehörigkeit der Steuerpflichtigen erforderlich sind.

Die Senatsverwaltung für Finanzen hat daraufhin das Verfahren überprüft und – im Einvernehmen mit den Kirchen – einen neuen, datenschutzgerechten Weg gefunden: Künftig wird den

²⁾ vgl. unten 4.10

Kirchensteuerstellen bei Eingang einer Steuererklärung ein Bogen mit den Grunddaten übermittelt, der den Kirchensteuerstellen ermöglicht, die Kirchensteuerpflicht festzustellen. Stellt sich heraus, daß es sich nicht um ein Mitglied handelt, ist der Vorgang erledigt. Auch bei Mitgliedern sollen die Kirchensteuerstellen im Regelfall nach Feststellung der Kirchensteuerpflicht nicht mehr die gesamten Steuererklärungen erhalten, sondern nur noch dann, wenn der Fall Anlaß zu einer Überprüfung gibt.

Die Änderung des Verfahrens hat zudem den Nebeneffekt, daß die Abwicklung der Kirchensteuererhebung beschleunigt wird.

Die Bereitschaft der Senatsverwaltung für Finanzen, ein hergebrachtes Verfahren vollständig zu ändern und datenschutzrechtliche Belange zu berücksichtigen, begrüße ich und rechne mit einer baldigen Umsetzung der Planung.

Private Personalcomputer in der Steuerverwaltung

Aufgrund einer von mir im Sommer 1988 eingeleiteten datenschutzrechtlichen Überprüfung des Einsatzes privater Personalcomputer in der Steuerverwaltung mußte ich angesichts der bisher getroffenen Maßnahmen dem Senator für Finanzen gegenüber eine Beanstandung aussprechen.

Wegen räumlicher Engpässe in den Finanzämtern ist den Betriebsprüfern gestattet worden, Betriebsprüfungsberichte nach Verständigung der Betriebsprüfungsstellen in der eigenen Wohnung zu fertigen. Damit wird in Kauf genommen, daß Materialsammlung und Aufbereitung sowie die Textfertigung in der Privatwohnung zu Risiken für die Wahrung des Steuergeheimnisses nach § 30 Abgabenordnung führt.

Als Konsequenz aus der Zulassung der Dienstausbübung in der Privatwohnung ist den Steuerprüfern gestattet worden, unter bestimmten Regelungen, die die ordnungsgemäße Aufgabenerledigung, die Wahrung des Steuergeheimnisses und zum Teil die Verfahrenssicherheit betreffen, ebenfalls in der Privatwohnung nach eigenem Ermessen beschaffte Geräte für die Dienstgeschäfte einzusetzen. Haupteinsatzgebiet ist dabei die Textverarbeitung, daneben werden Tabellenkalkulations- und im geringeren Umfang Datenbankprogramme eingesetzt.

Die Unterstützung der Arbeit der Betriebsprüfer folgt keinem einheitlichen Konzept, sondern erfolgt nach den individuellen Neigungen der Betriebsprüfer im Rahmen der genannten Regelungen. Obwohl die Finanzverwaltung die Eigeninitiative der Betriebsprüfer begrüßt, hat sie es bisher nicht für erforderlich gehalten, ein Konzept für eine weitgehend einheitliche, bedarfsgerechte und ordnungsgemäße Automationsunterstützung der Betriebsprüfer vorzulegen und zu realisieren. Ich schließe mich auch aus datenschutzrechtlichen Erwägungen der Auffassung des Rechnungshofes von Berlin an, daß die Finanzverwaltung von ihr als notwendig angesehene Arbeitsmittel ihren Beamten selbst in ausreichender Zahl zur Verfügung zu stellen hat. In diesem Fall könnte sie auch dafür sorgen, daß unabhängig von weiterbestehenden Kontrollproblemen einheitlich leistungsfähige, fachlich geprüfte und freigegebene, mit den entsprechenden Datensicherheitskomponenten ausgestattete Hard- und Software eingesetzt wird.

Der derzeitige Zustand soll durch eine Rundverfügung für die Oberfinanzdirektion steuerbarer und transparenter gemacht werden. Zu dem Entwurf dieser Verfügung habe ich Stellung bezogen. Ich habe die Rundverfügung grundsätzlich als geeignetes Steuerungsmittel für eine nur kurzfristig hinnehmbare Übergangssituation begrüßt und Anregungen zur Verbesserung der technischen Datensicherung und der Kontrollmöglichkeiten gegeben.

Allerdings bleiben dadurch zwei wesentliche datenschutzrechtliche Probleme nach wie vor ungelöst. Zum einen kann die Senatsverwaltung für Finanzen trotz aller flankierenden Regelungen bei der Verarbeitung personenbezogener Daten auf privaten Rechnern in der Wohnung der Betriebsprüfer die Ausführung der Rechtsvorschriften über den Datenschutz nicht sicherstellen. Sie kann insbesondere nicht dafür sorgen, daß die ordnungsgemäße Anwendung der DV-Programme, mit deren Hilfe personenbezogene Daten verarbeitet werden, überwacht wird.

Zum anderen ist der Berliner Datenschutzbeauftragte daran gehindert, seinen Kontrollaufgaben in der Privatwohnung des Steuerprüfers nachzukommen, es sei denn, dieser hat der Kontrolle in der Wohnung zugestimmt.

Meine Beanstandung habe ich deshalb mit folgenden Empfehlungen verbunden:

- Es ist dafür Sorge zu tragen, daß baldmöglichst die Sicherheit des Steuergeheimnisses und des Datenschutzes dadurch wieder hergestellt wird, daß die Betriebsprüfer alle dienstlichen Aufgaben, die sie bisher in der Privatwohnung erledigen durften, unter angemessenen und dem Steuergeheimnis nicht abträglichen Bedingungen in Diensträumen der Steuerverwaltung erledigen.
- Es sollte ein DV-Konzept für die Automationsunterstützung der Betriebsprüfer entwickelt werden, welches einerseits für eine kurze Übergangszeit die Datenverarbeitung in der Privatwohnung sicherer und zuverlässiger macht und andererseits dem vorrangigen Ziel der Rückführung der Arbeitserledigung in die Diensträume nicht nur nicht entgegensteht, sondern sie auch konzeptionell vorbereitet.

Automatisiertes Haushaltswesen

Im Sommer dieses Jahres ist mir der Hauptuntersuchungsbericht zum Verfahren Neukonzeption des Automatisierten Haushaltswesens zugeleitet worden. Die Realisierung dieses umfangreichen Verfahrens ist über mehrere Jahre konzipiert.

Das neue Verfahren soll in den bewirtschaftenden Dienststellen, den Haushaltsämtern der Bezirke, den Haushaltsreferaten der Senatsverwaltungen, der Haushaltsrevision der Senatsverwaltung für Finanzen sowie in den Bezirken und der Landeshauptkasse - zusammen ca. 450 Dienststellen - angewendet werden. Das Gesamtverfahren ist in die Teilverfahren Planung (Aufstellung des Haushaltsplans incl. der Nachträge, Investitions- und Finanzplanung), Haushaltswirtschaft (Ausführung des Haushaltsplans mit Berichtswesen), Buchführung und Rechnungslegung untergliedert. Die Teilverfahren sind wiederum in Teilprojekte aufgeteilt.

Bei dem Verfahren handelt es sich um ein dialogorientiertes Verfahren mit Einsatz von intelligenten Datenendgeräten. Das technische Konzept sieht einen Verbund von dezentralen APC und zentralem Host-Rechner im LED mit flächendeckendem Einsatz von Endgeräten (ca. 370 mehrplatzfähige Systeme mit ca. 800 Terminals) vor.

Es handelt sich um ein integriertes ADV-Verfahren, das mit ca. 450 Programmen die in mehr als 2000 Dateien gespeicherten Daten verarbeitet. Die Datenerfassung wird für die Haushaltsplan-Aufstellung (einschließlich der Finanz- und Investitionsplanung) zentral im LED auf einem Datensammelsystem, für alle übrigen Bereiche dezentral in den Kassen in Datenerfassungssystemen durchgeführt.

Das LED nimmt die Aufgaben eines zentralen Rechenzentrums wahr. Dabei wird von einem dreistufigen Netzkonzzept ausgegangen. In der untersten Netzebene sind die dezentralen Endgeräte bei den Anwendern angesiedelt. Zwischen dieser Ebene und der zentralen ADV-Anlage mit dem Host-Rechner beim LED sollte das Verwaltungsnetz für den ganzheitlichen Datentransport dienen, dessen Inbetriebnahme allerdings in Frage gestellt ist.

Die wichtigsten Zielvorgaben zur Verbesserung der Situation am Arbeitsplatz sind die Einführung eines Direktauskunfts- und Änderungsdienstes in den dezentralen Dienststellen zur schnellen Verfügbarkeit aktueller Informationen vor Ort sowie verbesserte und bedarfsgerechte Auswertungsmöglichkeiten.

Der Hauptuntersuchungsbericht läßt generell auf eine ausreichende Gewährleistung des Datenschutzes und der Datensicherheit schließen. Für viele datenschutzrelevante Bereiche sind hinreichende Vorkehrungen getroffen worden, deren detaillierte schriftliche Festlegung jedoch noch vorzunehmen ist. Vor allem über die Komplexe Zu- und Abgangskontrolle, Speicher- und Zugriffskontrolle, Test- und Freigabeverfahren sowie über die

Datenträgerbehandlung (Aufbewahrung, Transport und Vernichtung) sind eine Reihe von Aussagen getroffen worden, die allerdings noch abschließend beraten werden müssen.

4.3 Gesundheit und Soziales

AIDS

Nach wie vor kommt dem Schutz personenbezogener Daten von AIDS-Kranken und HIV-Infizierten große Bedeutung zu. Besonders betroffen sind auch in datenschutzrechtlicher Hinsicht die Kinder.

Beispielhaft ist die Weiterung eines früheren Falles, in dem un-erlaubt Daten über eine HIV-Infektion von einem Krankenhaus an ein Gesundheitsamt übermittelt wurden. Dieser Verstoß gegen die ärztliche Schweigepflicht wurde von mir im Jahr 1987 beanstandet. Vom Gesundheitsamt war zugesichert worden, daß die unzulässig übermittelten Informationen restlos aus den Unterlagen der Behörde getilgt würden.

Etwa zwei Jahre später wurde für das kindergartenreife Kind der betroffenen Mutter beim Gesundheitsamt eine Unbedenklichkeitsbescheinigung zum Besuch eines Kindergartens beantragt. Zum Erstaunen der Mutter wurde diese mit dem Hinweis auf eine mögliche HIV-Infektion des Kindes verweigert. Das Kind war also daran gehindert, einen Kindergarten wie andere Kinder zu besuchen. Bei der erneuten Überprüfung wurden zwei Mängel aufgedeckt, die zum Nachteil des Kindes zusammentrafen:

Einerseits stellte ich fest, daß zwar, wie vom Gesundheitsamt zugesichert, die übermittelten Datenträger aus der Akte entfernt worden waren. Es waren jedoch zwischenzeitlich wieder handschriftliche Gesprächsvermerke über die HIV-Infektion in die Akte genommen worden. Aufgrund meines Hinweises, daß ohne die unzulässige Datenübermittlung die Gespräche in dieser Form gar nicht stattgefunden hätten, wurde die Akte bereinigt.

Gleichwohl wurde die Unbedenklichkeitsbescheinigung mit dem Hinweis auf das HIV-Infektionsrisiko verweigert. Gemäß einer Absprache zwischen Amtsärzten und Gesundheitsverwaltungen sollte generell keine Unbedenklichkeitsbescheinigung für HIV-infizierte oder exponierte Kinder erteilt werden. Ich habe diesen Verstoß gegen die Integritätsbemühungen HIV-infizierter Menschen auch aus datenschutzrechtlicher Sicht beanstandet. Ohne gesetzliche Ermächtigung halte ich die Erhebung von HIV-Daten für derart eingreifende Verwaltungsentscheidungen für unzulässig. Die Anhörung von medizinischen Experten in einem Arbeitskreis der beteiligten Verwaltungen bestätigte auch aus medizinischer Sicht die Richtigkeit meiner Auffassung. Ich habe darauf hingewiesen, daß folglich auch nur mit dem ausdrücklichen Hinweis auf die Freiwilligkeit der Angaben nach einer HIV-Infektion gefragt werden darf.

Der HIV-Status dürfte daher künftig bei Feststellung der Kindergarten-tauglichkeit kein formales Entscheidungskriterium mehr sein. Nicht auszuschließen ist allerdings, daß eine manifeste HIV-Erkrankung sich auf die Erteilung der Unbedenklichkeitsbescheinigung auswirkt.

Der Vorfall zeigt, daß selbst unter dem schützenden Mantel der „Berliner Linie“ unvermutet aus verwaltungstechnischen Gründen die Bereitschaft zur Ausgrenzung aufkeimen kann.

Wegen der berechtigten Ängste der infizierten Menschen ist auch bei den *Forschungsvorhaben zum Thema AIDS* die Gewährleistung des Datenschutzes als oberstes Gebot zu beachten. Die zur Erforschung und Bekämpfung von AIDS bereitgestellten finanziellen Mittel könnten sonst zu einer zusätzlichen Gefährdung der Betroffenen werden. Ich habe bei der Vorbereitung mehrerer Forschungsprojekte mitgewirkt und dabei festgestellt, daß dem Datenschutz nicht von Anfang an ein angemessener Stellenwert eingeräumt worden war. Die Mängel konnten jeweils noch rechtzeitig behoben werden.

Erwähnt seien die „*Multizentrische Studie zur Langzeitbetreuung HIV-infizierter und HIV-exponierter Kinder*“ mit ihren sozialpsychologischen und medizinischen Teilprojekten sowie die noch nicht endgültig konzipierten Dokumentationsprogramme

„KLINAIDS und KLIMACS“. Allen Befragungen ist gemeinsam, daß sie sich ungewöhnlich direkt um intimste Daten des Geschlechtslebens und der Persönlichkeitsstruktur bemühen und gleichzeitig die sozialpsychologische „Vernetzung“ der Betroffenen aufdecken wollen. Die dabei abgefragten Details führen zu einem so hohen Reidentifizierungsrisiko, daß selbst beim Verzicht auf Name und Anschrift kaum eine hinreichende Anonymität der Angaben vorliegt. Deshalb war grundsätzlich das Einverständnis und die vollständige Information der befragten Personen zur Durchführung erforderlich.

Gesundheitsreformgesetz

Mit der Verkündung des Gesundheitsreformgesetzes ist zu Beginn des Jahres das Sozialgesetzbuch Buch V (SGB V) in Kraft getreten, das erhebliche Eingriffe auch in das informationelle Selbstbestimmungsrecht der Patienten enthält. Die Verbesserungsvorschläge der Konferenz der Datenschutzbeauftragten wurden nur zum Teil übernommen.

- Im Mittelpunkt der Problematik steht die stichprobenweise Überprüfung der Wirtschaftlichkeit der Versorgung nach § 106 SGB V. Die Begrenzung auf 8 % der Ärzte pro Jahr ist so hoch gegriffen, daß sie als gestaffelte Totalüberprüfung bewertet werden muß, zumal die Daten teilweise bis zu drei Jahren vorgehalten werden können (vgl. § 297 Abs. 1 i.V.m. § 304 Abs. 1 Ziffer 2 SGB V).
- Äußerst problematisch ist auch § 276 Abs. 4 SGB V. Dort wird der Medizinische Dienst ermächtigt, zwischen 8.00 und 18.00 Uhr die Räume der Krankenhäuser und Vorsorge- und Rehabilitationseinrichtungen zu betreten, um dort die Krankenunterlagen einzusehen und, soweit erforderlich, den Versicherten zu untersuchen. Dies kann zur erheblichen Beeinträchtigung der ärztlichen Schweigepflicht führen.
- Zwar wurde auf die Verwendung der Rentenversicherungsnummer bei der Einführung des Krankenversicherungsausweises verzichtet; auch die patientenbezogenen Leistungskonten wurden nicht eingerichtet. Geblieben ist jedoch nach wie vor das Risiko, daß aufgrund der Stichprobenprüfung nach § 106 SGB V auch Überwachungsmaßnahmen gegenüber Patienten ermöglicht werden.
- Unbeachtet blieb der Hinweis, daß die weitreichenden Kompetenzen der Verbände zu Rahmenvereinbarungen und anderen Verträgen der Forderung nach normenklarer, gesetzlicher Regelung nicht entsprechen.
- Auch die Auskunfts- und Einsichtsrechte gegenüber den Leistungsträgern bleiben hinter den Rechten der Patienten gegenüber dem Arzt zurück. So ist die Beschränkung des Auskunftsanspruches auf die Zeitspanne von zwei Jahren (§ 305 SGB V) sehr problematisch.
- Unbefriedigend ist die generalklauselartige Befugnis zur Datenübermittlung im Rahmen der Stichprobenprüfung nach § 289 SGB V.
- Auch die datenschutzrechtlichen Anforderungen an die zentrale Krankheitsdatei der Unfallversicherungsträger blieben unerfüllt.

Wichtige Fragen, auf die die Datenschutzbeauftragten schon in früherer Zeit hingewiesen hatten, blieben dagegen ungeregelt, wie z. B. die Erforderlichkeit der Diagnosenangabe auf Krankenscheinen. Angesichts der Anforderungen, die das Bundesverfassungsgericht in seinem Volkszählungsurteil an die Normenklarheit staatlicher Eingriffsbefugnisse stellt, deute ich nunmehr diese „Nichtregelung“ als Absicht des Gesetzgebers, die Angabe von Diagnosedaten auf Krankenscheinen nicht zuzulassen. Entsprechende Anfragen von Berliner Ärzten bei meiner Behörde habe ich in diesem Sinne beantwortet.

Gesundheitsdienst

Langjährige Auseinandersetzungen um das Akteneinsichtsrecht im Sozialpsychiatrischen Dienst fanden in diesem Jahr nach einer Entscheidung des Bundesverwaltungsgerichts ihren Ab-

schluß. In einem Fall, mit dem ich befaßt war, wurde der Petentin nach jahrelangen Auseinandersetzungen mit dem Bezirksamt endlich Akteneinsicht gewährt.

Die Petentin war in Kontakt mit dem Sozialpsychiatrischen Dienst eines Bezirksamtes und hatte im Jahr 1983 auf dem Sozialamt eine Auseinandersetzung mit den dortigen Mitarbeitern. Sie war daraufhin vorübergehend zwangsweise untergebracht worden und wollte durch die Akteneinsicht die Hintergründe klären.

Der Bezirk lehnte ihren Antrag u. a. mit der Begründung ab, daß Rechte Dritter entgegenstünden: So seien die Namen von anderen Personen, die vertrauliche Informationen gegeben hätten, zu schützen. Auch könne die Bekanntgabe des Inhalts der Akten den Gesundheitszustand der Betroffenen schädigen.

Eine Kompromißlösung, etwa im Wege einer Akteneinsicht durch eine neutrale Person, die den wesentlichen Inhalt - ohne Verletzung von möglichen Rechten Dritter - an den Betroffenen vermitteln könnte, lehnte der Bezirk ab. Auch die Schwärzung der Namen von Informanten in der Akte wurde vom Bezirk zurückgewiesen. Meine Bemühungen um die Verschaffung der Akteneinsicht blieben daher ohne Erfolg.

Die betroffene Bürgerin hatte gleichzeitig beim Verwaltungsgericht Klage auf Gewährung der Akteneinsicht erhoben, so daß letztlich das Gericht entscheiden mußte.

Das Verwaltungsgericht stellte in seinem Urteil fest, daß der Bezirk verpflichtet ist, die Einsicht über die beim Sozialpsychiatrischen Dienst geführten Akten zu gewähren.

Gegen dieses Urteil legte der Bezirk zwar Berufung ein, diese wurde jedoch zurückgezogen, als das Bundesverwaltungsgericht³⁾ in einem ähnlich gelagerten Fall eine Entscheidung traf, die ein psychiatrisches Krankenhaus ebenfalls zur Gewährung der Akteneinsicht durch den Patienten verpflichtete. Das Bundesverwaltungsgericht führte darin aus, daß allein die Behauptung der Gesundheitsgefährdung beim Betroffenen nicht ausreiche, die Akteneinsicht zu verweigern. Der Bürger sei weitgehend selbst in der Lage zu entscheiden, welche Gefahren er auf sich nehme. Nur wenn die Steuerungsfähigkeit so weit eingeschränkt sei, daß eine vernünftige Entscheidung durch den Betroffenen selbst nicht getroffen werden könne, komme ein Auskunftsverweigerungsrecht in Betracht.

Das Bundesverwaltungsgericht stützte die Entscheidung zur Gewährung der Akteneinsicht auf die Grundrechte der Artikel 1 Abs. 1 und 2 Abs. 1 GG.

Eine typisch berlinische Problematik wurde mir aus dem Bezirk Tiergarten vorgelegt. Es ging um das „*Mauerspringersyndrom*“, welches nicht nur literarisch und filmisch verarbeitet wurde, sondern im Gesundheitsamt mehrfach verwaltungsmäßige Wirklichkeit wurde: Menschen, die über die Berliner Mauer illegal in den Ostsektor der Stadt wechselten, wurden von den DDR-Behörden psychiatrisch untergebracht und mitunter auch medikamentös behandelt. Im Zuge ihrer Rückführung durch das Deutsche Rote Kreuz wurden diese Menschen im Westteil der Stadt dem Sozialpsychiatrischen Dienst zugeführt und dort untersucht. Dies ist in der Regel nur mit Einverständnis der Betroffenen zulässig. In den Fällen, in denen die Betreuung durch den Sozialpsychiatrischen Dienst von den Betroffenen abgelehnt wird, dürfen auch keine Vorgänge angelegt werden. Ich bestätigte die Auffassung einer Bezirksstadträtin für Gesundheit, die der Auffassung war, daß dennoch angelegte Akten zu vernichten seien.

Die ärztliche Schweigepflicht steht *Auskünften des Sozialpsychiatrischen Dienstes an andere Dienststellen* entgegen. Insbesondere dürfen gegenüber Polizeibehörden, die besonders häufig anfragen, nur dann Auskünfte gegeben werden, wenn der Betroffene einverstanden ist oder die Voraussetzungen der „mutmaßlichen Einwilligung“ oder des „übergesetzlichen Notstandes“ vorliegen.

Ich habe dies mit einigen Berliner Bezirken erörtert und Verhaltensrichtlinien empfohlen. Darüber hinaus habe ich der Senatsverwaltung für Gesundheit und Soziales empfohlen, Entscheidungshilfen zumindest in Form eines Rundschreibens zu geben, um der weitverbreiteten Unsicherheit entgegenzuwirken.

Die Überprüfung in einem Bezirk hatte ergeben, daß *Meldungen von „dritten Stellen“* (Nachbarn, anderen Behörden etc.) als Betreuungsvorgänge geführt wurden, obwohl das Einverständnis mit einer psychiatrischen Betreuung nicht immer nachweisbar war. Wegen des Prinzips der Freiwilligkeit der Betreuungsarbeit (vgl. § 3 Abs. 3 Gesetz über psychisch Kranke) habe ich empfohlen, derartige Vorgänge zu vernichten. Diese Angelegenheit bildete den Anlaß, eine Arbeitsgruppe bei der Senatsverwaltung für Gesundheit und Soziales über Probleme der Aktenführung im Sozialpsychiatrischen Dienst einzurichten.

Schließlich wurde ich auch wieder mit den Problemen des *Jugendgesundheitsdienstes* konfrontiert. Ähnlich wie der Sozialpsychiatrische Dienst eine freiwillige Beratung und Betreuung anbietet, wird auch der Jugendgesundheitsdienst für Kleinkinder und Säuglinge auf freiwilliger Basis beratend und betreuend tätig. Dieses Leistungsangebot wird von vielen Eltern im Bewußtsein der Freiwilligkeit angenommen. Obwohl ich in früheren Jahren darauf gedrängt habe, diese Beratungsvorgänge nicht ohne Einverständnis mit den Pflichtaufgaben des Schulgesundheitsdienstes nach § 22 Schulgesetz zu verknüpfen, scheint dies noch immer im großen Umfang zu geschehen. Dies führte dazu, daß sich eine Mutter mit den Angaben, die sie bei der freiwilligen Betreuung gemacht hatte, im Rahmen einer pflichtmäßigen Schulgesundheitsuntersuchung unter Druck gesetzt fühlte, weil diese Unterlagen ohne ihr Einverständnis beigegeben worden waren. Ich habe auf die Unzulässigkeit dieser Verfahrensweise hingewiesen und bewirkt, daß die Beeinträchtigung in diesem Einzelfall vom Bezirk rückgängig gemacht wurde.

Embryonenschutzgesetz

Die überragende Bedeutung, die der Datenschutz und das informationelle Selbstbestimmungsrecht auf dem Gebiet der modernen Gesetzgebung haben oder zumindest haben sollten, wird deutlich am Vorhaben eines Embryonenschutzgesetzes. Die Berliner Senatsverwaltungen waren angesichts eines Entwurfs der Bundesregierung aufgefordert, eine Stellungnahme zu entwerfen. Ich wurde zu den Beratungen hinzugezogen und habe Bedenken gegen das Gesetz vortragen. Was früher literarische Angstvorstellung war (vgl. Aldous Huxleys „*Brave new world*“), fordert heute schon die schützende Tätigkeit des Gesetzgebers heraus. Die künstliche Erzeugung menschlichen Lebens, die auch die Erzeugung menschlicher Abartigkeiten ermöglicht (Klonen, Chimärenbildung, Erzeugung menschlicher Embryonen zu Forschungszwecken), sollte durch diesen Entwurf verfassungsgerecht geregelt werden. Ich habe darauf hingewiesen, daß die künstliche Erzeugung menschlichen Lebens, auch soweit sie ethisch vertretbar ist, einer positiven detaillierten gesetzlichen Regelung bedarf, um die Rechte und Pflichten der Beteiligten insbesondere im Hinblick auf das informationelle Selbstbestimmungsrecht der werdenden Eltern und des erzeugten Kindes zu gewährleisten. Denn der künstliche Zeugungsvorgang ist Gegenstand unterschiedlicher rechtlicher Interessen, in deren Mittelpunkt das verfassungsrechtlich garantierte Recht des werdenden Kindes steht, Kenntnis von seiner wirklichen Abstammung zu erhalten. Dieses Recht darf bei der künstlichen Zeugung nicht zum Verfügungsgegenstand der behandelnden Ärzte oder etwa anderer dritter Personen werden.

Forschung mit medizinischen Daten

Der Personalrat eines Krankenhauses machte mich darauf aufmerksam, daß in der geburtshilflichen Abteilung dieses Krankenhauses Schwangere über *Nebenwirkungen von Arzneimitteln sowie den Alkohol-, Nikotin- und Drogenkonsum in der Schwangerschaft* befragt wurden. Dies geschah zwar auf freiwilliger Basis in Zusammenarbeit mit dem Bundesgesundheitsamt. Der Fragebogen enthielt jedoch u. a. Fragen nach dem Drogenkonsum, die die befragten Patientinnen zu einer Selbstbezeichnung hätten veranlassen können. Hätten diese Fragebögen in personenbezogener Form die Klinik verlassen, so wären sie dem potentiellen Zugriff der Strafverfolgungsbehörden ausgesetzt gewesen, da das Beschlagnahmeverbot sich nur auf Patientenunterlagen bezieht, die sich im Gewahrsam des behandelnden Arztes befinden. Aufgrund meines Hinweises hat der ärztliche Leiter des Krankenhauses verfügt, daß vor einer Klärung der datenschutzrechtlichen

³⁾ Az 3 C 4.86

Fragen keine ausgefüllten Fragebogen das Krankenhaus verlassen dürfen. Dieses Beispiel zeigt, daß es gerade auch im Interesse der Forscher sinnvoll ist, mich bereits bei der Konzipierung des Erhebungsverfahrens für ein Forschungsprojekt zu Rate zu ziehen. Geschieht dies nicht und treten während der Durchführung datenschutzrechtlich Mängel auf, so führt dies zwangsläufig zumindest zu einer Verzögerung, wenn nicht zum Abbruch des Forschungsvorhabens.

Demgegenüber haben mich die Kinderkliniken der Universitätsklinik Steglitz und Rudolf-Virchow in vorbildlicher Weise frühzeitig um Beratung bei der Vorbereitung einer multizentrischen Studie über *atonische Erkrankungen* (Allergien) im Säuglingsalter gebeten. Bei diesem Projekt sollen ab Anfang 1990 in diesen beiden Kliniken und in weiteren Kliniken im Bundesgebiet Mütter unmittelbar nach der Geburt ihres Kindes über allergene Umweltbelastungen in der Familie und während der Schwangerschaft von Klinikärzten befragt werden. Aufgrund meiner Empfehlungen sollen die erhobenen Daten in anonymisierter Form an das Bundesgesundheitsamt weitergegeben und dort auf einer Großrechenanlage ausgewertet werden. Auf freiwilliger Basis können sich Mütter auch an einer anschließenden Längsschnittuntersuchung beteiligen, weil die Neugeborenen über einen längeren Zeitraum hinweg auf allergene Belastungen hin untersucht werden sollen. Die dabei erhobenen Befunde werden in einem Untersuchungsheft dokumentiert, das den Eltern ausgehändigt wird und in das diese ihrerseits Auffälligkeiten des Kindes eintragen können. Die Eltern müssen die Möglichkeit haben, die Teilnahme an diesem Projekt jederzeit abzubrechen.

Offenbarung von Sozialdaten

Im Bereich der Sozialverwaltung gibt es anhaltende Probleme bei der Frage nach der Zulässigkeit der Offenbarung von Sozialdaten.

Eine Gruppe von vier Personen wollte einen nicht anwesenden Mitarbeiter der Familienfürsorge sprechen. Die Personen verließen die Beratungsräume, nachdem sie ihren Namen genannt hatten. Kaum jedoch hatten sie das Gebäude verlassen, stellte die Reinigungsfrau das Fehlen ihres Staubsaugers, den sie auf der Treppe abgestellt hatte, fest und befragte den noch anwesenden Sozialarbeiter nach dem Namen jener Familie und erfuhr ihn auch. Wenige Tage später erschien ein Kriminalbeamter, um eine Vernehmung dieses Mitarbeiters durchzuführen. Nach § 69 Abs. 1 Nr. 1 2. Alt. SGB X dürfen Sozialdaten, zu denen die Auskünfte des Mitarbeiters gehören, offenbart werden, wenn sie erforderlich sind für die Durchführung eines Strafverfahrens, das im Zusammenhang mit einer gesetzlichen Aufgabe nach dem Sozialgesetzbuch steht. Zu erwägen war hier, ob wegen des Zusammenhangs des *mutmaßlichen Diebstahls* mit der Sozialleistung die Datenoffenbarung auf diese Bestimmung gestützt werden konnte. Ich habe dies bejaht mit der Einschränkung, daß jedoch über eine Offenbarung nach § 69 SGB X allein der Sozialleistungsträger entscheiden könne. Bei der Abwägung kommt dem Verhältnismäßigkeitsprinzip unter dem Gesichtspunkt der „Geeignetheit der Maßnahme“ besondere Bedeutung zu. Da durch den Sozialdatenschutz kein strafrechtlicher Freiraum geschaffen werden soll und sowohl die Mitarbeiter als auch die Allgemeinheit zu schützen sind, halte ich es für zulässig, daß Straftaten, die als Begleitumstand eines Sozialleistungsverhältnisses begangen werden, von der Sozialbehörde unter Angabe der notwendigen Daten zur Anzeige gebracht werden können. Geeignet ist eine Datenoffenbarung oder gar eine Strafanzeige gegen einen Hilfeempfänger jedoch nur dann, wenn aus der Sicht der Sozialleistungsbehörde ein hinreichend konkreter Tatverdacht besteht und andere Möglichkeiten zur Schadensminderung oder zur Beseitigung des Taterfolges nicht bestehen.

Weiterhin Schwierigkeiten bereitete die Anwendung des § 74 Ziffer 2 a SGB X. Die Vorschrift enthält eine Offenbarungsbefugnis für die Geltendmachung eines *Unterhaltsanspruchs*, wenn der Verpflichtete nicht innerhalb einer angemessenen Frist nach einem Hinweis auf die in dieser Vorschrift enthaltene Offenbarungsbefugnis die erforderlichen Auskünfte erteilt hat. Diese in der Praxis bedeutsame Vorschrift wird oft unrichtig angewandt; Fehler unterlaufen insbesondere bei der Mahnung, die

mit der angemessenen Frist verbunden werden und den Hinweis auf die Offenbarungsbefugnis des Sozialgesetzbuches enthalten muß.

Von einem Sozialamt wurde einem Vermieter mitgeteilt, daß dessen Mieter Sozialhilfe bezog und in seinen Mieträumen eine Katze hielt. Diese offenkundige Verletzung des Sozialgeheimnisses wurde von dem Bezirk mit dem Hinweis bestritten, daß es sich hierbei um „*Trivialdaten*“ handle, auf die der Sozialdatenschutz nicht anwendbar sei. Diese Auffassung habe ich als unrichtig zurückgewiesen. Gerade wegen mietvertraglich möglicher Konsequenzen können derartige Daten nicht einfach abgetan werden. Mit Recht hat das Bundesverfassungsgericht festgestellt, daß es kein belangloses Datum mehr gibt.

Bereits früher⁴⁾ habe ich gegenüber einem Bezirksamt bemängelt, daß sich jeder Besucher des Sozialamtes in einer im Wartezimmer ausliegenden *Besucherliste* mit Namen, Anschrift und Grund des Besuches eintragen mußte. Dadurch wurde das Sozialgeheimnis beeinträchtigt, weil die nachfolgenden Besucher erfuhren, wer in ihrer unmittelbaren Nachbarschaft Sozialleistungen bezog.

Aufgrund mehrerer Beschwerden habe ich festgestellt, daß von diesem Verfahren nur teilweise abgerückt worden ist. In einer Außenstelle wurden erst nach meiner erneuten Intervention die Listen vollständig abgeschafft und vernichtet, da sie in dieser Form unzulässig waren und eine Aufbewahrung nicht mehr erforderlich ist. Auch im Rathaus müßten sich die Besucher jeweils in die nunmehr vom Sachbearbeiter geführten Listen mit Namen und Anschriften eintragen. Dies wurde damit begründet, daß einerseits eine Reihenfolge festgelegt werden müsse, wer als nächster bedient wird, und daß andererseits in einem Verwaltungsstreitverfahren nachgewiesen werden müsse, daß bestimmte Personen an bestimmten Sprechtagen im Sozialamt waren.

Ich habe deutlich gemacht, daß sich die Reihenfolge, nach der die Antragsteller bedient werden, auch auf andere Weise feststellen läßt. Das Führen einer Besucherliste ist zumindest nicht in der Form erforderlich, daß sich die Besucher mit Namen und Anschriften selbst eintragen. Diese Aufgabe könnten auch die Sachbearbeiter übernehmen. Soweit die Liste zu Beweis Zwecken herangezogen wird und dabei nicht die Namen der anderen Sozialhilfeempfänger abgedeckt oder geschwärzt sind, stellt das in jedem Einzelfall einen Verstoß gegen das Sozialgeheimnis dar. Für die Offenbarung der Namen und Anschriften der Nichtbetroffenen liegt keine Offenbarungsbefugnis vor. Auch die Aufbewahrungsfrist von einem Jahr halte ich für zu lang. Der Grundsatz der Erforderlichkeit beschränkt die Speicherung auch in zeitlicher Hinsicht. Erforderlich ist die Speicherung nur solange und nur in dem Umfang, wie die Aufgabe in bezug auf den Betroffenen aktuell ist.

Nach wie vor zu Problemen führt die Anwendung des § 68 SGB X im Hinblick auf *Amtshilfeersuchen der Polizei* gegenüber Sozialleistungsträgern. So wurde erneut ein Sozialhilfeempfänger im Sozialamt festgenommen, nachdem der Polizei nicht nur seine Anschrift, sondern auch sein Aufenthalt im Sozialamt mitgeteilt worden war. Meine Beanstandung führte zu erneuten Beratungen über das Rundschreiben der beteiligten Senatsverwaltungen⁵⁾. In dieser Beratung habe ich gefordert, daß die Senatsverwaltung für Justiz die Staatsanwaltschaft auf das in Berlin festgelegte Verfahren hinweist. Ich gehe davon aus, daß nach einem solchen Hinweis die Schwierigkeiten ausgeräumt werden.

Offenbarung aufgrund technischer Mängel

Ein Petent hat mir die Kopie einer automatisiert erstellten AOK-Bescheinigung im Rahmen des Deutsch-Österreichischen Abkommens über soziale Sicherheit übersandt, in der nicht nur seine persönlichen Angaben; sondern auch der Name, Vorname, Geburtsdatum und die Anschrift einer anderen Versicherten enthalten waren. Die Daten der anderen Versicherten sind später von einem AOK-Mitarbeiter auf der Bescheinigung gestrichen und diese dann dem Petenten übergeben worden.

⁴⁾ Jahresbericht 1985, Ziff. 4.5

⁵⁾ vgl. Jahresbericht 1985, Anlage 3

Die AOK hat mir mitgeteilt, daß aus dem in der Bezirksstelle vorliegenden Logbuch ersichtlich ist, daß es an dem einschlägigen Bildschirmarbeitsplatz an diesem Tage technische Probleme gegeben hat. Daraus ist der gleichzeitige Ausdruck von Personalien verschiedener Personen auf einem Vordruck zu erklären. Ein Programmfehler hat nicht vorgelegen. Der Geschäftsführer der AOK hat mißbilligt, daß der Vordruck in dieser Form herausgegeben wurde. Da ein fehlerfreier maschineller Ausdruck zunächst nicht möglich war, hätte eine handschriftliche Ausfertigung erfolgen müssen.

Den zusätzlichen Ausdruck des Namens, Vornamens, Geburtsdatums und der Anschrift einer anderen Versicherten in dem Berechtigungsschein habe ich gegenüber der AOK beanstandet.

4.4 Inneres

Öffentliche Sicherheit

Im Schengener Übereinkommen vom 14. Juni 1985 vereinbarten die Bundesrepublik, Frankreich und die Beneluxstaaten einen Abbau der zwischen ihnen bestehenden Grenzhindernisse. Da damit auch die polizeilichen Grenzkontrollen entfallen, ergibt sich für die Sicherheitsbehörden das Problem, auf welche Weise gleichwohl der derzeitige Sicherheitsstandard aufrechterhalten werden kann. Hierzu soll das Schengener Abkommen um einen Zusatzvertrag ergänzt werden, in dem eine Reihe legislativer und exekutiver Maßnahmen vereinbart werden sollen.

Im Mittelpunkt der Vereinbarung steht der Aufbau eines gemeinsamen, datengestützten Fahndungssystems. Es soll für die künftig nur noch an den Außengrenzen stattfindenden Grenzkontrollen die erforderlichen Fahndungsdaten aus den verschiedenen Mitgliedsländern zum Abruf bereitstellen (*Schengener Informationssystem*).

Aufgenommen werden sollen alle Personen, die zur Festnahme und gegebenenfalls Auslieferung, zur Aufenthaltsbestimmung, aber auch zur polizeilichen Beobachtung und zur vorübergehenden Ingewahrsamnahme für Zwecke der Gefahrenabwehr ausgeschrieben sind.

Es liegt auf der Hand, daß der dafür erforderliche grenzüberschreitende Datenverkehr erhebliche Gefahren für das informationelle Selbstbestimmungsrecht mit sich bringt. Insbesondere muß neben einer normenklaren Festlegung der einzelnen zu übermittelnden Daten hinreichend gesichert sein, daß der Bürger seine Rechte in allen Mitgliedsstaaten gleichermaßen wahrnehmen kann. Diese Rechte müssen auch nach der Übermittlung der Daten ins Ausland sichergestellt sein, einschließlich des Rechts, eine unabhängige Kontrollinstanz anzurufen.

Die Datenschutzbeauftragten Frankreichs, Luxemburgs und der Bundesrepublik haben im März dieses Jahres eine gemeinsame Erklärung abgegeben, in der sie einerseits die Kontrolle durch unabhängige Organe in allen Vertragsstaaten forderten, andererseits ein gemeinsames Organ vorschlugen, das sich aus Vertretern der nationalen Kontrollorgane zusammensetzt.

Die Sicherheitsarbeitskreise sowohl der Internationalen Konferenz der Datenschutzbeauftragten als auch der deutschen Datenschutzbeauftragten des Bundes und der Länder befassen sich intensiv mit den einzelnen Fragestellungen. Sie gehen vor allem davon aus, daß das Schengener Informationssystem als Modellfall betrachtet werden muß, an dem sich zeigt, welche Bedeutung dem Datenschutz künftig in Europa zukommen wird.

Inhaltlich ist zu fordern, daß der Datenschutz nicht hinter den Grundsätzen der Europaratskonvention Nr. 108 und der deutschen Datenschutzgesetzgebung zurückbleibt. Größte Bedeutung kommt den Prüf- und Löschfristen insbesondere dann zu, wenn die Daten ohne Beteiligung der Justiz in das System eingestellt werden. Mit der Berücksichtigung verdeckter Fahndungsmöglichkeiten (polizeiliche Beobachtung) dürfen nicht ohne parlamentarische Erörterung Festlegungen getroffen werden, die die anstehende Reform des Strafverfahrensrechtes vorwegnehmen und den Entscheidungsspielraum zuungunsten des Datenschutzes einengen.

Bereits im Jahr 1988 hatte ich aufgrund meiner Überprüfung die Vergabe sog. personenbezogener Hinweise im *Informationssystem Verbrechensbekämpfung (ISVB)* für dringend verbesserungsbedürftig erklärt⁶⁾. Neben inhaltlichen Bedenken hielt ich es auch für problematisch, daß in Einzelfällen personengebundene Hinweise nicht in das ISVB, sondern unmittelbar in INPOL-Dateien eingegeben wurden. Dies führte dazu, daß diese Daten zwar allen auswärtigen INPOL-Berechtigten, nicht jedoch allen ISVB-Berechtigten zur Verfügung standen, obwohl diese Daten fast ausschließlich regionale Bedeutung für Berlin hatten.

Bei der von mir seinerzeit herangezogenen Stichprobe stellte ich fest, daß nur in einem geringen Teil der Kriminalakten die Eingabe des Hinweises in die automatisierten Systeme vermerkt war oder aber die Gründe der Eingabe nicht erkennbar bzw. unzureichend waren. Desweiteren waren berechtigt eingegebene Hinweise, die aber wegen Zeitablaufs oder aufgrund des Verfahrensausgangs überholt waren, nicht gelöscht.

Inzwischen hat der Polizeipräsident das Verfahren der Eingabe, Löschung und Dokumentierung dieser Merkmale entsprechend meinen Empfehlungen neu geregelt und damit auch einen entsprechenden Beschluß des Abgeordnetenhauses umgesetzt. Mit diesem Beschluß wurde der Senat aufgefordert, die Speicherung der Merkmale „geisteskrank“, „geistesschwach“, „Prostitution“, „häufig wechselnder Aufenthaltsort“, „Ansteckungsgefahr“ bzw. „Vorsicht Blutkontakt“, „Land- und Stadtreicher“ sowie „Entmündigung“ zu unterlassen und die bestehenden Datensätze zu löschen.

Dieser Forderung wurde entsprochen, indem jetzt lediglich die Merkmale „bewaffnet“, „gewalttätig“, „Ausbrecher“, „Btm-Konsument“ und „Freitodgefahr“ gespeichert werden. Im übrigen wird eine Direkteingabe in das INPOL-System ohne gleichzeitige regionale Notierung im ISVB ausgeschlossen sein.

Meiner Empfehlung, den Eingabegrund durch ein besonderes Formular zu dokumentieren, ist der Polizeipräsident bislang nicht gefolgt, jedoch wird in einem Vermerk, der Eingang in die Kriminalakte findet, der Grund und die Herkunft der Erkenntnisse festgehalten. Durch den Ausdruck einer Eingabe- und einer Lösungsquittung, die ebenfalls der Kriminalakte beigelegt wird, erfolgt nach Ablauf der Laufzeit eines personenbezogenen Hinweises automatisch die fristgerechte Löschung der Eingabe.

Nicht entsprochen wurde meiner Empfehlung nach einer Revision sämtlicher vergebenen personenbezogener Hinweise. Zwar hält der Polizeipräsident ebenfalls eine Revision für erforderlich, betont jedoch, daß dies nicht kurzfristig realisiert werden könne. Auf die Durchführung der Revision werde ich weiterhin drängen.

Im Haushaltsjahr 1989 plante der Polizeipräsident die *Beschaffung von 30 Handfunkterminals*. Ich wurde vom Unterausschuß Datenschutz um Stellungnahme zur Datensicherheit gebeten.

Es handelt sich um Geräte mit einer LCD-Anzeige von insgesamt 24 und einem Speicher von 256 Zeichen. Die Übertragung soll im 2 m-Bandbereich erfolgen. Dafür werden im Berliner Stadtbereich eine Sende- und fünf Verteilstationen in Polizeigebäuden eingerichtet. Die Standorte sind z. Z. noch nicht endgültig festgelegt, da die Messungen für die Bestimmung der optimalen Funkstandorte durch die Fernmeldeabteilung der Polizei noch nicht abgeschlossen sind. Mit der Einrichtung der 2 m-Bandsendestationen sollen auch die in 13 Funkwagen fest eingebauten Abfragegeräte auf diese Technik umgerüstet werden.

Die Funkübertragung im 2 m-Band erfolgt im Stadtgebiet unverschlüsselt. Dies gilt auch für die Übertragung im Polizeinetz zum Netzknotenrechner. Erst die Übertragung von dort zum Bundeskriminalamt in Wiesbaden über die angemieteten Postleitungen erfolgt verschlüsselt.

Mit den Handgeräten sind nur Abfragen für Sach- und Personenfahndungen aus dem INPOL-Datenbestand vorgesehen. Dieser Datenbestand entspricht dem des ISVB auf den landeseigenen Rechnern. Eine technisch zwar schon heute mögliche Abfrage aus dem Berliner Bestand ist von der Polizei z. Z. nicht geplant und darüber hinaus nur mit einem besonderen Softwarepaket möglich.

⁶⁾ vgl. Jahresbericht 1988, Ziff. 4.5

Der berechtigte Benutzerkreis soll alle Polizeivollzugsbeamten (es ist derselbe Personenkreis, der auch ISVB-berechtigt ist) umfassen. Die Handfunkgeräte werden in den einzelnen Dienststellen verschlossen aufbewahrt und gegen Unterschrift an die betreffenden Kräfte ausgegeben. Dies entspricht der Sicherheitsstufe bei der Waffenaufbewahrung.

Der Zugriff auf den Datenbestand im BKA wird nur durch die Eingabe des achtstelligen Paßwortes eingeschränkt; dieses Paßwort ist nicht persönlich zugeteilt, sondern gilt jeweils pro Gerät.

Im Bedarfsfall (Entwendung, mißbräuchlicher Gebrauch usw.) kann das jeweilige Terminal über die interne Geräteerkennung vom BKA gesperrt werden. Diese interne Geräteerkennung ist vom Benutzer nicht ohne Manipulation am Gerät zu verändern. Eine Protokollierung der Abfragen im BKA erfolgt nicht.

Treffer bei Abfragen können nicht zwischengespeichert bzw. ausgedruckt werden. Dies ist nur von den ISVB-Terminals in den Polizeidienststellen möglich.

Kritisch aus datenschutzrechtlicher Sicht ist vor allem, daß die Paßwortzugriffsberechtigung pro Terminal gilt (d. h., daß in kurzer Zeit das Paßwort einem großen Kreis von Beamten bekannt sein dürfte) und zusätzlich keine Zugriffsprotokollierung stattfinden sollte. Somit wäre der Zugriff auf Fahndungsdaten nicht ausreichend kontrollierbar und würde zum Mißbrauch geradezu einladen. Auf meine Einwände hin wird jetzt der gesamte Datenfunkverkehr durch einen eigenen Rechner mitprotokolliert. Die Auswertung der Protokolle wird nur bei Verdacht eines Mißbrauchs vorgenommen.

Nicht ganz auszuschließen, aber durch die Protokollierung zu erkennen, ist der Mißbrauch mit Terminals der gleichen Bauart durch Unbefugte, da mit dem Hersteller der Datenfunkterminals lediglich eine Anzeigepflicht des Herstellers beim BKA vereinbart ist, wenn dieser solche Terminals außerpolizeilich vertreibt.

Ein weiteres Datenschutzrisiko liegt in der unverschlüsselten Funkübertragung im Berliner Stadtgebiet. Diese Datenübertragung ist nicht abhörsicher. Auch der Bundesdatenschutzbeauftragte hat festgestellt, daß auf den Funkstrecken - und dazu gehört ein Umkreis von etwa 30 km um das Datenfunkterminal - mitgehört und mit etwas Aufwand auch decodiert werden kann.

Dieser Schwachstelle kommt gerade im grenznahen Bereich besondere Bedeutung zu. Für die Zukunft ist deshalb beabsichtigt, daß in diesem Funknetz nur noch verschlüsselt gefunkt wird; hier soll auf den Hersteller eingewirkt werden, entsprechende Techniken zu entwickeln und anzubieten.

Das Argument der Polizei, daß der jetzt durchgeführte analoge Sprechfunkverkehr leichter abhörbar sei, ist zwar richtig, kann aber nicht als Argument zählen, bei dem Einsatz von neuen Techniken auf mögliche Verbesserungen des Datenschutzes zu verzichten.

Meldewesen

Ein Adreßbuch-Verlag möchte in Berlin, ähnlich wie in anderen großen Städten der Bundesrepublik, ein Adreßbuch herausgeben. Der Einwohnerteil soll nach den Vorstellungen des Verlegers wie folgt aufgeteilt sein: In einem namensalphabetisch geordneten Teil werden die über 18 Jahre alten Einwohner mit Familiennamen, Vornamen und postalischer Anschrift aufgeführt.

In dem folgenden *Straßenteil* sollen die Straßen Berlins in alphabetischer Reihenfolge aufgeführt werden, bei jeder Straße die Hausnummer angegeben und neben den Hausnummern in alphabetischer Reihenfolge die Namen und Vornamen der Einwohner genannt werden.

Die entsprechenden Daten sollen aus dem Melderegister bezogen werden. Nach § 29 Abs. 3 Meldegesetz darf Adreßbuch-Verlagen aus dem Melderegister Auskunft über Familiennamen, Vornamen, akademische Grade und die Anschriften der Einwohner, die das 18. Lebensjahr vollendet haben, erteilt werden. Jedoch hat der Betroffene das Recht, der Weitergabe seiner Daten zu widersprechen. Über dieses Recht ist der Einwohner bei der Anmeldung oder in sonstiger geeigneter Weise durch öffentliche Bekanntmachung zu unterrichten. Da es der Bürger damit

selbst in der Hand hat, ob sein Name im Stadtadreßbuch erscheinen soll oder nicht, habe ich gegen die Herausgabe eines alphabetischen Einwohnerverzeichnisses nichts einzuwenden.

Erhebliche Bedenken bestehen jedoch gegen die Veröffentlichung des Straßenteils: Hier kann nicht ein bestimmter Bürger gesucht werden, sondern eine vorher nicht bekannte Person durch das Bewohnen eines bestimmten Hauses herausgefunden werden. Im Gegensatz zum Namensverzeichnis, bei dem der Betroffene den Kreis der an ihm interessierten Personen übersehen kann, wird bei einer Veröffentlichung im Straßenverzeichnis der Betroffene Dritten bekannt, mit denen er nichts zu tun hat und mit deren Kontaktaufnahme er auch nicht rechnen muß. Das ist mit dem Grundsatz des informationellen Selbstbestimmungsrechts, wonach der Betroffene abschätzen können muß, welche ihn betreffenden Informationen in seiner sozialen Umwelt bekannt sind, nicht vereinbar.

Für diese Bewertung spricht auch, daß bei den Auskunftersuchen gegenüber den Meldestellen die erfragte Person namentlich zu bezeichnen ist. Dagegen kann nicht erfragt werden, welche Person in einem bestimmten Haus wohnt. Die entsprechenden Auskünfte, die von den Meldestellen nicht zu erhalten sind, sollten nach meiner Auffassung nicht auf dem Umweg über einen Straßenteil gegeben werden.

Im Zusammenhang mit den Wahlen zum Berliner Abgeordnetenhaus und den Bezirksverordnetenversammlungen am 29. Januar 1989 haben sich viele Bürger über die *Wahlwerbung* einzelner Parteien beschwert. Insbesondere wollten sie wissen, woher den Parteien ihre Anschriften bekannt geworden sind.

Nach § 29 Meldegesetz darf die Meldebehörde Parteien, Wählergemeinschaften und Einzelbewerbern im Zusammenhang mit Wahlen zum Abgeordnetenhaus von Berlin und zu den Bezirksverordnetenversammlungen in den sechs der Wahl vorangehenden Monaten sowie Trägern eines Volksbegehrens oder Bürgerbegehrens Auskunft aus dem Melderegister über Familiennamen, Vornamen, akademische Grade und gegenwärtige Anschriften von Wahlberechtigten erteilen. Entsprechende Auszüge aus dem Melderegister können nach Altersgruppen geordnet werden. Die Geburtstage der Wahlberechtigten dürfen dabei nicht mitgeteilt werden. Diese gesetzliche Regelung steht im Zusammenhang mit Artikel 21 Grundgesetz, wonach die Parteien an der politischen Willensbildung mitwirken.

Entgegen früheren Regelungen im Landeswahlgesetz haben die Wahlberechtigten jetzt das Recht, der Weitergabe ihrer Daten zu widersprechen; hierauf sind sie bei der Anmeldung und durch öffentliche Bekanntmachung hinzuweisen, wobei Fristen für die Ausübung des Widerspruchsrechts festgesetzt werden können. Diese öffentlichen Bekanntmachungen erfolgten im Landespresseamt und in den Berliner Tageszeitungen. Die Auskünfte und Auszüge aus dem Melderegister dürfen von den Parteien, Wählergemeinschaften und Einzelbewerbern nur für Zwecke der Wahlwerbung verwendet werden; sie sind innerhalb einer Woche nach dem Wahltag zu vernichten. Die Parteien, Wählergemeinschaften und Einzelbewerber müssen eine entsprechende schriftliche Verpflichtungserklärung abgeben. Die Meldebehörde kann die Auskunft und die Herausgabe der Auszüge mit Zusätzlichen Auflagen verbinden, um sicherzustellen, daß die Empfänger ihren Verpflichtungen nachkommen.

Im Gegensatz zu früheren Wahlen kam es kaum zu Beschwerden. In einem Fall hat eine Bürgerin trotz ihres rechtzeitig eingelegten Widerspruchs Wahlwerbung einer Partei erhalten. Bei meiner Überprüfung habe ich festgestellt, daß ein Mitarbeiter der Meldestelle die Sperre mit einer falschen Schlüsselzahl eingegeben hat. Somit wurde der Datensatz nicht für die Auskünfte an die Parteien zum Zwecke der Wahlwerbung, sondern für ebenfalls zulässige Datenübermittlungen an die öffentlich-rechtlichen Religionsgesellschaften nach § 27 Abs. 2 Meldegesetz gesperrt. Um Wiederholungen entgegenzuwirken, wird die zentrale ADV-Anwendungsrevision des Landeseinwohneramtes in Zukunft solche Eingaben von Sperren zusätzlich überprüfen.

Daß auch das aufwendige *Rückmeldefahren* der Meldeämter Lücken hat, zeigt folgender Fall: Eine Petentin hatte sich in ihrer bisherigen Nebenwohnung in Berlin mit Hauptwohnung angemeldet. Bis zur Anmeldung ihrer Hauptwohnung in Berlin hat sie

ihre Lohnsteuerkarten jährlich von der bundesdeutschen Heimatgemeinde erhalten. Dort ist sie auch 1973 aus der Kirche ausgetreten. In den Lohnsteuerkarten war seitdem auch keine Zugehörigkeit zu einer Konfession eingetragen. Ihre erstmalig in Berlin ausgestellte Lohnsteuerkarte enthielt nun wieder den Eintrag einer Konfession, obgleich sie bei der Ummeldung der Wohnsitze keine entsprechenden Angaben gemacht hatte.

Ich habe festgestellt, daß die Petentin bei der Anmeldung ihrer Nebenwohnung 1972 ihre Konfessionszugehörigkeit angegeben hat. Bei Erklärungen über die Haupt- und Nebenwohnsitzänderungen ist die Angabe der Konfession nicht vorgesehen, so daß der Berliner Meldebehörde nicht bekannt war, daß zwischenzeitlich ein Austritt aus der Kirche erfolgt ist.

Der Lohnsteuerkartenstelle der Heimatgemeinde hatte die Petentin den Kirchenaustritt mitgeteilt. Deshalb hat sie regelmäßig von dort eine Lohnsteuerkarte ohne das Merkmal der Konfessionszugehörigkeit erhalten. Bei der erstmaligen Anmeldung 1972 in Berlin gehörte die Petentin noch der Kirche an. Der Austritt erfolgte erst ein knappes Jahr später.

Sofern sich ein Einwohner eines Landes bei einer Meldebehörde eines anderen Landes angemeldet hat, übermittelt diese Meldebehörde der bisher zuständigen und allen für weitere Wohnungen des Einwohners zuständigen Meldebehörden nach § 2 der Ersten Meldedatenübermittlungsverordnung des Bundes u. a. die Zugehörigkeit zu einer öffentlich-rechtlichen Religionsgesellschaft. Diese sogenannte Rückmeldung wird von der bisher zuständigen Meldebehörde übermittelten Daten von den bei ihr über den Einwohner gespeicherten Daten ab, so unterrichtet sie hierüber die Meldebehörde der neuen Wohnung sowie alle für weitere Wohnungen des Einwohners zuständigen Meldebehörden. Eine Unterrichtung unterbleibt, wenn die bisher zuständigen Meldebehörden weniger Daten über den Einwohner gespeichert hat.

Der Berliner Meldebehörde war durch die Erklärung bei der Erstanmeldung 1972 die Konfessionszugehörigkeit bekannt und somit auch im automatisiert geführten Bestand gespeichert. Bei der Rückmeldung an die bundesdeutsche Meldebehörde wurde dieses Merkmal ebenfalls übermittelt. Dieser hatte die Petentin den Kirchenaustritt mitgeteilt, so daß diese Meldebehörde mithin weniger Daten gespeichert hatte als das Landeseinwohneramt Berlin. Aus diesem Grunde wurde die Berliner Meldebehörde nicht über die Abweichung unterrichtet.

Problematisch ist auch, welche Stelle für die Korrektur der Religionszugehörigkeit zuständig ist.

Ich teile die Auffassung der Senatsverwaltung für Inneres nicht, daß dies das Bezirksamt ist. Nach § 1 Abs. 2 Meldegesetz ist das Landeseinwohneramt Meldebehörde. Die Meldebehörde hat u. a. die Daten der Einwohner zu registrieren, um die für die rechtmäßige Erfüllung der Aufgaben öffentlicher Stellen erforderlichen Grunddaten feststellen und nachweisen zu können. Zu den Grunddaten zählt auch die rechtliche Zugehörigkeit zu einer Religionsgesellschaft, die durch die Finanzbehörden Berlins Steuern erhebt. Das bedeutet, daß nur das Landeseinwohneramt dieses Merkmal speichern, verändern oder löschen darf.

Das für die Wohnung des Einwohners zuständige Bezirksamt nimmt nur als Ausnahme von der Regel für bestimmte Daten die Aufgabe der Meldebehörde wahr. Dazu zählt u. a. nach § 2 Abs. 2 Nr. 2 die Speicherung der Tatsache, daß eine Lohnsteuerkarte erforderlich ist, ggf. weitere steuerrechtliche Daten (Steuerklasse, Freibeträge, Religionszugehörigkeit im Sinne des Absatzes 1 Nr. 10 des Ehegatten, Rechtsstellung und Zuordnung der Kinder, Vor- und Familiennamen sowie Anschrift der Pflege- und Stiefeltern) zum Zwecke der Ausstellung von Lohnsteuerkarten.

Zwar mag der Hinweis der Senatsverwaltung für Inneres auf die Häufigkeit von vergleichbaren Klärungsfällen im Ergebnis zutreffend sein, es ändert aber nichts daran, daß nach der eindeutigen gesetzlichen Aufgabenzuweisung ausschließlich das Landeseinwohneramt das Merkmal der rechtlichen Zugehörigkeit zu einer Religionsgesellschaft (des Betroffenen selbst) registrieren und damit auch ändern bzw. löschen darf. Das Bezirksamt darf nach

§ 2 Abs. 2 Nr. 2 Meldegesetz lediglich im Datensatz des Betroffenen die Religionszugehörigkeit des Ehegatten - aber nur diese - speichern, ändern oder löschen.

Ein nach mehrjährigem Aufenthalt in Bayern nach Berlin zurückgekehrtes Ehepaar hatte wegen Entführungsdrohungen gegen die Tochter sowohl beim Landeseinwohneramt Berlin als auch bei der Meldebehörde des bisherigen Wohnortes eine *Auskunftssperre* nach § 28 Abs. 5 Berliner Meldegesetz bzw. Artikel 34 Abs. 5 Bayerisches Meldegesetz beantragt. In beiden Fällen wurde dem Antrag entsprochen.

Trotz dieser Auskunftssperre wurde dem Ehepaar später von der Behörde des alten Wohnortes mitgeteilt, daß die Anschrift an Rechtsanwälte weitergegeben wird. Das Landeseinwohneramt stimmte zwar der Auskunftssperre zu, nahm aber einige Institutionen (z. B. Banken, Kreditinstitute, Krankenkassen, Versicherungsträger, die BEWAG, GASAG, BVG, Kauf- und Versandhäuser sowie Wohnungsbaugesellschaften) aus. Es geht dabei davon aus, daß bei Auskünften an diese Institutionen eine Gefährdung für den Betroffenen nicht eintritt und somit die Auskünfte erteilt werden können. Das Landeseinwohneramt hat dabei auf seine bisher geübte Verwaltungspraxis verwiesen, die von der Aufsichtsbehörde bestätigt wurde und einer gerichtlichen Überprüfung standgehalten hat.

Gleichwohl habe ich einen Mangel festgestellt, weil nach § 28 Abs. 5 Meldegesetz jede Melderegisterauskunft unzulässig ist, wenn der Betroffene der Meldebehörde das Vorliegen von Tatsachen glaubhaft gemacht hat, die die Annahme rechtfertigen, daß ihm oder einer anderen Person hieraus eine Gefahr für Leben, Gesundheit, persönliche Freiheit oder ähnliche schutzwürdige Belange erwachsen kann.

Die Auskunftssperre nach § 28 Abs. 5 Meldegesetz bezieht sich auf *alle* Arten von Melderegisterauskünften an private Dritte. Durch die Verwendung des Wortes „jede“ ist klargestellt, daß bei Vorliegen der tatbestandsmäßigen Voraussetzungen auch nur für eine oder mehrere der jeweiligen Auskunftsart unterliegenden Daten eine Auskunft unzulässig ist. Soweit dem Antrag auf Auskunftssperre stattgegeben worden ist, sind keine Auskünfte aus dem Melderegister nach § 28 Abs. 5 Meldegesetz mehr zulässig.

Auch der Bayerische Datenschutzbeauftragte hat gegenüber der seiner Prüfungskompetenz unterliegenden bayerischen Meldebehörde einen datenschutzrechtlichen Mangel hinsichtlich der Auskünfte an die Rechtsanwälte festgestellt.

Ein anderer Petent hatte im Jahre 1974 ein Kind adoptiert. Nach dem Tod des leiblichen Vaters hat die Ehefrau des Petenten im Zuge der Regelung des Nachlasses vom zuständigen Amtsgericht einen fehlerhaft adressierten Brief (Vorname der leiblichen Mutter, Nachname der Adoptivmutter) erhalten. Das Gericht hat dem Petenten mitgeteilt, daß die Daten aus dem Melderegister stammen und es beim Anschreiben zu einer Verwechslung gekommen ist. Der Petent befürchtet nun, daß das *Adoptionsgeheimnis* insbesondere gegenüber der leiblichen Mutter nicht gewahrt werden kann, weil im Datensatz des adoptierten Kindes auch frühere Wohnungen gespeichert sind, die es zum Teil gemeinsam mit der leiblichen Mutter bewohnt hat.

Durch verwaltungsinterne Anweisungen muß die Person, über die Auskunft erteilt werden soll, hinreichend bestimmt sein. Diese Voraussetzung ist regelmäßig bei der Auslieferung von drei Merkmalen erfüllt. Im konkreten Fall könnte die leibliche Mutter mit den ihr zweifelsfrei bekannten Informationen Vorname, Geburtsdatum und alte Wohnanschrift mit einer einfachen Melderegisterauskunft den Verbleib ihres adoptierten Kindes und damit die Umstände der Adoption ermitteln.

Das Landeseinwohneramt vertritt die Auffassung, daß die Speicherung des früheren Namens und früherer Anschriften Adoptierter nach dem Meldegesetz zulässig ist und eine Löschung der beispielsweise vor der Adoption liegenden Anschriften nicht zu erfolgen hat. Weiterhin meint es, daß nach § 1758 BGB lediglich die Offenbarung und nicht schon die Speicherung von Tatsachen unzulässig ist, die geeignet sind, die Adoption und ihre Umstände aufzudecken.

Dieser Argumentation ist folgendes entgegenzuhalten:

Die Meldebehörden sind gerade zu dem Zwecke eingerichtet worden, Auskünfte über die in ihrem Bereich gemeldeten Personen zu geben. Daher ist bereits bei der Speicherung zu berücksichtigen, ob eine Offenbarung zulässig wäre. Die Speicherung wäre nur zulässig, wenn entweder eine Einwilligung des Betroffenen und (kumulativ) des Annehmenden vorliegt oder die Speicherung im überwiegenden Interesse der Allgemeinheit liegt. Im vorliegenden Fall fehlt es an beidem. Darüber hinaus ist es zweifelhaft, ob diese Ausnahmeregelung des § 1758 BGB auf den Fall der Speicherung im Melderegister überhaupt anwendbar ist. Im Gegensatz zur Einzelfallabwägung, von der § 1758 BGB ausgeht, kommt es beim Melderegister zu pauschalen Auskunftsteilungen, wenn nur die Voraussetzungen des § 28 Meldegesetz vorliegen.

Daß es sich bei der früheren Anschrift und dem früheren Namen vor der Adoption um Tatsachen im Sinne des § 1758 BGB handelt, sieht das Landeseinwohneramt ebenso. Aus diesem Grund wird bei der Adoption mit einem speziellen Programm der frühere Name des Kindes gelöscht und ein neuer Datensatz aufgebaut. Der frühere Name steht damit nicht mehr als Suchmerkmal zur Verfügung.

Die vor der Adoption liegenden Anschriften will das LEA jedoch nicht löschen, sondern alle Deskriptoren (Schlüsselmerkmale, mit denen gesucht werden kann) entfernen. Die vor der Adoption liegenden Anschriften bleiben auf diese Weise zwar gespeichert, können aber nicht mehr als Suchmerkmal genutzt werden. Allerdings ist programmtechnisch nicht zu verhindern, daß bei nachträglichen Änderungen der Anschriften (z. B. Straßenumbenennungen, Hausnummeränderungen oder sonstige Änderungen der Hausanschrift, nicht aber spätere Umzüge) der Deskriptor wieder hinzugefügt wird. Damit bleibt also ein Restrisiko bestehen, das nach Auffassung des LEA nicht beseitigt werden kann.

Die Senatsverwaltung für Inneres hat vor dem Hintergrund der aktuellen Situation im Asylbereich zugestimmt, daß die Abteilung Ausländerangelegenheiten des Landeseinwohneramtes *einen Online-Zugriff auf das Ausländerzentralregister* erhält. Ich hatte zuvor das Landeseinwohneramt und die Innenverwaltung darauf hingewiesen, daß ich eine solche Anbindung an das Zentralregister für unzulässig halte, da eine Rechtsgrundlage für diese Übermittlungsform fehlt. Die Senatsverwaltung hat sich über meine Einwände hinweggesetzt, da sie der Auffassung ist, daß die Belastungssituation der Ausländerbehörde es rechtfertigt, im Vorgriff auf eine erwartete gesetzliche Regelung im Ausländerzentralregistergesetz ohne bestehende Rechtsgrundlage vorzugehen. Ich habe den für das Ausländerzentralregister zuständigen Bundesbeauftragten für den Datenschutz gebeten, die Angelegenheit auch von dort zu überprüfen.

Amtliche Statistik

Der Entwurf eines *Landesstatistikgesetzes* wurde erwartungsgemäß in der abgelaufenen Legislaturperiode nicht mehr beraten. Er sollte zwar mit geringfügigen Änderungen im Herbst dieses Jahres in das neugewählte Abgeordnetenhaus wieder eingebracht werden, dies scheiterte jedoch an den Einwänden der Senatsverwaltung für Justiz. Ich halte die Beratungen dieses Gesetzesentwurfes für vordringlich, damit die amtliche Statistik in Berlin zum ersten Mal eine bereichsspezifische gesetzliche Grundlage erhält. Dabei werde ich auf weitere datenschutzrechtliche Verbesserungen im Entwurf dringen⁷⁾.

Sämtliche Erhebungsunterlagen der *Volkszählung 1987*, insbesondere die Haushaltsmantelbogen mit Namen und Anschriften sowie die Wohnungs- und Personenbogen sind bis zum 26. April 1989 vom Statistischen Landesamt vernichtet worden. Die auf dem speziell für diesen Zweck installierten Großrechner des Statistischen Landesamtes gespeicherten Einzeldatensätze sind entsprechend den Vorschriften des Volkszählungsgesetzes anonymisiert worden, indem die Ordnungsnummern nach einem bestimmten Verfahren verfremdet wurden. Dieses Verfahren hat eine Arbeitsgruppe der Konferenz der Datenschutzbeauftragten

unter meiner Mitwirkung überprüft. Es schließt mit hinreichender Sicherheit einen Rückgriff auf die ursprünglichen laufenden Nummern und Ordnungsnummern aus. Allerdings ist zu betonen, daß nach der Rechtsprechung des Bundesverfassungsgerichts die Einzeldatensätze aus der Volkszählung auch nach diesem gesetzlich vorgeschriebenen Anonymisierungsverfahren weiterhin personenbezogen bleiben und damit sowohl der statistischen Geheimhaltungspflicht als auch dem Datenschutzgesetz unterliegen.

Bei der Veröffentlichung und Weitergabe von Volkszählungsdaten ist die Beachtung des Statistikgeheimnisses nach § 16 Bundesstatistikgesetz von entscheidender Bedeutung. Dies gilt auch für die Veröffentlichung von Tabellen mit sogenannten „*Tabelleneinsen*“. Das Statistische Landesamt entwickelt hierfür gegenwärtig ein Prüfverfahren, das durch Auf- und Abrundung niedriger Zahlen eine Beachtung des Statistikgeheimnisses bei der Veröffentlichung von Tabellen mit statistischen Ergebnissen sicherstellen soll. Auf den damit verbundenen geringfügigen Informationsverlust werden die Dateninteressenten ausdrücklich hingewiesen. Ich halte dieses Verfahren für geeignet, die Einhaltung des Statistikgeheimnisses bei der Veröffentlichung von Tabellen oder der Weitergabe von Auswertungen sicherzustellen. Allerdings ist es eine Illusion zu glauben, man könne durch schematische Rechenoperationen feststellen, ob das Risiko der Reidentifikation unzulässig hoch ist oder nicht. Auch bei Auswertungen, die sich auf große Gebiete mit hoher Einwohnerzahl beziehen, wird das Statistische Landesamt vor der Weitergabe an Dritte zu prüfen haben, ob im Einzelfall aufgrund der besonderen Struktur und des Aussagegehalts der Tabelle die Gefahr besteht, daß der Empfänger der Daten Bezüge zu einer bestimmten Person herstellen und über sie etwas erfahren kann, was er bisher nicht wußte.

Das Verwaltungsgericht Berlin hat in mehreren Urteilen die *Mikrozensus*-Erhebung für rechtmäßig erklärt⁸⁾. In einem dieser Verfahren wurde ich in der mündlichen Verhandlung als sachverständiger Zeuge gehört. Dabei habe ich den Prozeß der Datenverarbeitung im Statistischen Landesamt und dem Landesamt für Elektronische Datenverarbeitung erläutert und erklärt, daß ich bei der Durchführung des Mikrozensus in Berlin bisher keine erheblichen datenschutzrechtlichen Mängel festgestellt habe. Das Gericht hat sich in diesem Verfahren von Vertretern des Statistischen Landesamtes und des Statistischen Bundesamtes auch eingehend die Vorgehensweise bei der Bildung der Stichprobe und der Auswahlbezirke erläutern lassen, weil deren Rechtmäßigkeit bezweifelt worden war. Bezeichnenderweise erklärte eine Klägerin nach Abschluß der mündlichen Verhandlung, wenn man sie von vornherein so ausführlich informiert hätte, hätte sie möglicherweise von einer Klage abgesehen. Hier wird deutlich, daß die Informationen, die die amtliche Statistik jedem befragten Bürger zukommen läßt, nach wie vor verbesserungsbedürftig sind.

Der wissenschaftliche Beirat für Mikrozensus und Volkszählung hat die Ergebnisse der Begleitforschung zur Mikrozensus-Erhebung in seinem Bericht „*Mikrozensus im Wandel*“ zusammengefaßt. Dieser Bericht läßt keine Bereitschaft erkennen, vom Grundsatz der Auskunftspflicht bei der Mikrozensus-Erhebung abzugehen. Allerdings sollen in Zukunft unter Umständen in größerem Umfang Zusatzfragen auf freiwilliger Basis gestellt werden. Die Bundesregierung wird demnächst über den Entwurf für ein Mikrozensusgesetz 1990 beschließen, das das gegenwärtige Mikrozensusgesetz ablösen wird.

Bereits beschlossen hat die Bundesregierung den Entwurf eines Gesetzes über die Durchführung einer Repräsentativstatistik auf dem Gebiet des Wohnungswesens (*Gebäude- und Wohnungsstichprobengesetz*). Dieser Gesetzesentwurf ist in der Öffentlichkeit bereits heftig diskutiert worden, weil der Katalog der darin vorgesehenen Erhebungsmerkmale weit über die *Gebäudevorerhebung 1987* und den Mikrozensus hinausgeht. Ich habe empfohlen, daß der Gesetzgeber bei bestimmten, besonders sensiblen Fragen (z. B. nach der sozialen Stellung, der Höhe des monatlichen Nettoeinkommens nach Einkommensklassen und nach der Form des Zusammenlebens) Ausnahmen von der gene-

⁷⁾ vgl. Jahresbericht 1988, Ziff. 4.5

⁸⁾ vgl. z. B. Az 7 A 1.88

rellen Auskunftspflicht machen sollte. Zudem sind eine ganze Reihe von Erhebungsmerkmalen im Gesetzentwurf zu unbestimmt umschrieben. Im Gesetzgebungsverfahren sollte deshalb gleichzeitig über den eigentlichen Fragebogen beraten werden, wie dies auch beim Volkszählungsgesetz 1987 geschehen ist, damit der genaue Umfang der erstmals für den 15. Oktober 1990 vorgesehenen Datenerhebung vom Parlament festgelegt wird. Zudem erweckt der Titel des Gesetzes den irreführenden Eindruck, als gehe es gar nicht um die Erhebung personenbezogener, sondern nur gebäude- und wohnungsbezogener Daten. Insofern ist eine Klarstellung im Entwurf erforderlich. Einzelangaben über Hauseigentümer aus der Bautätigkeitsstatistik dürfen für die Auswahl der Stichprobe nicht herangezogen werden, bevor das Gebäude- und Wohnungsstichprobengesetz in Kraft getreten ist und die Bauherren auf die zukünftige Verwendung ihrer Angaben für die Zwecke der Stichprobenbildung hingewiesen worden sind.

Die Übermittlung von Tabellen mit Einserfeldern sollte abweichend von der jetzigen Fassung des Entwurfs nur in den Fällen zugelassen werden, in denen kein Personenbezug mehr hergestellt werden kann.

Sollten die geplanten Sonder- und Zusatzaufbereitungen durch das Statistische Bundesamt dazu führen, daß die Einzelangaben sowohl in den Statistischen Landesämtern als auch im Bundesamt vorgehalten werden, wäre dies eine unverhältnismäßige Doppelspeicherung personenbezogener Daten.

Auf das Erhebungsverfahren und den Umgang mit den Einzelangaben bei der Gebäude- und Wohnungstichprobe werden die bereichsspezifischen Datenschutzvorschriften des Bundesstatistikgesetzes anzuwenden sein. Darüber sollte der befragte Bürger ausführlich aufgeklärt werden.

Anläßlich der Wahlen zum Berliner Abgeordnetenhaus und zu den Bezirksverordnetenversammlungen am 29. Januar 1989 haben sich mehrere Bürger mit Beschwerden und Anfragen zur repräsentativen *Wahlstatistik* nach § 27 Landeswahlgesetz an mich gewandt. Der Landesgesetzgeber hat die Anordnung dieser Statistik mit der ausdrücklichen Regelung verbunden, daß die Stimmabgabe einzelner Personen nicht erkennbar werden darf. Anders als in den Statistikgesetzen fehlen jedoch konkrete Verfahrensvorschriften, wie die Einhaltung dieser gesetzlichen Regelung sichergestellt werden kann. Mir liegen keinerlei Hinweise darauf vor, daß bei der Wahl am 29. Januar 1989 der Grundsatz der geheimen Wahl durch die Durchführung der repräsentativen Wahlstatistik beeinträchtigt sein könnte. Die einbezogenen Stimmbezirke sind ihrer Größe nach so ausgewählt worden, daß die Stimmabgabe des einzelnen Wählers nicht erkennbar war. Von der Einbeziehung der Briefwahlbezirke wurde von vornherein zum Schutz des Wahlheimnisses abgesehen. Gleichwohl habe ich empfohlen, Verfahrensvorschriften zur Durchführung der repräsentativen Wahlstatistik, insbesondere zur getrennten Auswertung der Wahlverzeichnisse und der Stimmzettel in die Wahlordnung aufzunehmen. Für die nächste Wahl wurde Prüfung zugesagt.

Die Bundesregierung hat in diesem Jahr einen neuen Entwurf zur Novellierung des *Hochschulstatistikgesetzes* beschlossen, der entgegen früheren Entwürfen nicht mehr die umstrittene Studienverlaufsstatistik vorsieht. Stattdessen soll die frühere Prüfungskandidatenstatistik in die Studentenstatistik integriert werden. Ich würde es begrüßen, wenn durch eine zügige Verabschiedung dieses Gesetzentwurfs die jahrelange Rechtsunsicherheit im Bereich der Hochschulstatistik endlich beseitigt werden könnte und den Anforderungen des Bundesverfassungsgerichts dabei Rechnung getragen würde. Dies hat auch Rückwirkungen auf die Novellierung des Berliner Hochschulgesetzes⁹⁾.

Seit dem Oktober dieses Jahres wird zum ersten Mal seit sechs Jahren wieder die Erhebung des wissenschaftlichen und künstlerischen Personals noch auf der Grundlage des alten Hochschulstatistikgesetzes durchgeführt. Dazu übermitteln die Hochschulen dem Statistischen Landesamt Namen und Anschriften des bei ihnen beschäftigten Personals. Im Gegensatz zu früheren Befragungen erhält das wissenschaftliche und künstlerische Hochschulpersonal erstmals die Möglichkeit, die vorgeschriebenen

Angaben direkt gegenüber dem Statistischen Landesamt auf dem Postwege und nicht über ihre Hochschule zu machen. Soweit die Fragebogen dennoch über die Hochschule auf dem Fachpostwege zurückgesandt werden, ist ihre Verwendung für Verwaltungszwecke der Hochschulen unzulässig. Entsprechende Zusagen haben die Berliner Hochschulen bereits nach dem Urteil des Bundesverfassungsgerichts zum Volkszählungsgesetz 1983 gemacht.

Die Kommission der Europäischen Gemeinschaften hat den Entwurf einer Verordnung zur Übermittlung von statistischen Angaben an das *Statistische Amt der Europäischen Gemeinschaften* vorgelegt. Dieser Entwurf entspricht nicht den Vorgaben des Bundesstatistikgesetzes zur Geheimhaltung von statistischen Einzelangaben. Von der Übermittlungspflicht werden lediglich Angaben ausgeschlossen, die den privaten Lebensbereich natürlicher Personen betreffen. Der Entwurf enthält keine ausreichenden Regelungen über Maßnahmen zur Datensicherung und Abschottung im Statistischen Amt der Europäischen Gemeinschaften. Auch fehlt bisher ein strafbewehrtes Statistikgeheimnis auf der Ebene des Gemeinschaftsrechts. Die Teilnehmer der 11. Internationalen Konferenz der Datenschutzbeauftragten haben dieses Problem diskutiert und sind übereingekommen, auf nationaler Ebene auf eine Verbesserung der Datenschutzbestimmungen im Verordnungsentwurf zu dringen.

Personalwesen

Auf der Grundlage des Berichts der „Interministeriellen Arbeitsgruppe zur strukturellen Fortentwicklung des Personalaktenrechts im öffentlichen Dienst“ in der Fassung von Juli 1988¹⁰⁾ ist ein Referentenentwurf eines *Gesetzes zur Neuordnung des Personalaktenrechts* erarbeitet worden, mit dem sowohl das Bundesbeamtenengesetz als auch das Beamtenrechtsrahmengesetz geändert werden sollen.

Mit dem Vorhaben, mit *beamtenrechtlichen* Regelungen zum Personalaktenrecht voranzugehen, könnten sich meine Befürchtungen bestätigen, daß für Angestellte und Arbeiter im öffentlichen Dienst die datenschutzfreundlicheren Entscheidungen des Bundesarbeitsgerichts zum Arbeitnehmerdatenrecht weitestgehend unberücksichtigt bleiben. Ich halte demgegenüber eine einheitliche Regelung in einem sowohl für die private Wirtschaft als auch den öffentlichen Dienst geltenden Gesetz zum Arbeitnehmerdatenschutz für angezeigt.

Gleichwohl ist die Absicht der Bundesregierung zu begrüßen, noch in dieser Legislaturperiode des Deutschen Bundestages Schritte zu unternehmen, das Personalaktenrecht auf eine materiell-rechtliche Grundlagen zu stellen.

Aus der Befugnis des einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen, folgt, daß die Erhebung, Speicherung und sonstige Verarbeitung personenbezogener Daten nur dann zulässig ist, wenn sie aufgrund einer verfassungsgemäß zustande gekommenen gesetzlichen Befugnisnorm erfolgt, aus der sich die Voraussetzungen und der Umfang von Grundrechtsbeschränkungen klar und für den Betroffenen erkennbar und normenklar ergeben. Diesem Aspekt haben sich auch beabsichtigte Einschränkungen nach den „hergebrachten Grundsätzen des *Berufsbeamtenrechts*“ unterzuordnen. Darüber hinaus dürfen nach dem Grundrechte der Verhältnismäßigkeit Grundrechte des Bürgers im Rahmen seines allgemeinen Freiheitsanspruchs von der öffentlichen Gewalt nur so weit beschränkt werden, als dies zum Schutz öffentlicher Interessen unerlässlich ist.

Zwar steht der Beamte in einem freiwillig übernommenen Dienst- und Treueverhältnis zu seinem Dienstherrn und ist insoweit über die allgemeinen Bürgerpflichten hinaus gegenüber dem Staat verpflichtet. Gleichzeitig ist er jedoch auch Bürger, der seine Grundrechte gegenüber den staatlichen Stellen, mithin auch gegenüber seinem Dienstherrn geltend machen kann. Dieser Konflikt kann unter Beachtung des informationellen Selbstbestimmungsrechts nur in der Weise gelöst werden, daß

⁹⁾ vgl. unten 4.8

¹⁰⁾ Jahresbericht 1988, Ziff. 4.5

allein Grundrechtsbeschränkungen zulässig sind, die durch Sinn und Zweck des konkreten Dienst- und Treueverhältnisses des Beamten erforderlich werden.

Das heißt, daß sich eine gesetzliche Regelung des Personalaktenrechts ausschließlich daran zu orientieren hat, welche Informationen in einem konkreten Zusammenhang mit dem Beamtenverhältnis stehen, d. h., die Rechtsstellung, die dienstliche Eignung, Verwendung und Tätigkeit des Beamten betreffen sowie zur Begründung, Durchführung und Abwicklung des Dienstverhältnisses, also zur rechtmäßigen Aufgabenerfüllung des Dienstherrn erforderlich sind. Der vom Bundesverwaltungsgericht in ständiger Rechtsprechung betonte Grundsatz, die Personalakte habe ein möglichst vollständiges Bild von der Persönlichkeit des Beamten zu ergeben, darf im Lichte des informationellen Selbstbestimmungsrechts nicht mehr verabsolutiert werden. Scheidungsurteile, nicht zum Tragen kommende Darlehensanträge mit Schilderungen persönlicher Umstände u. ä. gehören nicht in die Personalakte, weil sie weder dem Schutz öffentlicher Interessen noch dem Sinn und Zweck den beamtenrechtlichen Dienst- und Treueverhältnisses dienen. Sie sind nicht einmal geeignet zur „Erhaltung der Funktionsfähigkeit des Personalaktenwesens“.

Es ist begrüßenswert, daß die ursprünglichen Forderungen der Interministeriellen Arbeitsgruppe zur „Vollständigkeit“ der Personalakte („die Personalakte soll vollständig und lückenlos Aufschluß über den beruflichen Werdegang und insoweit über die Person des Beamten geben“) in dem Gesetzentwurf keinen Eingang gefunden haben. Ebenso weist die Beschränkung der aufzunehmenden Vorgänge über persönliche Verhältnisse des Beamten auf solche, die „mit dessen Dienstverhältnis in einem unmittelbaren inneren Zusammenhang stehen“, in die richtige Richtung.

Mängel erweisen sich allerdings insbesondere bei der vorgesehenen Regelung der automatisierten Verarbeitung personenbezogener Daten von Beamten. Die Begründung des generellen Verzichts auf Vorschriften über die Erhebung, Verarbeitung und Nutzung sowie den technisch-organisatorischen Schutz automatisiert geführter Personaldaten unter Hinweis auf die einschlägigen Vorschriften der §§ 22 ff. BDSG überzeugt schon deshalb nicht, weil damit auf Vorschriften abgestellt wird, deren zukünftige Fassung derzeit noch niemand kennt, und die im Sinne einer bereichsspezifischen Regelung nicht hinreichend präzise und normenklar sind und deshalb den verfassungsrechtlichen Anforderungen an Befugnisnormen für Eingriffe in die informationelle Selbstbestimmung nicht entsprechen.

Im übrigen wird diese Regelung selbst der Erklärung der Bundesregierung nicht gerecht, „keine Personalinformationssysteme einzuführen, die sich als umfassendes Kontrollinstrument oder dazu eignen, Persönlichkeitsprofile zu erstellen“. Eine grundlegende Überarbeitung ist daher unumgänglich.

Der Arbeitskreis Personalwesen der Konferenz der Datenschutzbeauftragten hat Detailüberlegungen hierzu formuliert. Darin werden insbesondere folgende Positionen vertreten:

- Bei der Beschreibung des Personalakteninhalts sollte jeder Hinweis auf die „persönlichen Verhältnisse des Beamten“ unterbleiben.
- Die Sammlung einiger bestimmter, besonders sensibler Unterlagen sollte nicht als Bestandteil der Personalakte angesehen werden, obwohl sie „die persönlichen oder dienstlichen Verhältnisse des Beamten berühren“. Dies sollte insbesondere für Beihilfeakten gelten. Der Inhalt der Beihilfeakte ist nicht weniger sensitiv als der der vom Sozialgeheimnis geschützten Kindergeldakte.
- Vorgesetzte gehören nicht zu den „im Rahmen der Personalverwaltung mit der Bearbeitung von Personalangelegenheiten beauftragten Beschäftigten“. Daß sie Zugang zur Personalakte haben, ist keineswegs selbstverständlich. So ist ein Zugang durch Fachvorgesetzte regelmäßig zur rechtmäßigen Aufgabenerfüllung nicht erforderlich und daher unzulässig, es sei denn, daß diese auch Dienstvorgesetztereigenschaft haben, weil sie selbständig dienst- oder arbeitsrechtliche

Verhältnisse begründen, verändern und auflösen dürfen. Auch kann nicht jeder¹¹⁾ Bearbeitungszweck den Zugang zur Personalakte rechtfertigen.

- Der Vorschlag, dem Beamten ein Recht zur Äußerung vor der Aufnahme von Beschwerden und belastenden Behauptungen in die Personalakte zu geben, entspricht nicht nur den Grundsätzen der informationellen Selbstbestimmung, sondern auch dem Grundsatz der Personalaktenwahrheit. Hier ist der Gesetzentwurf jedoch unvollständig, da auch andere Unterlagen, wie z. B. Beurteilungen, für den Beamten ungünstig sind oder ihm nachteilig werden können. Darüber hinaus ist bei Zweifeln an der Richtigkeit belastender Unterlagen das Äußerungsrecht des Beamten nicht ausreichend.
- Zu begrüßen ist, daß der Gesetzentwurf die Führung von Nebenakten (Vorgänge aus der Grundakte oder den Teilakten) zuläßt, die praktisch unumgänglich, in der Vergangenheit jedoch immer wieder Gegenstand von Auseinandersetzungen gewesen ist. Gerade unter diesem Gesichtspunkt sollte über eine reine Deklaration hinaus unbedingt auch der Inhalt dieser Nebenakten von vornherein gesetzlich eingegrenzt werden.
- Die Absicht, das Recht auf Einsicht in die Personalakte gesetzlich zu konkretisieren wird begrüßt. Allerdings sind kleinliche Einschränkungen („soweit dienstliche Gründe nicht entgegenstehen“) dem Recht auf informationelle Selbstbestimmung unangemessen und sollten daher, zumindest im Gesetz, unterbleiben.

Zudem ist unverständlich, daß einem Bevollmächtigten des Beamten nach dessen Willen nicht gleiche Einsichtsrechte wie dem Beamten selbst eingeräumt werden sollen.

Behörden sollte generell nicht „die Personalakte“ (d. h. einschließlich sämtlicher Teilakten, wie Beihilfeakten u. a.) vorgelegt werden, sondern nur der zur (konkreten) rechtmäßigen Aufgabenerfüllung jeweils erforderliche Teil.

Auskünfte an Dritte dürfen nur mit Einwilligung des Beamten oder aufgrund einer besonderen gesetzlichen Befugnisnorm erteilt werden.

- Zwar sieht der Entwurf vor, daß Beschwerden, die sich als unbegründet, und Tatsachenbehauptungen, die sich als falsch erwiesen haben, mit Zustimmung des Beamten aus der Personalakte zu entfernen und zu vernichten sind. Jedoch müssen sämtliche Unterlagen einbezogen werden, die entweder gar nicht zur Personalakte hätten genommen werden dürfen oder aber sich nachträglich als zur rechtmäßigen Aufgabenerfüllung nicht erforderlich erweisen.
- Müssen Vorgänge, die auch andere Bedienstete betreffen, zur Personalakte genommen werden, so sind deren personenbezogene Daten unleserlich zu machen.
- Der ärztlichen Schweigepflicht unterliegende Vorgänge, die beim amtsärztlichen Dienst u. ä. geführt werden, müssen ausnahmslos der Einsichtnahme durch den Behördenleiter, dessen Vertreter sowie die mit der Bearbeitung von Personalangelegenheiten beauftragten Beschäftigten entzogen bleiben.

Ungeachtet der Gesetzgebung bleiben nach wie vor *Einzelprobleme* zu lösen.

Ein Fortschritt ist beim Austausch von Personalakten solcher Bediensteter erzielt worden, die als Überhangkräfte des Landes Berlin in der sogenannten *Personalüberhangliste*¹²⁾ geführt werden.

Die Senatsverwaltung für Inneres hat in einem Rundschreiben vom 9. März 1989 mitgeteilt, daß zwar grundsätzlich eine Akten-einsicht zulässig, aber nicht in jedem Fall erforderlich sei, und somit differenziert vorgegangen werden müsse.

So sollen zunächst die Personalwirtschaftsstellen eine erste Grobauswahl anhand der in der Personalüberhangliste enthaltenen Amts- und Berufsbezeichnungen, der Besoldungs-, Ver-

¹¹⁾ Jahresbericht 1986, Ziff. 4.3

¹²⁾ vgl. Jahresbericht 1988, Ziff. 4.5

gütungs- oder Lohngruppen (einschl. der Fallgruppen) sowie der derzeitigen Beschäftigungsdienststelle treffen. Dadurch könnte ein Großteil der Personalüberhangkräfte von vornherein vom Auswahlverfahren ausgenommen werden. Im übrigen sollten dann vorrangig Informationen durch persönliche Kontaktaufnahme mit den entsprechenden Dienststellen selbst eingeholt werden. Erst wenn Überhangkräfte nicht sofort zu erreichen oder zu kurzfristigen Auskünften bereit sind, wird empfohlen, entscheidungsrelevante Informationen über den beruflichen Werdegang bei der Dienstbehörde der Überhangkräfte direkt einzuholen, ohne die Personalakte anzufordern. Hierzu sollen die Dienstbehörden auf Anforderung von anderen Dienstbehörden in konkreten Stellenbesetzungsfällen formularmäßig festgelegte Informationen an Stelle der Personalakten übersenden. Dabei weist der Innensenator auf die Notwendigkeit hin, diese Angaben ebenso vertraulich zu behandeln wie die Personalakten selbst.

Nach Abschluß des Stellenbesetzungs- oder Auswahlverfahrens sollen diese besonderen Unterlagen dann vernichtet werden. Erst bei einem weitergehenden Informationsbedarf solle die Personalakte nach dem bisherigen Verfahren angefordert werden.

Eine Verletzung des *Personaldatengeheimnisses* habe ich in dem nachfolgend geschilderten Fall festgestellt, der wegen seiner Komplexität besonders interessant ist:

Unter den Mitgliedern des Personalrats eines städtischen Krankenhauses war es zu Differenzen gekommen, in deren Folge einige Personalratsmitglieder von ihren Ämtern zurücktraten, so daß Neuwahlen notwendig waren. Der Rücktritt wurde u.a. damit begründet, daß die im Amt verbliebenen Personalratsmitglieder sich bei der Personalstelle für die Umsetzung einer Sekretärin im Personalratsbüro eingesetzt hatten, mit deren Arbeitsleistung sie unzufrieden waren. Daraufhin bat die weiter amtierende Personalratsmehrheit die Rechtsabteilungen zweier Gewerkschaften um gutachtliche Überprüfung, ob ein Rücktritt mit dieser Begründung zulässig sei. Zur Erläuterung dieser Frage wurde den Gewerkschaften auch ein Vermerk übersandt, in dem die Arbeitsleistung der Sekretärin bemängelt worden war, wobei der Name der Betroffenen, soweit im Original des Vermerks genannt, in den Ablichtungen unkenntlich gemacht worden war.

Trotzdem wurde die Vorgehensweise des Personalrats datenschutzrechtlichen Anforderungen nicht gerecht, da für die Eingeweihten der Personenbezug jederzeit herstellbar war. Personaldaten sind überaus sensible Daten, die ihrer Bedeutung nach grundsätzlich geheimzuhalten sind. Ihre Übermittlung, insbesondere an Stellen außerhalb der öffentlichen Verwaltung, unterliegt deshalb im Hinblick auf das Recht der betroffenen Dienstkraft auf informationelle Selbstbestimmung hinsichtlich der Erforderlichkeit besonders strengen Anforderungen. Personaldaten unterliegen grundsätzlich auch der personalvertretungsrechtlichen Schweigepflicht (§ 11 PersVG).

Zwar müssen auch Personalvertretungsorgane berechtigt sein, zur Wahrung ihrer Aufgaben und Befugnisse nach Maßgabe des Erforderlichkeitsgrundsatzes Personaldaten zu übermitteln. Der Gesetzgeber hat den Personalvertretungen das Recht zugestanden, selbst darüber zu befinden, welcher Organisationen sie sich zur Unterstützung ihrer Arbeit bedienen, insbesondere auch um eine wirksame Interessenvertretung zu gewährleisten.

Bei sorgfältiger Prüfung hätte der Personalrat jedoch erkennen können, daß es einen rechtlich bedeutsamen „Mißbrauch des Rücktrittsrechts“ von Personalratsmitgliedern nicht gibt.

Selbst wenn diese Auffassung nicht geteilt wird, hätte sich der Personalrat darauf beschränken müssen, die Frage des „Mißbrauchs“ des Rücktrittsrechts abstrakt und ohne Übermittlung von Personaldaten an nichtöffentliche Stellen überprüfen zu lassen. Somit war die Übermittlung personenbezogener Daten bei der Prüfung nicht erforderlich und deshalb unzulässig. Ich habe die Weitergabe der Personaldaten daher beanstandet.

Ein interessantes Schlaglicht auf das Verhältnis zwischen Dienststellen und Personalräten im Zusammenhang mit datenschutzrechtlichen Fragen wirft der Fortgang der geschilderten Angelegenheit: Zunächst hatte der zuständige Bezirksstadtrat es abgelehnt, der Angelegenheit nachzugehen, da weder das Bezirksamt noch die zuständige Krankenhausleitung eine Dienst-

aufsicht über den Personalrat der Krankenanstalt ausübe. Ungeachtet der Tatsache, daß die Personalvertretung insbesondere bei der Wahrung ihrer personalvertretungsrechtlichen Rechte sowie der Erfüllung ihrer personalvertretungsrechtlichen Pflichten nicht den Weisungen des Leiters der Dienststelle unterworfen ist, und diesem insoweit direkte Eingriffsmöglichkeiten verwehrt sind, konnte ich in meiner Erwiderung darauf hinweisen, daß die Dienststelle in ihrer Eigenschaft als Dienstherr oder Arbeitgeber jedoch in ihrem Bereich für einen datenschutzrechtlichen Umgang mit Personaldaten Sorge zu tragen hat. Die Verletzung dieser Verpflichtung, nicht aber die Wahrnehmung personalvertretungsrechtlicher Rechte und Pflichten, war Gegenstand meiner Beanstandung. Meiner Bitte, auch ohne direkte Eingriffsmöglichkeiten für die Zukunft auf einen sorgfältigeren Umgang mit Personaldaten durch den Personalrat hinzuwirken, wurde schließlich entsprochen.

4.5. Justiz

Automatisierung des Schuldnerverzeichnisses

Nach § 915 ZPO hat das Amtsgericht als Vollstreckungsgericht ein Verzeichnis der Personen zu führen, die eine eidesstattliche Erklärung nach § 807 ZPO (in der Regel wegen Zahlungsunfähigkeit) abgegeben haben, gegen die Haft wegen Nichterscheinens zur Abgabe der eidesstattlichen Versicherung angeordnet worden ist, bei denen die Vollstreckung der Steuerschuld erfolglos verlaufen ist (§ 284 Abgabenordnung), oder bei denen der Antrag auf Einleitung des Konkursverfahrens mangels Masse abgelehnt worden ist (§ 107 Konkursordnung).

Abzüge des Schuldnerverzeichnisses erhalten u.a. die Industrie- und Handelskammer sowie die SCHUFA. Bisher wurde das Zentrale Schuldnerverzeichnis beim Amtsgericht Schöneberg sowie die regionalen Schuldnerverzeichnisse bei den übrigen Amtsgerichten manuell geführt. Wegen der gestiegenen Anzahl der Verfahren, und um die Vorgänge zügiger bearbeiten zu können, sollen die Schuldnerverzeichnisse künftig automatisiert geführt werden.

Obwohl mit der geplanten Novellierung der Rechtsvorschriften für das Schuldnerverzeichnis eine ausreichende Rechtsgrundlage für die automatisierte Führung des Schuldnerverzeichnisses erst im Entwurf vorliegt, habe ich keine grundsätzlichen Einwände gegen die Automatisierung erhoben. Deswegen stand eine datenschutzrechtliche Bewertung unter dem Vorbehalt, daß eine Anpassung des Verfahrens an geänderte Rechtsvorschriften möglich sein muß.

Wegen der besonderen Auswirkungen auf die schutzwürdigen Belange der Schuldner ist ein besonderes Augenmaß auf die Korrektheit der Eintragungen im Schuldnerverzeichnis zu legen. Darüber hinaus sollten die Folgen möglicher Fehleintragungen begrenzt gemacht werden. Ich empfahl daher, mit der Automatisierung wieder eine Protokollierung der Auskünfte aus dem Schuldnerverzeichnis vorzusehen, um fehlerhaften „Auskünften“ nachgehen zu können.

Der mittlerweile vorliegende Entwurf für ein Gesetz zur Änderung von Vorschriften über das Schuldnerverzeichnis sieht neuerdings eine Gebührenpflicht für Auskünfte aus dem Schuldnerverzeichnis vor. Daraus ergibt sich für die Zukunft eine Pflicht zur Dokumentation dieser Auskünfte, die die Rückverfolgung der Auskünfte möglich machen würde.

Im übrigen habe ich Empfehlungen zur Verbesserung der technisch-organisatorischen Maßnahmen abgegeben, die die Eingabekontrolle und die Sicherheit der geplanten Vernetzung der dezentralen Schuldnerverzeichnisse mit dem zentralen Schuldnerverzeichnis betreffen.

Zentrales Handelsregister

Eine Firma in Frankfurt plante, ein - privatwirtschaftlich betriebenes - Zentrales Handelsregister zu errichten und wollte dazu einen Abzug sämtlicher Handelsregistereintragungen bei den 440 Registergerichten. Der Antrag auf Mikroverfilmung des kompletten Registerinhalts war von einigen Gerichten abgelehnt worden.

Das OLG München vertrat dazu die Auffassung, daß eine Sachentscheidung über den Antrag vom Registergericht zu treffen sei. Demgegenüber meinte das OLG Frankfurt, daß dafür nicht das Registergericht, sondern die Justizverwaltung zuständig sei.

Der Bundesgerichtshof¹³⁾, dem die Sache zur Entscheidung vorlag, schloß sich dem OLG Frankfurt an. Zwar bestimme das Registergericht über die Einsicht in das Handelsregister, jedoch handele es sich bei Übernahme des gesamten Bestandes des Handelsregisters nicht um eine Einsicht, sondern um etwas wesensmäßig anderes. Das Handelsregister solle hier nicht mehr zur Gewinnung von Informationen – also entsprechend der eigentlichen Bestimmung – genutzt werden, sondern zum Aufbau einer eigenen Datei in Konkurrenz zum Handelsregister. Die Erteilung der Genehmigung dazu sei Sache der Justizverwaltung. Ein Recht auf Gestattung der vollständigen Ablichtung des Handelsregisters gebe es nicht. Die Justizverwaltung sei berechtigt, das Vorhaben, für das keine gesetzliche Grundlage bestehe und bei dem Belange des Datenschutzes berührt seien, abzulehnen.

Aufgrund dieser Entscheidung des Bundesgerichtshofs wird es nicht zu einem Zentralen Handelsregister in privater Hand kommen.

Anordnung der Veröffentlichung von Verurteilungen in der Tagespresse

Seit Jahren kritisiere ich die Berliner Handhabung einer Bestimmung des Strafgesetzbuches, die ein Relikt des mittelalterlichen Prangers darstellt: Bei bestimmten Straftatbeständen (z. B. Beleidigung und falsche Verdächtigung) hat das Gericht auf Antrag des Verletzten oder eines sonst zum Strafantrag Berechtigten anzuordnen, daß die Verurteilung öffentlich bekannt gemacht wird: In der Regel durch eine entsprechende Anzeige in einer Tageszeitung (§ 200 StGB).

In einer internen Anordnung hatte der Polizeipräsident vor Jahren bestimmt, daß bei der Beleidigung von Polizeibeamten der Antrag auf Veröffentlichung ohne Einschaltung des Beamten von der Dienststelle gestellt wird. Als Begründung wurde genannt, die Beleidigung gelte in der Regel nicht den Polizeibeamten selbst, sondern diesen in ihrer Funktion als Repräsentanten des Staates.

Diese routinemäßige Ausübung des Antragsrechts widersprach in erheblichem Maße dem Grundsatz der Verhältnismäßigkeit. Der regelmäßig geringfügigen Ehrverletzung steht ein gravierender Eingriff in die Persönlichkeitsrechte der Betroffenen gegenüber, zumal die Veröffentlichung bereits den Normzweck verfehlen dürfte, dem Beleidigten Genugtuung zu verschaffen. Der vom Polizeipräsidenten vorgegebene Zweck, den Ruf der Polizei als solcher wiederherzustellen, dürfte mit dieser Maßnahme ohnehin konterkariert werden.

Obwohl bereits 1986 unter anderem aufgrund meines Drängens die Praxis des Polizeipräsidenten auf schwerwiegende Fälle beschränkt wurde, kam es erneut zu Beschwerden. Nunmehr hat der Polizeipräsident eine Anweisung erlassen, nach der von der Vorschrift nur noch besonders restriktiver Gebrauch zu machen ist und er sich die Entscheidung über den Antrag persönlich vorbehält.

Ungeachtet dieser begrüßenswerten Entwicklung muß angestrebt werden, diese völlig überholte Vorschrift aus dem Strafgesetzbuch zu eliminieren. Leider waren entsprechende Vorstöße bisher erfolglos.

4.6 Kulturelle Angelegenheiten

Im Geschäftsbereich der Senatsverwaltung für Kulturelle Angelegenheiten mahne ich seit Jahren die Erstellung eines Entwurfs für ein Archivgesetz und für ein Bibliotheksgesetz an.

Die Verzögerung der Vorlage eines Entwurfs für ein *Archivgesetz* wurde jahrelang mit dem Argument begründet, man müsse erst das Inkrafttreten eines Bundesarchivgesetzes abwarten,

bevor der Landesgesetzgeber tätig werden kann. Dieses Gesetz liegt seit Januar 1988 vor, aber weder der vorherige noch der jetzige Senat haben bisher einen Entwurf vorgestellt.

Dieses Gesetz ist, wie ich seit Jahren betone, äußerst dringlich: Es gibt derzeit eine Vielzahl von Forschungsprojekten, deren Ziel eine mikrohistorische Aufarbeitung insbesondere der nationalsozialistischen Zeit ist. Um Geschichte so detailliert darstellen zu können, haben die Forscher ein großes Interesse am Zugang zu den Akten aus dieser Zeit, insbesondere auch an medizinischen Unterlagen. Es kann nicht angehen, daß auf Dauer über den Zugang zu diesen Akten nach freiem Ermessen oder in Analogie zum Bundesarchivgesetz (so die Praxis der Senatsverwaltung für Inneres beim Berlin Document Center) entschieden wird.

Auch ein *Bibliotheksgesetz* habe ich seit Jahren gefordert. Nach Beratungen im Unterausschuß Datenschutz des Abgeordnetenhauses herrschte die Meinung vor, der Umgang mit den Benutzerdaten einer einzelnen Bibliothek bedürfe auch nach der Automatisierung keiner gesetzlichen Regelung, vielmehr genügen entsprechende Regelungen in den Benutzungsbedingungen. Auch hierzu sind allerdings seit Jahren Änderungen angemahnt, ohne daß bisher konkrete Schritte eingeleitet worden wären.

Inzwischen wurde mir ein Sollkonzept zur Einführung eines automationsgestützten Bibliotheksverbunds vorgelegt, in den die zwölf Bibliotheken der Bezirksämter mit ihren Nebenstellen sowie die Amerika-Gedenkbibliothek einbezogen werden sollen. Geplant ist eine Verbundkatalogisierung und ein Benutzerverbund. Hinzu kommt die Unterstützung der Akquisition. In allen Bereichen fallen personenbezogene Daten an: Häufig wird übersehen, daß auch die Angaben über Autoren in den Katalogen personenbezogene Daten darstellen, und auch die Abwicklung der Akquisition ist nicht möglich ohne die Verarbeitung der Daten von Lieferanten und Bibliotheksmitarbeitern.

Der Verbund mit einer entsprechenden Zentrale, die in der Amerika-Gedenkbibliothek stehen soll, setzt einen Online-Anschluß aller Beteiligten an ein zentrales Verfahren und damit die Übermittlung aller Daten der Bezirke untereinander und an die Zentrale voraus.

Ein derartiger Verbund, der jedenfalls hinsichtlich der Benutzer die landesweite Übermittlung hochsensibler Daten voraussetzt, ist im Gegensatz zur internen Automatisierung in einer Bibliothek nur auf der Grundlage eines Landesbibliotheksgesetzes möglich. Soll der geplante Bibliotheksverbund auf rechtmäßige Weise eingeführt werden, ist die Erarbeitung einer gesetzlichen Grundlage dringend erforderlich.

4.7 Schule, Berufsbildung und Sport

Schulrecht

Die notwendige Novellierung des *Schulgesetzes* läßt weiterhin auf sich warten. Bisher hat mir die Senatsschulverwaltung nicht einmal einen Arbeitsentwurf zur Stellungnahme zugeleitet oder meine bereits vor geraumer Zeit gegebenen konkreten Empfehlungen¹⁴⁾ aufgegriffen. Ich halte es nach wie vor für unumgänglich, daß der Landesgesetzgeber bereichsspezifische Datenschutzvorschriften für den Schulbereich erläßt. Diese sind nicht abhängig von einer Neufassung des Bundesdatenschutzgesetzes oder des Berliner Datenschutzgesetzes und sollten daher auch nicht länger aufgeschoben werden.

Über die gegenwärtig im Schulbereich geltenden datenschutzrechtlichen Bestimmungen, vorwiegend *Verwaltungsvorschriften*, hat das Bezirksamt Steglitz – Abteilung Volksbildung – eine umfassende Textsammlung erstellt, die auch in anderen Bezirken Beachtung finden sollte. Sie enthält in übersichtlicher Form alle einschlägigen Bestimmungen und Formblätter sowie praktische Vorschläge zur Beachtung des Datenschutzes bei der Verarbeitung von Schüler- und Elterndaten.

Die noch vom alten Senat erlassenen Ausführungsvorschriften über die dienstliche Beurteilung der Beamten des Schul- und Schulaufsichtsdienstes (*AV-Lehrerbeurteilung*) sind vom Verwaltungsgericht Berlin wegen eines Fehlers im personalvertretungsrechtlichen Mitbestimmungsverfahren aufgehoben worden.

¹³⁾ Az IV a ARZ (VZ) 9/88

¹⁴⁾ vgl. Jahresbericht 1987, Ziff. 5.5

Die Schulverwaltung will diese Entscheidung hinnehmen und auf die zentrale Erfassung der Lehrerbeurteilungen verzichten. Dies begrüße ich, denn es entspricht meiner von Anfang an vertretenen Auffassung, daß die ausnahmslose Übermittlung aller dienstlichen Beurteilungen an die Senatsverwaltung für Schule unverhältnismäßig wäre.

Die Senatsschulverwaltung hat außerdem entschieden, daß die umstrittenen Sachverhaltsfeststellungen zur Teilnahme von Lehrern an der Friedensdemonstration im Oktober 1983 aus den *Personalakten* entfernt werden. Auch dies begrüße ich als datenschutzfreundliche Entscheidung. Ich habe allerdings empfohlen, auf den beabsichtigten Hinweis auf das entsprechende Rundschreiben der Senatsverwaltung in der Personalakte zu verzichten, weil dieses wiederum Rückschlüsse auf den Inhalt der entfernten Sachverhaltsfeststellungen zulassen würde. Datenschutzgerecht wäre eine Form der Tilgung aus der Personalakte, bei der der betroffene Lehrer auf einem Einlegeblatt bestätigt, daß die getilgte Seite im Einvernehmen zwischen ihm und dem Dienstherrn vernichtet oder ihm ausgehändigt worden sei.

Die von der Senatsschulverwaltung in Kraft gesetzten Ausführungsvorschriften über Noten und Zeugnisse (*AV Noten und Zeugnisse*) sehen entgegen meinen Empfehlungen vor, daß Halbjahreszeugnisse Angaben über Fehlzeiten oder Verspätungen enthalten dürfen¹⁵. Noch vor den Wahlen zum Abgeordnetenhaus teilte mir die Senatsschulverwaltung jedoch mit, aufgrund meiner Einwände und Hinweise auf die datenschutzgerechte Praxis in Bayern habe sie angeregt, die Angelegenheit im Schulausschuß der Kultusministerkonferenz zu behandeln. Im Mai dieses Jahres legte die Senatsverwaltung den Entwurf von Verwaltungsvorschriften zur Änderung der AV Noten und Zeugnisse vor, mit dem meinen Anregungen in vollem Umfang entsprochen werden sollte. Nachdem der Landesschulbeirat diesem Entwurf zugestimmt hatte, hielt die Senatsschulverwaltung im August völlig unerwartet an der Verpflichtung zur Aufnahme von Fehlzeiten und Verspätungen in die Halbjahreszeugnisse fest. Lediglich Erziehungs- und Ordnungsmaßnahmen werden in kein Zeugnis mehr aufgenommen. Damit wird ein inkonsequenter Rechtszustand aufrechterhalten: Die Aufnahme von Fehlzeiten und Verspätungen unterbleibt ausdrücklich in Abgangs- und Abschluszeugnissen, bei Halbjahreszeugnissen soll sie aber möglich sein. Ich sehe kein Erfordernis für diesen erweiterten Informationsgehalt der Halbjahreszeugnisse. Wenn der Lehrer den Eltern eines Schülers mitteilen will, daß sich dessen unentschuldigte Fehlzeiten häufen, wäre es pädagogisch geradezu fahrlässig, dies erst auf dem nächsten Halbjahreszeugnis zu tun. Ohnehin hat der Lehrer im Spannungsfeld der Artikel 6 und 7 GG bei der Erfüllung seines Erziehungsauftrags möglichst engen Kontakt zu den Eltern seiner Schüler zu halten. Der Schüler sollte aber nicht gezwungen werden, bei Bewerbungen Dritten (vor allem Arbeitgebern) seine Fehlzeiten zu offenbaren. Die Chancen, diese (evtl. krankheitsbedingten) Fehlzeiten mündlich zu erläutern, wird der Schüler meist nicht erhalten, weil er aufgrund der „Papierform“ gar nicht erst zum Vorstellungsgespräch eingeladen wird. Es ist zumindest verwunderlich, daß die Senatsschulverwaltung in Berlin sich nicht zu einer datenschutzgerechten Lösung dieses Problems verstehen kann, wie sie z. B. in Bayern und Baden-Württemberg gefunden worden ist. Dort wird generell darauf verzichtet, Bemerkungen über Fehlzeiten jedenfalls in den Klassenstufen in das Zeugnis aufzunehmen, in denen sich Schüler um Ausbildungsplätze bewerben.

Forschung in der Schule

Im Rahmen eines Forschungsprojekts „*Planung und Realisierung von Einzelintegration behinderter Kinder in Regeleinrichtungen*“ bereiten Forscherinnen der Technischen Universität Berlin eine statistische Erhebung im Verwaltungsbezirk Spandau vor. Dazu sollten Daten über behinderte Schüler aus den Akten der Behindertenfürsorge Spandau bezogen auf die Regel- und Sonderschulen dieses Bezirks ausgewertet werden. Ich habe darauf hingewiesen, daß diese Daten für Zwecke des Jugendwohlfahrtsgesetzes erhoben worden sind und damit dem Sozialgeheimnis unterliegen. Sie dürfen nur unter den Voraussetzungen des § 75 SGB X

für wissenschaftliche Forschung oder Planung im Sozialleistungsbereich offenbart werden. Aufgrund meiner Empfehlungen wurde ein datenschutzgerechtes Verfahren gefunden, bei dem die Mitarbeiterinnen der Behindertenfürsorge ausschließlich anonymisierte Angaben in Erhebungsbogen eintragen und den Forscherinnen zur Auswertung zur Verfügung stellen.

Datenschutz bei Betriebspraktika

Die Schülerinnen und Schüler der allgemeinbildenden Schulen in Berlin haben im Rahmen ihrer schulischen Ausbildung Betriebspraktika auch im Bereich der Jugendgesundheitsdienste abzuleisten (Schnupperpraktikum). Dabei nehmen die Praktikanten an den im Vorfeld der ärztlichen Reihenuntersuchungen durchgeführten Tests (z. B. Seh- und Hörtests) teil. Im Rahmen ihrer praktischen Tätigkeit können sie auch Einsicht in die in den Fürsorgestellen geführten Gesundheitsbögen nehmen.

Ich habe die Senatsverwaltung für Schule, Berufsbildung und Sport darauf hingewiesen, daß es in diesem Bereich um personenbezogene Daten geht, die einem besonderen Schutz unterstehen, der erheblich über das allgemeine Datenschutzrecht hinausgeht. Da die „Schnupperpraktikanten“ nicht auf das Datengeheimnis nach § 8 Berliner Datenschutzgesetz verpflichtet werden können, weil es sich bei ihnen nicht um „bei der Datenverarbeitung beschäftigte Personen“ handelt und sie als solche auch nicht unter die strafrechtliche Vorschrift des § 203 StGB fallen, kann den datenschutzrechtlichen Belangen nur dadurch Rechnung getragen werden, daß die Eltern aller zu untersuchenden Schüler um eine entsprechende Einverständniserklärung gebeten werden. In der Regel müssen Eltern vor Beginn der Reihenuntersuchungen einen Fragebogen ausfüllen, in den ohne großen Aufwand eine Einverständniserklärung zur Teilnahme von „Schnupperpraktikanten“ aufgenommen werden kann. Soweit Eltern damit nicht einverstanden sind, sollte ihr Kind ohne Hinzuziehung eines Praktikanten untersucht werden.

4.8 Wissenschaft und Forschung

Hochschulgesetzgebung

Bereits in meinem Jahresbericht 1986¹⁶ habe ich auf die Notwendigkeit hingewiesen, die *Erhebung und Verarbeitung von Studentendaten* insbesondere bei der Immatrikulation im Hochschulgesetz bereichsspezifisch zu regeln. Dies gilt auch für die Verarbeitung von Personaldaten in den Hochschulen. Entsprechende Vorschläge hatte ich der Senatsverwaltung für Wissenschaft und Forschung bereits in der vergangenen Legislaturperiode gemacht. Im Gegensatz zur Senatsverwaltung für Schule, Berufsbildung und Sport hat die Senatsverwaltung für Wissenschaft und Forschung Gespräche mit mir über die Schaffung der notwendigen bereichsspezifischen Rechtsgrundlagen aufgenommen und mir im Sommer dieses Jahres einen ersten Entwurf zugeleitet, der z. T. meine Empfehlungen aufgreift, aber noch verbesserungsbedürftig ist.

Einigkeit besteht bereits über eine allgemeine Befugnisnorm zur Erhebung und Nutzung von Studentendaten für Hochschulzwecke. Der genaue Datenumfang soll durch Rechtsverordnung festgelegt werden. Der Hochschulgesetzgeber sollte sich im übrigen darauf beschränken, die bereichsspezifisch erforderlichen Ausnahmen vom Zweckbindungsgebot z. B. bei der Datenübermittlung an die Ausländerbehörde oder das Studentenwerk zu regeln.

Bei der Vorbereitung der Novellierung des Berliner Hochschulgesetzes hat sich die Senatsverwaltung für Wissenschaft und Forschung an mich mit der Frage gewandt, ob es mit der rechtlich gebotenen Vertraulichkeit bei der Behandlung von Personaleinzelangelegenheiten vereinbar wäre, wenn die Kuratorien – wie in der Koalitionsvereinbarung vorgesehen – die Funktion der obersten Dienstbehörde erhielten und zudem um Mitglieder erweitert würden, die in keinem Dienst- oder Beschäftigungsverhältnis zur Universität stehen.

Ich habe auf die Rechtsprechung des Bundesverwaltungsgerichts verwiesen, nach der jeder Dienstherr verpflichtet ist, den

¹⁵) vgl. Jahresbericht 1988, Ziff. 4.8

¹⁶) Ziff. 4.4

Kreis der mit Personalakten befaßten Personen möglichst eng begrenzt zu halten. Personalunterlagen genießen sowohl im dienstlichen Interesse als auch im schutzwürdigen persönlich-privaten Interesse des Beamten einen besonderen Vertrauensschutz. Diese Rechtsprechung des Bundesverwaltungsgerichts ist auch im Zusammenhang mit dem vom Bundesverfassungsgericht im Volkszählungsurteil aus dem allgemeinen Persönlichkeitsrecht abgeleiteten Recht auf informationelle Selbstbestimmung zu sehen. Das Persönlichkeitsrecht jedes Bediensteten einer Hochschule und jedes externen Stellenbewerbers verbietet es, daß seine Personalunterlagen aus Anlaß einer Personaleinzeltatscheidung einem praktisch nur schwer einzugrenzenden Personenkreis wie den Mitgliedern der Kuratorien zugänglich gemacht werden. Die Kuratorien setzten sich bis 1986 aus 22 Mitgliedern zusammen und sollten nach Planungen aus 20 Mitgliedern bestehen. Hinzu käme jeweils die gleiche Anzahl von Stellvertretern, für die ebenfalls Fotokopien der betreffenden Personalunterlagen zu fertigen wären.

Dies ist aus der Sicht des Datenschutzes selbst dann nicht akzeptabel, wenn alle Mitglieder der Kuratorien - auch soweit sie nicht zum staatlichen Bereich gehören - förmlich zur Verschwiegenheit verpflichtet werden. Die höchststrichterliche Rechtsprechung begrenzt bereits den Kreis der Beschäftigten eines Dienstherrn, die mit Personalangelegenheiten befaßt werden dürfen, und begnügt sich nicht mit dem Hinweis auf deren Verschwiegenheitspflicht.

Ich verkenne nicht, daß das Hochschulgesetz in der bis 1986 geltenden Fassung bereits einmal den Kuratorien die Funktion der obersten Dienstbehörde zugewiesen hatte. Dieses Hochschulgesetz stammte jedoch aus der Zeit vor dem Volkszählungsurteil von 1983. Der Landesgesetzgeber hat mit der Übertragung der Funktion der obersten Dienstbehörde auf die Personalkommission im Hochschulgesetz von 1986 einen Rechtszustand hergestellt, der den verfassungsrechtlichen Vorgaben näher steht als der frühere Rechtszustand. Eine Rückkehr zu diesem alten Rechtszustand wäre deshalb mit gravierenden verfassungsrechtlichen Risiken verbunden.

Auch die Funktion der einfachen Dienstbehörde darf aus den genannten Gründen nicht einem Gremium mit der Größe und Heterogenität des Kuratoriums übertragen werden.

Dagegen halte ich die Beibehaltung des gegenwärtigen Rechtszustandes, wonach die Behandlung von Personaleinzelsachen der Personalkommission als einem sehr viel kleineren Gremium aus Vertretern der Hochschule und des Staates vorbehalten bleibt, verfassungsrechtlich für hinnehmbar.

Im neuen Berliner Hochschulgesetz soll die Stellung der Frauenbeauftragten gestärkt werden. Soweit den Frauenbeauftragten die Möglichkeit eröffnet werden soll, an Personalauswahlgesprächen teilzunehmen und in Personalakten und Bewerbungsunterlagen Einsicht zu nehmen, was für eine effektive Aufgabenerfüllung sicherlich zweckmäßig wäre, sollte hierfür eine bereichsspezifische Rechtsgrundlage im Hochschulgesetz geschaffen werden. Anderenfalls wäre jeweils die Einwilligung aller betroffenen Personen (z. B. auch der Mitbewerber) einzuholen¹⁷⁾.

Auch sollte der Hochschulgesetzgeber den Umgang mit personenbezogenen Angaben im Rahmen von Berufungsverfahren genauer regeln. Soweit die Berufungskommissionen ihre Empfehlung, bestimmte Bewerber nicht zu berücksichtigen, begründen, sind damit in der Regel negative Werturteile verbunden, die streng vertraulich und nicht „fachbereichsratsöffentlich“ behandelt werden sollten. In jedem Fall sollte die Fertigung von Kopien derart sensibler Vorgänge strikt begrenzt und die Rückgabe und zentrale Vernichtung notwendiger Fotokopien durch das Fachbereichssekretariat vorgeschrieben werden.

Die Verordnung über das Wahlrecht an den Hochschulen des Landes Berlin (*Hochschul-Wahlrechtsverordnung*) vom 5. November 1987 schreibt bei nicht-studentischen Wahlberechtigten die Aufnahme des Geburtsdatums in das Wählerverzeichnis vor, das in dieser Form zur Einsichtnahme durch die wahlberechtigten Mitglieder der Hochschule auszulegen ist.

Auch eine solche bereichsspezifische Regelung muß sich an den vom Bundesverfassungsgericht im Volkszählungsurteil formulierten Anforderungen, namentlich am Grundsatz der Verhältnismäßigkeit, messen lassen. Stellen, die zur Erfüllung ihrer Aufgaben personenbezogene Daten erheben und übermitteln, müssen sich auf das zum Erreichen des angegebenen Zwecks erforderliche Minimum beschränken. Zweck des Wählerverzeichnisses ist es, den Wahlberechtigten die Möglichkeit zu geben, rechtzeitig vor der Wahl Gründe vorzutragen, die eine Wahlbeteiligung anderer Mitglieder der Hochschule ausschließen könnten. Dazu müssen die jeweils einzeln aufgeführten Personen hinreichend bestimmt sein. Dies dürfte auch bei nicht-studentischen Hochschulmitgliedern durch Angabe des Namens, Vornamens sowie der Dienstbezeichnung und der Dienststelle gewährleistet sein. Selbst wenn diese Merkmale auf mehrere Personen zutreffen sollten, wäre kein Grund für die öffentliche Auslegung weiterer personenbezogener Daten gegeben, da der Wahlvorstand über Einsprüche entscheiden muß und im Rahmen dieser Entscheidung ohnehin eine genaue Identitätsprüfung vorzunehmen hat. Zu diesem Zweck kann der Wahlvorstand parallel eine eigene Liste führen, die auch die Geburtsdaten enthält. Daß es einer allgemeinen Offenbarung der Geburtsdaten nicht bedarf, wird im übrigen schon daraus deutlich, daß sich der Inhalt des Wählerverzeichnisses bei Studenten auf Namen und Matrikelnummer beschränkt.

Ich habe dem Senator für Wissenschaft und Forschung bereits in der vergangenen Legislaturperiode mitgeteilt, daß ich es für erforderlich halte, die Hochschulwahlrechtsverordnung zumindest hinsichtlich der Auslegungspflicht zu konkretisieren. Beispielgebend ist insoweit § 16 Abs. 1 Landeswahlordnung, der die Auslegung auf das erforderliche und damit datenschutzrechtlich zulässige Maß beschränkt. Unabhängig davon sollte bis zur notwendigen Novellierung der Hochschul-Wahlrechtsverordnung bei der Auslegung der Wählerverzeichnisse auf die Angabe der Geburtsdaten verzichtet werden. Der Senator für Wissenschaft und Forschung hat mitgeteilt, daß er meine Empfehlungen bei der nächsten Novellierung der Hochschulwahlrechtsverordnung berücksichtigen wird. Bis zu dieser Änderung sind die Präsidenten der Kuratorialhochschulen gebeten worden, sicherzustellen, daß die Wahlvorstände auf die öffentliche Auslegung der Geburtsdaten verzichten.

Der vom Bundeskabinett im Juli beschlossene Entwurf für ein novelliertes *Hochschulstatistikgesetz*¹⁸⁾ muß daraufhin überprüft werden, ob er sich auf die sekundärstatistische Auswertung von Daten beschränkt, die die Hochschulen zunächst für eigene Verwaltungszwecke erheben. Daten, die ausschließlich für statistische Zwecke benötigt werden, sind direkt beim Betroffenen zu erheben.

4.9 Organisation und Geschäftsordnung

Vordrucke

In der letzten Zeit sind mir Vordrucke nicht nur von Bürgern zur Prüfung auf eine datenschutzgerechte Gestaltung im Hinblick auf § 9 Abs. 2 BlnDSG vorgelegt worden, sondern auch einzelne Verwaltungen sind an mich herangetreten.

Meine Bewertung richtet sich nach den in meinem Jahresbericht 1986¹⁹⁾ bekanntgemachten Grundsätzen, die die Senatsverwaltung für Inneres per Rundschreiben allen Vordrucksachbearbeitern zur Kenntnis gegeben hat. Auf dieses Rundschreiben wird auch in den vom Senat erlassenen Vordruckgrundsätzen verwiesen.

Selbst wenn das Problembewußtsein der Mitarbeiter bei der Gestaltung von Formularen gestiegen ist, läßt sich doch feststellen, daß es der Verwaltung immer wieder Schwierigkeiten bereitet, in den Formularen die Rechtsgrundlagen genau aufzuführen, aufgrund derer die Daten erhoben werden oder die Hinweise auf die Freiwilligkeit der Angaben anzubringen. Nur so kann das Verwaltungshandeln transparent gemacht werden und die Akzeptanz erhöht werden. Hinzu kommt, daß häufig personenbezogene Daten nicht wie in § 9 Abs. 2 BlnDSG gefordert, aufgrund gesetz-

¹⁷⁾ Vgl. Jahresbericht 1988, Ziff. 4.5

¹⁸⁾ Vgl. oben Ziff. 4.4

¹⁹⁾ Ziff. 4.5

licher Bestimmungen, sondern aufgrund von Verwaltungsvorschriften erhoben werden. So werden beispielsweise bei Beihilfeanträgen die personenbezogenen Daten aufgrund der Beihilfevorschriften erhoben. Hier müssen materiell-rechtliche Vorschriften geschaffen werden, wie ich es auch sonst im Personaldatenbereich wiederholt gefordert habe.

In einem anderen Vordruck erhält der Antragsteller den Hinweis, daß er verpflichtet sei, die im Formular geforderten Angaben zu machen. Dieser Hinweis ist irreführend, weil die Daten nur aufgrund einer Rechtsvorschrift oder auf freiwilliger Basis erhoben werden dürfen, nicht aber, weil es ein Vordruck so sieht.

Im Sozialleistungsbereich wird bei der Vordruckgestaltung häufig davon ausgegangen, daß ein Hinweis auf die Mitwirkungspflicht nach § 60 SGB I ausreichend sei. Dem ist nicht so, weil der Antragsteller daraus nicht die materielle Erforderlichkeit entnehmen kann, also warum er bei der Datenerhebung zur Mitwirkung verpflichtet ist. Dies muß ihm immer unter Hinweis auf die speziellesatzliche Regelung erklärt werden.

Bei *Entbindungsklauseln* (z. B. von der ärztlichen Schweigepflicht, dem Sozialgeheimnis) habe ich oftmals festgestellt, daß diese zu pauschal und damit nicht wirksam gefaßt sind. Aus dem Erklärungsinhalt selbst ist häufig nicht ersichtlich, in welchem Umfang und zu welchem Zweck beispielsweise ein Arzt von der Schweigepflicht entbunden werden soll. Eine Einwilligungsklausel muß im Sinne eines „informed consent“ Zweck und Ausmaß und insbesondere die Erforderlichkeit der Datenoffenbarung bzw. -übermittlung erkennen lassen.

Auch die Gestaltung der *Anmeldekarten der Volkshochschulen* entspricht nicht den datenschutzrechtlichen Anforderungen, weil einzelne Angaben wie z. B. Beruf, Alter und Telefonnummer gefordert werden, ohne daß dafür eine Rechtsgrundlage vorhanden ist. Die Betroffenen werden nur teilweise auf die Freiwilligkeit der Angaben hingewiesen. Die Senatsverwaltung für Schule, Berufsbildung und Sport hat mir zugesagt, daß die Anmeldekarten um die Hinweise auf die Freiwilligkeit ergänzt werden.

Weiterhin werden bei Vorliegen von Ermäßigungsgründen (z. B. Bezug von Sozialhilfe, arbeitslos, Übersiedler) bei der Anmeldung diese mit einer gut lesbaren Abkürzung (z. B. „SH“, „Alhi“) eingetragen oder in entsprechenden Kästchen angekreuzt. Der Hörer ist verpflichtet, die Anmeldekarte beim Besuch des Kurses mit sich zu führen und dem Dozenten auf Verlangen vorzulegen. Somit wird er unter Umständen gezwungen, ein personenbezogenes Datum zu offenbaren, das dem Sozialgeheimnis unterliegt. Dies ist datenschutzrechtlich nicht hinnehmbar.

Die Anmeldekarten werden im Durchschreibeverfahren ausgefüllt. Das Original verbleibt bei der Volkshochschule, die Durchschrift dient dem Betroffenen zur Vorlage als Anmeldekarte. Eine Volkshochschule wollte auf der Anmeldekarte den Klartext weglassen. Dennoch kann der Insider aus der Platzierung des durchgedruckten Kreuzes ziemlich genaue Rückschlüsse ziehen. Darüber hinaus ist anhand der Höhe des entrichteten Entgeltes ebenfalls erkennbar, ob es sich um eine ermäßigte oder reguläre Teilnahme am Kurs handelt. Da nur wenige Ermäßigungsgründe in Betracht kommen, sind auch auf diesem Wege Rückschlüsse möglich.

Eine andere Volkshochschule wollte mit der Vergabe von Ziffern für die Ermäßigungsgründe das Problem lösen. Den Personen, denen die Anmeldekarten vorgelegt werden (z. B. Dozenten), dürften regelmäßig die Bedeutung der Ziffern bekannt sein. Im übrigen sind ebenfalls Rückschlüsse wegen der Höhe des Betrages möglich.

Eine weitere Volkshochschule will die Formulare unverändert bis zum 2. Semester 1990 - also noch ein Jahr - benutzen. Wegen der Vorlagepflicht der Anmeldekarte muß eine andere Lösung für die Übergangszeit gefunden werden.

Ich habe daher angeregt, die gesamten Bearbeitungsdaten nicht durchzuschreiben. Sofern dies nicht möglich sein sollte, habe ich empfohlen, für das *Deckblatt* eine spezielle Papierart zu verwenden, mit dem in bestimmten Teilbereichen nicht durchgeschrieben werden kann. Somit werden auch die Kreuze nicht auf der Teilnehmerkarte erkennbar. Damit können diese Rubriken auf der Teilnehmerkarte selbst entfallen. Weiterhin habe ich ange-

regt, daß auf der Teilnehmerkarte selbst statt umfangreicher Berechnungen (die auf dem Deckblatt, das bei der Volkshochschule verbleibt, durchaus erforderlich sein können) der einfache Hinweis „Bezahlt“ erfolgt. Damit müßte der Teilnehmer keine über das erforderliche Maß hinausgehenden personenbezogenen Daten offenbaren, und das Problem wäre gelöst.

Durchsetzung des Löschungsanspruchs

Immer wieder fragen Bürger an, warum eine an sich erledigte Eintragung in einem Register weiterhin gespeichert bleibt. Das gilt beispielsweise für Eintragungen bei der SCHUFA, die nicht unmittelbar nach Begleichung des Kredits gelöscht werden, sondern erst nach Ablauf von weiteren drei Jahren. Auch im polizeilichen Informationssystem bleiben personenbezogene Notierungen auch dann für eine bestimmte weitere Zeit gespeichert, wenn das Ermittlungsverfahren eingestellt worden ist oder wenn ein anschließendes gerichtliches Strafverfahren mit einem Freispruch endete.

Auch im zentralen Schuldnerverzeichnis, in dem die Personen registriert sind, die eine eidesstattliche Versicherung abgegeben haben oder gegen die Haft angeordnet worden ist, weil sie zum Termin der eidesstattlichen Versicherung nicht erschienen sind, werden die Eintragungen nicht unmittelbar nach Begleichung der Schulden gelöscht, sondern noch weitere drei Jahre aufbewahrt. Auf den ersten Blick ist es unverständlich, Daten noch zu speichern, obwohl der Umstand, der zu ihrer Speicherung geführt hat, weggefallen ist oder sich erledigt hat.

Jedoch führt dies nicht zu einer unverhältnismäßigen Einschränkung des Rechts auf informationelle Selbstbestimmung. Die genannten Register - und weitere, bei denen ähnlich verfahren wird - sollen nicht allein Auskunft über den momentanen aktuellen Stand geben. Vielmehr ist für die Beurteilung eines Sachverhalts auch die Kenntnis eines überschaubaren Zeitraums in der näheren Vergangenheit erforderlich.

Das Bundesverfassungsgericht hat in einer kürzlich ergangenen Entscheidung dies am Beispiel des Schuldnerverzeichnisses bestätigt und weiter ausgeführt, daß die Eintragung im Schuldnerverzeichnis lediglich erste Anhaltspunkte vermittele, jedoch noch keine abschließende Beurteilung der Zuverlässigkeit und Kreditwürdigkeit des eingetragenen Schuldners ermögliche. Die Eintragung führe auch dann, wenn sie über den Zeitpunkt der Schuldentilgung hinaus bestehen bliebe, nicht zu einem der Beeinflussung und Kontrolle weitgehend entzogenen Geschäfts- bzw. Sozialprofil der Schuldner. Ein unzumutbarer Eingriff in das informationelle Selbstbestimmungsrecht liege somit nicht vor.

Aus datenschutzrechtlicher Sicht ist jedoch zu fordern, daß die Fristen für die Löschungen sowohl in allgemein zugänglichen Registern als auch in internen Informationssystemen differenziert gestaltet werden und möglichst kurz bemessen sein sollten.

Außerdem ist sicherzustellen, daß die Löschungen, sofern sie manuell veranlaßt werden müssen, auch tatsächlich erfolgen und nicht wegen anderer Arbeiten zurückgestellt werden.

4.10 Bezirksämter

In der Zeit vom Dezember 1982 bis zum März 1988 sind mit jeweils etwa halbjährigem Abstand alle Bezirksämter von Berlin einer eingehenden technisch-organisatorischen Überprüfung unterzogen worden.

In die Prüfung einbezogen wurden

- grundsätzlich alle Anwender automatisierter Datenverarbeitung, also die an den zentralen LED-Verfahren angeschlossenen Stellen (Bezirkseinwohnerämter, Wohnungsämter, Vermessungsämter), die Datenerfassungsstellen in den Abteilungen Personal und Verwaltung und Finanzen (Bezirkskassen), die Zentrale Textverarbeitung und der Einsatz von Personalcomputern;
- alle Stellen, bei denen ich Einzelvorgänge zu behandeln hatte;
- die aus datenschutzrechtlicher Sicht wichtigsten manuell geführten personenbezogenen Sammlungen (z. B. die Sozial-

leistungs- oder Fürsorgekartei), der ausgehende Fachpostverkehr und die Aktenvernichtung;

- bereits bekannte oder nach den Erfahrungen aus anderen Bezirken zu vermutende datenschutzrechtliche Schwachstellen oder Problembereiche;
- Stellen, die mit personenbezogenen Daten arbeiten und deren Aufgabenbereiche und Arbeitsabläufe noch nicht ausreichend bekannt waren.

Die Kontrollbesuche schlossen die nachgeordneten öffentlichen Stellen, z. B. die Krankenhausbetriebe und Schulen, die in anderen Zusammenhängen geprüft worden waren, nicht mit ein. Sie konzentrierten sich also unmittelbar auf die Abteilungen der Bezirksämter. Grundsätzlich sollten alle Abteilungen eines Bezirksamtes von den Kontrollbesuchen erfaßt werden. Davon wurden Ausnahmen gemacht, wenn eine Abteilung in anderem Zusammenhang datenschutzrechtlich überprüft worden war.

Zentrale ADV-Verfahren

Die Nutzung zentraler ADV-Verfahren ist die herkömmliche Form der Nutzung der Informationstechnik durch die Bezirksämter. Sie werden im Auftrag der Bezirksämter von der zuständigen Hauptverwaltung administriert und koordiniert sowie vom Landesamt für Elektronische Datenverarbeitung (LED) betrieben. Dabei sind die Bezirke häufig nicht die einzigen Auftraggeber, sondern teilen sich diese Funktion mit anderen Behörden (z. B. Verfahren Einwohnerwesen zusammen mit dem Landeseinwohneramt, Personalbezugsverfahren zusammen mit anderen Abrechnungsstellen).

Die Benutzung der Verfahren durch die Bezirke erfolgt teilweise off-line mit dezentraler Datenerfassung in den Bezirken und Datenträgeraustausch mit dem LED (z. B. Lohn, Vergütung, Besoldung und Bezirkskasse) oder on-line im Dialogverfahren mit Hilfe von Datensichtgeräten.

In der Regel werden mit den Verfahren bezirkseigene oder übertragene Vorbehaltsaufgaben abgewickelt. In beiden Fällen sind die Bezirksämter - genauer die jeweils zuständigen Ämter - als speichernde Stellen i. S. v. § 4 Abs. 3 Nr. 1 BlnDSG für die datenschutzgerechte Gestaltung der Systeme verantwortlich. Der mir häufig entgegengehaltene Hinweis, daß die jeweilige Hauptverwaltung das System eingeführt hat und weiterhin betreut, geht insoweit fehl. Die Bezirke haben ihre Verantwortung - bei zentralen Systemen selbstverständlich in koordinierter Form - wahrzunehmen und ausreichende Einflußmöglichkeiten auf die entwickelnde, planende oder administrierende Hauptverwaltung zu schaffen und auszuüben.

Die Überprüfungen, aber auch die Bearbeitung einer Vielzahl von Einzeleingaben und -anfragen hat gezeigt, daß sich die Bezirksämter nicht immer dieser Verantwortung bewußt sind, vielmehr zum Abschieben der Verantwortung auf die Hauptverwaltung neigen. Der oben²⁰⁾ geschilderte Fall aus dem Neuköllner Wohnungsamt bietet hierzu ein treffendes Beispiel. Im Rahmen der Planungen zu einem neuen landesweiten IuK-Konzept muß daher eine erhebliche Stärkung des Verantwortungsbewußtseins der Bezirksämter erfolgen.

Ein weiteres Grundsatzproblem bei zentralen Großsystemen stellt sich mit der *Zugriffsbefugnis der Bezirke auf die Daten anderer Bezirke*, ohne daß eine Zuständigkeit für die Arbeit mit diesen Daten gegeben ist. Diskutiert wurden diese Probleme im Zusammenhang mit der Kaufpreissammlung und den bezirklichen Komponenten des Verfahrens Einwohnerwesen. In beiden Fällen ist es bisher nicht zu einem Einvernehmen gekommen. Die Argumente der Bezirke und der jeweiligen aufsichtführenden Hauptverwaltungen beschränken sich auf Praktikabilitätsgesichtspunkte, bleiben aber pauschal und zahlenmäßig unbelegt. Selbst wenn schwerwiegende sachliche Gründe für die bezirksübergreifende Zugriffsbefugnis nachgewiesen werden, wäre eine gesetzliche Regelung erforderlich. Andernfalls bleibt der Zugriff rechtswidrig und ist zu unterbinden.

Bei den Kontrollbesuchen habe ich auch die *Handhabung der Verfahren* durch die Bezirke untersucht.

Die Datenerfassung in den Lohn- und Gehaltsstellen erfolgt in Datensammelsystemen auf Erfassungskassetten. Gravierende datenschutzrechtliche Mängel wurden nicht festgestellt. Es fiel jedoch auf, daß von den erfaßten Kassetten keine Sicherungskopien erzeugt werden, so daß im Ernstfall Daten zerstört oder zumindest für einen gewissen Zeitraum nicht mehr rekonstruiert werden können.

Die Datenerfassung der Bezirkskassen für das Personenkontenverfahren erfolgt mittels Datensammelsystemen auf Magnetbändern. Die Zentraleinheit und der Datenträgerschrank mit den Magnetbändern der einzelnen Wochentage befinden sich abseits von den Erfassungsplätzen in einem gesonderten Rechnerraum. Dieser Rechnerraum ist in vielen Fällen zweckentfremdet worden: als Aufbewahrungsort für Garderobe und andere Utensilien der Erfassungskräfte, als Küche mit Kühlschrank und Abwaschgelegenheit, als Sozialraum. Hinsichtlich der dort untergebrachten Datenträger kann in diesen Fällen eine zuverlässige Abgangskontrolle nicht mehr gewährleistet werden.

Die Ergebnisse der Verarbeitung im Personenkontenverfahren im LED werden als Listen an die Bezirkskassen zurückgegeben. Bei den früheren Kontrollbesuchen in den Bezirken habe ich festgestellt, daß diese Listen vom LED-Botenverkehr nicht wie die Magnetbänder in verschließbaren Containern, sondern in Plastiktüten versandt wurden. Bei der Auslieferung wurden zumindest in einem Bezirksamt Container und Plastiktüten mit Inhalt ohne Quittung einfach neben der Pfortnerloge abgestellt und unbeaufsichtigt gelassen. Ich habe daraufhin angeregt, daß die Listen auch in den Containern verschlossen werden. Bei den letzten Kontrollbesuchen in Bezirksämtern habe ich dann feststellen können, daß meinen Anregungen gefolgt wurde.

Das neue Personenkontenauskunftsverfahren ist bei den letzten Kontrollbesuchen in das Kontrollprogramm aufgenommen worden. Dabei wurde festgestellt, daß hinsichtlich der Speicher-, Benutzer- und Zugriffskontrolle Mängel vorlagen. Es wurden meist zu kurze Paßwörter benutzt, und es erfolgte kein Abbruch nach einer Höchstzahl von Paßwortfehlangeben.

Die meisten zentralen ADV-Verfahren werden von der Abteilung Bau- und Wohnungswesen genutzt: Wohngeld, Fehlbelegungsabgabe, Wohnberechtigungsschein, Mietpreisangelegenheiten, Liegenschaftskataster, Kaufpreissammlung. Diese Verfahren werden ausschließlich im On-line-Verfahren über nicht-intelligente Terminals abgewickelt.

Bei der Benutzung des *ADV-Verfahrens Einwohnerwesen* in den Bezirkseinwohnerämtern habe ich während der Kontrollbesuche beobachtet, daß die persönlich ausgestellten maschinenlesbaren Benutzerausweise im Kartenleser blieben, wenn der betreffende Mitarbeiter das Terminal verließ, und andere Mitarbeiter mit derselben Karte Abfragen am System tätigten. Auch wurden solche Ausweise in nicht bedienten Terminals oder unbeaufsichtigt neben ihnen liegend vorgefunden. Mit solchen Praktiken werden die Benutzer-, Speicher-, Zugriffs- und Eingabekontrollmaßnahmen am ADV-System unterlaufen.

Dezentrale Verfahren²¹⁾

Dezentrale Verfahren in den Bezirksämtern gab es über Jahre hinweg nur für die *Textverarbeitung*. Solche Systeme sind trotz ihrer Spezialisierung für die Textverarbeitung programmierbare Datenverarbeitungsanlagen, die mit geeigneter Softwareausstattung auch Dateiverarbeitung ermöglichen. Aus diesem Grunde habe ich bei der Textverarbeitung auch geprüft, ob personenbezogene Dateien geführt wurden. Dabei habe ich durchweg Telefonverzeichnisse, Geschäftsverteilungspläne und Verteiler für Serienbriefe (Adressaten von regelmäßigen Informationen verschiedener Art) angetroffen. Ich mußte in all diesen Fällen auf einer Meldung zum allgemeinen Dateienregister nach § 22 BlnDSG, der Veröffentlichung im Amtsblatt und Landespresse-dienst nach § 12 BlnDSG und die Aufnahme dieser Dateien im internen Dateienverzeichnis nach § 16 Satz 2 Nr. 2 BlnDSG bestehen, sofern dies noch nicht geschehen war. Ansonsten bestanden gegen die Führung dieser Dateien sowohl in rechtlicher wie auch in technisch-organisatorischer Hinsicht keine Bedenken.

²⁰⁾ Ziff. 4.1

²¹⁾ Vgl. zu den grundsätzlichen Problemen der dezentralen Datenverarbeitung oben Ziff. 2.5 und 2.6

Inzwischen werden in den Bezirksämtern vermehrt *Personalcomputer* (PC) für verschiedene Anwendungen eingesetzt. Dies ist häufig unkoordiniert mit anderen Bezirken in isolierten Aufgabenbereichen aufgrund von Eigeninitiativen von Mitarbeitern geschehen. Diese an sich zu begrüßenden Initiativen bergen aus datenschutzrechtlicher Sicht erhebliche Risiken:

- Datenschutzaspekte werden bei der Entwicklung und Einführung nicht berücksichtigt, da die Datenschutzproblematik nicht bekannt oder bewußt ist und beratende Instanzen (interner Datenschutzbeauftragter, Kontaktmann für den Datenschutz, Berliner Datenschutzbeauftragter) von den Projekten nicht oder erst zu spät erfahren.
- Die Programmierung erfolgt aufgrund meist autodidaktisch erworbener Kenntnisse, die den Anforderungen ordnungsgemäßer Programmierung bei Verwaltungsverfahren nicht entsprechen, weil keine systematischen Programmier- und Testmethoden angewendet wurden.
- Die Revisionsfähigkeit ist nicht gegeben, weil weder Dokumentationen für Verfahren und Programme existieren noch Protokolle über die Verfahrensabläufe automatisch geführt werden.
- Ein formelles Freigabeverfahren, welches die Verantwortungsübernahme für die Anwendung durch die für die automatisierte Sachaufgabe verantwortlichen Personen dokumentiert, wird meist nicht durchgeführt.
- Die Funktionsfähigkeit der DV-anwendenden Stelle gerät in die Abhängigkeit von der Arbeitsfähigkeit und -bereitschaft des Programmierers.

Die Risiken werden häufig noch dadurch verstärkt, daß im Dienst privat beschaffte PCs als Arbeitshilfe eingesetzt werden. Sofern darauf personenbezogene Daten verarbeitet werden, besteht die Gefahr, daß das Bezirksamt als datenschutzrechtlicher „Herr der Daten“ sich vom „Herrn des PC“ abhängig macht. Für den Bereich der Senatsverwaltung für Inneres zum Beispiel ist bereits 1985 festgestellt worden, daß die Voraussetzungen für eine datenschutzgerechte und ordnungsgemäße Datenverarbeitung auf privaten PCs kaum geschaffen werden können und daß in Folge dessen der Einsatz privater PCs im Dienst nicht gestattet werden könne.

Für die Konzeption des technisch-organisatorischen Umfeldes bei PC-Anwendungen habe ich die Beachtung meiner „Grundsätze zum Datenschutz, Isolierte Rechner und Personalcomputer“ empfohlen, die derzeit in einer überarbeiteten Fassung vorliegen.

Bei den Prüfungen der technisch-organisatorischen Maßnahmen beim PC-Einsatz in Bezirksämtern habe ich wiederholt Mängel festgestellt. Dabei ergaben sich folgende Schwerpunkte:

- Der Zugriff auf Daten und Programme ist bei PCs, die mit dem Industriestandard-Betriebssystem MS-DOS betrieben werden, vom Betriebssystem nicht geschützt, so daß hierfür spezielle Sicherheitskomponenten eingesetzt werden müssen. Dies war häufig nicht der Fall. Inzwischen jedoch ist erkennbar, daß der Einsatz solcher zusätzlichen Sicherheitskomponenten üblich wird.

Es ist dabei allerdings zu beachten, daß organisatorisch die Zugriffsprofile der Berechtigten festgelegt und auf die Sicherheitskomponenten abgebildet werden müssen. Ich habe festgestellt, daß in einem Fall meiner Empfehlung, Paßwortverfahren einzusetzen, zwar gefolgt wurde, der Effekt jedoch wieder dadurch zunichte gemacht wurde, daß jedem Berechtigten das gleiche Paßwort zugeordnet wurde. Die häufig karikierte Möglichkeit, daß Paßworte auf einem Zettel auf dem Schreibtisch oder an der Tastatur notiert werden, habe ich auch in der Praxis vorgefunden.

- Probleme sind bei der Unterbringung und Verwaltung beweglicher Datenträger immer wieder aufgetreten. Auch die selbstverständliche Forderung nach datenschutzgerechtem Verschluß von Datenträgern wird nicht immer erfüllt. Die Sicherstellung der Vollständigkeit und der Authentizität der Datenträger ist in den seltensten Fällen gegeben. Daher kann in diesen Fällen von einer zuverlässigen Abgangskontrolle nicht die Rede sein (Nr. 2 der Anlage zu § 5 Abs. 1 BlnDSG).

- Ein schwerwiegendes und selbst von den Herstellern bisher nicht zufriedenstellend gelöstes Problem ist die Gewährleistung ordnungsgemäßer Datenverarbeitung mit PCs durch eine technisch erzwungene Funktionentrennung von System- und Programmgestalter und Benutzer. Formelle Freigabeverfahren verlieren ihren Sinn, wenn die Benutzer nach eigenem Gutdünken die Programme verändern können oder neue Standardprogrammversionen laden können. Hier hat sich beim Einsatz von PCs bei der Rücklaufkontrolle in den Ämtern für die Volkszählung 1987 die zentrale Programmbestückung der bezirklichen Ämter durch das Statistische Landesamt mit ablauffähigen, d.h. bereits kompilierten Programmen bewährt. Auf längere Sicht wird das Problem aber erst gelöst sein, wenn zuverlässige Methoden der Programmversiegelung auf dem Markt verfügbar sein werden.

Einige Bezirksämter haben inzwischen für ihren Bereich verbindliche Rahmenarbeitsanweisungen für den Einsatz von Arbeitsplatzcomputern erlassen, was ich als wesentliche Voraussetzung für eine wirksame Organisationskontrolle begrüße.

Neben den bisher behandelten Einplatz-PCs sind auch schon erste Anwendungen von Mehrplatzsystemen geprüft worden. So wird ein Mehrplatzsystem mit dem Betriebssystem SINIX (UNIX-Derivat der Fa. Siemens) in einem Bezirksamt für verschiedene Anwendungen mit und ohne personenbezogenen Daten eingesetzt, eine der Anwendungen betrifft sogar Personaldaten. Bei solchen Anwendungen ist es für eine datenschutzgerechte Gestaltung notwendig, daß die personenbezogenen Daten im Speicher verschlüsselt werden, da sonst Benutzer mit hoher Zugriffsberechtigung die Möglichkeit haben, unbefugt Daten zu lesen und zu ändern, darunter u. U. die eigenen Personaldaten.

Da davon auszugehen ist, daß Mehrplatzsysteme dieser Art oder als PC-Netze in Zukunft verstärkt multifunktional oder gar als Bürokommunikations- und -informationssysteme auch in den Bezirken eingesetzt werden, werde ich mein Augenmerk in Zukunft auf den datenschutzgerechten Einsatz solcher Systeme lenken.

Insgesamt betrachtet wird sich demnächst eine erhebliche Schwerpunktverlagerung der Automation in den Bezirksämtern hin zur individuellen Datenverarbeitung ergeben.

Dafür sprechen verschiedene Hinweise:

- Der Trend, kleinere bezirkliche Verfahren mit Hilfe von Einplatzsystemen automatisiert zu unterstützen, hält weiter an.
- Neue, zwischen den Bezirken abgestimmte Verfahren mit Hilfe von Ein- und Mehrplatzsystemen, werden für gleichartige Aufgaben in allen Bezirken eingesetzt (Beispiele: Stellenverwaltung, Lehrer-Informations- und -verwaltungssystem).
- Es besteht das politische Ziel, moderne Bürokommunikationssysteme in allen Teilen der Verwaltung, so auch in den Bezirken, einzuführen.

Im Rahmen der Neuorientierung der Datenverarbeitung in der Berliner Landesverwaltung (Orientierungsrahmen) ist festgelegt, daß die Bezirke eine verstärkte Planungshoheit - und damit natürlich auch Planungsverantwortung - für den Einsatz von Informations- und Kommunikationstechnik in ihrem Bereich erhalten sollen. Soweit bisher bekannt, wird auch der neue Senat an dieser grundsätzlichen Tendenz nichts ändern.

Dies bedeutet nicht nur, daß dafür neue, bisher meist nicht befriedigte Personal- und Qualifikationsanforderungen auf die Bezirke zukommen, die jedoch notwendig sind, um komplexere Systeme wie z. B. Bürokommunikationssysteme nutzbringend einsetzen zu können, sondern auch, daß neue datenschutzrechtliche Probleme grundsätzlicher Art bewältigt werden müssen. Dies kann auch bedeuten, daß die nach § 16 BlnDSG gebotenen personellen und organisatorischen Vorkehrungen zur Sicherstellung des Datenschutzes in den Bezirken in ihrer Wirksamkeit überprüft werden müssen.

Nicht-automatisierte Datenverarbeitung

Der weitaus größte Teil der Verwaltungstätigkeit der Bezirksämter wird mit herkömmlichen Mitteln - Akten und Karteien - erledigt. Nach § 5 Abs. 1 BlnDSG sind auch bei diesen manuellen Unterlagen technisch-organisatorische Maßnahmen zu treffen, die die Unterlagen vor unbefugtem Zugriff bewahren sollen. Die Feststellungen, die ich hierzu getroffen habe, werden sich in besonderem Maße auf andere Verwaltungen übertragen lassen.

Die *technisch-organisatorischen Maßnahmen für den Verschluss von Unterlagen* sind erst dann als ausreichend anzusehen, wenn sie den unbefugten Zugriff entweder durch die Kontrolle der Zugriffsbefugten oder durch ein Sicherheitsschloß verhindern. Dies bedeutet in der Praxis, daß Akten und Karteien mit schutzbedürftigem Inhalt in Behältnissen und Schränken unterzubringen sind, die mit einem Sicherheitsschloß ausgestattet sind und daß diese Schlösser außerhalb der Dienstzeit geschlossen sind, wenn andere Personen (z. B. Reinigungskräfte) außerhalb der Dienstzeit Zutritt zum Raum erhalten. Ist dies nicht der Fall, weil zum Beispiel nur innerhalb der Dienstzeit gereinigt wird, so reicht ein Raumverschluss mit Sicherheitsschloß aus.

Es hat sich gezeigt, daß bei Anlegung dieses Maßstabes in allen Bezirksämtern in allerdings unterschiedlichem Umfang personenbezogene Unterlagen nicht ausreichend sicher untergebracht waren. Folgende Beispiele seien dafür angeführt:

- Zwar waren die Originale von Vaterschaftsanerkennungsurkunden beim Leitenden Amtsvormund durchgängig angemessen untergebracht, die Akten in den Sachgebieten, die Abschriften dieser Urkunden als vollstreckbare Titel enthielten, wurden dagegen häufig völlig unzureichend in offenen oder nicht ausreichend verschließbaren Schränken oder in offenen Regalen untergebracht.
- In verschiedenen Fällen habe ich festgestellt, daß die Büroausstattung zwar zufriedenstellend war, daß jedoch Beschädigungen an Schranktüren, Türgriffen und Schlössern nicht behoben wurden, manchmal „damit man leichter an die Vorgänge herankommt“. Ebenso habe ich häufig festgestellt, daß zwar die Schränke mit Sicherheitsschlössern ausgestattet waren, die Schlüssel aber unauffindbar blieben, ein sicherer Beweis dafür, daß ein abendlicher Verschluss nicht stattfindet. In einem Falle waren aus ordnungsgemäßen Aktenschränken, die Unterlagen enthielten, die dem Sozialgeheimnis unterliegen, die Schiebetüren ausgebaut worden, um sie während der Dienstzeit nicht hin- und herschieben zu müssen.
- In einigen Fällen waren sensible personenbezogene Unterlagen (z. B. Wohngeldakten oder die Sozialleistungskartei) in Räumen offen untergebracht, in denen auch Kopiergeräte standen und die daher ständig von nicht zugriffsbefugten Mitarbeitern frequentiert wurden.
- Gelegentlich wurden Altakten in Kartons in Zimmerecken oder auf Schränken vorgefunden, die auf diese Weise ausgesondert waren, weil die Aktenkammer voll war. Darüberhinaus fiel häufig die überlange Aufbewahrung von Akten auf, weil Aussonderungsfristen nicht festgelegt waren.

Es fiel durchgängig auf, daß das Niveau der Akten- und Karteienunterbringung innerhalb der Bezirksämter sehr unterschiedlich ist. Meistens sind gerade die mit sensiblen Bürgerdaten arbeitenden Leistungsverwaltungen gegenüber anderen Abteilungen, die stark mit Personaldaten arbeiten, im Nachteil. Offenbar ist in Bereichen, in denen Personalvertretungen die Interessen der Bediensteten vertreten, die Sensibilität größer als dort, wo es „nur“ um den Bürger geht. Auch die Tatsache, daß Stahlschränke mit Sicherheitsschloß für die Unterbringung von Formularen verwendet werden, während wenige Türen weiter sensible Akten in offenen Regalen gelagert wurden, macht deutlich, daß dem Datenschutz nicht immer die ihm zukommende Priorität eingeräumt wird.

In diesem Zusammenhang sei auch erwähnt, daß auf die Schlüsselaufbewahrung beim Pförtner zu achten ist. Wird das Schlüsselbrett z. B. morgens in den Strom der eintreffenden Mitarbeiter zwecks Selbstbedienung gestellt, kann die Sicherheit des Raumverschlusses nicht mehr gewährleistet werden.

Analog zu Nr. 9 der Anlage zu § 5 Abs. 1 BlnDSG (bzw. § 6 Bundesdatenschutzgesetz) ist auch beim Transport personenbezogener Unterlagen für eine ausreichende *Transportkontrolle* zu sorgen. Danach ist durch technische oder organisatorische Maßnahmen unter Beachtung des Verhältnismäßigkeitsgrundsatzes sicherzustellen, daß beim Transport der Unterlagen, diese nicht unbefugt gelesen, verändert oder vernichtet werden können.

Daher stellt der *unverschlossene Versand* solcher Unterlagen einen Verstoß gegen die jeweils geltenden Datenschutzbestimmungen dar, denn die Daten können einem unüberschaubaren Personenkreis offenbart werden. Weder die Boten, noch die Bediensteten der Bundespost, noch andere im Postweg beteiligte Mitarbeiter dürfen Einsicht in solche Unterlagen erhalten.

Die Gemeinsame Geschäftsordnung der Berliner Verwaltung vom 4. Dezember 1984 sieht vor, daß Unterlagen mit zu schützenden Daten in verschlossenen Umlaufmappen oder Umschlägen zu versenden sind. Da diese Vorschriften sich naturgemäß nur an die absendenden Stellen richten, habe ich bei meinen Prüfungen vor allem darauf geachtet, in welcher Weise das geprüfte Bezirksamt seine Post versendet. Dabei habe ich regelmäßig Mängel feststellen müssen. So wurden z. B. folgende Unterlagen in vielen Fällen offen versendet: Sozialhilfeakten, Hilflösen- und Pflegegeldakten, Wohngeldakten, Erste-Hilfe-Bögen mit medizinischen Angaben, dienstliche Beurteilungen, Krank- und Gesundheitsmeldungen, Vaterschaftsfeststellungen, Erbscheine, Unfallanzeigen, Pfändungs- und Überweisungsbeschlüsse, Einweisungsbeschlüsse, Mahnbesccheide, zurückgesandte Ermittlungsakten der Staatsanwaltschaft.

Daß aufgrund der Posteingänge in manchmal noch stärkerem Umfang solche Verstöße durch Hauptverwaltungen und ihnen unterstellten Behörden (vor allem im Bereich der Justiz) festgestellt wurden, sei am Rande erwähnt.

Im Rahmen des Postverkehrs wird gelegentlich immer noch durch die Offenbarung von Daten, die eigentlich vertraulich zu behandeln sind, gegen einschlägige Rechtsvorschriften, wie etwa § 30 Verwaltungsverfahrensgesetz, § 35 SGB X oder ggf. auch §§ 5 Abs. 1, 8, 11 BlnDSG verstoßen:

- Zusatzdaten auf dem Adreßfeld, die für die postalische Zusendung nicht notwendig sind wie z. B. Geburtsdatum, -ort, Aktenzeichen, die Rückschlüsse auf die Beziehung eines Bürgers zur Verwaltung durch Dritte zulassen.
- Absenderangaben wie z. B. „Sozialpsychiatrischer Dienst“ oder „Amtsvormundschaft - Unterhaltsvorschußstelle“, mit denen in die Persönlichkeitsrechte des Empfängers eingegriffen wird.
- Kurzmitteilungen per Vordruckpostkarte mit Einladungen, Bitten um Anrufe oder Einzeldaten in Sozialhilfeangelegenheiten, die im übrigen auch gegen § 58 Abs. 1 GGO I verstoßen.

Die Überprüfung der *Raumsituation der Poststellen* erbrachte sehr unterschiedliche Ergebnisse. Häufig ist sie jedoch verbesserungsbedürftig. Neben der manchmal unzureichenden Einbruchssicherung nach außen fiel auf, daß in vielen Verteilstellen keine verschließbaren Fächerschränke für die einzelnen zu beliefernden Verwaltungseinheiten vorhanden waren, sondern in mehrere aufeinandergestapelte Körbe verteilt wird, in denen dann nach Dienstschuß die Post liegt.

Die sorgsame *Vernichtung von Datenträgern*, insbesondere Akten, ist eine wesentliche Voraussetzung für eine datenschutzgerechte Verwaltungsorganisation. Datenschutzrechtlich ist sie als besondere Form der Löschung nach § 3 Abs. 1 BlnDSG eine Phase der Datenverarbeitung. Mit der Löschung sind Daten ungeachtet der verwendeten Verfahren für immer unkenntlich zu machen. Für die Vernichtung von Datenträgern bedarf es je nach Vernichtungsart gewisser Investitionen, auf jeden Fall aber einer durchdachten Organisation, die dafür sorgt, daß zu vernichtendes Gut vollständig, sicher und ohne Risiken für die Vertraulichkeit der darauf befindlichen Daten der Vernichtung zugeführt wird. Neben Akten sind auch Karteien, Kohlepapier, Einmalfarbbänder, Adremaplatten, Disketten und Mikrofilme bei der Vernichtung zu berücksichtigen. Selbstverständlich gehören auch vertippte Briefe, überzählige Durchschläge und nicht mehr benötigte

Fotokopien dazu, Informationsträger also, die im laufenden Geschäftsbetrieb anfallen und nicht nur bei gesonderten Aktionen ausgesondert werden.

Grundsätzlich organisieren die Bezirke die Entsorgung von Datenträgern in eigener Verantwortung. Die Kontrollbesuche in den Bezirken ergaben, daß alle Bezirksämter Vorkehrungen zur Aktenvernichtung getroffen hatten, daß aber Mängel verschiedenster Art immer wieder festgestellt werden mußten.

Anlagen zur Vernichtung von Akten und anderen papierenen Unterlagen (Reißwölfe, Shredder) werden in den meisten Bezirken eingesetzt. Bis auf wenige Ausnahmen jedoch entsprachen sie zur Zeit der Kontrollbesuche nicht den Anforderungen, die unter Berücksichtigung des Standes der Technik zu verlangen wären. Häufig wurden Reißwölfe vorgefunden, die eine Schnittbreite von 6 oder 8 mm aufwiesen, was nicht dafür ausreicht, um die Unterlagen als vollständig vernichtet anzusehen. Da bis vor einiger Zeit Reißwölfe, die die einem Bezirksamt angemessene Kapazität aufweisen, nur mit Schnittbreiten ab 4 mm auf dem Markt erhältlich waren, habe ich empfohlen, dies als Maßstab zu erachten. Im Herbst 1985 trat jedoch die DIN-Norm 32757, Teil 1 über die Vernichtung von Informationsträgern in Kraft. Dort werden in bezug auf die Partikelgrößen fünf Sicherheitsstufen unterschieden. Die dort definierte Sicherheitsstufe 3 wird von ausreichend dimensionierten Reißwölfen mittlerweile erreicht und sollte daher für personenbezogene Unterlagen angestrebt werden: Schnittbreite bis 2 mm oder bis 4 mm, dann aber höchstens 60 mm lang. Ähnliche Aussagen macht die Norm auch für die Vernichtung von Mikrofilmen und anderen Datenträgern.

Ich habe nur in einem Fall eine normgerechte Vernichtungsanlage für die zentrale Vernichtung in einem Bezirksamt vorgefunden. Ich gehe davon aus, daß die Sicherheitsstufe 3 der DIN-Norm 32757 bei künftigen Ausschreibungen verbindlich sein wird.

Die Beachtung der Norm ist allerdings keine Garantie für die ordnungsgemäße Aktenvernichtung. Die beste Technik nützt z. B. nichts, wenn das unverrichtete Gut neben dem allgemein zugänglichen Reißwolf zwischengelagert wird.

In vielen Fällen lassen Bezirksämter ihre Unterlagen unter ihrer Aufsicht in der Müllverbrennungsanlage der Berliner Stadtreinigungs-Betriebe in Ruhleben verbrennen. Diese Art der Aktenvernichtung entspricht zwar nicht dem Recycling-Gedanken, ist jedoch aus Sicht des Datenschutzes optimal.

Einige Bezirksämter lassen die Informationsträger im Rahmen von Auftragsdatenverarbeitung nach § 2 Abs. 1 BlnDSG von Fremdfirmen vernichten. Die datenschutzrechtliche Verantwortung bleibt jedoch bei den Auftraggebern. Deshalb bedarf es bei der Vernichtung durch Fremdfirmen sorgfältiger Vertragsgestaltung und geeigneter Kontrollen, die die ordnungsgemäße Aktenvernichtung in ausreichendem Maße sicherstellen. Dieses habe ich jedoch nicht immer vorgefunden.

Ich habe für die Datenträgervernichtung Empfehlungen in einem Faltblatt²²⁾ zusammengefaßt, das bei mir erhältlich ist.

Allgemeine Feststellungen

Bei den Kontrollbesuchen war die Frage nach der Sicherstellung des Datenschutzes im Bezirksamt im Sinne des § 16 BlnDSG durch die Verantwortlichen einer der Schwerpunkte. Dabei standen die Einhaltung der Ordnungsmäßigkeit der Datenverarbeitung und die Führung der internen Dateienübersicht im Vordergrund. Auch die im Gesetz nicht explizit geforderte, aber aus den Bestimmungen des § 16 BlnDSG abzuleitende und in der Praxis auch bewährte Benennung einer Kontaktperson für den Datenschutz wurde sowohl hinsichtlich der Akzeptanz dieser Funktion durch die Vorgesetzten als auch der praktischen Umsetzung der neuartigen Aufgabe durch die damit betrauten Personen untersucht.

In zwei Bezirksämtern wurden vorbildliche Lösungen vorgefunden: Durch eine Geschäftsanweisung für die Organisation des Datenschutzes wurden die Kontaktpersonen und die Datenschutzbeauftragten nach SGB X benannt. Neben einer detaillierten Aufgabenbeschreibung für diese Personen wurde bestimmt, daß in allen Abteilungen der Bezirksämter spezielle Kontakte auf Datenschutzbelange achten und mit der Kontaktperson oder mit dem internen Datenschutzbeauftragten eng zusammenarbeiten sollen.

Bedingt durch unterschiedliche personelle und organisatorische Voraussetzungen haben die Kontaktpersonen für den Datenschutz und die Datenschutzbeauftragten nach SGB X ihre Aufgabe unterschiedlich, aber überwiegend zufriedenstellend wahrnehmen können. Einige ließen sich durch frühzeitigen Kontakt mit meiner Dienststelle bei der Lösung ihrer Probleme unterstützen. In einzelnen Fällen wurden von den internen Datenschutzinstanzen von sich aus datenschutzbezogene Überprüfungen im eigenen Hause durchgeführt.

In allen Fällen wurden die nach § 16 Satz 2 Nr. 1 BlnDSG vorgeschriebenen Dateienübersichten geführt. Die Qualität dieser Übersichten ließ jedoch in vielen Fällen zu wünschen übrig. Da die speichernden Stellen innerhalb des Bezirksamtes teils schleppend, teils unvollständig an die Kontaktperson für den Datenschutz melden, konnte die notwendige Aktualität und Vollständigkeit in vielen Fällen nicht erreicht werden.

Mehrere Bezirksämter haben für die Erfassung der ihnen zu meldenden Dateien und Karteien eigene Formblätter entwickelt, die zumindest die erforderlichen Informationen übersichtlich und einheitlich dokumentieren.

In diesem Zusammenhang ist zu betonen, daß gerade auch für die Verantwortlichen in den Bezirksämtern die interne Dateienübersicht nach § 16 Satz 2 Nr. 1 BlnDSG ein notwendiges Instrument zur Überprüfung des Datenschutzes und der Ordnungsmäßigkeit der Datenverarbeitung in ihrem Hause ist. Es zeigte sich bei allen Prüfungen, daß die Qualität der Arbeit der internen Datenschutzinstanzen, ihre Akzeptanz bei den Verantwortlichen und die Qualität der internen Dateienübersicht in auffälliger Weise mit dem Gesamteindruck bei meinen datenschutzrechtlichen Kontrollbesuchen korrelierten.

5. Nachträge zu Feststellungen aus den Vorjahren

Nutzung des Melderegisters in Bußgeldverfahren (Jahresbericht 1988, Ziff. 4.5)

Bei der Überprüfung der Anschrift solcher Personen, denen Anhörungsbogen in Bußgeldverfahren bei der Volkszählung nicht zugestellt werden konnte, hat das Landeseinwohneramt entgegen meiner ursprünglichen Annahme die entsprechenden Auskünfte an das Statistische Landesamt protokolliert, weil in diesen Fällen auch das Geburtsdatum übermittelt wurde. Damit ist die melderechtlich gebotene Übermittlungskontrolle eingehalten worden. Dennoch halte ich eine Änderung des Meldegesetzes und die Einführung einer Protokollierungspflicht auch in solchen Fällen für geboten, in denen öffentliche Stellen einfache Melderegisterauskünfte erteilt werden. Werden privaten Personen einfache Melderegisterauskünfte erteilt, sollte nur die Tatsache des Zugriffs auf den einzelnen Datensatz, nicht aber der Name des Empfängers protokolliert werden.

Prüfung der Datenverarbeitung im Berliner Gesundheitswesen (Jahresbericht 1987 Ziff. 3.3 und Jahresbericht 1988 Ziff. 4.4)

Nachdem von Seiten der Gesellschaft für Systemforschung und Dienstleistungen im Gesundheitswesen mbH (GSD) und der Berliner Krankenhausbetriebe alle datenschutzrechtlichen Forderungen, welche sich aus der Überprüfung 1987/88 ergaben und die durch das vom Senat in Auftrag gegebene Gutachten weitgehend bestätigt wurden, bereits realisiert oder zugesagt worden sind, blieb noch der Punkt der weitgehenden Vernetzung der Krankenhausbetriebe untereinander und zum Rechenzentrum der GSD offen.

²²⁾ vgl. auch Jahresbericht 1988, Anlage 8

Um die von mir geforderte Abschottung der einzelnen Krankenhausdatenbestände untereinander und zur GSD zu gewährleisten, wird jeder Krankenhausbetrieb mit einem eigenen Rechner mit der jeweils notwendigen Kapazität ausgestattet. Diese Rechner sollen jedoch, um eine kostengünstige Gesamtadministration zu ermöglichen und auch evtl. für diese Aufgabe fehlendes Fachpersonal bei den Krankenhausbetrieben zu ersetzen, mit dem GSD-Rechenzentrum über Datenverarbeitungsleitungen verbunden werden. Dieser Lösung habe ich unter folgenden Voraussetzungen zugestimmt, daß

- über diese Leitungen nur Betriebsdaten (Fehler-, Netzzustandsdaten) für die Fehlererkennung und die Gesamtadministration zur GSD übertragen werden können,
- von den Systemspezialisten der GSD keine Datenbestände der Krankenhausbetriebe über diese Leitungen abgefragt werden können,
- geänderte oder neue Programme zwar über diese Leitungen zu den jeweiligen KHB übertragen werden können, aber die Freigabe nur durch deren Mitarbeiter erfolgen kann,
- festgestellte Fehler, die nicht von den Angestellten der Krankenhausbetriebe beseitigt werden können, nur im Rechenzentrum des jeweiligen KHB durch Mitarbeiter der GSD beseitigt werden dürfen (das Fachpersonal oder die Krankenhausführung sind zu verständigen).

Darüber hinaus soll ich bei der schrittweisen Realisierung dieses Konzeptes informiert und beteiligt werden.

Verwaltungsnetz

(Jahresbericht 1987, Ziff. 3.1; 1988, Ziff. 4.1)

Das Verwaltungsnetz der Berliner Verwaltung hat sich in der vorgesehenen Form als nicht realisierbar erwiesen. Aus diesem Grunde wurde der Auftrag an die installierende Firma vertraglich aufgelöst. Eine schlüssige Neuplanung liegt noch nicht vor. Zu dieser werde ich dann zu gegebener Zeit an Hand der bereits beim ersten Projekt definierten datenschutzrechtlichen Gestaltungskriterien Stellung beziehen.

Forschung mit Sozialdaten

(Jahresbericht 1988, Ziff. 4.4)

Das Forschungsprojekt über die „Lebenssituation von Sozialhilfeempfängern“ zum Thema „Wege aus der Sozialhilfe“ wurde im Auftrag der Senatsverwaltung für Gesundheit und Soziales entsprechend meinen Empfehlungen datenschutzrechtlich durchgeführt. Die Sozialhilfeempfänger in drei Bezirken wurden von den Sozialämtern angeschrieben und konnten selbst entscheiden, ob sie sich im Rahmen dieses Forschungsprojekts befragen lassen wollten. Sie wurden dabei ausdrücklich darauf hingewiesen, daß sie bei einer Nichtteilnahme keine - sozialhilferechtlichen oder sonstigen - Nachteile zu befürchten haben. Die teilnahmeberechtigten Sozialhilfeempfänger sandten Rückantwortkarten an das private Sozialforschungsinstitut, das diese wiederum den Sozialämtern zur Verfügung stellte, damit dort die Namen aus einer Adreßliste für Erinnerungsschreiben gestrichen werden konnten. Nur diejenigen Personen, die nicht reagiert hatten, wurden schriftlich erinnert, wobei jeweils auf die Freiwilligkeit der Teilnahme hingewiesen wurde. Ich begrüße es, daß die Forscher nach anfänglichem Widerstand meine Vorschläge für ein datenschutzgerechtes Erhebungsverfahren in vollem Umfang umgesetzt haben.

Todesursachenstatistik

(Jahresbericht 1988, Ziff. 4.5)

Die Senatsverwaltung für Inneres wird vor der von mir für erforderlich gehaltenen Änderung des Berichtsweges in der Todesursachenstatistik die Novellierung des Bevölkerungsstatistikgesetzes auf Bundesebene abwarten. Dem habe ich in der Erwartung zugestimmt, daß das Bevölkerungsstatistikgesetz noch in dieser Legislaturperiode den Vorgaben des Bundesverfassungsgerichts angepaßt wird. Ein entsprechender Beschluß der Bundesregierung liegt bereits vor.

6. Zusammenarbeit mit anderen Stellen

Europäische Zusammenarbeit

Aufgrund des mir auf der 11. Internationalen Konferenz der Datenschutzbeauftragten erteilten Mandats als Vorsitzender des ständigen Ausschusses für Telekommunikation habe ich Kontakte mit der Zuständigen Generaldirektion XIII der EG vorbereitet. Ziel meiner Bemühungen ist es, ein Verfahren mit der EG zu erreichen, das die Beteiligung des Datenschutzes vor Erlaß von Richtlinien und vor der Förderung von Telekommunikationsprojekten sicherstellt. In dem zuständigen Ausschuß sollen konkrete Vorschläge für eine entsprechende Regelung ausgearbeitet werden.

Konferenz der Datenschutzbeauftragten

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat in drei Sitzungen unter Vorsitz des Datenschutzbeauftragten des Saarlandes beraten.

36. Konferenz am 5./6. April 1989

- Entschließung zur Neuregelung des Bundesdatenschutzgesetzes
- Entschließung zum Entwurf eines Rentenreformgesetzes
- Entschließung zu § 100 a StPO

37. Konferenz am 30. Mai 1989

- Entschließung zu den Entwürfen eines Bundesverfassungsschutzgesetzes, eines MAD-Gesetzes und eines BND-Gesetzes

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

Abgeordnetenhaus

Die Behandlung von Datenschutzproblemen in den Ausschüssen des Abgeordnetenhauses sowie den Gesprächen mit Fraktionen und einzelnen Abgeordneten wurde durch den Wechsel der Legislaturperiode bestimmt. In der alten Legislaturperiode habe ich insbesondere den *Untersuchungsausschuß zur Aufklärung von möglichen Fehlentwicklungen beim Landesamt für Verfassungsschutz* unterstützt. Dabei handelte es sich einmal um eine technische Unterstützung bei der Überprüfung von Daten durch den Ausschuß sowie um eine Stellungnahme über das Ergebnis meiner Überprüfungen der Behandlung personenbezogener Daten in Zusammenhang mit der Publikation „die tageszeitung“ beim Landesamt für Verfassungsschutz. Darüber habe ich ausführlich oben unter 2.2 berichtet.

In der neuen Legislaturperiode habe ich mich in dem *Rechtsausschuß* vor allem gegen Teile der Novellierung des Verfassungsschutzgesetzes gewandt, die aus meiner Sicht die Wahrung der Persönlichkeitsrechte der Betroffenen nicht hinlänglich garantieren. (vgl. dazu im einzelnen oben unter 2.2)

Im *Unterausschuß Datenschutz* wurde vor allem der Jahresbericht 1988 erörtert. Im Ausschuß wurde insbesondere deutlich, daß es nicht mehr länger hingenommen werden kann, wenn seit Jahren angemahnte Gesetze, wie das Archiv- und das Statistikgesetz noch immer nicht in das Abgeordnetenhaus eingebracht worden sind.

Ferner beschäftigte sich der Unterausschuß mit der Anhörung der für das Amt des Berliner Datenschutzbeauftragten in die engere Wahl gekommenen Bewerber.

Aufsichtsbehörde nach dem Bundesdatenschutzgesetz

Die gute Zusammenarbeit mit der Aufsichtsbehörde für den Datenschutz bei der Senatsverwaltung für Inneres wurde fortgesetzt. Gegenstand der Abstimmung waren vor allem: Das Landesstatistikgesetz, die Änderung des Verfassungsschutzgesetzes, Datenschutz beim Einsatz neuer Telekommunikations- und

Bürokommunikationssysteme, die Neufassung des Berliner Datenschutzgesetzes, die Notwendigkeit der Schaffung eines Datenverarbeitungsgesetzes und der Datenschutz bei der Personaldatenverarbeitung.

Meldungen zum Dateienregister

Das von mir zu führende Dateienregister enthält nunmehr 1782 (Stand 30. September 1989) Dateien (Vorjahr: 1726) von 398 (372) Stellen. Für interessierte Bürger und öffentliche Stellen steht eine Zusammenfassung des Dateienregisters zur Verfügung. Eine aktualisierte Neuauflage wird im Frühjahr 1990 vorliegen.

Berlin, 27. Oktober 1989

Dr. Hans-Joachim Kerkau

Anlagen (Übersicht)

1. Entschlieungen der Konferenz der Datenschutzbeauftragten des Bundes und der Lnder sowie der Datenschutzkommission Rheinland-Pfalz
 - 1.1 Entschlieung vom 5./6. April 1989 zum Strafverfahrensnderungsgesetz vom 3. November 1988
 - 1.2 Entschlieung zur Neuregelung des Bundesdatenschutzgesetzes vom 5./6. April 1989
 - 1.3 Entschlieung zum Entwurf eines Rentenreformgesetzes vom 5./6. April 1989
 - 1.4 Entschlieung zu § 100 a StPO vom 5./6. Mai 1989
 - 1.5 Entschlieung zu den Entwrfen eines Bundesverfassungsschutzgesetzes, eines MAD-Gesetzes und eines BND-Gesetzes vom 30. Mai 1989
2. Beschlsse der Internationalen Konferenz der Datenschutzbeauftragten
 - 2.1 Berliner Resolution der 11. Internationalen Konferenz der Datenschutzbeauftragten vom 30. August 1989
 - 2.2 Zusatzerklrung der Datenschutzbeauftragten der EG-Lnder
 - 2.3 Entschlieung der 11. Internationalen Konferenz der Datenschutzbeauftragten vom 30. August 1989 ber die Arbeitsgruppe Telekommunikation und Medien
 - 2.4 Beschlu der 11. Internationalen Konferenz der Datenschutzbeauftragten vom 30. August 1989 zu ISDN auf Vorschlag der Arbeitsgruppe Telekommunikation und Medien
3. Empfehlungen fr den datenschutzgerechten Einsatz von UNIX-Systemen

Anlage 1.1

**Entschließung
der Konferenz der Datenschutzbeauftragten
des Bundes und der Länder
* und der Datenschutzkommission Rheinland-Pfalz
vom 5./6. April 1989
zum Entwurf eines Gesetzes zur Änderung und Ergänzung
des Strafverfahrensrechts
(Strafverfahrensänderungsgesetz vom 3. November 1988)**

Die Konferenz begrüßt, daß ein Entwurf zur Regelung des Datenschutzes im Strafverfahrensrecht vorgelegt worden ist und daß darin für die besonderen Ermittlungs- und Fahndungsmethoden eigenständige Befugnisnormen vorgesehen sind sowie Regelungen zur Verarbeitung personenbezogener Daten und zur Akteneinsicht in die Strafprozeßordnung aufgenommen werden sollen.

Die im Entwurf vorgesehenen Datenschutzregelungen sind an den verfassungsrechtlichen Grundsätzen der Verhältnismäßigkeit und Normenklarheit zu messen. Weil im Bereich der Grundrechtsausübung nach der Rechtsprechung des Bundesverfassungsgerichts alle wesentlichen Entscheidungen vom Gesetzgeber selbst zu treffen sind, ist die gesamte Informationsverarbeitung wegen ihres Eingriffscharakters in der Strafprozeßordnung präzise und umfassend gesetzlich zu regeln.

Der vorliegende Entwurf entspricht den sich aus dem Recht auf informationelle Selbstbestimmung ergebenden Anforderungen noch nicht; er ist im übrigen unvollständig. Die Datenschutzkonferenz hebt deshalb unter gleichzeitiger Bezugnahme auf ihren Beschluß vom November 1986 folgende Kritikpunkte hervor:

1. Zu den Regelungen über die Ermittlungs- und Fahndungsmethoden

- Die Erhebung und Weiterverarbeitung personenbezogener Daten durch Strafverfolgungsorgane greift empfindlich in das Persönlichkeitsrecht der Bürger ein. Umso wichtiger ist es, nach dem Grad der Betroffenheit im Gesetz Abstufungen vorzunehmen. Zwischen dem Beschuldigten, dem Verdächtigen, dem von Vorfeldermittlungen Betroffenen und dem erkennbar nicht Verdächtigen (z. B. Geschädigten, Zeugen) sollte daher unterschieden werden. Vor allem die Regelungen über „Kontakt- und Begleitpersonen“, „andere Personen“ und „Dritte“ werden dem nicht gerecht.
- Es muß klargestellt werden, daß die Ermittlungsgeneralklausel keine Eingriffe gestattet, die in ihrer Eingriffstiefe den besonders geregelten gleichkommen. So wären z. B. die Voraussetzungen des Einsatzes von V-Leuten besonders zu regeln. Auch weiterentwickelte „besondere Fahndungs- und Ermittlungsmethoden“ dürfen nicht auf die Ermittlungsgeneralklausel gestützt werden. In die Strafprozeßordnung sind Verfahrensregelungen aufzunehmen, die eine Information etwa der zuständigen Parlamentsausschüsse über die beabsichtigte Anwendung vorsehen. Vor dem Einsatz qualitativ neuer Methoden müssen auf jeden Fall gesetzliche Regelungen geschaffen werden.
- Der Entwurf betont zu recht, daß bei jeder einzelnen Ermittlungs- und Datenverarbeitungsmaßnahme der Grundsatz der Verhältnismäßigkeit zu beachten ist. Dies muß bereits in einzelnen Befugnisnormen zum Ausdruck kommen. Die bislang vorgesehenen Straftatenkataloge sind mit dem Ziel einer Einschränkung zu überprüfen; die bloße Anknüpfung an den Begriff der „Straftat mit erheblicher Bedeutung“ ohne weitere Differenzierung reicht nicht aus.
- Die Anordnung von Ermittlungs- und Fahndungsmethoden, die besonders stark in das Recht auf informationelle Selbstbestimmung eingreifen, ist dem Richter vorzubehalten. Gleiches gilt, wenn mit solchen besonderen Methoden erhobene Daten für andere Strafverfahren oder für andere - polizeiliche - Zwecke verwendet werden sollen.

- Wegen der Tiefe der Eingriffe bei besonderen Ermittlungs- und Fahndungsmethoden darf der Richtervorbehalt - von besonderen Eilfällen abgesehen - nicht durch Entscheidungen der Staatsanwaltschaft oder der Polizei ersetzt werden. Soweit ausnahmsweise die Staatsanwaltschaft oder die Polizei eine Anordnung treffen muß, dürfen erlangte Daten nicht weiter verwendet werden, wenn die richterliche Bestätigung ausbleibt; erhobene Daten sind zu löschen.
- Die Verwendung von durch besondere Ermittlungs- oder Fahndungsmethoden erlangten Daten für polizeiliche Zwecke muß neben dem Richtervorbehalt voraussetzen, daß das Polizeirecht vergleichbare Eingriffe gestattet oder daß die Daten zur Abwehr einer gegenwärtigen Gefahr für Leib oder Leben erforderlich sind.

2. Zu den besonderen Regelungen über die Datenverarbeitung

Regelungen über die Datenverarbeitung im Strafverfahren setzen eine Gesamtkonzeption über die Informationsverarbeitung bei den Strafverfolgungsbehörden voraus. Notwendig sind insbesondere klare Bestimmungen über die Zusammenarbeit zwischen Staatsanwaltschaft und Polizei. Der vorliegende Entwurf läßt den hierzu notwendigen Konsens jedoch nicht erkennen.

- Der Gesetzgeber sollte möglichst genau regeln, welche Arten von Daten für „Zwecke des Strafverfahrens“, für Zwecke anderer Strafverfahren oder für die Aufklärung künftiger Straftaten in automatisierten Dateien landes- oder bundesweit zur Verfügung stehen sollen und in welchem Verhältnis hierzu das Bundeszentralregister steht.
- Der Gesetzgeber muß, auch um Doppelspeicherungen zwischen staatsanwaltschaftlichen und polizeilichen Informationssystemen zu vermeiden, eindeutig festlegen, wem die Entscheidungsbefugnis über die bei der Strafverfolgung angefallenen Daten zusteht und für welche Zwecke sie verwendet werden dürfen.
- Daten, die für bloße Tätigkeitsnachweise gespeichert werden (Vorgangsverwaltung), dürfen für andere Zwecke nicht verwendet werden und müssen nach kurzen Fristen gelöscht werden.
- Die vorgesehene Speicherung von Daten über Personen, die „bei einer künftigen Strafverfolgung als Zeugen in Betracht kommen“, oder die „Opfer einer Straftat werden könnten“, gibt zu Bedenken Anlaß, weil das Anlegen von Dateien über besondere Personengruppen wie z. B. Prostituierte, Homosexuelle und ausländische Gastwirte als erlaubt angesehen werden könnte.
- Die Datenspeicherung über Personen, die mangels hinreichendem Tatverdacht freigesprochen worden sind oder bei denen das Ermittlungsverfahren eingestellt oder die Anklage nicht zugelassen worden ist, darf nur unter engeren Voraussetzungen erfolgen.

3. Zur Akteneinsicht

Strafakten sind wegen ihres teilweise sehr sensiblen Inhalts geheimzuhalten. Sie dürfen deshalb auch anderen öffentlichen Stellen nur unter engeren Voraussetzungen zugänglich sein. Nicht am Strafverfahren beteiligte Personen dürfen auch über Rechtsanwälte allenfalls in besonderen Ausnahmefällen Einsicht oder Auskunft aus Strafakten erhalten.

4. Fehlende Regelungen

Regelungsbedürftig sind außerdem vor allem:

- die engere Festlegung der Zulässigkeit erkennungsdienstlicher Behandlungen und der Voraussetzungen für den Fahndungsabgleich sowie die weitere Verwendung der dabei gewonnenen Daten,
- die Verbesserung des Schutzes der Persönlichkeitsrechte bei der Erhebung persönlicher Daten von Angeklagten und Zeugen in Strafverfahren,
- der allenfalls begrenzte Einsatz der Genomanalyse im Strafverfahren.

Anlage 1.2

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder sowie der Datenschutzkommission Rheinland-Pfalz hat bei Stimmhaltung von Bayern in ihrer Sitzung vom 5./6. April 1989 zur

Neuregelung des Bundesdatenschutzgesetzes

folgende Entschließung gefaßt:

1. Die Datenschutzbeauftragten begrüßen die Beschlüsse des Bundesrates zur Neufassung des Bundesdatenschutzgesetzes. Sie sehen darin eine Bestätigung ihrer bisher dazu vertretenen Meinung und erinnern an ihre Beschlüsse vom 14. März 1986 und vom 6. Juni 1988.
2. Die Datenschutzbeauftragten betonen nochmals die Notwendigkeit,
 - die Datenerhebung im Bundesdatenschutzgesetz zu regeln;
 - die Verarbeitung personenbezogener Daten in Akten in das Bundesdatenschutzgesetz einzubeziehen;
 - die lückenlose Kontrolle durch die Datenschutzbeauftragten zu gewährleisten;
 - im öffentlichen und nicht-öffentlichen Bereich, ungeachtet aller erforderlichen Differenzierung, einen gleichwertigen Datenschutz sicherzustellen.
3. Die Datenschutzbeauftragten weisen schließlich mit Nachdruck darauf hin, daß eine Verabschiedung des Regierungsentwurfs ohne die gebotene Nachbesserung, aber auch eine weitere Verzögerung des Gesetzgebungsvorhabens die Gefahr einer Rechtszersplitterung verstärken würde, die sich schon jetzt deutlich abzeichnet.

Anlage 1.3

**Entschließung
der Konferenz der Datenschutzbeauftragten
des Bundes und der Länder
sowie der Datenschutzkommission Rheinland-Pfalz
vom 5./6. April 1989
zum Entwurf eines Renten-Reform-Gesetzes 1992**

Die Rentenversicherung erfaßt den weit überwiegenden Teil der Bevölkerung mit Daten über das Einkommen sowie über familiäre und gesundheitliche Verhältnisse. Sowohl Pflichtmitglieder als auch freiwillige Versicherte haben nur einen sehr begrenzten Einfluß auf die Erhebung, Speicherung, Verwendung und Weitergabe ihrer Daten. Dies führt zu Eingriffen in das Recht auf informationelle Selbstbestimmung, die einer verfassungsmäßigen gesetzlichen Grundlage bedürfen.

Der Zwang zur Angabe personenbezogener Daten im Rahmen des Versicherungsverhältnisses setzt voraus, daß der Gesetzgeber den Verwendungszweck sowie Art und Umfang der erforderlichen Daten präzise bestimmt. Die Verwendung der Daten ist grundsätzlich auf den gesetzlich bestimmten Zweck zu begrenzen. Bei Anwendung dieser Grundsätze sind zur Verbesserung des Datenschutzes Änderungen oder Ergänzungen des Rentenreformgesetzes notwendig. Dies gilt insbesondere in folgenden Punkten:

1. Für die Erhebung, Verarbeitung und Offenbarung von Versicherungsdaten, insbesondere von Gesundheitsdaten, bedarf es konkreter Befugnisnormen, die auf die verschiedenen Aufgaben der Rentenversicherungsträger abstellen.
2. Um die zweckgebundene Verwendung der Versicherten-daten sicherzustellen, müssen auch die Aufgaben der Rentenversicherung normenklar und übersichtlich im Gesetz dargestellt werden.
3. In das Gesetz sollten Regelungen über Aufbewahrungs- und Löschungsfristen aufgenommen werden.

4. Im Gesetz ist klarzustellen,
 - welche versicherungserheblichen Daten im Versicherungskonto gespeichert werden dürfen;
 - welche Stellen am sogenannten Rentenauskunftsverfahren teilnehmen und worüber Auskünfte erteilt werden;
 - welche Aufgaben der Deutschen Bundespost im Zusammenhang mit der Rentenversicherung obliegen und welche Datenübermittlungen zwischen Rentenversicherungsträgern, Bundespost und anderen Beteiligten erfolgen;
 - welche Daten in der Zentraldatei bei der Datenstelle der Rentenversicherungsträger (VDR) geführt werden und wer auf diese Daten Zugriff hat.
5. Um für die eigenen Mitarbeiter der Rentenversicherungsträger den Sozial- und Personaldatenschutz zu gewährleisten, sollte die organisatorische und personelle Trennung der Sachbearbeitung von der Personaldatenverarbeitung vorgeschrieben werden.
6. Eine eindeutige Klarstellung der Rechtsaufsicht und der Datenschutzkontrolle über die Datenstelle der Rentenversicherungsträger ist erforderlich.

Anlage 1.4

**Entschließung
der Konferenz der Datenschutzbeauftragten
des Bundes und der Länder
sowie der Datenschutzkommission Rheinland-Pfalz
vom 5./6. April 1989
zu den Änderungen des Gesetzes
zu Artikel 10 GG und der Strafprozeßordnung
im Rahmen der Poststrukturreform**

Der im Rahmen der Ausschußberatungen zur Poststrukturreform aus den Reihen des Bundestages eingebrachte Entwurf zur Änderung des Gesetzes zu Artikel 10 GG (Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses) soll die Verfassungsschutzbehörden des Bundes und der Länder, den Militärischen Abschirmdienst und den Bundesnachrichtendienst u. a. dazu ermächtigen, den Fernmeldeverkehr zu überwachen und aufzuzeichnen. Bisher war den Diensten nach dem Gesetz zu Artikel 10 GG nur gestattet, „den Fernschreibverkehr mitzulesen, den Fernmeldeverkehr abzuhören und auf Tonträger aufzunehmen“. Auch die Überwachungsvorschriften der Strafprozeßordnung (§§ 100 a, 100 b) sollen entsprechend verändert werden.

Während in der Vergangenheit neben dem Briefverkehr nur Telefongespräche und Fernschreiben kontrolliert und ausgewertet werden durften, soll dies nach dem Entwurf in Zukunft für den gesamten Fernmeldeverkehr (z. B. Btx, Temex, Telefax, Datel-Dienste, ISDN) zulässig sein. Daraus ließe sich ableiten, daß auch Abrechnungs-, Verbindungs- und Nutzungsdaten sowie im Rahmen elektronischer Dienste gespeicherte Inhaltsdaten (z. B. bei Mailboxen, Btx usw.) kontrolliert werden dürfen. Damit würde jedenfalls für den Bereich der Strafprozeßordnung auch eine rückwirkende Kontrolle legalisiert. Nicht auszuschließen ist außerdem, daß Dienstbetreiber dazu verpflichtet werden, für Überwachungszwecke in größerem Umfang Daten zu speichern, als für ihre betrieblichen Belange erforderlich und zulässig ist.

Die Datenschutzbeauftragten sind deshalb der Auffassung, daß derart weitgehende Eingriffe in Grundrechte einer gründlichen Prüfung durch alle Beteiligten bedürfen. Deshalb sollten im Rahmen der vom Bundestag als dringlich angesehenen Poststrukturreform das Gesetz zu Artikel 10 GG und die Strafprozeßordnung nur insoweit geändert werden, als dies in einem unmittelbaren Zusammenhang zu den geplanten ordnungspolitischen Änderungen der Telekommunikation steht. In Betracht käme insofern lediglich die Einbeziehung der Betreiber privater Telekommunikationsdienste in die Regelungen, die bislang nur für die Post gelten.

Anlage 1.5

**Entscheidung
der Konferenz der Datenschutzbeauftragten
des Bundes und der Länder
und der Datenschutzkommission Rheinland-Pfalz
zu den Entwürfen eines Bundesverfassungsschutzgesetzes
(BVerfSchG), eines MAD-Gesetzes (MADG)
und eines BND-Gesetzes (BNDG)
vom 30. Mai 1989**

I.

Mit den von der Bundesregierung vorgelegten Entwürfen sollen die nach der Rechtsprechung des Bundesverfassungsgerichts erforderlichen bereichsspezifischen Rechtsgrundlagen für die Informationsverarbeitung der Verfassungsschutzbehörden und Nachrichtendienste geschaffen werden. So dringend die Beseitigung der bestehenden Regelungsdefizite auch ist, müssen sich neue Gesetze gerade in diesem Bereich in besonderem Maße daran messen lassen, daß in die Freiheitsrechte der Bürger nicht unverhältnismäßig eingegriffen wird. Dieser Vorgabe werden auch die nunmehr vorgelegten Entwürfe in vielerlei Hinsicht nicht gerecht.

II.

1. Da sich der zulässige Umfang der Informationsverarbeitung nach den Aufgaben der datenverarbeitenden Stelle bemißt, bedarf es einer abschließenden, möglichst genauen gesetzlichen Beschreibung dieser Aufgaben. Für den Einzelnen muß erkennbar sein, wann er die Schwelle von der Ausübung der Grundrechte zur verfassungsfeindlichen Bestrebung überschreitet. Die in § 3 Abs. 1 verwendeten Begriffe, wie etwa „Bestrebungen gegen die freiheitliche demokratische Grundordnung“ oder „Gefährdung auswärtiger Belange“ stellen dies nicht sicher. Insbesondere bleibt unklar,
 - ob der Begriff der Bestrebungen das Handeln einer Mehrzahl von Personen in einem gewissen Grad von Organisation voraussetzt oder auch das Tätigwerden einer einzelnen Person beinhaltet;
 - ob es zulässig sein soll, Informationen auch über solche Bestrebungen zu sammeln und zu speichern, die erkennbar nicht gegen die freiheitliche demokratische Grundordnung gerichtet sind, an denen aber Personen beteiligt sind, die an anderen gegen diese Grundordnung gerichteten Bestrebungen mitwirken;
 - ob und gegebenenfalls in welchem Umfang Informationen über nicht extremistische Organisationen gesammelt und gespeichert werden dürfen, die Gegenstand extremistischer Beeinflussung(-versuche) sind.

Zur weiteren Umschreibung der Aufgaben könnte auch der Inhalt von § 92 StGB mit herangezogen werden.

2. Bei einer derartig vagen Umschreibung der Aufgaben wäre es um so notwendiger, die Voraussetzungen für die Erhebung, Speicherung und sonstige Verwendung personenbezogener Daten je nach dem, welche seiner ganz unterschiedlichen Aufgaben (Spionageabwehr, Extremismus- und Terrorismusbeobachtung, Sicherheitsüberprüfung) der Verfassungsschutz wahrnimmt, differenziert, präzise und für den Bürger transparent zu regeln. Stattdessen sieht der Entwurf pauschale Befugnisse für den Verfassungsschutz vor. Außerdem fehlen Regelungen darüber, ob und gegebenenfalls in welchem Umfang, für welche Zwecke und mit welchen Speicherungsfristen Daten über unverdächtige und unbeteiligte Personen erhoben und gespeichert werden dürfen.
3. Unklar ist, welche rechtlichen Grenzen dem Einsatz nachrichtendienstlicher Mittel gesetzt sind. Außerdem muß klar gestellt werden, daß die Befugnis zum Einsatz nachrichtendienstlicher Mittel kein genereller Rechtfertigungsgrund für Verstöße gegen Straftatbestände ist, gegen wen sich der Einsatz nachrichtendienstlicher Mittel richten darf und was mit den gegebenenfalls dabei über Unverdächtige gewonnenen Daten geschehen darf. Auch im übrigen sollten beim Einsatz nachrichtendienstlicher Mittel, die in ihrer Art und Schwere einer Beschränkung des Brief-, Post- und Fernmeldegeheimnisses gleichkommen, entsprechende Schutzrechte wie im Gesetz zu Artikel 10 Grundgesetz vorgesehen werden (z. B. Verwertungsverbot, Unterrichtungen).

4. Der Entwurf regelt im wesentlichen lediglich die Speicherung personenbezogener Daten in Dateien, obwohl die Informationstechnik es schon heute ermöglicht, auch komplexe Datensammlungen – bestehend aus Akten, Dateien und anderen Unterlagen – gezielt mit Hilfe automatischer Verfahren zu erschließen.
5. Bei der Regelung insbesondere für die gemeinsamen Verbunddateien der Verfassungsschutzbehörden sollte auch klargestellt werden, daß in Textdateien nur Daten über solche Personen gespeichert werden dürfen, die selbst in Verdacht stehen, eine der im Gesetzentwurf aufgezählten Straftaten zu planen, zu begehen oder begangen zu haben. Darüber hinaus ist sicherzustellen, daß in der Datei die für die Bewertung und Überprüfung von Textzusätzen maßgeblichen Unterlagen angegeben werden.
6. Die Frage, ob Einsicht in amtliche Register zulässig sein soll, kann nur bereichsspezifisch geregelt werden. Die Zulässigkeit der Einsichtnahme in Register rechtfertigt nicht die Einrichtung von on-line-Anschlüssen.
7. Das Zweckbindungsgebot ist sowohl für Übermittlungen an den Verfassungsschutz als auch für solche durch den Verfassungsschutz nicht ausreichend berücksichtigt. Die nunmehr vorgesehenen Übermittlungseinschränkungen reichen vor allem deshalb nicht aus, weil die übermittelnde Stelle nicht ausdrücklich verpflichtet wird zu prüfen, ob schutzwürdige Belange entgegenstehen. Auch innerhalb des Bundesamtes für Verfassungsschutz darf nicht jede Information unabhängig von ihrer Herkunft für jede Aufgabe verwendet werden.
8. Aus dem Trennungsgebot für Polizei- und Nachrichtendienste folgt insbesondere, daß die Übermittlung von Daten, die die Polizei unter Einsatz des Verfassungsschutz vorenthaltener Befugnisse, z. B. bei Hausdurchsuchungen, gewonnen hat, nur nach Maßgabe einschränkender Verwertungsregelungen erfolgen darf. Die Ansatzpunkte, die im Entwurf der letzten Legislaturperiode enthalten waren, sollten wieder aufgegriffen werden.
Die Informationshilfe der Grenzpolizeien für den Verfassungsschutz muß einschränkend geregelt werden.
9. Es fehlen auch befriedigende Lösungsregelungen. Abgesehen davon, daß die Löschung von Daten in Akten nicht einmal erwähnt wird, sollten schon im Gesetz Regelfristen für die Überprüfung und Löschung der verarbeiteten Daten festgelegt werden. Dabei sollte zwischen den einzelnen Aufgabenbereichen des Bundesamtes für Verfassungsschutz unterschieden werden.
10. Die Einschränkungen des Auskunftsrechts der Bürger sind bereichsspezifisch im Bundesverfassungsschutzgesetz zu regeln. Ein Auskunftsanspruch besteht in der Regel, wenn die Speicherung nur auf einer Sicherheitsüberprüfung beruht. Im übrigen bedarf es einer Abwägung im Einzelfall. Die Ablehnung ist gegenüber dem Betroffenen soweit zu begründen, daß er sachgerecht darüber entscheiden kann, ob und welche Rechtsmittel er einlegen will. Außerdem ist der Betroffene auf sein Recht hinzuweisen, sich an den Datenschutzbeauftragten zu wenden.
11. Die Datenschutzbeauftragten begrüßen es, daß die Beteiligung des Verfassungsschutzes an Sicherheitsüberprüfungen und Überprüfungen im Rahmen des vorbeugenden personellen Sabotageschutzes in einem eigenen Geheimhaltungsgesetz geregelt werden sollen. Sofern über die Sicherheitsüberprüfung hinaus eine Mitwirkung an anderen Verfahren für unabdingbar gehalten wird, sind diese gesetzlich zu regeln.
12. Soweit die Entwürfe für ein MAD-Gesetz und ein BND-Gesetz auf das Bundesverfassungsschutzgesetz verweisen, gilt die hierzu geäußerte Kritik. Die in den Entwürfen vorgesehene Verweisungstechnik erhöht für den Bürger die Schwierigkeit, aus den Gesetzen klar zu erkennen, welche personenbezogenen Daten die Dienste bei welcher Gelegenheit über ihn verarbeiten dürfen. Darüber hinaus bestehen Zweifel, ob die für das Bundesamt für Verfassungsschutz vorgesehenen Befugnisse pauschal auch für den Militärischen Abschirmdienst notwendig sind, der als Teil der Streitkräfte ein gegenüber dem Bundesamt für Verfassungsschutz deutlich unterschiedliches Operationsgebiet hat.

Anlage 2.1

**Berliner Resolution
der Internationalen Konferenz der Datenschutzbeauftragten
vom 30. August 1989**

Die Telekommunikation befindet sich weltweit in einer raschen Entwicklung. Über internationale Datennetze werden in wachsendem Umfang auch personenbezogene Daten transferiert, etwa im Zusammenhang mit der Verwendung von Kreditkarten, bei Reise-Buchungs-Systemen und innerhalb multinationaler Unternehmen. Die Nutzung dieser Technologie kann bedeutende Vorteile mit sich bringen. Aber zugleich wird es schwieriger, die Rechte derer zu schützen, deren persönliche Daten rund um die Welt übermittelt werden.

Der Europarat, die OECD, die Vereinten Nationen und weitere internationale Organisationen haben Empfehlungen und Leitlinien zum Datenschutz verabschiedet. Sie enthalten einen gemeinsamen Bestand von Grundsätzen für eine faire Praxis, wie sie etwa in der Konvention des Europarats (Konvention No. 108) und in den OECD-Leitlinien zum Ausdruck kommen. Sie bezwecken den Schutz der Privatheit des einzelnen.

Bisher haben sich acht Staaten durch Beitritt zur Konvention des Europarats international verpflichtet, einen bestimmten Datenschutzstandard einzuhalten. Die Datenschutz-Kontrollinstanzen dieser Länder haben in gewissem Umfang die Befugnis, den grenzüberschreitenden Datenfluß zu kontrollieren, wenn dies zum Schutz einzelner nötig ist. Bei dieser Kontrolle ergeben sich allerdings schwerwiegende praktische Probleme. Datenübermittlung ins Ausland bedeutet deshalb für den einzelnen in der Mehrzahl der Fälle, daß er nicht mehr die Gewißheit haben kann, daß die Grundsätze, die in nationalen Gesetzen und in den verschiedenen internationalen Übereinkommen festgelegt sind, auf seine oder ihre Daten angewandt werden. Zum Beispiel kann es dann keine Garantie geben, daß die Daten auf dem neuesten Stand und genau sind und nur für bestimmte Zwecke verwendet werden. Der einzelne kann auch sein Recht, einen Datenschutzbeauftragten anzurufen, nicht wahrnehmen.

Das Problem eines wirksamen internationalen Datenschutzes läßt sich nur durch gleichwertige gesetzliche Sicherungen in den übermittelnden und empfangenden Ländern lösen. Diese Lösung wird auch von den oben genannten Empfehlungen und Leitlinien vorgezeichnet.

Nach Auffassung der Datenschutzbeauftragten muß bei der Entwicklung und Nutzung internationaler Datendienste dem Datenschutz die gleiche Priorität gegeben werden, wie der Förderung der Datenverarbeitung und der Telekommunikation. Sie empfehlen deshalb:

- Die Regierungen sollten sowohl einzeln als auch im Rahmen internationaler Organisationen darauf hinarbeiten, daß so bald wie möglich gleichwertige gesetzliche Sicherungen geschaffen werden.
- Wer personenbezogene Daten über die Grenzen vermittelt, muß den Schutz beim Empfänger prüfen, daß die Beachtung der Rechte der Betroffenen tatsächlich sichergestellt wird.

Das Ziel dieser Maßnahmen muß sein:

- Die Datenschutzgrundsätze der Konvention 108 und der OECD-Leitlinien werden unabhängig von einer grenzüberschreitenden Übermittlung gewährleistet;
- international operierende Datenverarbeitungssysteme müssen so aufgebaut sein, daß der einzelne ohne unzumutbare Schwierigkeiten seine Datenschutzrechte wahrnehmen kann;
- Berichtigungen, Aktualisierungen und Löschungen von Daten müssen auch im Ausland nachvollzogen werden, wenn die Daten zuvor dorthin übermittelt worden sind;
- die durch den internationalen Datenaustausch erhöhten Gefahren für das Recht des einzelnen, über die Verwendung ihrer Daten zu bestimmen, müssen durch internationale Zusammenarbeit der Datenschutzbeauftragten ausgeglichen werden.

Anlage 2.2

**Zusatz Erklärung
der Datenschutzbeauftragten der EG-Länder**

Die Datenschutzbeauftragten der Länder der Europäischen Gemeinschaft sind der Überzeugung, daß die Existenz und die Aktivitäten der Gemeinschaft einerseits besondere Vorkehrungen des Datenschutzes erforderlich machen, andererseits aber auch verbesserte Möglichkeiten bieten, den Datenschutz über nationale Grenzen hinaus wirksam zu machen.

- Der für Ende 1992 angestrebte EG-Binnenmarkt ist auf den freien Austausch von auch personenbezogenen Informationen gerichtet, etwa in den Bereichen Direktmarketing/ Adressenhandel und Kreditinformation.
- Entscheidungen der Europäischen Gemeinschaft verpflichten in zunehmendem Umfang die Mitgliedsländer zur Erhebung und Verarbeitung personenbezogener Daten - so etwa im Bereich der Landwirtschaftsstatistik - und zur grenzüberschreitenden Datenübermittlung - so beispielsweise im Umwelt-, Gesundheits- und Sozialbereich.
- Einige Länder der Europäischen Gemeinschaft arbeiten an einem Pilot-Projekt für gemeinsame polizeiliche Fahndungsdateien (Schengener Informationssystem) - gewissermaßen als Ersatz für die wegfallenden Kontrollen an den Binnengrenzen.
- Die Einrichtungen der EG selbst führen zunehmend personenbezogene Datenbanken. Diese Einrichtungen unterliegen jedoch keinem Datenschutzgesetz und sind daher nicht an die Grundsätze des Datenschutzes gebunden.

Die Europäische Gemeinschaft und ihre Mitgliedstaaten werden aufgefordert, in ihre Planungen für „Europa '92“ die Notwendigkeit eines umfassenden und konsistenten Ansatzes zur Verwirklichung der Grundsätze des Datenschutzes in den Mitgliedsländern und in bezug auf die Aktivitäten der Gemeinschaft selbst einzubeziehen.

Im einzelnen schlägt die Konferenz vor:

- Durch entsprechende Rechtsakte der Europäischen Gemeinschaft sollten die Grundsätze der Europaratskonvention 108 für alle Mitgliedsstaaten ebenso wie für die Institutionen der EG selbst verbindlich gemacht werden.
- Eine unabhängige Datenschutzkontrollinstanz sollte eingerichtet werden. Sie sollte die Einrichtungen der EG in allen Datenschutzfragen beraten, die Verarbeitung personenbezogener Daten innerhalb der Einrichtungen der EG kontrollieren, Eingaben von Betroffenen entgegennehmen und mit den nationalen Datenschutzorganen zusammenarbeiten.

Die Commission Nationale de l'Informatique et des Libertés (die französische Datenschutzkommission) wird gebeten, diese Vorschläge alsbald dem Vorsitzenden des Ministerrats sowie den Präsidenten des Europaparlaments und der EG-Kommission zu unterbreiten und um Unterstützung zu werben.

Anlage 2.3

**Entschliebung
der Elften Internationalen Konferenz der Datenschutzbeauftragten
vom 30. August 1989
über die Arbeitsgruppe Telekommunikation und Medien**

Die Ausarbeitung des Entwurfs für eine Entschliebung war Anlaß zu einem sehr nützlichen Informationsaustausch zwischen den teilnehmenden Delegationen.

Die Empfehlungen und Entscheidungen, die wir in unseren jeweiligen Ländern ausgesprochen bzw. getroffen haben, sollten die internationale Dimension der Netze und Dienstleistungen berücksichtigen.

Die Informationen über die Entwicklungen, die sich jenseits unserer Grenzen vollziehen, dürfen uns nicht ausschließlich von unseren nationalen Organen übermittelt werden.

Die Netze und Dienstleistungen werden in unseren jeweiligen Ländern nicht gleichzeitig bzw. im selben Rhythmus weiterentwickelt.

Unsere Erfahrungen haben gezeigt, daß die Effizienz des Datenschutzes in diesem Bereich - über die Prinzipien hinaus - auf praktischen Maßnahmen beruht, über die von den nationalen Verwaltungsinstanzen Informationen nicht leicht zu erhalten sind.

Daher beschließt die Konferenz, daß diese Arbeitsgruppe ihre Arbeit in Berlin fortsetzt und daß nach Möglichkeit jede Delegation ihre Erfahrungen, insbesondere in folgenden Bereichen, einbringen sollte:

- detaillierte Rechnungslegung
- Modalitäten zur Aufnahme in die Teilnehmerverzeichnisse, Verwendung der Teilnehmerverzeichnisse
- verschiedene Kategorien der Telematischen Dienste (elektronische Post, Fernkäufe, Informationsdienste usw.)
- Fernmeßverfahren
- ISDN
- Zelluläres Telefon (digitaler Mobilfunk)
- automatische Anrufeinrichtungen
- Sicherheit der Netze
- Kabelnetze für Dialogfernsehen.

Anlage 2.4

Beschluß

**der Internationalen Konferenz der Datenschutzbeauftragten
vom 30. August 1989**

zu ISDN

auf Vorschlag der Arbeitsgruppe Telekommunikation und Medien

Die nationale und internationale Entwicklung der Telekommunikation ist derzeit gekennzeichnet durch die Einführung dienstintegrierender, digitalisierter Netze. Diese sind die Träger vielfältiger Dienste.

Die Entwicklung führt sowohl für die Netzträger als auch für die Diensteanbieter zur Verarbeitung von erheblich mehr personenbezogenen Daten als dies bei bisherigen Netzen der Fall war. Diese Situation erfordert nationale und internationale Vorkehrungen zum Schutz personenbezogener Daten.

Die Internationale Konferenz der Datenschutzbeauftragten stellt fest, daß hierzu erhebliche Anstrengungen erforderlich sind. Insbesondere darf der Datenschutz nicht als Hindernis für die Entwicklung des Internationalen Informationsmarktes gesehen werden, sondern er stellt vielmehr eine notwendige Ergän-

zung der technischen Entwicklung dar, die für die Akzeptanz der neuen Telekommunikationstechnologien unerlässlich ist, er stellt vielleicht sogar ein beschleunigendes Element dieser Entwicklung dar.

Sie geht bei offenen Netzen von folgenden Grundsätzen aus:

- Abrechnungsdaten dürfen nur und nur so lange gespeichert werden, wie dies erforderlich ist, um Rechnungen zu erstellen oder auf eventuelle Anfechtungen zu reagieren; ferner zur Erstellung detaillierter Rechnungen, die ausschließlich für diejenigen Teilnehmer bestimmt sind, die sie angefordert haben. Die Vereinfachung der Tarifsysteme kommt dem Datenschutz entgegen.
- Für bestimmte Telekommunikationsdienste (Telefon, Kabelfernsehen mit Rückkanal, Datenübermittlungsdienste, Autobahngebühreneinzug usw.) müssen anonyme Zahleinrichtungen geschaffen werden. Ungeachtet der Abrechnungsprobleme macht es die Mehrwertigkeit der Netze erforderlich, diese mit den technischen Möglichkeiten eines anonymen Zugangs auszustatten.
- Daten, die für die Vermittlung erforderlich sind, sind unverzüglich zu löschen; Inhaltsdaten dürfen nur gespeichert werden, wenn sie für die Abwicklung des Dienstes erforderlich sind.
- Vorkehrungen sollten getroffen werden, die jenen Teilnehmern, die wünschen, in Teilnehmerverzeichnisse aufgenommen zu werden, garantieren, daß sie nicht Objekt unerwünschter kommerzieller Werbung werden. Das Recht, daß unentgeltlich in den Teilnehmerverzeichnissen kein Eintrag erscheint, sollte angestrebt werden. Daten, die die Erreichbarkeit von Teilnehmern sicherstellen sollen, dürfen nicht zur Erstellung von Personenprofilen führen, die eine Verhaltenskontrolle erlauben.
- Maßnahmen zur Datensicherung insbesondere gegen den Zugang nicht autorisierter Personen, die Manipulation, das Mithören oder zur Gewährleistung der Authentizität des Senders müssen auf höchstem technischen Niveau und zu akzeptablen Preisen angeboten werden.
- Angemessene Kontrollinstitutionen sind sowohl national als auch international einzurichten.
- In lokalen Netzen und bei Telekommunikationsendgeräten ist bereits bei der Normierung und Genehmigung auf den Datenschutz Rücksicht zu nehmen.

Insbesondere erfordern folgende Dienstmerkmale besondere Aufmerksamkeit

- Die Anzeige des anrufenden Teilnehmers muß sowohl vom Anrufer als auch vom Angerufenen unterdrückt werden können; Mißbrauch muß durch Maßnahmen im Netz verhindert werden.
- Freisprecheinrichtungen müssen so gestaltet werden, daß nur mit Kenntnis der Gesprächsteilnehmer mitgehört oder aufgezeichnet werden kann.
- Beim Zugang zu Anrufbeantwortern, Voice- und Mailboxsystemen sowie Datenübermittlungsdiensten sind hinreichende Zugangssicherungen einzuführen.

Anlage 3

Empfehlungen für den datenschutzgerechten Einsatz von UNIX-Systemen

1. Systemverwaltung

a) Auswahl und Qualifizierung des Systemverwalters

Die sorgfältige Auswahl und Qualifizierung eines befähigten und zuverlässigen Systemverwalters und mindestens eines Vertreters ist die Grundvoraussetzung für ein sicheres Anwendungs- verfahren.

Eine ausreichende Schulung des Systemverwalters sollte unbedingt vor der Einführung und Einrichtung des Systems durchgeführt worden sein, denn gerade in dieser Einrichtungsphase kommt es auf die Sorgfalt und Kompetenz des Systemverwalters an.

Dem Systemverwalter muß, insbesondere wenn ihm noch andere Dienstgeschäfte übertragen worden sind, während der Einführungsphase ein wesentlicher Mehrarbeitsaufwand zugestanden werden, gerade um ein einwandfreies Zugriffs- und Kontrollprofil erstellen zu können. Nur vor Aufnahme des Betriebes kann der Systemverwalter die unten beschriebenen Risiken begrenzen bzw. ganz vermeiden.

b) Organisation der Systemverwaltung

Zunächst ist selbstverständlich, daß die Vergabe der „root“- und „admin“-Paßwörter außerordentlich restriktiv gehandhabt werden sollte.

Das Zugriffsrecht zu der „root“-Kennung sollte nur dem Systemverwalter zustehen. Für den Fall seines unvorbereiteten Ausfalls sollte zur Sicherheit das dafür benötigte Paßwort versiegelt bei einer zentralen Stelle hinterlegt werden und nur bei Notfällen (Systemabsturz, Fehler im Kernel usw.), bei denen die „root“-Kennung erforderlich ist, dem Vertreter bekanntgegeben werden. Der Systemverwalter muß dann nach seiner Rückkehr dieses Paßwort sofort wieder ändern und neu hinterlegen.

Wenn System und Verfahren eingerichtet worden sind, ist bei stabilen Systemen der Zugriff unter der „root“-Kennung nur in seltenen Ausnahmefällen notwendig. Wegen der erforderlichen Ausbildung und nicht zuletzt wegen der o. g. Risiken für die Sicherheit der Datenverarbeitung ist es sinnvoll, bei großen Organisationseinheiten, die mehrere UNIX-Systeme einsetzen, die Systemverwaltung von zentraler Stelle, z. B. von der für die Organisation und Datenverarbeitung zentral zuständigen Stelle durchführen zu lassen. Dies hätte auch den für den Datenschutz gewichtigen Vorteil, daß die systemnahe, dafür anwendungsferne Systemadministration in Händen läge, die mit der Anwendung selbst keine Interessen verbinden.

Eine ähnliche Organisation ist auch für weite Bereiche der anwendungsnäheren Systemadministration unter der „admin“-Kennung sinnvoll. Hier ist allerdings zu bedenken, daß das Eingreifen mit der „admin“-Kennung beim Betrieb des Systems häufiger notwendig sein kann, um z. B. kleinere Störungen zu beseitigen oder die Sicherungen durchzuführen. Hier sollte in Betracht gezogen werden, daß für diese Funktionen eine beschränkte Systemverwaltung im Bereich der Anwender vorgesehen wird.

c) Beschränkung der Systemverwaltung

Bei neueren UNIX-Systemen ist es möglich, mit dem „chroot“-Kommando begrenzte Arbeitsumgebungen auch für die Systemverwaltung zu schaffen. Damit läßt sich der Kompetenzumfang für anwendungsnahe Administratoren auf jene Funktionen beschränken, die häufig und schnell ausgeführt werden müssen.

Systemverwalterkommandos sollten nur von zwei Arbeitsplätzen (Konsole und einem besonders gesicherten Terminal) abgesetzt werden können. Hierzu ist die Datei „/etc/securetty“ bei der Installation dementsprechend aufzubauen.

Standardmäßig ist über das „su“-Kommando ein Einloggen mit der Systemverwalterkennung darüberhinaus von jedem Bildschirm möglich. Die Möglichkeit sollte durch Wegnahme der Ausführungsberechtigung für das „su“-Kommando mittels „chmod“ ganz aufgehoben werden.

d) Verschlüsselung

Die Verschlüsselung mittels „crypt“ bietet die einzige Möglichkeit, sensible Datenbestände auch vor dem Systemverwalter zu schützen. Dies kann bei bestimmten Anwendungen unabdingbar sein, z. B. wenn der Systemverwalter mit den Daten eigene Interessen verbinden könnte (z. B. Personaldateien).

2. Die Verfügbarkeit von Systemkommandos (Shell-Berechtigung)

a) Vergabe der Shell-Berechtigung

Der Zugriff auf das Betriebssystem, die sog. Shell-Berechtigung, ist für den Benutzer eines Anwendungsverfahrens nicht erforderlich und sollte daher ausgeschlossen werden. Dies ist mit UNIX in Verbindung mit menügesteuerten Anwendungsprogrammen ohne weiteres möglich, in dem als LOGIN-Kommando für die Anwender in der Datei „/etc/passwd“ bereits der Aufruf des Anwendungsprogramms eingetragen ist. Dieser Weg ist der Eintragung des Programmaufrufs in die Datei „profile“ des Anwenders in jedem Fall vorzuziehen. Grundsätzlich gilt, daß ein Anwender keine Shell-Berechtigung haben sollte, er also im Teilhabetrieb mit seinem Anwendungsverfahren arbeiten sollte. Die Shell-Berechtigung ist im allgemeinen nur für Administrations- und Programmieraufgaben erforderlich.

Muß aus organisatorischen Gründen oder bei Notfällen einem Anwender die Möglichkeit des Zugriffs auf die Betriebssystemebene gestattet werden, sollten ihm durch die Einrichtung einer eingeschränkten Shell-Berechtigung („rsh“-Kommando) nur die Befehle freigegeben werden, die er für die notwendigen Maßnahmen benötigt. Hierfür ist eine zusätzliche Benutzerkennung und ein besonderes Dateiverzeichnis einzurichten, in der die erlaubten Befehle oder Teilbefehle hinterlegt werden. Darüberhinaus muß in der Datei „profile“ des betreffenden Benutzers zumindest die Zuweisung des Suchpfades eingetragen sein und exportiert werden.

Die Programmentwicklung und -pflege sollte möglichst auf einem dafür vorgesehenen Entwicklungsrechner durchgeführt werden. Ist dies nicht möglich, sollte die Testverarbeitung zeitlich von der Wirkverarbeitung mit Personenbezug getrennt werden.

b) Abwehr von Manipulationsversuchen

In vielen Fällen, so bei dem beschriebenen Trick mit dem „su“-Kommando oder mit den sog. Spoofs, ist das ein- oder mehrfache Drücken der Taste CTRL-D als erste Vorsichtsmaßnahme zu empfehlen. Dies führt in den meisten Fällen zur Abwehr der Manipulation.

Gegen den Trick mit dem „su“-Kommando hilft es natürlich, wenn der Systemverwalter in den beschriebenen (vorgetäuschten) Notfällen selbst beim System anmeldet, anstatt das „su“-Kommando abzusetzen (Spoof-Login-Trick mit CTRL-D s. o. ausschalten!).

In jedem Fall ist darauf zu achten, daß der Pfadsuchalgorithmus erst die Systemdateiverzeichnisse durchläuft und erst zum Schluß das eigene Benutzer-Dateiverzeichnis durchsucht (z. B. sollte in der Variablen PATH=/bin/sh:/usr/menu: und nicht umgekehrt PATH=:/usr/menu:/bin/sh stehen). Damit wird vermieden, daß eigene Systemprogramme (z. B. su) aufgerufen werden, die dann zur Manipulation benutzt werden können.

Eine regelmäßige Kontrolle der Datei „/etc/passwd“ sollte vom Systemadministrator immer durchgeführt werden. Die Datei ist relativ leicht überschaubar und Unregelmäßigkeiten können somit leicht erkannt und beseitigt werden.

3. Umgang mit SUID- und SGID-Rechten (s-Bits)

Die s-Bits sollten grundsätzlich möglichst wenig genutzt werden. Da beim Schreiben in eine Datei die Einstellung sämtlicher Zugriffsrechte unverändert erhalten bleibt, darf für einen Nicht-eigentümer dieser Dateien nie eine Schreiberlaubnis bestehen. Sonst können die oben angedeuteten Manipulationen leicht vorgenommen werden.

Die eingestellten Default-Werte für die Zugriffsberechtigung sollen grundsätzlich, aber insbesondere bei mit dem s-Bit versehenen Dateien, immer so gering wie möglich sein (Vorschlag: -rw-r--r-- oder -rw-rw-r--). Für die eigene Prozeßumgebung kann mit dem Kommando „umask“ eine andere allgemeine Zugriffsberechtigung vergeben werden. Sie gilt nur für die aktuellen Prozesse und diesen Benutzer. Da auch die Bürokommunikationssoftware meist derartige Rechte benutzt, sollte jeder Anwender, der personenbezogene Daten verarbeitet und speichert, sehr restriktiv mit der Zugriffsberechtigung umgehen.

Neuere UNIX-Versionen eliminieren beim Schreiben in eine mit dem s-Bit versehene Datei automatisch das s-Bit, damit der leichtfertige privilegierte Benutzer vor den u. U. zerstörerischen Folgen der leichtfertig gesetzten Schreiberlaubnis bei Dateien mit dem s-Bit geschützt wird. Es muß als geringeres Übel in Kauf genommen werden, nach dem Schreiben in solchen Dateien das s-Bit jeweils neu setzen zu müssen.

Es empfiehlt sich für den Systemverwalter, vor Inbetriebnahme einer UNIX-Anlage mit Hilfe des „find“-Kommandos alle „root“-SUID und -SGID-Programme herauszusuchen und zu überprüfen. Wenn das gesetzte Bit nicht erforderlich ist, sollte es vor Inbetriebnahme gelöscht werden.

4. Umgang mit Paßwörtern

Die meisten der am Markt befindlichen UNIX-Systeme verlangen heute ein mindestens vier Stellen langes Paßwort. Selbst dies ist aber nicht ausreichend. Die Paßwörter sollten sechs bis acht Zeichen lang sein und möglichst nicht Wörter der allgemeinen Umgangssprache bzw. Namen, Kosennamen oder Dienststellenbezeichnungen enthalten. Eine Eingabe von mehr als acht Zeichen ist sinnlos, da das Unix-Betriebssystem nur acht Zeichen auswertet.

Ganz allgemein ist zu empfehlen, das Paßwörter auch in beliebiger Reihenfolge Sonderzeichen enthalten. Dies ist aus Sicht der Zugriffskontrolle ein sehr wichtiger Umstand, da für das Betriebssystem UNIX heute bereits Disketten auf dem Markt sind, mit denen eine Entschlüsselung von über 90 % der gängigen Paßwörter möglich ist. Bei den durchgeführten Versuchen sind aber Paßwörter, die Buchstaben und Sonderzeichen enthalten, nicht erraten worden.

Grundsätzlich ist zusätzlich zu empfehlen, daß entweder durch den Hersteller oder durch eigene Programme sichergestellt wird, daß eine Kennung, deren Paßwort mehrmals (3 bis 5 Versuche) falsch eingegeben worden ist, systemweit gesperrt wird. Nur der Systemadministrator darf in der Lage sein, diese Sperre wieder aufzuheben.

Darüber hinaus könnten durch Organisationsanweisungen bzw. Prozeduren, die automatisch die Paßwortveränderung beobachten, regelmäßige Paßwortänderungen verlangt bzw. erzwungen werden.

Es ist bei der Installation des Systems darauf zu achten, daß alle Benutzerkennungen, insbesondere auch die an die Funktionsträger („root“, „admin“) gebundenen oder für spezielle Zwecke eingerichteten Kennungen mit neuen Paßwörtern gesichert werden. Das von der Liefer- oder Herstellerfirma standardmäßig vergebene Paßwort für „root“ und „admin“ ist allgemein bekannt.

Es ist darauf zu achten, daß auch die Kennungen „gast“ und „mgast“ mit Paßwort gesichert werden.

5. Der Schutz der Hardware

Auch bei UNIX-Systemen ist auf die Einhaltung einer sicheren Zugangskontrolle zu achten, obwohl sie in der Regel in sog. Büroumgebung eingesetzt und installiert sind.

Von Bedeutung für den Datenschutz sind die Installationspläne für die einzelnen Hardware-Komponenten. Sie müssen den in der Anlage zu den Datenschutzgesetzen genannten Kontrollanforderungen genügen. Besondere Sorgfalt sollte in die Auswahl der Aufstellungsorte der Zentraleinheit, der Drucker und gegebenenfalls der Datenfernübertragungseinrichtungen gelegt werden.

Die Zentraleinheit muß davor geschützt werden, daß ein unbefugtes Neuladen (Booten) des Systems erfolgen kann. Dies bedeutet, daß entweder

- die Zentraleinheit mit den Laufwerken für bewegliche Datenträger (Bänder, Kassetten, Disketten etc.) in einem verschlossenen und nur Befugten zugänglichen Raum untergebracht wird oder
- die Laufwerke für bewegliche Datenträger gegen die unbefugte Nutzung durch Sicherheitsverschlüsselung geschützt werden.

Die Drucker, insbesondere der zentrale Drucker, müssen so aufgestellt werden, daß Unbefugte Schreiben oder Dateiausdrucke mit sensiblem Inhalt weder lesen noch kopieren noch entfernen können!

6. Löschen von Dateien

Bei Dateien, die mit dem „rm“-Befehl gelöscht werden, ist zu bedenken, daß lediglich der „i-node“ der Datei (Identifikation der Datei) gelöscht wird. Die Daten auf dem Speichermedium bleiben jedoch unverändert bestehen. Mit entsprechenden Programmen können die Datenbestände wieder lesbar und damit kopierbar gemacht werden.

Es wird daher empfohlen, Löschmodulare zu verwenden, die die zu löschenden Dateien überschreiben (z. B. mit Nullen).

7. Protokollierung

Datenschutzrechtliche Risiken bergen die Speicherabzüge („core“-Dateien), weil in diesen Speicherabzügen natürlich auch personenbezogene Daten stehen können.

Der Systemverwalter sollte daher nach Auswertung der Protokolldateien diese möglichst durch Überschreiben löschen.

Sollten bei besonders sensiblen Anwendungen zusätzliche Protokollierungen erforderlich und installiert worden sein, so ist darauf zu achten, daß durch die Protokolldateien keine zusätzlichen Risiken (z. B. durch falsches Setzen des s-Bits) eingebaut werden.

Grundsätzlich gilt, daß Protokolldateien nur solange aufgehoben werden sollten; bis sie ihre Kontrollfunktion erfüllt haben, denn auch Protokolldateien können bei Personenbezug mißbräuchlich benutzt werden. Es ist daher selbstverständlich darauf zu achten, daß die Protokolldateien nur durch den Systemverwalter manuell oder per Programm nach vorher festgelegten Kriterien ausgewertet 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.

- Abfall 1986/26
 Abgabenordnung 1988/9
 Abgangskontrolle 104
 Abgeordnetenhaus 14, 121; 1984/28; 1985/17; 1986/28; 1987/30; 1988/34; 1989/40
 Abgeordnetenhaus-Informationssystem (ADIS) 1988/14
 Abiturienten 118
 Ablichtung 42, 55, 87, 113
 Abonnentenverwaltung 106
 Abruf, unbefugter 76, 107; 1986/16
 Adoption 108, 109; 1985/4; 1986/6; 1987/27
 Adrema-Platten 115
 Adressenmittlung 26
 Adreßbuch 1985/6; 1989/26
 Adreßlisten 58, 115
 ADV-Gesetz 1985/3, 26
 ADV-Grundsätze 1984/18
 AIDS 1987/3, 4, 19, 23; 1988/18; 1989/22
 Akten 25, 49, 58
 Akten, Aufbewahrung 1986/16; 1987/28; 1988/21, 33
 Akten, Vollständigkeitsprinzip 56
 Akteneinsicht 25, 28, 50, 59
 s. a. Einsichtsrecht
 Akteneinsicht, Sozialgesetzbuch 59
 Aktenführung 110; 1986/25; 1987/30; 1988/21
 Aktenvernichtung 63; 1987/29; 1988/33, 41
 Allgemeine Geschäftsbedingungen 1984/6
 Allgemeine Ortskrankenkasse 1984/16
 Allgemeines Sicherheits- und Ordnungsgesetz 107; 1984/3, 10; 1985/3, 7, 26, 27; 1986/16; 1987/22; 1988/4
 Alliierte 1987/5
 Alternative Liste (AL) 1989/8
 Altlasten 1986/26; 1987/30
 Amerika-Gedenkbibliothek 85; 1984/28; 1986/16
 Amsanwaltschaft, s. Staatsanwaltschaft
 Amtsarzt 1984/9; 1985/23; 1987/21
 Amtsblatt, Dateiveröffentlichung 57
 Amtsgeheimnis 55
 Amtsgericht 54
 Amtshilfe 25
 Anonymisierung 34, 40, 51, 104; 1987/8
 Anordnung über Mitteilungen in Strafsachen 40, 41, 44, 108; 1984/12, 24; 1985/3, 23; 1986/5, 23; 1988/5
 Anordnung über Mitteilungen in Zivilsachen 54; 1984/25
 Anrufungen 9, 25, 32, 50, 89, 121; 1984/29; 1986/29
 Anschriften 115
 Anstaltszählung 1987/10
 Anzapfen 77
 APIS 1987/23; 1988/25
 Arbeitsplatzcomputer 1986/3
 Arbeitsrecht 1988/5
 Archive 46, 88, 106; 1984/3; 1985/11, 26
 Archivgesetz 1985/3; 1986/3, 4; 1987/4; 1988/5, 29, 1989/32
 Asbest 1988/22
 ASOG, s. Allgemeines Sicherheits- und Ordnungsgesetz
 ASTA, s. Staatsanwaltschaft
 Asylverfahren 1986/7
 Aufklärung bei der Erhebung 42
 Aufsichtsbehörde für den Datenschutz 27, 45, 61, 64, 88, 120; 1984/29; 1985/24; 1986/29; 1987/30; 1988/34; 1989/40
 Auftragsdatenverarbeitung 112; 1984/17
 Ausbildungsförderung, s. Bundesausbildungsförderungsgesetz
 Auskunft 25, 35, 52, 116; 1985/23; 1986/6
 Auskunft, Gebührenpflicht 28
 Auskunft, Sicherheitsbehörden 35
 Auskunftssperre 108, 109; 1989/27
 Auskunftsverweigerung 35
 Ausländer 33, 53, 82, 117
 Ausländerbehörde 58, 111, 119; 1986/7; 1987/29
 Ausländerzentralregister 1987/36; 1989/28
 ärztliche Schweigepflicht, s. medizinische Daten
 BAföG, s. Bundesausbildungsförderungsgesetz
 Bankauskünfte 1984/6
 Bankdienste 1987/12
 Banken, Bildschirmtext 60
 Basisdokumentation Psychiatrie 1984/9
 Bau- und Planungsakten 73
 Bau- und Wohnungswesen 116; 1988/16
 Beamtenrecht 56; 1984/3, 9, 18; 1985/3, 26; 1986/3
 Beamtenversorgungsgesetz 72
 Bebauungsplan 74
 BEHALA 105
 Beihilfe 1984/20; 1987/5
 Belegfluß 54
 Benutzerkontrolle 86
 Beratung 13, 26, 32, 43, 50, 64, 89, 121; 1984/29; 1986/29
 bereichsspezifischer Datenschutz 28, 31, 45; 1984/3, 12; 1985/3, 26
 Berichtigungsanspruch 35
 BERKOM 1988/14; 1989/19
 Berliner Datenschutzgesetz 24, 121; 1985/26; 1988/5
 Berliner Entwässerungswerke 105
 Berliner Pfandbriefbank 1985/16
 Berliner Philharmonisches Orchester 106
 Berliner Stadtreinigungsbetriebe 57; 1985/16
 Berliner Wasserwerke 105
 Beschwerden s. Anrufung
 Betriebsdatenbank 85; 1985/24
 Betriebskrankenkasse des Landes und der Stadt Berlin 1984/17
 BEWAG 36
 Bezirksamter 109, 116; 1984/16; 1985/16; 1986/24, 38; 1989/35
 Bezirkseinswohneramt 54
 Bezirksverordnetenversammlungen 15, 73
 Bibliotheken 85, 105; 1985/11, 26; 1986/16, 24
 Bibliotheksgesetz 1985/3; 1988/29; 1989/32
 Bildschirmtext 33, 37, 45, 59, 67, 75, 87, 101; 1984/12, 28; 1985/12; 1986/12; 1987/15; 1989/17
 Bildschirmtext, Anbieter 1984/14; 1985/17
 Bildschirmtext, Betreiber 1984/14
 Bildschirmtext, externe Rechner 101
 Bildschirmtext, Staatsvertrag 75, 88, 123
 Bildschirmtext, Zustimmungsgesetz 101, 120
 Blutspendedienst 1984/8
 Breitbandkommunikation 59, 101; 1987/16; 1988/14
 Broschüren 27
 Bundesausbildungsförderungsgesetz 63
 Bundesbaugesetz 119
 Bundesdatenschutzgesetz, Novellierung 65, 88, 89, 120, 121; 1986/4; 1988/5, 12, 36
 Bundeskindergeldgesetz s. Kindergeld
 Bundeskriminalamt 44
 Bundessozialhilfegesetz 72
 Bundesstatistikgesetz 31; 1986/8; 1987/4
 Bundesverfassungsgericht 1984/3; 1986/5; 1987/4
 Bundeszentralregister, unbeschränkte Auskunft 40, 56, 88, 120; 1984/28
 Bußgeldverfahren 1984/22; 1989/39
 Bürokommunikationssysteme 1988/3, 24; 1989/13
 BVG 104; 1986/9; 1988/31
 Chipkarte 1985/14; 1986/4
 Codes 34, 60, 77, 101; 1984/6
 Computerkriminalität 1984/5; 1986/4; 1989/19
 Computermißbrauch 1984/4
 Datei 25, 31, 49, 55, 58; 1985/18
 Dateienregister 12, 24, 26, 27, 30, 43, 57, 64, 86, 88, 105, 120, 121; 1985/24; 1986/29; 1987/30; 1988/34; 1989/41
 Datenangst 99
 Datengeheimnis 55
 Datenschektheft 50
 Datenschutzbeauftragter, Kontrollrechte 120; 1988/10
 Datenschutzbeauftragter, Rolle 99; 1989/3
 Datenschutzbeauftragter, Zuständigkeit 25
 Datensicherung bei manuellen Datensammlungen 114
 Datensicherung 37, 42, 57, 58, 64, 93, 116; 1984/5
 DATEX 1987/11
 Deutsche Klassenlotterie Berlin 85
 Deutsche Oper Berlin 105
 Deutsches Bibliotheksinstitut 105
 Dezentralisierung 1986/3; 1988/3; 1989/36
 Diagnosestatistik 1986/10; 1988/19
 Dienststelle, Aufbau 16, 24, 33, 50, 121
 Digitalisierung 1988/12
 Disziplinarstelle 1988/24
 Dokumentation 1984/6
 EG-Arbeitskräftestichprobe 1984/23
 Eigenbetriebe 104
 Einheitliche Patientendatenverarbeitung 63

- Einladungskarteien 105
 Einsichtsrecht 25, 41, 59, 66, 100; 1985/20
 Einsichtsrecht, medizinische Daten 100; 1986/11; 1987/18; 1988/5, 19
 Einsichtsrecht, Schülerbogen 41
 Einwilligung 24, 26, 31, 34, 51, 57, 59, 67; 1985/22
 Elektronischer Lotse 1987/27
 Elektronisches Telefonbuch 1987/16
 Emissionskataster 1986/26
 Entmündigung 1986/5; 1988/5
 Einwohnerdatenbank, s. Melderegister
 Embryonenschutzgesetz 1989/23
 Epidemiologie, s. Forschungsprojekte
 Erforderlichkeit 25, 41, 58, 61
 Erhebung 40, 51, 56, 110
 erkennungsdienstliche Unterlagen 1984/11
 Erziehungs- und Ordnungsmaßnahmen 1988/29
 EUROCAT 50
 Europa 1988/6, 12
 Europarat 28, 46; 1985/3, 35; 1987/37; 1989/4
 Europäische Gemeinschaften 28, 50; 1988/6, 12; 1989/4, 29
 Euroscheck 1987/13
 externe Schreibkräfte 1984/9
 Fahndung, Kraftfahrzeuge 79
 Fahrzeugregister 1984/22; 1987/4
 Familienkrankenhilfe 72
 Farbbänder 1988/42
 Fehlbelegungsabgabe 72, 75
 Fehleintragung 54
 Fehlspeicherung 107
 Fehlzustellung 1987/29
 Fensterbriefumschläge 43
 Ferngespräche, Erfassung, s. Telefondatenerfassung
 Fernmeldeordnung 1984/12
 Fernwartung 63; 1985/34; 1986/15
 Fernwirkdienste 101, 102; 1984/16; 1985/14; 1986/13; 1987/17; 1988/14
 Feuersozietät 1984/16
 Feuerwehr 79
 Finanzverwaltung 88
 Flughafen 1985/4
 Formulare 26
 Forschung 33, 50, 59, 61, 82, 87, 112, 117; 1987/25, 26, 37; 1988/19, 29;
 1989/11, 22, 23, 33
 Forschungsnetz 1987/12, 14
 Forsten 1985/5
 Fotos 1986/11
 Freiwilligkeit 1988/11, 21
 Fremdfirmen 63, 84, 86
 Friedhöfe 1985/5
 Funk 42
 Führerscheine 1988/30
 Führungsinformationen 1988/15
 Führungszeugnis 57; 1987/28
 Funktionstrennung 86, 101, 114; 1984/6
 GASAG 36, 104
 Geburtsdaten 41; 1985/18; 1986/6
 Gebührenpflicht bei Auskünften 28
 Geldautomaten 1986/27
 Gemeinsame Geschäftsordnung für die Berliner Verwaltung 89, 106;
 1985/3, 10
 genetischer Fingerabdruck 1988/6; 1989/9, 12
 Gentechnologie 1987/4; 1988/6; 1989/9
 Gesetzverteilungsplan 115
 Gesetz über Abbau der Fehlsubventionierung
 s. Fehlbelegungsabgabe
 Gesetz über psychisch Kranke 121; 1985/3
 Gesundheitsdaten, s. medizinische Daten
 Gesundheitsstrukturreform 1988/5, 6, 37; 1989/22
 Gewerbeanzeige 1987/28
 Gewerbeordnung 62, 87
 Gewerberegister 31, 62, 87, 88
 GGO, s. Gemeinsame Geschäftsordnung
 Glaubwürdigkeit kindlicher Zeugen 36
 grenzüberschreitende Datenverarbeitung 1989/3, 4
 Grundbuch 1987/24
 Grundrecht auf Datenschutz 28
 Grundrechte 30
 GSD 1987/13; 1988/17; 1989/39
 Hacking 1984/4; 1987/11
 Haftpflichtversicherung 1988/19
 Handels- und Gaststättenzählung 1985/11
 Handelsregister 1988/28; 1989/31
 Handfunkterminals 1989/25
 Hausbesetzungen 80, 120
 Haushaltsbegleitgesetz 100
 Haushaltsstrukturgesetze 72
 Haushaltswesen 1987/18; 1988/17; 1989/21
 Herstellerfirmen 63
 HIV, s. AIDS
 Hochschulen 25, 32, 50, 57, 63; 1986/11; 1988/32
 Hochschulgesetz 1986/22; 1989/33
 Hochschulstatistikgesetz 58; 1984/24; 1989/29, 34
 home-banking 60; 1987/12
 Humangenetik 1989/11
 Identitätsfeststellung 1984/11
 IDN 1987/11
 illegale Beschäftigung, Bekämpfung 72
 Impfliste 1988/30
 in-camera-Verfahren 90
 Industrie- und Handelskammer 45, 61; 1988/31
 Information des Bürgers 27
 Information des Datenschutzbeauftragten 26, 43, 64, 113
 informationelles Selbstbestimmungsrecht 25; 1984/3
 Informationsgesellschaft 49, 1989/3
 Informationsgleichgewicht 15, 30
 Informationssystem Verbrechensbekämpfung 36, 79, 108; 1984/10;
 1985/8; 1986/16; 1987/23; 1989/25
 Informationsverarbeitung, Entwicklung 49; 1988/3
 INPOL-System 44; 1985/8
 Institutionsleihe 44
 intelligente Schnittstelle 1985/6
 Internationale Konferenz der Datenschutzbeauftragten 1989/44, 46
 interner Datenschutzbeauftragter 105, 112, 116
 internes Dateienregister 105
 Intimbereich 39
 isolierte Rechner 63, 114; 1985/5
 ISDN 1986/3; 1989/5, 12, 47
 ISVB, s. Informationssystem Verbrechensbekämpfung
 Jubiläen 1986/22; 1987/29
 Jugendgerichtshilfe 58, 110
 Justizmitteilungsgesetz 1987/24
 Justizverwaltung 50, 60
 Justizvollzugsanstalten 55, 81, 87; 1985/17
 Kabelkommunikation 33, 37, 39, 46, 67, 102
 Kabelpilotprojekt 101; 1984/15; 1985/3, 15; 1986/13; 1987/16; 1988/14;
 1989/17, 18
 Kammergericht 1985/5
 KAN, s. Kriminalaktennachweis
 Kassenarzt 1986/5, 10
 Kaufpreissammlung 119; 1984/27
 Kindergeld 72, 100; 1984/19
 Kirchen 24, 27, 32
 Kirchensteuer 1984/17; 1989/20
 Klassenliste 118
 Kleinrechner 84, 114; 1988/41; s. a. Personalcomputer
 Klinische Nachsorgeregister 50
 Konferenz der Datenschutzbeauftragten 18, 43, 64, 88, 120; 1984/28;
 1985/24; 1986/28; 1987/30; 1988/34; 1989/40
 Konsolprotokolle 63
 Konten- und Gehaltspfändung 1988/9
 Kontrollen von Amts wegen 11, 24, 25, 26, 32, 50, 68
 Kontrollmitteilungen 1987/18
 Konverter 102
 Kosten- und Behandlungsplan 110; 1984/9, 34
 Kostenrechnung 1988/22
 Kostenübernahme, Krankenhaus 1986/10; 1987/29
 Kostenübernahmescheine 81
 KPM 105
 KpS-Richtlinien 27, 43, 56, 79, 119; 1984/12, 27
 Kraftfahrzeuge 25, 79
 Krankenakten, s. medizinische Daten
 Krankenbett 1986/11
 Krankengeschichtenverordnung 120; 1984/8
 Krankenhausstatistik 1988/19
 Krankenhäuser 1987/13; s. a. medizinische Daten
 Krankenkassen 1985/21; 1986/10
 Krebsregister 50, 88; 1984/8
 Kriminalaktennachweis 44
 Kriminalpolizeiliche personenbezogene Daten, s. KpS-Richtlinien
 Kriminalpolizeiliche Beratungsstelle 1987/24
 krw 1987/13; 1988/17
 kulturelle Einrichtungen 105
 Landesamt für Elektronische Datenverarbeitung 62, 63; 1988/3
 Landesamt für Verfassungsschutz, s. Verfassungsschutz
 Landesarchiv, s. Archive
 Landeseinwohneramt 1986/5; 1987/29
 Landeskrankenhausgesetz 1984/3, 70, 30

- Landesmeldegesetz 35, 45, 53, 64, 77, 107, 121; 1984/3, 21
 Landesstatistikgesetz 104; 1984/3; 1987/20; 1988/5, 21; 1989/28
 Landesversicherungsanstalt 1984/16
 Landeswahlordnung, s. Wahlen
 Lastschriftinzug 1984/17
 LED, s. Landesamt für Elektronische Datenverarbeitung
 Lehrerindividualdatei 118; 1986/22
 Leichenschauschein 1988/22
 Liegenschaftskataster 75; 1984/17
 Lohnsteuerkarte 43, 54, 57; 1986/28; 1987/30
 Lohnsteuerstellen 119
 Löschungsanspruch 35; 1989/35
 Mahnverfahren 1987/25
 Mail-box-Rechner 1988/15
 manuelle Datensammlungen 89, 91, 93, 112, 114, 117
 Max-Planck-Gesellschaft 61, 87
 Medienforum Berlin 1985/15; 1987/18
 Medienprivileg 8, 38, 65, 68
 medizinische Daten 25, 27, 31, 40, 49, 63, 100, 112, 120; 1984/3, 7;
 1985/20; 1986/10; 1987/14, 20; 1988/4, 19; 1989/22
 Meldegesetz 35, 45, 53, 64, 77, 107, 121; 1984/3; 1985/3, 6, 26;
 1986/3, 5, 39; 1988/27; 1989/26
 Meldepflicht, s. Meldegesetz, Melderechtsrahmengesetz
 Melderechtsrahmengesetz 27, 31, 44, 55, 100; 1985/26
 Melderegister 54, 63, 64, 78, 87, 107; 1984/21; 1985/6, 23;
 1986/5; 1988/10, 16, 26
 Menschenrechtskonvention 28
 Mieterlisten 73
 Mietobergrenzen 1984/27
 Mietspiegel 1988/16; 1989/19
 Mietpreisstellen 73
 Mikrocomputer 1984/18
 Mikroverfilmung 1984/32; 1988/21, 42
 Mikrozensus 1984/23; 1985/11; 1986/8; 1987/6, 20; 1989/28
 Mischverwaltung 44
 MiStra, s. Anordnung über Mitteilungen in Strafsachen
 Mitschnitten 1987/11
 MiZi, s. Anordnung über Mitteilungen in Zivilsachen
 Modellprogramm Psychiatrie, s. psychiatrische Daten
 Museum für Verkehr und Technik 121
 Nachrichtendienstliches Informationssystem (NADIS) 35; 1989/5, 7
 Nebenstellenanlagen 1989/12
 Nebentätigkeit 1986/11; 1987/29; 1988/23
 Netze 1987/4, 11
 Neue Medien 32, 37, 45, 49, 59, 67, 75, 91, 100; 1984/12, 28, 30;
 1985/31; 1986/12; 1987/15, 31; 1988/12; 1989/17
 Neue Medien, Grundsätze 64, 67; 1984/30
 nichteheliche Kinder 1988/26
 Notare 87
 Novellierung des Bundesdatenschutzgesetzes,
 s. Bundesdatenschutzgesetz
 Oberfinanzdirektion 1987/8
 OECD 28, 46
 Öffentlichkeit 1986/19
 one-line-Anschlüsse 39, 49, 78, 84, 115
 ONGUM 1987/13
 Ordnungsmäßigkeit der Datenverarbeitung 114
 Ordnungsmerkmal 53, 77; 1985/6
 Ordnungsverwaltung 1986/5
 Organleihe 44
 Orientierungsrahmen 1988/3; 1989/37
 Orwell 99
 Öffentliche Lebensversicherung 1984/16
 öffentliche Wirtschaftsunternehmen 1984/16
 Öffentlichkeitsarbeit 33, 50, 89, 121; 1984/29
 Parteien 1987/26
 Paß 126; 1986/4; 1987/3
 Pay - TV 102; 1985/15; 1987/16; 1988/14; 1989/18
 Personalakten 26, 40, 67; 1984/18; 1985/18; 1986/20, 23; 1987/4, 5, 21, 39;
 1988/23, 24; 1989/29
 Personalausweis 26, 31, 42, 55, 87, 106, 120, 126; 1985/6; 1986/5;
 1987/3, 4; 1988/25, 26
 Personalausweisgesetz 44, 100, 106; 1984/4; 1986/3
 Personalbezugsdatei 1984/24; 1988/22
 Personalcomputer 1985/4, 32; 1986/3, 7, 14, 17; 1987/7, 22, 24;
 1988/3, 22; 1989/15
 Personaldaten 25, 32, 40, 45, 49, 56, 66, 67; 1984/9, 18; 1985/5, 18;
 1986/3, 15, 20, 28; 1987/21; 1988/23, 29, 32
 Personalfragebogen 1984/19
 Personalinformationssystem 1986/20; 1987/4
 Personalarat 1985/19; 1986/21; 1989/31
 Personalüberhangliste 1988/23; 1989/30
 Personalverzeichnis 41
 Personenbeförderungsgesetz 62
 personengebundene Hinweise 1988/26; 1989/25
 Personenkennzeichen 53; 1984/4
 Persönlichkeitsprofil 39, 67, 68
 Persönlichkeitsrecht 59, 73
 Petitionsausschuß 1984/26; 1985/24; 1986/29
 Pfändungen 1987/21
 Pflegschaft 54
 Pinnwand 1987/16
 Planung 51, 52, 59, 73; 1985/11
 Polizei, Ordnungsaufgaben,
 s. Allgemeines Sicherheits- und Ordnungsgesetz,
 Ausländerbehörde, Melderegister, Paß, Personalausweis
 Polizei, Strafverfolgung, s. Fahndung, Informationssystem,
 Verbrechensbekämpfung, INPOL-System, KAN,
 KpS-Richtlinien, Strafverfolgung, Strafprozeßordnung
 Polizeiliche Beobachtung 1984/11; 1985/7
 Polizeiliche Kriminalstatistik 1986/9
 Polizeitechnische Untersuchungsstelle 1988/7
 POS 1987/12
 Poststrukturgesetz 1988/12, 39; 1989/17, 44
 Postverkehr 43; 1986/25; 1987/28; 1989/38
 Presse 1986/19
 private Computernutzung 1984/18; 1986/24, 35; 1989/21
 private EDV-Unternehmen 84
 Privatisierung 1988/4, 17
 Programmdokumentation 106, 114
 Programmtests 86, 113
 Protokollierung 1988/27
 Protokollisten 116
 Prozeßordnungen 1984/25; 1985/22
 psychiatrische Daten 53, 66; 1984/8; 1985/20
 psychiatrische Gutachten 41
 Quellabzugsverfahren 57
 Rasterfahndung 33, 35, 43; 1984/11
 Rechenzentren, Funktionentrennung 114
 Rechenzentrum 62, 114; 1986/27
 Rechenzentrum, Datenträgerarchiv 86
 regelmäßige Übermittlungen 1986/6, 39
 Regionales Bezugssystem 1988/16, 21
 Reichsversicherungsordnung 72
 Religionsgemeinschaften 24, 27, 32, 45, 64; 1989/27
 remote station 62, 84
 Rentenreformgesetz 1989/44
 Rentenversicherungsnummer 1988/19
 Rufname 1988/27
 Rundfunkgebühren 81, 88
 Rückkanal 102
 Rückmeldeverfahren 1986/16; 1987/29; 1989/26
 Sachakte 1989/6
 Sanierung 74
 Satellitenfernsehen 37
 Schadensersatz 24, 28, 32
 Schengener Übereinkommen 1989/25
 Schlüssel, Aufbewahrung 117
 Schufa 61; 1984/7; 1985/3; 1986/4, 5, 27; 1988/31
 Schuldnerverzeichnis 61; 1984/28; 1989/31
 Schule 25, 32, 36, 41, 50, 57, 87, 118, 120; 1984/28; 1985/5, 24; 1986/3;
 1988/29
 Schülerunterlagen 1986/3, 23; 1987/30; 1988/30
 Schulfragebogen 36
 Schulgesetz 1987/25; 1988/29; 1989/32
 Schulpsychologischer Dienst 118; 1987/25, 40; 1988/34, 40
 Schutzgemeinschaft für allgemeine Kreditsicherung s. Schufa
 Schweiz 65
 Schwerbehinderte 1984/26
 Selbsthilfeeinrichtungen 57
 Senatsinformationssystem (SIS) 1988/14
 Sender Freies Berlin 24, 45
 Seriennummer, s. Personalausweis
 Sicherheitsgesetze 1986/30; 1988/4
 Sicherheitsüberprüfungen 1987/22
 SITA 1989/4
 sonderpädagogisches Gutachten 1987/26
 Sozialbericht 64
 Sozialdaten, s. Sozialgesetzbuch X
 Sozialgeheimnis, s. Sozialgesetzbuch X
 Sozialgesetzbuch I, Mitwirkung (§ 60) 26; 1985/22
 Sozialgesetzbuch V, 1989/22
 Sozialgesetzbuch X 25, 26, 27, 31, 44, 50, 58, 64, 72, 81, 109;
 1984/25; 1985/22; 1986/25; 1989/24
 Sozialgesetzbuch X, Aktenführung 1984/25, 34; 1986/25

- Sozialgesetzbuch X, Ausländer 100, 111
 Sozialgesetzbuch X, Datenschutzbeauftragte 112
 Sozialgesetzbuch X, Offenbarung für Forschung und Planung 59, 82; 1988/20
 Sozialgesetzbuch X, Offenbarung für Strafverfahren 82, 100, 111; 1984/26; 1988/20; 1989/24
 Sozialgesetzbuch X, Zweckbindung 83
 Sozialhilfe, Ausländer 58, 82
 Sozialhilfe 58, 87; 1988/20
 Sozialhilfestatistik 64; 1986/28
 Sozialleistungsträger 1984/16
 Sozialpsychiatrischer Dienst 1989/22
 Sozialversicherungsausweis 1988/5, 19
 Sozialversicherungsnummer 1988/5, 19
 Sozialwissenschaftliche Untersuchungen 33; 1988/18
 Sparkasse der Stadt Berlin West 1984/16; 1988/31
 speichernde Stelle 62, 109; 1986/24, 38
 Speicherverschlüsselung 1987/11
 Sperrung 1984/22; 1985/6
 Spezialgesetze s. bereichsspezifische Regelungen
 Sprachspeicherdienst 1987/16
 Spurendokumentationssysteme 1984/12; 1986/17
 Staatsanwaltschaft 60, 64, 115; 1984/28; 1988/5, 27
 stand-alone-Rechner 63
 Statistik 31, 59, 64, 102, 104; 1984/23; 1985/11; 1986/3
 Statistisches Informationssystem 1986/9; 1987/20; 1988/21
 Statistisches Landesamt 1988/11
 Städtebauförderungsgesetz 74
 Sterilisation 1986/10
 Steuerfahndung 88
 Steuerverwaltung 88; 1987/18; 1988/9, 17; 1989/20
 Strafgesetzbuch, § 200 81; 1989/32
 Strafprozeßordnung 1984/10; 1986/4; 1987/24; 1988/4, 5; 1989/43
 Straftaten 1988/29
 Strafverfolgung 37, 79; 1984/10
 Strafvollzug, s. Justizvollzugsanstalten
 Straßensperre 1988/26
 Straßenverkehrsgesetz 1987/4
 Studentendaten s. Hochschulen
 Suizid 1987/20
 SWIFT 1987/13; 1989/4
 Synchronknoten 1986/15
 Tageszeitung 1989/5
 Taxifahrer 62; 1984/28; 1986/27
 Technische Prüfstellen für den Kraftfahrzeugverkehr 64
 Teilhaber-/Teilnehmersysteme 1987/11, 14
 Telebus 1984/26
 Telefon, Benutzung 42
 Telefonaufzeichnung 1986/5; 1988/33
 Telefondatenerfassung 63, 87, 120; 1986/5; 1987/5
 Telekommunikation 1988/39; 1989/4, 46
 Telekommunikationsordnung 1986/14, 32; 1987/16; 1988/12
 Telekopierer 1988/21
 Teletex 37, 38
 Telex 1988/13
 Testdaten 86, 113; 1984/18
 Textverarbeitung 84, 85; 1985/5; 1989/36
 Todesursachenstatistik 104; 1989/40
 Tonbandaufzeichnung 1988/6
 Transparenz der Datenverarbeitung 30, 86, 104, 114
 Transportkontrolle 86
 Umwandlung von Mietwohnungen 73
 Umweltschutz 1986/26
 unbeschränkte Auskunft, s. Bundeszentralregister
 UNESCO 46
 Unfallstatistik 1987/28
 Universitätsklinikum Steglitz 112
 UNIX 1989/14, 48
 Unterhaltsansprüche 58; 1984/26
 Unterricht 1986/24
 Unterschriftenliste 55
 USA 1984/6
 Übergangsbonus 1987/22; 1988/4, 38
 Übermittlung an nichtöffentliche Stellen 26, 31, 65, 121
 Übermittlung nichtöffentlicher Stellen an Behörden 31
 Überweisungsträger 58, 81, 120
 Verfahrensdokumentation 114
 Verfahrensentwicklung 113
 Verfassungsschutz 25, 35, 80, 108, 120; 1984/3; 1987/5; 1988/34; 1989/5, 45
 Verfassungsschutzgesetz 1985/3, 8, 26, 29; 1986/30; 1989/8
 Verkehrszählung 1985/11; 1986/9
 Verletzlichkeit 1987/11
 Vermessungsamt 1985/6
 Vernetzung, s. Netze
 Vernichtung von Datenträgern 63, 115; 1988/42; 1989/38
 Veröffentlichung von Verurteilungen 81
 Versand von Schriftstücken s. Postverkehr
 Vertraulichkeit 111; 1984/9; 1985/23; 1986/27; 1987/28; 1988/31
 Verurteilungen, Veröffentlichung 81
 Verwaltungsnetz 1987/11; 1988/3, 15; 1989/40
 Verwaltungsprozeßordnung 90
 Verwaltungsverfahrensgesetz 1988/5
 Verwechslungen 61
 Verwertungsverbot 66
 Videoaufzeichnungen 1986/11; 1988/8
 Videotext 37; 1986/13; 1988/14
 Vieh- und Schlachthof Spandau 105
 Virusprogramme 1988/4
 Volksbegehren 55
 Volkszählung 1983 99, 100, 103, 120; 1984/3, 23
 Volkszählung 1987 1984/23; 1985/11; 1986/7; 1987/3, 5; 1988/8, 25, 27; 1989/28
 Vordrucke 53, 87; 1986/25; 1987/28; 1988/33; 1989/34
 Wahlen 54, 55, 59, 68; 1985/17; 1989/29
 Warnkartei 40
 Wählerliste, s. Wahlen
 Wasseruhr 1987/16
 Weltbanktagung 1988/25
 Werbung 28
 Wettbewerbsunternehmen, Krankenhäuser 112
 Wirtschaftskriminalität 77; 1984/6; 1986/4
 Wohnung 100; 1988/16, 27
 Wohnungsamt 1989/19
 Wohnungsbau-Kreditanstalt 1985/16
 Wohnungsbau-Rechenzentrum 85, 120; 1984/17
 Zahlungsverkehr 1987/12, 34
 Zentrale Vormundschaftskasse / Unterhaltsvorschußkasse 85
 Zeugnisse 1988/30; 1989/33
 Zugriffsberechtigung 55
 Zugriffskontrolle 86; 1985/8
 Zustimmung, s. Einwilligung
 Zweckbindung 66