Abgeordnetenhaus von Berlin

9. Wahlperiode

Drucksache 9/1458

29. 12. 83

31 Seiten

Mitteilungen des Präsidenten

- Nr. 166 -

Druckschluß: 18. November 1983, 12.00 Uhr

Ausgegeben am 29. Dezember 1983

Der Präsident
Peter Rebsch

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

BERICHT
DES BERLINER DATENSCHUTZBEAUFTRAGTEN
zum 31. Dezember 1983

Inhaltsverzeichnis

Der Berliner Datenschutzbeauftragte beginnt im Jahresbericht 1983[1] mit einer allgemeinen Standortbestimmung, die auf der Schwelle zu 1984 ein Fazit insbesondere aus den Diskussionen um die Volkszählung zieht (1.1). Schwerpunkte des Berichts sind die Ergebnisse der Datenschutzkontrolle (2. 3), die Darstellung neuer Entwicklungen und fortbestehender Probleme zu Feststellungen aus den Vorjahren (4) und die Zusammenarbeit auf dem Gebiet des Datenschutzes (5). Ein Stichwortverzeichnis zu allen seit 1979 erschienenen Jahresberichten schließt den Bericht ab (Anlage 5).

[1] Nach § 26 Abs. 2 Berliner Datenschutzgesetz berichtet der Berliner Datenschutzbeauftragte dem Abgeordnetenhaus und dem Regierenden Bürgermeister jährlich. Es liegen folgende Berichte vor:
- Bericht über die Aufnahme der Tätigkeit des Berliner Datenschutzbeauftragten vom Januar 1980, Mitteilungen des Präsidenten - Nr. 40 -, Drs 8/277 vom 22. Januar 1980
- Bericht des Berliner Datenschutzbeauftragten zum 31. Dezember 1980 (Jahresbericht 1980), Mitteilungen des Präsidenten - Nr. 107 -, Drs 8/666 vom 28. Januar 1981
- Bericht des Berliner Datenschutzbeauftragten zum 31. Dezember 1981 (Jahresbericht 1981), Mitteilungen des Präsidenten - Nr. 20 -, Drs 9/248 vom 29. Dezember 1981
- Bericht des Berliner Datenschutzbeauftragten zum 31. Dezember 1982 (Jahresbericht 1982), Mitteilungen des Präsidenten - Nr. 92 -, Drs 9/885 vom 29. Dezember 1982.

1. Überblick

1.1 Zur Situation

1984 ante portas

„Ein Ministerialbeamter richtet sich nicht nach einem Roman". Diese Antwort erhielt ich auf meinen Hinweis auf das Orwell-Jahr 1984.

In der Tat kann man fragen, was die moderne Entwicklung der Daten- und Kommunikationstechniken mit Orwell zu tun hat. Denn der in den vierziger Jahren von Orwell glänzend beschriebene, vom Großen Bruder regierte Unrechtsstaat Ozeanien kommt ohne moderne Datenverarbeitungstechnik aus, deren Ansätze damals weitgehend unbekannt waren. Orwell und zahlreiche Beispiele aus der Geschichte zeigen vielmehr, daß Diktaturen auch ohne die Entwicklung der Datenverarbeitung entstehen und sich ausbreiten können. Die Möglichkeiten einer untechnischen „Gleichschaltung" haben viele von uns in der Vergangenheit noch erlebt. Die Diskussion über „1984" bleibt aber aktuell, wenn man die zum Teil veralteten Instrumente Orwells durch neue Entwicklungen, wie etwa die Kommunikationstechniken, ersetzt.

So etwas Ähnliches wie die Angst vor dem Großen Bruder, nämlich das Gefühl zahlreicher Menschen, sie könnten hilfloses Objekt einer für sie nicht durchschaubaren Überwachung sein, war in diesem Frühjahr anläßlich der Volkszählung deutlich zu beobachten.

Als ich daraufhin in öffentlichen Veranstaltungen meine Überzeugung dargelegt habe, daß die Menschen selbst, also jeder einzelne Bürger, seinen persönlichen Freiheitsraum vor Fehlentwicklungen und Mißbräuchen der Datenverarbeitung schützen könne, wobei ihm die zur Datenschutzkontrolle eingerichteten Stellen behilflich sein würden, bin ich auf Skepsis gestoßen. Gerade der Verlauf der Volkszählung, insbesondere die Entscheidung des Bundesverfassungsgerichts[2] vom April 1983 haben jedoch gezeigt, daß dieser Schutz stärker wirkt als viele Bürger geglaubt haben.

Wir sind von Orwells Unrechtsstaat weit entfernt. Trotzdem steht Orwell für die ständige Aufgabe, alles zu tun, um das Entstehen des von ihm beschriebenen Staatswesens oder auch nur eines ähnlichen Staatsgebildes, ja bereits gewisser Vorformen, die sich in diese Richtung entwickeln können, entschieden zu verhindern. Auf den Datenschutz bezogen heißt dies, daß wir mehr als bisher verpflichtet sind, über die mit den Vorteilen moderner Datenverarbeitung verbundenen Nachteile nachzudenken, Unzulänglichkeiten abzustellen und das Unbehagen der Bürger sehr ernst zu nehmen.

Allerdings darf bei einem Vergleich der bisher aufgetretenen Datenschutzprobleme nicht verkannt werden, daß die Volkszählungsproblematik zwar auf sehr breite Resonanz gestoßen ist, aber nicht zu den schwerwiegendsten, tief in die Persönlichkeitssphäre des Einzelnen hineinreichenden Datenschutzfragen gehört, wie z.B. der Umgang mit Gesundheitsdaten.

Datenangst und „Übersensibilisierung"

Die Diskussion um die Volkszählung hat folgendes deutlich gezeigt: Ein differenziertes Bild von den wirklichen Risiken der Datenverarbeitung ist in der Öffentlichkeit (noch) nicht entstanden. Trotzdem ist ein wachsendes Datenbewußtsein bei den Bürgern zu beobachten, das häufig über das der Verwaltungsbeamten und auch einiger Politiker hinausreicht. So war für die Diskussion um die Volkszählung charakteristisch, wie wenig selbst leitende Mitarbeiter der öffentlichen Verwaltung die Haltung der Bürger richtig einzuschätzen verstanden und wie stark die Bürger durch widersprüchliche Erklärungen, nicht zuletzt von Politikern verschiedener Parteien, die den Gesetzen erst zugestimmt und sie anschließend kritisiert hatten, verunsichert worden sind.

Andererseits stand die Kritik vielfach in keinem Verhältnis zur Reaktion bei vergleichsweise schwerwiegenden Eingriffen, insbesondere dann, wenn die theoretischen Möglichkeiten der Datenverarbeitung die Grundlage eines Horrorszenarios bildeten und dabei die realen Möglichkeiten stark verzeichnet wurden.

[2] Abgedruckt in Neue Juristische Wochenschrift 1983, S. 1307

Sensiblen Reaktionen stand unsensibles Verhalten bei vielen anderen Problemen gegenüber, so daß von einer Übersensibilisierung allgemein nicht gesprochen werden kann. Die Unsicherheiten über den Datenschutz sind angesichts der stürmischen Entwicklung der Technik einerseits, der Berichterstattung in den Medien und des kurzen Zeitraumes, in dem Datenschutzüberlegungen diskutiert werden, andererseits nicht verwunderlich.

In der Diskussion über einen vernünftigen Datenschutz wäre daher eine Versachlichung wünschenswert.

Die Bürger als Betroffene

Die Diskussion um die Volkszählung hat mit einem Vorurteil gründlich aufgeräumt: Daß nämlich nur gesellschaftliche Minderheiten vom Datenschutz betroffen werden. Um keine Mißverständnisse aufkommen zu lassen: Auch der Bürger, der sich nicht rechtstreu verhält, hat Anspruch darauf, daß ihm gegenüber die Datenschutzgesetze peinlich genau beachtet werden. Daß aber der Umgang mit den Daten im Grunde jeden angeht, das ist in der Diskussion deutlich geworden. Die Vielzahl von Fällen aus der alltäglichen Datenschutzpraxis zeigt, wie leicht der Einzelne aufgrund von Zufällen in die „Mühlen" des Apparates gelangen kann.

Die Rolle der Datenschutzbeauftragten

Viele Kritiker der Volkszählung haben erwartet, daß sich die Datenschutzbeauftragten ihren Unmut vollständig zu eigen machen und sich an die Spitze einer Boykottbewegung setzen. Dies wollten und durften sie nicht. Nach meiner Auffassung wäre damit meiner Aufgabe, den Datenschutz der Bürger zu fördern, langfristig nicht gedient. Die mehreren tausend Bürgeranliegen, die ich seit Beginn meiner Tätigkeit bearbeitet habe, erfordern vor allem die Kleinarbeit am Einzelfall, um für den Bürger günstige Entscheidungen zu erreichen. Als vor allem Emotionen weckender Kampfbegriff, den man dem jeweiligen politischen Gegner vorhält, wäre der Datenschutz nicht geeignet, in diesen zahlreichen Einzelfällen dem Bürger gegenüber der Verwaltung zu helfen.

Erstrebenswert wäre vielmehr, wenn möglichst in allen politischen Parteien Einigkeit über einen Kernbestand an Datenschutzvorstellungen bestünde. Der Datenschutz muß deswegen nicht aus der politischen Diskussion herausgehalten, sondern nach meiner Auffassung gerade in die politischen Parteien hineingetragen werden. Dieses zu fördern muß mein Ziel sein, wenn ich einen möglichst großen Teil meiner Aufgaben befriedigend lösen möchte. Boykottaufrufe schaden diesem Ziel.

Darüber hinaus konnte ich der Seite der uneingeschränkten Kritiker nicht beitreten, weil ich als Datenschutzbeauftragter ordnungsgemäß zustandegekommene Gesetze respektieren muß. Bedenken mußten allerdings während des Gesetzgebungsverfahrens und gegenüber dem Bundesverfassungsgericht geäußert werden. Beides ist geschehen.

Da die Datenschutzbeauftragten feststellen mußten, daß diesen Bedenken nicht überall hinreichend Rechnung getragen wurde, war es konsequent, daß sie auf der Basis des Volkszählungsgesetzes einen Forderungskatalog aufstellten, der die Verfassungsmäßigkeit der Durchführung des Gesetzes sicherstellen sollte.

Die Erfahrungen mit der Volkszählung zeigen, daß die aufgetretenen Probleme - zumindest zu einem erheblichen Teil - durch eine rechtliche Regelung, die dem Forderungskatalog der Datenschutzbeauftragten entspricht, hätten vermieden werden können. Für eine derartige Regelung würde allerdings ebenso wie für jede andere gelten, daß sie keine absolute Garantie für die Einhaltung bieten kann, da Verstöße niemals völlig ausgeschlossen werden können. Es kann sich immer nur darum handeln, die Chance eines erfolgreichen Mißbrauchs möglichst klein zu halten. Es hat keinen Sinn, wegen der denkbaren Mißbrauchsmöglichkeit Neues zu boykottieren, weil die Verweigerung ebenso wie die schrankenlose Durchsetzung bestimmter Maßnahmen den Ausgleich verschiedener, durchaus berechtigter Interessen unmöglich macht. Unsere pluralistische Gesellschaft ist von der Verfassung und der Sache her auf einen derartigen Ausgleich angelegt. Die Wirksamkeit rechtlicher Regeln, die auf solchen Ausgleich gerichtet sind, überzeugen gerade kritisch denkende

Bürger häufig nicht, obwohl keine rechtlich zulässige und auch keine vernünftige Alternative ersichtlich ist. Umso wichtiger ist es, die zugunsten des Bürgers geschaffenen Rechtsregeln energisch durchzusetzen.

1.2 Fortentwicklung des Datenschutzrechts

Unter den *gesetzgeberischen* Maßnahmen, die im Berichtsjahr von Einfluß auf die Situation des Datenschutzes waren, hatte wiederum[3] eine Änderung des Bundeskindergeldgesetzes negative Auswirkungen: Nämlich die im Gesetz zur Wiederbelebung der Wirtschaft und Beschäftigung und zur Entlastung des Bundeshaushalts (Haushaltsbegleitgesetz 1983[4]) vorgenommene Änderung der §§ 8 ff. Danach wird das Kindergeld für das zweite und jedes weitere Kind stufenweise bis auf einen bestimmten Sockelbetrag gemindert, wenn das Jahreseinkommen des Berechtigten und seines nicht dauernd von ihm getrennt lebenden Ehegatten einen bestimmten Freibetrag um eine Mindestsumme übersteigt.

Diese Bestimmung macht es erforderlich, daß der Berechtigte sowohl sein eigenes als auch das Einkommen seines Ehegatten an die Kindergeldstelle mitteilt, wenn er über den Sockelbetrag hinausgehende Leistungen beansprucht. Für die Mitarbeiter des öffentlichen Dienstes, für die das Kindergeld vom Dienstherren ausbezahlt wird, besteht die Gefahr, daß nunmehr auch das Einkommen des jeweiligen Ehegatten in die Personalakte Eingang findet. Der Vollzug der Bestimmung hat darüber hinaus gezeigt, daß sich die Kindergeldstellen nicht entsprechend der gesetzlichen Vorgabe mit der Summe des Jahreseinkommens begnügen, sondern mittels eines entsprechenden Formblattes eine detaillierte Aufstellung der Einkünfte des Ehegatten verlangen. Dies wird damit begründet, daß dem (hierzu berechtigten) Finanzamt eine genaue Überprüfung möglich sein müsse. Die Konferenz der Datenschutzbeauftragten hat diese Vorgehensweise mißbilligt und wenigstens einen datenschutzfreundlichen Vollzug des Gesetzes gefordert.

Als eine Rücknahme von Datenschutzregelungen stellen sich die im Rahmen der Verabschiedung des 3. Kapitels des X Buches des Sozialgesetzbuches vorgenommenen Änderungen des § 71 SGB X dar[5]. Danach ist nunmehr die Offenbarung von Sozialdaten auch zulässig an Kreiswehrersatzämter sowie an die Ausländerbehörden, um diesen ausländerrechtlich zulässige Maßnahmen zu ermöglichen. Das zuvor bestehende Verbot der Offenbarung von Sozialdaten an die Ausländerbehörde war in vielen Fällen nicht eingehalten worden.

Von großer, wenn auch wegen der alliierten Vorbehaltsrechte für Berlin nur mittelbarer Bedeutung ist die Verabschiedung des 4. Gesetzes zur Änderung des Gesetzes über Personalausweise, aufgrund dessen der sogenannte fälschungssichere und maschinenlesbare Personalausweis bundesweit eingeführt werden soll (vgl. dazu unten 2.5)[6].

Für den Berliner Landesgesetzgeber stellt die Verabschiedung des Gesetzes zum Staatsvertrag über Bildschirmtext (Btx-Zustimmungsgesetz Berlin) den datenschutzrechtlich bedeutendsten Schritt dar[7]. Für die Entwicklung der Neuen Medien wurden hier datenschutzrechtliche Regelungen vorgegeben, die auch für die künftigen Mediengesetze von großer Bedeutung sein werden (vgl. unten 2.1).

Erwähnenswert ist ferner die Verabschiedung eines ersten Gesetzes zur Ausführung des Melderechtsrahmengesetzes[8], mit dem der Begriff der Hauptwohnung im Gesetz über das Meldewesen an die Vorgaben des Melderechtsrahmengesetzes angepaßt wurde. In Beratung ist auch ein Gesetz zur Änderung des Feuerwehrgesetzes, nach dem bei Großschadensereignissen die zur Hilfeleistung eingesetzten Kräfte berechtigt sind, die Personalien Verletzter, Erkrankter, Obdachloser oder Evakuierter ohne weiteres zu erheben, an eine für die Auskunftserteilung zuständige Behörde zu übermitteln und sie den Angehörigen oder sonstigen Berechtigten mitzuteilen.

Mit dem Urteil des Bundesverfassungsgerichts zur Volkszählung vom 15. Dezember 1983[9] hat die Rechtsprechung den Datenschutz als Recht des Bürgers, grundsätzlich selbst über Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten zu entscheiden, einen hervorragenden grundrechtlichen Rang eingeräumt. Einschränkungen dieses Grundrechts sind danach nur im überwiegenden Allgemeininteresse zulässig. Das in seiner Bedeutung weit über die Volkszählung hinausreichende Urteil werde ich sorgfältig daraufhin analysieren, welche Auswirkungen es auf geltende Gesetze, Gesetzgebungsvorhaben und die Verwaltungspraxis hat.

Der Bundesgerichtshof (BGH) hat sich in zwei Entscheidungen zu der lange umstrittenen Frage geäußert, unter welchen Voraussetzungen Patienten ein Recht auf Einsicht in ärztliche Unterlagen haben. Der BGH hat bestätigt, daß der Patient gegenüber dem Arzt oder einem Krankenhaus grundsätzlich auch außerhalb eines Rechtsstreits Anspruch auf Einsicht in die ihn betreffenden Krankenunterlagen hat, soweit sie Aufzeichnungen über objektive physische Befunde und Berichte über Behandlungsmaßnahmen (Medikation, Operation usw.) betreffen. Dabei hat der BGH auch zur Art und den Grenzen einer solchen Einsichtsgewährung Stellung genommen. Erneut unterstrichen wurde das „therapeutische Privileg", durch das der Patient vor gesundheitlichen Schäden geschützt werden soll, die gerade durch die Auskunft über seine tatsächliche Erkrankung zu befürchten sind.

In einer gleichzeitig ergangenen zweiten Entscheidung hat der BGH die Geltung dieser Grundsätze für den Bereich psychiatrischer Behandlungen eingeschränkt. Er stützt dies vor allem darauf, daß hier eine klare Trennung zwischen objektiver und subjektiver Seite der therapeutischen Maßnahmen nicht möglich sei. Als Vorinstanz hatte das Berliner Kammergericht hierzu eine gegenteilige Auffassung vertreten[10].

In Berlin hat das Kammergericht eine rechtskräftige Entscheidung zu der Frage gefällt, unter welchen Voraussetzungen Sozialdaten über den Aufenthalt eines Sozialleistungsempfängers an Strafverfolgungsbehörden offenbart werden dürfen[11]. Diese Entscheidung dürfte nur der Anfang für die Aufarbeitung der vielfältigen Probleme des Sozialdatenschutzes durch die Rechtsprechung sein (vgl. unten 2.7).

2. Kontrolle der Einhaltung der Datenschutzvorschriften - Schwerpunkte -

Die für 1983 vorgesehenen Schwerpunkte[12] - Überprüfungen und Beratungen im Bereich Neue Medien, kulturelle Einrichtungen, öffentliche Sicherheit, Datenverarbeitung bei Eigenbetrieben und im Gesundheitswesen - habe ich wie vorgesehen, in Angriff genommen. Durch den mit der Volkszählung verbundenen Arbeitsaufwand werden einzelne Arbeiten im Bereich öffentliche Sicherheit und im Gesundheitswesen - später als vorgesehen - erst 1984 abgeschlossen werden können.

2.1 Neue Medien

Von aktueller Bedeutung für den Datenschutz bei Neuen Medien ist vor allem das Bildschirmtextsystem, dessen schrittweise Ausbreitung auf das Bundesgebiet anläßlich der Internationalen Funkausstellung Berlin im Herbst 1983 begonnen hat, sowie das Kabelpilotprojekt Berlin, für das der Senat eine gesetzliche Regelung vorbereitet.

Für die verschiedenen Projekte, die noch während der Planungsphase starken Veränderungen unterlagen (Bildschirmtext, Kabelpilotprojekt und Kabelkommunikation), hatte ich jeweils Vorschläge zur Ausgestaltung des Datenschutzes vorgelegt. Damit soll erreicht werden, daß typischen Gefahren beim Umgang mit personenbezogenen Daten, die bei Diensten der Neuen Medien entstehen können, bei der technischen, organisatorischen und rechtlichen Ausgestaltung von vornherein begegnet wird. Für den Bildschirmtext hat sich dieses Verfahren

[3] Vgl. bereits Jahresbericht 1982, S. 5, 1.2
[4] BGBl. I, S. 1857, vom 23. Dezember 1982; GVBl. S. 2187 vom 31. Dezember 1982
[5] BGBl. I, S. 1450 vom 9. November 1982, GVBl. S. 2002 vom 3. Dezember 1982
[6] BGBl. S. 194, vom 1. März 1983
[7] GVBl. S. 971, vom 7. Juli 1983
[8] GVBl. S. 434, vom 15. März 1983
[9] 1 BvR 209 1983 u. a.
[10] BGH Neue Juristische Wochenschrift 1983, S. 328 und S. 330; KG 20 U 967 - Urteil vom 1. Juni 1981
[11] Kammergericht AZ (3) Ss 314/82 vom 26. Mai 1983
[12] Jahresbericht 1982, 6.2, S. 21

bewährt, da die den Datenschutz betreffenden Vorschläge weitgehend verwirklicht worden sind. Diese Feststellung darf aber nicht zu der Annahme verleiten, die Datenschutzdiskussion sei auf dem Gebiet des Bildschirmtextes abgeschlossen. Mit der bundesweiten Ausbreitung kommt vielmehr die Phase, in der sich erst erweisen muß, ob sich die Regeln in der Praxis bewähren oder ob Fehlentwicklungen ein Nachsteuern des Gesetzgebers erforderlich machen.

Bildschirmtext

Der 1983 in Kraft getretene *Staatsvertrag* enthält erstmals für das gesamte Bundesgebiet geltende Datenschutzvorschriften für einen Bereich der Neuen Medien. Mit ihrer Hilfe sollen personenbezogene Daten etwa bei der Warenbestellung in Kaufhäusern, bei Transaktionen im Verkehr mit Banken und Sparkassen, bei Buchungen von Reisen, bei Tests durch psychologische Institute, bei Finanzierungsberatungen etc. geschützt werden. Damit ist das Stadium der Diskussion, das 1980 mit den Grundsätzen der Datenschutzbeauftragten bei den Neuen Medien vom 11. Dezember 1980 begann und von den bemerkenswerten Abschlußberichten zur Begleitforschung in Berlin und Nordrhein-Westfalen fortgeführt wurde, vorerst abgeschlossen. Dabei ist positiv festzustellen, daß in der mehrjährigen Diskussion der wesentliche Teil der Datenschutzforderungen im Staatsvertrag verankert werden konnte. Auf die als Anlage beigefügte Synopse der einzelnen Vorschläge und ihrer Verwirklichung im Staatsvertrag wird verwiesen[13].

Im folgenden werden noch einmal die Punkte dargestellt, die bisher nicht oder nicht vollständig im Gesetz berücksichtigt worden sind. Ich werde die Praxis in den nächsten Jahren aufmerksam daraufhin beobachten, ob insoweit ein Regelungsbedarf besteht und werde entsprechende Vorschläge an den Senat und das Abgeordnetenhaus herantragen.

Die Datenschutzbeauftragten hatten sich dafür ausgesprochen, daß die *Abrechnungsdaten* nur von der Bundespost aufbewahrt und damit den Anbietern in personenbezogener Form nicht bekannt werden. Um den Etat der Post nicht zu sehr zu belasten, hat der Gesetzgeber eine Lösung gewählt, die es in Einzelfällen - wenn Schuldner sich beharrlich weigern, ihre Schuld zu bezahlen - gestattet, daß die Daten der Teilnehmer an die Anbieter übermittelt werden. Sofern sich die Zahl dieser Fälle in engen Grenzen hält, erscheint mir dieses Verfahren datenschutzrechtlich durchaus vertretbar. Eine endgültige Beurteilung wird davon abhängen, in welchem Umfang derartige Übermittlungen von der Post erfolgen. Dies werde ich in den nächsten Jahren beobachten. Das Gutachten, das Professor Dr. Hans-Ullrich Gallwas im Rahmen der Begleitforschung abgegeben hat, kommt u. a. zu der bis dahin nicht erhobenen Forderung, daß die Anbieterfunktion und die Funktion des Betreibers eines externen Rechners voneinander getrennt sein sollten. Dahinter steckt die begründete Befürchtung, daß Anbieter, die gleichzeitig mit eigenen externen Rechnern am System beteiligt sind, wesentlich erweiterte Möglichkeiten zur Verwendung der aus dem System kommenden personenbezogenen Daten haben. Aufgrund ihrer aus dem öffentlichen Bereich ausgelagerten Speicher- und Verarbeitungspotentiale wird ein unkontrollierbarer Datengebrauch befürchtet. Eine funktionale Trennung zwischen Anbieter und Betreiber externer Rechner würde zwar den Datenschutz erheblich verbessern, da die Flexibilität des Anbieters hinsichtlich des Gebrauchs der Daten durch das Interesse des Service-Rechenzentrums an einem ordnungsgemäßen und datenschutzgerechten Betriebsablauf beschränkt werden kann. Die Forderung nach der Funktionentrennung würde allerdings erhebliche Änderungen der gegenwärtigen Praxis zur Folge haben. Die Erfahrungen der nächsten Jahre müssen zeigen, ob für eine derartige Regelung tatsächlich Bedarf besteht.

Im Berliner Btx-Zustimmungsgesetz ist auch der *Forderung nach einer einheitlichen Datenschutzkontrolle* weitgehend Rechnung getragen. Die Regelung entspricht der von mir vertretenen Rechtsauffassung, daß es sich bei der Eröffnung der Neuen Medien, wie auch des Bildschirmtextes um eine Veranstaltung der jeweiligen Länder handelt, die damit auch die sich aus der Eröffnung der Kommunikationswege ergebenden „Verkehrssicherungspflichten" tragen. Unter diesem Blickwinkel erklärt sich die Aufgabe der Datenschutzbeauftragten zu beobachten, ob die Landesverwaltungen diesen Pflichten nachkommen. Daneben bleibt die gesetzliche Zuständigkeitsverteilung zwischen der Aufsicht über den privaten Bereich und der Kontrolle des öffentlichen Bereichs bestehen. Dies hat für Bildschirmtext zur Konsequenz, daß das einheitliche technische System nur kontrolliert werden kann, wenn die zuständigen Stellen eng zusammenarbeiten. Vorschläge für eine entsprechende Zusammenarbeit werden von den Datenschutzbeauftragten des Bundes und der Länder zur Zeit vorbereitet.

Eine mit den Neuen Medien verbundene Rechtsfrage war die nach der Abgrenzung von Bundes- und Landeskompetenzen, wobei sich das Problem der Einordnung der *Btx-Zentralen* zuspitzte. Von mir wird weiterhin die Auffassung vertreten, daß die Btx-Zentrale, soweit sie Nutzungsaufgaben wahrnimmt, vom Landesbeauftragten zu kontrollieren ist. Um unnötige Kontroversen zu vermeiden, werde ich mich - soweit meine Tätigkeit über die Informationssammlung hinausgeht - um eine Abstimmung mit dem Bundesbeauftragten bemühen.

Im Rahmen einer gemeinsamen Bestandsaufnahme hat Ende September im Fernmeldetechnischen Zentralamt der Deutschen Bundespost eine Informationsveranstaltung stattgefunden, an der Datenschutzbeauftragte aus Bund und Ländern teilgenommen haben. Dabei hat die Deutsche Bundespost nunmehr auch datenschutzrechtlich relevante Details der technischen Ausgestaltung des Bildschirmtextsystems, insbesondere zur Speicherung personenbezogener Daten für Betriebs- und Abrechnungszwecke den Datenschutzbeauftragten des Bundes und der Länder bereitgestellt. Ziel der Bestandsaufnahme ist, festzustellen, ob das Bildschirmtextsystem den Anforderungen des Bildschirmtextstaatsvertrages und den Datenschutzvorschriften entspricht.

Im vergangenen Jahr ist bei der Nutzung des Bildschirmtextes eine Gruppe von Fällen aufgefallen, in denen Teilnehmer im Namen anderer Teilnehmer beleidigende oder belästigende Äußerungen über Bildschirmtext verbreitet haben. Diese *Mißbräuche* traten verstärkt bei den Teilnehmern auf, die kein persönliches Kennwort eingegeben hatten. In diesen Fällen konnten sich Dritte, sofern ihnen die Teilnehmernummer bekannt war, als fremde Teilnehmer ausgeben. Um die Jahreswende 1982/83 hat die Post daher ihre Software so verändert, daß zusätzlich die Eingabe eines persönlichen Kennwortes erforderlich wird. Damit hat sich die Chance eines Mißbrauchs erheblich reduziert. Sie kann weiter durch einen Wechsel des Kennwortes in bestimmten Zeitabständen verringert werden.

In Zukunft ist zu prüfen, ob sich die jetzt geltenden rechtlichen Vorschriften in der Praxis bewähren und wie ihre Einhaltung kontrolliert werden kann. Hier bestehen insbesondere für den Bereich der privaten, an das Netz angeschlossenen Computer erhebliche Zweifel. Es wird eine besondere Aufgabe der Datenschutzbeauftragten sein, zusammen mit den zuständigen Stellen für eine sorgfältige Kontrolle zu sorgen. Sollte dies nicht möglich sein, müßte die daraus resultierende Frage nach einer Änderung der Vorschriften erneut diskutiert werden.

Entsprechend der Vorgabe von §3 Abs. 3 Bildschirmtext-Zustimmungsgesetz werde ich künftig im Rahmen des Jahresberichtes über die festgestellten Mängel und meine Vorschläge zu ihrer Behebung und zur Verbesserung des Datenschutzes berichten.

Kabelpilotprojekt

In Berlin soll auf der Grundlage des Beschlusses der Ministerpräsidenten der Länder vom 11. Mai 1978 ein Pilotprojekt durchgeführt werden, mit dem die Möglichkeit der Verbreitung von Kommunikationsdiensten über Breitbandkabel erprobt werden soll (Kabelpilotprojekt). Dadurch sollen dem Teilnehmer neue Breitbanddienste, z. B. der Empfang bewegter Bilder, die Benutzung eines Rückkanals, Filmabruf etc. eröffnet werden. Darüber hinaus könnten „Fernwirkdienste" eingesetzt werden, die „fernwirken", z. B. Geräte in der Wohnung an- und abschalten, und „fernmessen", z. B. elektronisch die Zählerstände bei Elektrizität, Gas und Wasser ablesen.

[13] Anlage 1

Aus diesem umfassenden Angebot können sich auch aus datenschutzrechtlicher Sicht besondere Gefahren ergeben. Neben den beim Bildschirmtext beobachteten Gefahren, die sich angesichts des großen Angebots beim Kabelpilotprojekt verstärken, ist besonders die Möglichkeit ernst zu nehmen, daß mit den Diensten des Fernwirkens und Fernmessens in den verfassungsrechtlich besonders geschützten häuslichen Bereich (Art. 13 GG) eingegriffen werden kann. Zum Schutz dieser Sphäre sind ebenfalls bereichsspezifische Datenschutzvorschriften erforderlich.

Ursprünglich beabsichtigte der Senat, für das nur auf einen kurzen Zeitraum angelegte Kabelpilotprojekt keine gesetzliche Grundlage, sondern ausschließlich privatrechtliche Rahmenbedingungen zu schaffen. Gegen dieses Vorhaben hatte ich Bedenken, weil der Datenschutz im sogenannten privaten Bereich nicht den strengen Anforderungen unterliegt wie im öffentlichen Bereich. Zudem gehe ich davon aus, daß es sich bei der Bereitstellung neuer Kommunikationsdienste um eine öffentliche Aufgabe handelt. Mit dieser Aufgabe ist die Verpflichtung des jeweiligen Landes verbunden, Mißbräuchen und Fehlentwicklungen zu begegnen. Das Land trägt also auch hier eine Art Verkehrssicherungspflicht. Angesichts der zeitlich begrenzten Bedeutung des Kabelpilotprojektes hatte ich meine Bedenken gegen die privatrechtliche Form jedoch zurückgestellt, als sich der Senat mir gegenüber bereit erklärt hatte, daß durch die Wahl der privatrechtlichen Form (GmbH) keine Verschlechterung der datenschutzrechtlichen Situation eintreten würde. Dies wurde durch eine sogenannte Unterwerfungsklausel sichergestellt.

Zur Gewährleistung des Datenschutzes beim ursprünglich geplanten Kabelpilotprojekt Berlin hatte ich ausführliche Vorschläge vorgelegt, die in ihrem Regelungsgehalt Art. 9 Btx-Staatsvertrag entsprechen und die Kontrolle des Datenschutzes durch den Berliner Datenschutzbeauftragten sicherstellen.

In den Entwurf des Grundvertrages für das Kabelpilotprojekt Berlin wurde daraufhin folgende Datenschutzvorschrift in § 7 aufgenommen:

Die Trägerorganisation unterwirft sich der Kontrolle des Berliner Datenschutzbeauftragten und verpflichtet sich, diesen in entsprechender Anwendung von § 25 Berliner Datenschutzgesetz zu unterstützen. Kontrollbefugnisse anderer Stellen bleiben unberührt.

Die materiellen Datenschutzregelungen sollten in die allgemeinen Geschäftsbedingungen Eingang finden.

Zwischenzeitlich plant der Senator für Kulturelle Angelegenheiten, für das Kabelpilotprojekt eine auch von mir befürwortete gesetzliche Grundlage zu schaffen. Er bekennt sich damit nunmehr erfreulicherweise eindeutig zur öffentlichen Verantwortung für das Kabelpilotprojekt. Aus ihr ergibt sich auch die logische Konsequenz, daß der öffentliche Datenschutz für die Neuen Medien und das Kabelpilotprojekt gelten muß. Dieses Verfahren hat den Vorteil, daß nunmehr auch die materiellen Vorschläge zum Datenschutz gesetzlich geregelt werden.

Entwicklungstendenzen der Kabelkommunikation

Im Rahmen der noch vom Senator für Wissenschaft und Kulturelle Angelegenheiten eingesetzten Kommission für ein Medienerprobungsgesetz hatte ich Gelegenheit, mich über den aktuellen Stand der Technik sowie die praktischen Möglichkeiten von Kommunikationssystemen zu unterrichten. Folgende für den Datenschutz relevante Probleme haben sich dabei herausgestellt:

1. Die Programmauswahl und Steuerung anderer Kommunikationsvorgänge erfolgt mit Hilfe von mikroprozessorgesteuerten dezentralen Einrichtungen, sogenannten Konvertern. Diese sollen in der Wohnung oder vor dem Haus des Abnehmers installiert werden.
2. Mit Fernwirkdiensten, wie z. B. Fernmessen, Fernanzeigen, Ferneinstellen, Fernschalten sollen Dienste angeboten werden, die aufgrund des Rückkanals bei der Kabelkommunikation möglich werden und in erheblichem Umfange in die Privatsphäre des Wohnungsinhabers eindringen können. So könnten ständig Strom-, Wasser- und Gasverbrauch abgelesen werden. Es könnten bestimmte Geräte ein- und ausgeschaltet werden. Es besteht die Möglichkeit, durch installierte Kameras etwa die Wohnung zu überwachen, um bei älteren Mitbürgern die häusliche Pflege zu erleichtern.

Der Anschluß von privaten Endeinrichtungen bei der Telekommunikation (im allgemeinen Fernsehgeräte mit Tastaturen, aber auch Kameras) an das Netz erfolgt über *mikroprozessorgesteuerte* Konverter. Es ist noch offen, ob diese Konverter bei jedem Teilnehmer installiert werden oder aber als sogenannte Vorfeldeinrichtungen mehrere Teilnehmeranschlüsse steuern sollen (z. B. alle Anschlüsse eines Hauses).

Der Konverter erfüllt folgende Funktionen:

- Auswahl der vom Teilnehmer gewünschten Programme dadurch, daß er das Funktionsmodul und damit die Endeinrichtung auf die gewünschte Empfangsfrequenz einstellt,
- Aussendung der Empfängerkennung zur Identifizierung des Teilnehmers, Berechtigungsprüfung (vergleichbar mit Btx) und Entschlüsselung, sofern die übertragenen Signale verschlüsselt sind (evtl. sinnvoll bei Pay-TV),
- Verwaltung von codezahlgeschützten Kanälen (einige Kanäle können möglicherweise nur sichtbar gemacht werden, wenn der Empfänger eine bestimmte Codezahl eingibt),
- Sperrung von Teilnehmereinrichtungen,
- Durchführung von Alarmierungsfunktionen von der Zentrale aus (es wird die Möglichkeit geben, daß Teilnehmern, deren Einrichtungen in Betrieb oder in einem sogenannten Stand-by-Betrieb sind, bestimmte Nachrichten sichtbar gemacht werden können).

Die Funktionen des Konverters können vom Teilnehmer in einem vorgegebenen Maße (Programmauswahl, Auswahl von Diensten usw.) gesteuert werden. Von einer Zentrale aus sind sie über einen schmalbandigen Datenkanal programmierbar. Ferner können bestimmte gespeicherte Daten, etwa zur Gebührenberechnung abgerufen werden.

Das Leistungsprofil der Konverter, die nach Angaben der Deutschen Bundespost nicht Bestandteil des Postnetzes sein werden, ist wesentlicher Ansatzpunkt für Datenschutzüberlegungen. Hier entscheidet sich, ob es Anbietern möglich sein wird, Daten über das Benutzerverhalten zu gewinnen, aus denen sich Benutzerprofile ableiten lassen. Unter Datenschutzgesichtspunkten ist es daher wichtig, daß eine öffentlich-rechtlich organisierte Kabelzentrale folgende Funktionen wahrnimmt:

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

Die *Fernwirkdienste* reichen in die Wohnung des Betroffenen hinein. Wegen der durch Art. 13 GG garantierten Unverletzlichkeit der Wohnung dürfen derartige Eingriffe nur unter ganz besonderen Voraussetzungen vorgenommen werden.

Daher habe ich folgende Regelung vorgeschlagen:

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

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

(3) Die Einrichtung von Fernwirkdiensten ist nur zulässig, wenn

- beim Betroffenen ein Anzeigegerät installiert ist, das jederzeit erkennen läßt, wann ein Dienst in Anspruch genommen wird und welcher Art der Dienst ist,
- der Betroffene jederzeit den Dienst abstellen kann.

Im Zweifel gilt das Abschalten eines Dienstes durch den Betroffenen als Widerruf der Einwilligung.

2.2 Statistik und Volkszählung

Die ursprünglich für 1983 vorgesehene Volkszählung hat einen Verwaltungsbereich in den Mittelpunkt des öffentlichen Interesses gerückt, der trotz des gewaltigen Umfangs der von ihm verarbeiteten Daten bislang wenig Aufmerksamkeit erfahren hat: Die amtliche Statistik.

Zwar hat der Umstand, daß sich die Statistiker selbst stets einem besonderen Statistikgeheimnis verpflichtet fühlten, bisher dafür gesorgt, daß Probleme mit dem Datenschutz kaum zu verzeichnen waren. Dies darf jedoch nicht darüber hinwegtäuschen, daß auch hier Defizite bestehen, die nicht nur im Hinblick auf die Volkszählung diskussionsbedürftig sind.

Volkszählung

Im Frühjahr 1983 wurde die Volkszählung zu einem Schwerpunkt meiner Arbeit. Das der Zählung zugrundeliegende Gesetz über eine Volks-, Berufs-, Wohnungs- und Arbeitsstättenzählung (Volkszählungsgesetz 1983)[14] war im März 1982 ohne größere Diskussion verabschiedet worden. Es stand in der Folgezeit zunächst nicht im Blickpunkt der Öffentlichkeit. Der Bundesbeauftragte für den Datenschutz hatte im Gesetzgebungsverfahren die Möglichkeit zur Stellungnahme. Seinen damals erhobenen Forderungen bezüglich des Datenschutzes im Volkszählungsgesetz wurde nicht vollständig entsprochen. Dies gilt z.B. für die Zulässigkeit des Abgleichs mit dem Melderegister. Erst mit dem Näherrücken des Stichtages nahm das Interesse der Öffentlichkeit an der Volkszählung zu. Diesem Interesse wurde von den für die Volkszählung zuständigen Stellen nicht ausreichend Rechnung getragen. Die gestiegene Sensibilisierung der Bevölkerung auf dem Gebiet des Datenschutzes wurde nicht richtig eingeschätzt.

Aus den oben (1.1) angeführten Gründen war es mir nur möglich, durch extensive Auslegung des Volkszählungsgesetzes die datenschutzrechtlichen Belange zu wahren.

Als besonders problematisch erwiesen sich folgende Vorschriften des Volkszählungsgesetzes:

- §9 Abs. 1: Der Melderegisterabgleich
- §9 Abs. 1 Satz 2: Das Benachteiligungsverbot
- §9 Abs. 2 ff: Die Übermittlungsvorschriften

Beim gesetzlich zugelassenen *Melderegisterabgleich* erschien unter datenschutzrechtlichen Gesichtspunkten vor allem die Verknüpfung zwischen statistischer Erhebung und Verwaltungsvollzug problematisch. In Berlin sollte dieser Vergleich mit Hilfe von Begleitlisten durchgeführt werden, die Volkszählungsbogen selber sollten nicht an die Meldebehörde gehen. Eine Berichtigung des Melderegisters sollte nicht von Amts wegen erfolgen, sondern erst nach einem förmlichen melderechtlichen Verfahren. In dessen Verlauf sollte der Betroffene Gelegenheit zur Stellungnahme erhalten. Durch diese Maßnahme wäre gesichert, daß der Melderegisterabgleich und die Volkszählung relativ getrennt ablaufen würden.

Ein weiterer Kritikpunkt aus datenschutzrechtlicher Sicht mußte das *Benachteiligungsverbot* des §9 Abs. 1 Satz 2, Abs. 2 Satz 3, Abs. 3 Satz 3 Volkszählungsgesetz sein. Die Formulierung entsprach zwar der Vorschrift §11 Abs. 3 Satz 3 Bundesstatistikgesetz, ihre Auslegung im Volkszählungsgesetz im Zusammenhang mit der Melderegisterberichtigung warf allerdings einige Fragen auf. Im Bundesstatistikgesetz bezieht sich diese Vorschrift nämlich nicht auf das Ergebnis eines Datenabgleichs, sondern unmittelbar auf die Verwertung der in einer Statistik erfaßten Daten. Die Übertragung dieser Vorschrift in das Volkszählungsgesetz führt dazu, daß nach dem zulässigen Abgleich mit dem Melderegister in den Fällen, in denen es zu einer Korrektur gekommen ist, im Melderegister Erkenntnisse aus der Volkszählung enthalten sind. Bei extensiver Auslegung mußte die Vorschrift dazu führen, daß eine so korrigierte Angabe aus dem Melderegister nicht verwendet werden darf, weil sonst nicht zuverlässig ausgeschlossen werden könnte, daß diese berichtige Angabe sich nicht doch für den Betroffenen nachteilig auswirken kann. Eine solche Konsequenz wäre jedoch widersinnig. Aus systematischen Gründen konnte daher §9 Abs. 2 Satz 2 Volkszählungsgesetz nur so verstanden werden, daß der Abgleich selbst nicht zu Maßnahmen gegen den Betroffenen führen darf. Die Verhängung eines Bußgeldes wegen eines anläßlich der Volkszählung entdeckten Verstoßes gegen das Meldegesetz war demnach verboten. Erlaubt mußte hingegen die Auskunft über das korrigierte Merkmal im Rahmen der regelmäßigen Datenübermittlung aus dem Melderegister sein.

Ferner waren die gesamten *Übermittlungsvorschriften* des §9 ungenau und zu wenig bestimmt. In Berlin hätten diese Vorschriften jedoch keine so große Bedeutung erlangt, da hier durch Senatsbeschluß bestimmt ist, daß statistische Auswertungen allein vom Statistischen Landesamt vorgenommen werden. Von dort werden Daten nur in statistisch aufbereiteter Form an andere weitergegeben.

Als ein weiteres gravierendes Problem stellte sich auch mehr und mehr der *Einsatz der Zähler* heraus. Zahlreiche Bürger wandten sich mit Bedenken an mich, daß der Zähler beim Abgeben und Einsammeln des Bogens Einblicke in ihren ganz privaten Lebensraum gewinnen und ihre Angaben auf dem Bogen lesen könnte. Zum Schutz der Privatsphäre hat der Senator für Inneres daher zugestanden, daß die Bogen direkt in der Zählungsdienststelle ausgefüllt werden könnten. Außerdem konnte der Bogen auch per Post zurückgesandt oder dem Zähler im verschlossenen Umschlag zurückgegeben werden. Die Zähler sollten belehrt werden, daß sie auch hinsichtlich aller Wahrnehmungen im Rahmen der Zählertätigkeit der Geheimhaltungspflicht unterliegen. Ferner sollten die Zähler nicht in ihrer unmittelbaren Nachbarschaft eingesetzt werden. Dem Zähler mußte nicht Zugang zur Wohnung gewährt werden.

Ein vollständiger Katalog meiner Forderungen sowie der Forderungen der Konferenz der Datenschutzbeauftragten, die fast gleichen Inhalts sind, ist als Anlage 3 abgedruckt.

Im Rahmen der Vorbereitung der Volkszählung wurden von mir seit Anfang Februar ausführliche Gespräche mit dem Innensenator und dem Statistischen Landesamt über diese Probleme geführt. Der von mir im Februar 1983 vorgelegte Forderungskatalog zur Wahrung des Datenschutzes bei der Volkszählung wurde durch Schreiben des Innensenators vom 8. April 1983 akzeptiert. Ich konnte aufgrund der Zusammenarbeit mit den zuständigen Berliner Stellen die Überzeugung gewinnen, daß alle Anstrengungen unternommen wurden, um eine datenschutzgerechte Durchführung der Volkszählung zu ermöglichen.

Die schriftlichen, mündlichen und telefonischen *Anfragen der Bürger* zur Volkszählung waren so zahlreich, daß es meinen Mitarbeitern und mir nur sehr schwer möglich gewesen wäre, jede Frage individuell zu beantworten. Häufig wurden auch gleiche Fragen gestellt. Hauptsächlich bewegte die Bürger die Frage nach Sinn und Zweck einer solchen Zählung, die Sorge, daß von den gespeicherten Daten wieder auf die einzelne natürliche Person geschlossen werden kann, die Befürchtung, daß die gesammelten Angaben an andere Stellen weitergegeben würden und so Finanzamt oder andere Behörden ihnen nicht zustehende Fakten erhalten könnten, sowie die Angst, daß die Korrektur des Melderegisters für den einzelnen nachteilige Folgen haben könnte. Es wurde daher von mir ein Informationsblatt verfaßt, in dem die wichtigsten Vorschriften des Volkszählungsgesetzes erläutert, sowie über Ablauf und Organisation der Volkszählung unterrichtet wurde. Dieses Blatt, dem jeweils noch meine Forderungen zum Datenschutz bei der Volkszählung, sowie der Beschluß der Konferenz der Datenschutzbeauftragten und ein Gesetzestext des Volkszählungsgesetzes beigelegt wurden, wurde mit einem Anschreiben an interessierte Bürger versandt. Nach dem Urteil des Bundesverfassungsgerichts wurde diese Aktion eingestellt. Ferner wurden bis Ende April 1983 von meinen Mitarbeitern und mir ca. 40 Informationsveranstaltungen besucht, um dort über

[14] Vom 25. März 1982 (BGBl. I, S. 369, GVBl., S. 775)

den Datenschutz bei der Volkszählung zu diskutieren. Es waren unterschiedliche Gruppierungen, die um eine Teilnahme des Datenschutzbeauftragten baten, vor allem Parteien, Verbände, Hochschulen und Schulen.

Bei allen diesen Veranstaltungen und aus den Anfragen wurde deutlich, daß bei einer größeren Zahl von Bürgern ein tiefsitzendes Mißtrauen gegen diese Volkszählung bestand. Der Spruch des Bundesverfassungsgerichts, mit dem die bevorstehende Zählung ausgesetzt wurde, hat bestätigt, daß die Bedenken der Öffentlichkeit nicht aus der Luft gegriffen waren. Der Umstand, daß an eine mögliche neue Volkszählung strenge Anforderungen von seiten des Gerichts gestellt werden, ist geeignet, dieses Mißtrauen abzubauen.

Bei der Volkszählung wurde deutlich, daß das Interesse an datenschutzrechtlichen Problemen stark gestiegen ist. Ursachen der Entwicklung waren aus meiner Sicht:

1. Die mangelnde psychologische Vorbereitung der Bevölkerung und die fehlende Information. Den meisten Bürgern war, wie ich bei zahlreichen Diskussionen feststellen konnte, der Inhalt der Fragebogen unbekannt. So konnte auch von Volkszählungsgegnern mit Fragen argumentiert werden, die gar nicht gestellt worden sind,
2. die problematische Regelung im Gesetz (insbesondere §9) und gewisse Diskrepanzen zwischen Gesetz und Erhebungsbogen,
3. die widersprüchlichen Äußerungen einiger Politiker, die für die Volkszählung gestimmt und anschließend dagegen gesprochen haben,
4. Mängel bei der Durchführung des Gesetzes.

Ich glaube, daß nur das Zusammentreffen dieser Punkte zur weiten Verbreitung der Kritik beigetragen hat. Einen Schlußstrich unter diese Diskussion hat das Urteil des Bundesverfassungsgerichts vom 5. Dezember 1983 gezogen. Soweit sich aus diesem Urteil auch rechtliche und praktische Konsequenzen für Berlin ableiten lassen, werde ich dazu gesondert Stellung nehmen.

Statistik

Die Notwendigkeit, den Schutz statistischer Daten durch ein *Landesstatistikgesetz* auch im Bereich des Landes zu stärken, ergibt sich bereits aus der Tatsache, daß im Gegensatz zur Regelung für den Bereich der Bundesstatistik (§11 Bundesstatistikgesetz) für Landesstatistiken und Kommunalstatistiken kein spezielles gesetzliches Statistikgeheimnis besteht. Die entsprechenden Bundesvorschriften gelten lediglich für jene Fälle, in denen Daten der Bundesstatistik übermittelt worden sind, nach dem gesetzlich geregelten Prinzip, daß die Geheimhaltungsvorschriften der Weitergabe der Daten an andere öffentliche Stellen folgen. Dies bedeutet, daß auf Landesebene nur ein partieller gesetzlicher Schutz im Sinne des Statistikgeheimnisses vorhanden ist und im übrigen die Vorschriften über das Amtsgeheimnis gelten. Dieser Zustand ist außerordentlich unbefriedigend, nicht nur weil gleiche Sachverhalte rechtlich unterschiedlich behandelt werden, sondern auch weil damit für die Weitergabe statistischer Daten die dem §10 Bundesdatenschutzgesetz entsprechenden Ländervorschriften gelten. Die statistischen Daten werden damit auch nicht „amtshilfefest". Dies sollte bei dem in Berlin in Vorbereitung befindlichen Landesstatistikgesetz berücksichtigt werden. Es ist mir zugesagt worden, daß ich den Entwurf zur Stellungnahme erhalte.

An mich wurde die Frage herangetragen, ob das Statistische Landesamt an das Bundesgesundheitsamt bestimmte Daten zur Erstellung einer *Todesursachenstatistik* übermitteln dürfe. Ich habe dagegen keine Bedenken erhoben. Denn der vom Statistischen Landesamt an das Bundesgesundheitsamt zu übermittelnde Datensatz enthält bezogen auf einen Bezirk in der Regel nur anonymisierte Daten, da davon ausgegangen werden kann, daß zu jeder Todesursachengruppe mehrere Fälle innerhalb eines „Meldeblocks", d. h. Zahl der Todesfälle innerhalb eines Jahres auftreten werden. Dennoch ist nicht auszuschließen, daß in einer statistischen Gruppe für eine Todesursache nur ein einziger Fall auftritt. Die Anonymität kann bei solchen Fällen nur dann bejaht werden, wenn ein Reindividualisierungsrisiko verneint werden muß. Nach meiner Überprüfung setzt die Reindividualisierung voraus, daß ein Zusatzwissen über die Namen einzelner Betroffener vorliegt. Dieses Zusatzwissen kann wegen der entsprechenden Berufs- und Amtsgeheimnisse weder von Ärzten noch vom Statistischen Landesamt rechtmäßig erlangt werden. Damit beschränkt sich das Risiko darauf, daß ein Mitarbeiter aufgrund von Todesanzeigen o. ä. wegen der Übereinstimmung von Altersangaben Kenntnis des Betroffenen erhält. Dieses Risiko ist angesichts des damit verbundenen Aufwandes und des zu erwartenden vernachlässigbaren Interesses der Mitarbeiter des Bundesgesundheitsamtes nicht als hinreichendes Argument gegen die Anonymität der Daten zu werten.

2.3 Datenverarbeitung in den Eigenbetrieben

Technisch-organisatorische Überprüfungen wurden bei den Berliner Gaswerken (GASAG) und den Berliner Verkehrs-Betrieben (BVG) durchgeführt. Aufgrund der baulichen und damit verbundenen organisatorischen und technischen Neugestaltung des Rechenzentrums der Berliner Stadtreinigung (BSR) mußte die Überprüfung bei diesem Eigenbetrieb auf den Dezember 1983 verlegt werden, so daß die Ergebnisse der Prüfung in diesem Bericht nicht dargestellt werden können.

Die technisch-organisatorische Überprüfung bei der GASAG und der BVG konzentrierte sich im wesentlichen auf die datenschutzgerechte *Organisation der automatisierten Datenverarbeitung,* insbesondere also auf die Einhaltung der Kontrollanforderungen der Anlage zu §5 Berliner Datenschutzgesetz. Die Ordnungsmäßigkeit der Datenverarbeitung wurde nur beiläufig geprüft, da diese auch Gegenstand regelmäßiger und relativ häufiger Untersuchungen von Wirtschaftsprüfungsgesellschaften ist.

Die Eigenbetriebe, die personenbezogene Daten überwiegend zur ökonomischen Abwicklung der eigenen Geschäfte benötigen, sehen nach meinem Eindruck ein hohes Geschäftsrisiko darin, daß ihre Daten mißbraucht werden oder in falsche Hände geraten können. Datenschutz und Ordnungsmäßigkeit der Datenverarbeitung sind zumindest im geprüften technisch-organisatorischen Bereich nicht nur lästige Pflicht zur Abwendung gelegentlich als abstrakt empfundener Risiken für schutzwürdige Belange Dritter, sondern Voraussetzung für die rationelle Abwicklung von Datenverarbeitung.

Infolgedessen konnte ich feststellen, daß die Betriebe aus eigener Motivation heraus planvolle Datenschutzmaßnahmen getroffen haben, und daß die Regelungen für die interne Datenschutzkontrolle (§16 Berliner Datenschutzgesetz) ernsthaft umgesetzt werden. Daher war die Zahl der festgestellten Mängel gering. Bemerkenswert ist jedoch eine Feststellung, die in beiden geprüften Eigenbetrieben zum Tragen kommt: Die Datenverarbeitung der Betriebe hat sich im Laufe der Jahre ständig ausgedehnt, ist organisatorisch komplexer geworden und an die Grenzen beschränkter räumlicher Kapazität gestoßen. Folgen davon sind diverse Kompromisse und Sicherheitsabstriche in der internen Organisation des Sicherheitsbereiches, die in einem auffälligen Kontrast zur wirkungsvollen Abschottung (Zugangskontrolle) nach außen stehen. So wurde u. a. festgestellt:

- Die Anzahl der Personen, die zum Zutritt zum Rechenzentrum befugt sind, ist größer als für die Aufgabenabwicklung im Rechenzentrum erforderlich.
- Die Funktionentrennung zwischen Rechenzentrum, Datenträgerarchiv und Arbeitsvor- und -nachbereitung ist nicht strikt genug und baulich zu wenig unterstützt. In einem Betrieb bestand sogar eine personelle und räumliche Identität zwischen Arbeitsvorbereitung und Datenträgerarchiv.
- Eigentlich voneinander zu trennende Funktionsbereiche im Sicherheitsbereich werden gegenseitig als Zugang verwendet.

Konsequenz dieser Mängel ist eine zu geringe Transparenz und Kontrollierbarkeit der Abläufe im Sicherheitsbereich, die vor allem Risiken für die Abgangskontrolle beinhaltet.

Den Eigenbetrieben waren diese Mängel bewußt. Dennoch ist die Reaktion der Eigenbetriebe unterschiedlich, obwohl ich

bei meinen Empfehlungen zur organisatorischen Umgestaltung auf die wirtschaftlichen Belange Rücksicht genommen habe.

Die GASAG hat mit dem Hinweis, daß die Wirtschaftsprüfungsfirma die Mängel zwar auch erkannt, letztlich aber hingenommen hat, eine Diskussion über meine Empfehlungen nicht aufgenommen und sich auf die Umsetzung marginaler Empfehlungen beschränkt.

Die BVG dagegen hat mich bereits ausführlich über die vorgesehenen Umbaumaßnahmen in ihrem Sicherheitsbereich unterrichtet, die nur geringe Kosten verursachen, aber eine erhebliche Verbesserung des organisatorischen Datenschutzes bedeuten.

Bei den fünf weiteren Eigenbetrieben, dem Vieh- und Schlachthof Spandau, der Staatlichen Porzellan-Manufaktur Berlin (KPM), den Berliner Hafen- und Lagerhausbetrieben (BEHALA), den Berliner Wasserwerken (BWW) und den Berliner Entwässerungswerken (BEW) habe ich zunächst Gespräche über folgende Themen geführt:

- Stellung und Kompetenzen des „internen Datenschutzbeauftragten",
- Übersicht über vorhandene (auch interne) Dateien und Karteien (§ 16 Berliner Datenschutzgesetz),
- Veröffentlichungen im Amtsblatt für Berlin (§ 12 Berliner Datenschutzgesetz),
- Meldungen der automatisch betriebenen Dateien an den Berliner Datenschutzbeauftragten (§ 22 Berliner Datenschutzgesetz).

Dabei hatten diese Eigenbetriebe auch Gelegenheit, bereits aufgetretene datenschutzrechtliche Probleme an mich heranzutragen.

Hinsichtlich der Grundeinstellung zum Datenschutz mußte ich große Unterschiede zwischen den geprüften Eigenbetrieben feststellen. Betriebe mit eigener automatisierter Datenverarbeitung haben dabei in stärkerem Maße die erforderlichen organisatorischen Maßnahmen und entsprechenden Anweisungen für den Schutz personenbezogener Daten getroffen.

Sofern die Aufgaben eines *„internen Datenschutzbeauftragten"* bisher dem Leiter des Personalamtes, dem Leiter der EDV-Abteilung oder dem Verwaltungsleiter übertragen waren, habe ich angeregt, nach Möglichkeit dem Beispiel einiger Eigenbetriebe zu folgen und einen Mitarbeiter der Revision, zumindest aber der Organisationsabteilung mit dieser Aufgabe zu betrauen. Dadurch soll der Gefahr der „Eigenkontrolle" begegnet werden.

Darüber hinaus habe ich angeregt, daß in analoger Anwendung des § 29 Bundesdatenschutzgesetz dem internen Datenschutzbeauftragten zukünftig auch Mitwirkungsmöglichkeiten bei der Auswahl der in der Datenverarbeitung tätigen Personen eingeräumt werden, soweit personenbezogene Daten verarbeitet werden.

Bemängeln mußte ich, daß bislang nicht bei allen Eigenbetrieben die nach § 16 Berliner Datenschutzgesetz erforderliche *Zusammenstellung sämtlicher Dateien* (einschließlich der internen Datensammlungen) vorgenommen wurde. Bei einem Eigenbetrieb war zwar eine korrekte Auflistung der automatisch geführten Dateien vorhanden, es fehlten jedoch die manuellen Dateien.

Der Vieh- und Schlachthof hatte zum Dateienregister „Fehlanzeige" gemeldet. Dies beruhte auf dem Irrtum, daß mit der Meldung des Landesverwaltungsamtes über die beim Landesamt für Elektronische Datenverarbeitung geführte Datei „Berechnung, Zahlbarmachung und Abrechnung von Bezügen" auch die Daten des Vieh- und Schlachthofes abgedeckt seien.

Das Landesverwaltungsamt nimmt jedoch für diesen Eigenbetrieb die Berechnung, Zahlbarmachung und Abrechnung von Bezügen nicht aufgrund einer Übertragungsanordnung gem. § 8 a Allgemeines Zuständigkeitsgesetz (AZG) wahr, sondern auf Grund einer Verwaltungsvereinbarung. Insofern handelt es sich um eine auftragsweise Datenverarbeitung mit der Folge, daß der Vieh- und Schlachthof speichernde Stelle und zur Meldung zum Dateienregister verpflichtet ist. Die Nachmeldung ist unterdessen erfolgt.

Das gleiche Problem hat sich bei der BEHALA gezeigt, die die Berechnung, Zahlbarmachung und Abrechnung von Bezügen ihrer Mitarbeiter auftragsweise bei der GASAG vornehmen läßt. Da die erforderliche Meldung zum Dateienregister bisher nicht abgegeben wurde, mußte ich auch hier auf die notwendige Nachmeldung hinweisen.

Sowohl bei der KPM als auch bei der BEHALA wurden aus der besonderen Situation als Wettbewerbsunternehmen nicht die daraus resultierenden datenschutzrechtlichen Folgerungen gezogen. So mußte ich beide Betriebe darauf aufmerksam machen, daß - obwohl für sie die Meldungen zum Allgemeinen Dateienregister entfallen - gem. § 22 Satz 5 i.V.m. § 1 Abs. 2 Berliner Datenschutzgesetz die automatisch geführten Dateien zum Besonderen Dateienregister zu melden sind.

2.4 Kulturelle Einrichtungen

Im Geschäftsbereich des Senators für Kulturelle Angelegenheiten habe ich folgende Stellen überprüft:

- Museumspädagogischer Dienst
- Archäologisches Landesamt
- Verwaltung der Staatlichen Schlösser und Gärten
- Staatliches Prüfungsamt für Bibliothekare
- Staatliches Prüfungsamt für Musiklehrer
- Akademie der Künste
- Deutsche Oper Berlin
- Deutsches Bibliotheksinstitut

In den beiden letztgenannten Stellen wurden die technischen und organisatorischen Abläufe der automatisierten Datenverarbeitung geprüft.

Fast alle Stellen haben miteinander gemein, daß personenbezogene Daten in *Karteien für Einladungen* und Informationen von Interessenten aus dem staatlichen und dem nicht-staatlichen Bereich geführt werden.

Diese Dateien sind auch für andere Stellen interessant, wenn es darum geht, ihren Adressenbestand zu erweitern. Einladungsdateien werden daher zwischen den verschiedenen Stellen mitunter abgeglichen und ausgetauscht. Dies bedeutet, daß diese Dateien keinen internen Charakter haben und somit der Veröffentlichungspflicht nach § 12 Berliner Datenschutzgesetz unterliegen. In der Regel liegt die Einwilligung für die Aufnahme in eine derartige Datei seitens der Betroffenen vor. Allerdings sollten die Betroffenen darauf hingewiesen werden, daß sie so lange in der Datei bleiben, wie sie sich nicht gegenteilig erklären. Dies ist erforderlich, da mangels anderer Rechtsvorschriften die Einwilligung die Voraussetzung für die Führung der Datei ist. Die Betroffenen sollten ferner über die Möglichkeit und die Zwecke der Weitergabe informiert werden.

Bei den meisten Stellen mußte ich die Art der Aufbewahrung personenbezogener Unterlagen bemängeln. Hier sollten die von mir unten (Abschnitt 3.1) dargelegten Anforderungen an die Unterbringung manueller Datensammlungen Beachtung finden. Insbesondere gilt dies für das Datenmaterial, welches im Archiv der Akademie der Künste gelagert wird und welches als besonders sensitiv eingeschätzt werden muß. Die hier getroffenen Maßnahmen zur Sicherung des Materials waren nur unzureichend.

Wegen der Anwendungen automatisierter Datenverarbeitung habe ich das Deutsche Bibliotheksinstitut und die Deutsche Oper Berlin intensiveren Prüfungen unterzogen. Dabei ist davon auszugehen, daß in diesem Bereich in der Regel nur wenig sensitive Daten verarbeitet werden.

Das *Deutsche Bibliotheksinstitut* ist zuständig für bestimmte zentrale DV-gestützte Dienstleistungen für das deutsche Bibliothekswesen wie z. B. die Führung einer Zeitschriftendatenbank und eines sogenannten Zeitschriftendienstes, Verlegung und Erstellung des Handbuchs der öffentlichen Bibliotheken, statistische Auswertungen sowie die Entwicklung von ADV-Verfahren für Bibliotheken. Soweit Personenbezug bei diesen ADV-Anwendungen vorliegt, ist nicht von einer hohen Sensitivität der Daten auszugehen, so daß in Anwendung des Satzes 2 des § 5 Abs. 1

Berliner Datenschutzgsetz ein besonders hoher Aufwand für Datenschutzmaßnahmen nicht gefordert werden kann. Die Ordnungsmäßigkeit und Transparenz des ADV-Einsatzes ist jedoch unabhängig von der Relativierung der Anforderungen an den technischen und organisatorischen Datenschutz zu betrachten, da kontrollierbar bleiben muß, ob es bei der geringen Sensitivität der Verfahren auch bleibt.

Die Überprüfung ergab in diesem Zusammenhang einige Mängel, deren Behebung jedoch keine besonderen Probleme aufwerfen sollte und gegen deren Feststellung keine wesentlichen Einwände vorgebracht wurden. Offenbar war dem Datenschutz wegen der geringen Sensitivität der personenbezogenen Daten keine besondere Beachtung geschenkt worden. So wurde z.B. den Melde- und Veröffentlichungspflichten bisher nicht nachgekommen: Die Anforderungen des § 16 Berliner Datenschutzgesetz wurden nur insoweit umgesetzt, als ein interner Datenschutzbeauftragter bestellt ist. Dieser ist jedoch nicht mit ausreichenden Kompetenzen ausgestattet, um seinen Aufgaben gerecht zu werden.

Die Überprüfung der *Deutschen Oper Berlin* bezog sich im wesentlichen auf die Umsetzung der Arbeitsanweisungen zum Zahlungsverfahren Personalbezüge und zu Datensicherung und Datenschutz, zu denen ich Anfang des Jahres Gelegenheit zur Stellungnahme hatte. Ich hatte in meiner Stellungnahme auf einige Ungenauigkeiten in diesen Arbeitsanweisungen hingewiesen, die dann bei der Überprüfung weitgehend ausgeräumt waren. Wesentlicher Schwachpunkt war die bereits im Jahre 1979 im Bericht des Rechnungshofes beanstandete Abhängigkeit von einer SoftwareFirma, die die Programmdokumentation als Firmengeheimnis zurückbehielt. Der Deutschen Oper Berlin war somit die in § 16 Berliner Datenschutzgesetz geforderte Überwachung der ordnungsgemäßen Anwendung der Datenverarbeitungsprogramme nicht möglich und die prüfenden Instanzen waren an einer sachgerechten Prüftätigkeit gehindert. Der Mißstand ist mittlerweile weitgehend behoben worden, da nunmehr Dokumentationsunterlagen vorliegen und Maßnahmen zur Organisationskontrolle und zur ordnungsgemäßen Freigabe und Handhabung von Programmen getroffen wurden. Die Einschaltung des Landesamtes für Elektronische Datenverarbeitung in die notwendig gewordene Überarbeitung des ADV-Einsatzes in der Deutschen Oper und in die Planung weiterer ADV-Anwendungen (Kartenvertrieb und -abrechnung) ist sicher geeignet gewesen, der Datenverarbeitung in der Deutschen Oper die zwingend erforderliche Transparenz zu geben.

Das *Berliner Philharmonische Orchester* beabsichtigt in Kürze, für die Abonnenten-Verwaltung ein automatisiertes Verfahren einzuführen. Ich hatte bereits vor längerer Zeit Gelegenheit, zum geplanten Verfahren Stellung zu beziehen. Meinen Einwänden und Hinweisen ist bei der Bearbeitung des Konzeptes in vollem Umfang gefolgt worden.

Ähnlich wie beim Statistischen Landesamt werden auch im *Landesarchiv* eine Vielzahl personenbezogener Unterlagen aufbewahrt, ohne daß Aufgabe und Verfahren gesetzlich geregelt wären. Dieser Mangel, dem angesichts der Sensibilität einer Vielzahl von Unterlagen große Bedeutung zukommt, ist umso gravierender, als die Gemeinsame Geschäftsordnung für die Berliner Verwaltung jede Stelle verpflichtet, Akten vor der Vernichtung dem Landesarchiv zur Archivierung anzubieten.

Die Datenschutzbeauftragten haben auf dieses Defizit bereits in den vergangenen Jahren aufmerksam gemacht und Vorschläge für eine angemessene Lösung der datenschutzrechtlichen Probleme vorgelegt[15]. Im vergangenen Jahr bestand Gelegenheit, zu verschiedenen Gesetzesentwürfen des Bundes und mehrerer Bundesländer Stellung zu nehmen. Auch beim Senator für Kulturelle Angelegenheiten wird ein Gesetzentwurf vorbereitet.

Vor der endgültigen Beschlußfassung über die Entwürfe waren noch einige Punkte zu diskutieren, insbesondere

- die Definition der Aufgaben der Archive,
- eine genaue Umschreibung der Zulässigkeit der Abgabe an bzw. der Übernahme von Daten,
- die Rechte sekundär Betroffener, wie Ehegatten und nahe Verwandte,
- die Behandlung medizinischer Daten.

Ein Arbeitskreis der Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat auch hierzu Lösungen entwickelt.

Ich gehe davon aus, daß es in Berlin gelingen wird, die Vorstellungen der Datenschutzbeauftragten im Archivgesetz zu berücksichtigen; das gleiche gilt für die entsprechende Anpassung der Gemeinsamen Geschäftsordnung (GGO I).

2.5 Ordnungsaufgaben, Öffentliche Sicherheit und Strafverfolgung

Zur Situation des Datenschutzes

Der Datenschutz im Bereich der öffentlichen Sicherheit steht nach wie vor im Blickpunkt. Dies hat u. a. zur Folge, daß von verschiedenen Interessengruppen eher holzschnittartig pro oder contra Datenschutz argumentiert wird. Damit besteht die Gefahr, daß einzelne Sachprobleme verzeichnet werden und eine abgewogene Lösung erschwert wird. Um dieser Tendenz zu begegnen, habe ich mit meinen Mitarbeitern verstärkt das Gespräch mit allen beteiligten Gruppen aus diesem Bereich gesucht. Dabei fand ich auch besondere Unterstützung bei den im Abgeordnetenhaus vertretenen Fraktionen. So hatte der Vorsitzende des Ausschusses für Inneres, Sicherheit und Ordnung zu einer Aussprache zwischen Polizeivertretern, Vertretern der Berufsvertretungen von Polizeibeamten und dem Datenschutzbeauftragten eingeladen. Weiter hatte der Fraktionsvorsitzende der CDU ein Gespräch zwischen Polizeibeamten und dem Datenschutzbeauftragten organisiert. Auf einer Veranstaltung des Verbandes der Verwaltungsjuristen fand eine Diskussion aller Beteiligten statt. Diese Veranstaltungen haben das Ziel, Mißverständnisse abzubauen und wirklich bestehende Probleme, wie sie sich etwa aus dem Spannungsverhältnis zwischen Polizei und Sozialarbeit i. w. S.[16] ergeben, sowie deren Ursache (Abfassung der bestehenden Vorschriften, Unkenntnis vorhandener Vorschriften) festzustellen.

Der damit eingeleitete Klärungsprozeß ist noch nicht abgeschlossen. Nach Abschluß der Diskussionen werde ich das Ergebnis sowie die offen gebliebenen Fragen zusammenfassen. Soweit erforderlich werde ich an den Senat und die Fraktionen herantreten und Vorschläge für das weitere Vorgehen damit verbinden.

Maschinenlesbarer Personalausweis

Neben der Volkszählung stand die für 1984 vorgesehene Einführung eines maschinenlesbaren Personalausweises im Mittelpunkt der öffentlichen Diskussion.

Allerdings haben sich die Alliierten in Berlin vorbehalten, Einführung und Ausgestaltung des Personalausweises zu regeln, so daß das Bundespersonalausweisgesetz in Berlin nicht angewendet wird. Abgesehen davon wirft diese Form des Ausweispapiers einige grundsätzliche Fragen auf, die in jedem Fall auch für Berlin Bedeutung gewinnen können.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder war bereits im Jahr 1979 an der Formulierung des damaligen Referentenentwurfes beteiligt. Sie hatte die automatische Lesbarkeit des Ausweises nur dann für hinnehmbar erklärt, wenn ein datenschutzgerechtes Melderecht sowie bereichsspezifische Datenschutzregelungen für Sicherheitsbehörden einen ausreichenden Schutz der Persönlichkeitsrechte der Bürger sicherstellen. Der Deutsche Bundestag hatte in einer Entschließung vom 17. Januar 1980 diese Position aufgegriffen[17].

In einem erneuten Beschluß hat die Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 13. September 1983 die Forderungen bekräftigt und sowohl im Hinblick auf den Inhalt des Personalausweisgesetzes und der entsprechenden Ausführungsvorschriften als auch im Hinblick auf die bereichsspezifischen Datenschutzregelungen konkretisiert.

[15] Vgl. Jahresbericht 1982, 5.1, S. 20

[16] Näheres dazu vgl. auch unten im Abschnitt Sozialwesen, 2.7

[17] Vgl. Bundestagsdrucksache 8/3498

Das im Bundesgebiet am 1. November 1984 in Kraft tretende Personalausweisgesetz enthält Lücken, die durch die Zusicherung einer datenschutzgerechten Interpretation, aber auch durch eine gesetzliche Klarstellung ausgefüllt werden müssen: Um die Entstehung von Bewegungsbildern unbescholtener Bürger zu verhindern, muß auf die *Protokollierung* von Einzelabfragen mit Hilfe des maschinenlesbaren Ausweises durch die Polizeibehörden verzichtet werden; um zu verhindern, daß aus der Seriennummer des Personalausweises eine verfassungsrechtlich bedenkliche Personenkennzahl wird, muß im Bereich der Gefahrenabwehr und Strafverfolgung auf die *Verwendung der Seriennummer* verzichtet werden; auch Privatunternehmen muß die Einrichtung von Dateien mit Hilfe des Personalausweises untersagt werden, wie dies ausdrücklich - wohl aufgrund eines Versehens - nur für öffentliche, nicht aber für nicht-öffentliche Stellen vorgeschrieben ist. Die datenschutzrechtlichen Anforderungen an die innerstaatliche Verwendung des Ausweises müssen auch im internationalen Bereich umgesetzt werden.

Die *Ausführungsgesetze* oder -vorschriften der Länder zum Verfahren der Personalausweisausstellung müssen die Persönlichkeitsrechte der Betroffenen hinreichend berücksichtigen. Hierzu gehört, daß eine erkennungsdienstliche Behandlung bei Ausweisausstellung nur als letztes Mittel zulässig sein darf, daß auf die Angabe „unveränderliche Kennzeichen" verzichtet wird, daß eine Verknüpfung des entstehenden Personalausweisregisters mit anderen Dateien verhindert wird und eine eindeutige Regelung zum Verfahren bei Verlust des Ausweises festgelegt wird.

Die von den Datenschutzbeauftragten geforderten bereichsspezifischen Datenschutzregelungen existieren in Berlin ebensowenig wie in den meisten anderen Bundesländern.

Insbesondere enthält das Allgemeine Gesetz zum Schutz der öffentlichen Sicherheit und Ordnung in Berlin *(Allgemeines Sicherheits- und Ordnungsgesetz - ASOG)* keine hinreichenden Regelungen der polizeilichen Datenverarbeitung. Die rechtlichen Voraussetzungen für die polizeiliche Beobachtung und die Identitätsfestellung sind ebenfalls unzureichend geregelt. Auf Grund der vorhandenen Regelungen wäre die von den Sicherheitsbehörden ins Auge gefaßte, über den derzeitigen Umfang der Kontrollen hinausgehende Nutzung des Ausweises nicht möglich. Über diesen grundsätzlichen Sachverhalt hinaus fehlen auch flankierende Vorschriften, die z.B. den Informationsaustausch zwischen Polizei und Nachrichtendiensten, zwischen Polizei und Zollverwaltung sowie den Umfang von Fahndungsabfragen bei den verschiedenen Kontakten des Bürgers mit der Polizei regeln.

Im übrigen ist auch der Bundesgesetzgeber aufgerufen, für den Bereich der Strafverfolgung entsprechende Präzisierungen der *Strafprozeßordnung* vorzunehmen.

Landesmeldegesetz

Im Hinblick auf die Vorbehalte der Datenschutzbeauftragten gegenüber der Einführung des maschinenlesbaren Ausweises ergibt sich eine zusätzliche Notwendigkeit für eine datenschutzgerechte Ausgestaltung des Landesmeldegesetzes in Berlin. Zwar ist das Melderechtsrahmengesetz des Bundes seit August 1980 in Kraft, die Umsetzung in Landesrecht steht jedoch noch immer aus. Es ist allerdings zu erwarten, daß im Laufe des nächsten Jahres das Gesetzgebungsverfahren in Berlin abgeschlossen wird. Über meine Bedenken gegen den vom Senat eingebrachten Entwurf für ein Landesmeldegesetz habe ich bereits im Jahresbericht 1982 berichtet[18]. Der Ausschuß für Inneres, Sicherheit und Ordnung des Abgeordnetenhauses gibt mir während der laufenden Beratungen Gelegenheit, meine Position zur Geltung zu bringen.

Einwohnerwesen

Die derzeitige Praxis des Meldewesens wird bestimmt durch die Nutzung des Informationssystems Einwohnerwesen des Polizeipräsidenten, das die umfassendste personenbezogene Datei meines Zuständigkeitsbereiches darstellt. Seine vielfältigen Wirkungen auf die Beziehungen zwischen Bürgern und eingreifender Verwaltung waren auch in diesem Jahr Gegenstand vieler Eingaben und Prüfvorgänge.

Es wurden dabei im wesentlichen folgende Problemkreise offenkundig:

- Falsche Daten über Bürger führen zu Verletzungen schutzwürdiger Belange in verschiedener Weise (Fehlspeicherungen),
- die Daten werden für außerdienstliche Zwecke genutzt,
- der Zugriff auf Daten, die einer Auskunftssperre unterliegen, ist nicht ausreichend eingeschränkt (Unzulänglichkeiten der Auskunftssperre).

Zu dem Problem *Fehlspeicherung* seien folgende Beispiele angeführt:

- Ein Bürger beschwerte sich darüber, daß er bei einer Ummeldung nach seinen Entlassungspapieren aus der Untersuchungshaft gefragt wurde, obwohl er zu keiner Zeit in Haft gewesen war. Es stellte sich heraus, daß aufgrund einer Namensverwechslung, die auf der Gleichheit von Geburtsdatum und einem Vornamen beruhte, die Unterbringung in einer Untersuchungshaftanstalt in seinen Datensatz eingetragen worden war.
- Eine Bürgerin beschwerte sich darüber, daß ihr Ehemann als Polizeibeamter aus der Einwohnerdatenbank erfahren hatte, daß sie schwerbeschädigt sei, obwohl dies keineswegs zutraf. Nachprüfungen ergaben, daß die Eintragung gegenstandlos war und das Merkmal „Schwerbeschädigung" bereits bei der Ersterfassung der Einwohnerdatenbank irrtümlich vermerkt worden war.
- Eine andere Bürgerin beschwerte sich darüber, daß sie bereits seit längerem keine Wahlunterlagen erhalten hatte. Es stellte sich heraus, daß sie zwei Staatsbürgerschaften besitzt und die deutsche Staatsbürgerschaft, an der amtlich keine Zweifel bestanden, bei der Ersterfassung versehentlich nicht eingetragen worden war.

Bei der Ersterfassung der Einwohnerdatenbank Mitte der 70-iger Jahre sind offensichtlich Erfassungsfehler aufgetreten, die erst heute aufgrund daraus resultierender Fehler im Verwaltungsvollzug entdeckt werden. Die Ursache solcher Fehler, die bei Erfassungsaufgaben dieser Größenordnung wohl unvermeidbar sind, lassen sich heute nicht mehr nachvollziehen. Sie beruhen im wesentlichen auf der fehlerhaften Übertragung von korrekten Akten und Karteien in die Datenbank. In diesen Fällen kann ich den Bürgern nur empfehlen, sich bei Anzeichen für Fehlspeicherungen an die Meldebehörden bzw. Bezirkseinwohnerämter direkt zu wenden und in Problemfällen meine Hilfe in Anspruch zu nehmen. Die Entdeckung solcher Fehler, die - wie obige Beispiele zeigen - durchaus gravierende Folgen haben können, ist nur dem Bürger selbst möglich. Die Beseitigung solcher Fehler ist nach meinen Erfahrungen unproblematisch.

Zur Vermeidung von Fehlspeicherungen bei Neueingaben in die Einwohnerdatenbank beabsichtigt der Polizeipräsident in Berlin nunmehr, den Zugriff zu Änderungszwecken durch technische Maßnahmen nur noch zu ermöglichen, wenn Familienname und Geburtsdatum zur Identifizierung des Datensatzes herangezogen werden und durch weitere Angaben gegebenenfalls eine Eindeutigkeit hergestellt werden kann. Darüber hinaus wird jetzt bei der Protokollierung von „letzte Änderungen" vermerkt, wenn die Änderung einer Eintragung aufgrund einer vorhergehenden Fehleintragung erfolgte. Dies ist insbesondere bei diskriminierenden Fehleintragungen von Bedeutung.

Der Kreis derjenigen, die die Möglichkeit haben, *Einsicht* in die Daten der Einwohnerdatenbank zu nehmen, ist sehr groß. Fast alle Polizeibeamten, Mitarbeiter der Meldebehörden und der Bezirkseinwohnerämter können Daten aus der Einwohnerdatenbank abrufen oder abrufen lassen. So nimmt es nicht Wunder, daß sich Bürger in mehreren Angelegenheiten darüber beschwert haben, daß Personen, die zum obengenannten Personenkreis gehören oder Beziehungen zu diesem Personenkreis haben, sich mit Kenntnissen brüsteten, die sie sich ohne Einwohnerdatenbank wohl nicht hätten verschaffen können. In einem bekannt gewor-

[18] S. 9f.

denen Fall hat der Polizeipräsident in Berlin harte disziplinarische Maßnahmen ergriffen, die er immer treffen wird, wenn ihm die Bediensteten, die solche unbefugten Zugriffe vorgenommen hatten, namentlich bekannt werden.

Die automatische Protokollierung der Zugriffe an die Einwohnerdatenbank zu Auskunftszwecken wie beim Informationssystem Verbrechensbekämpfung erfolgt aus Kapazitätsgründen bisher nicht.

Aus verschiedenen Gründen können *Auskunftssperren* für Datensätze in der Einwohnerdatenbank verfügt werden, so z.B. auf begründeten Antrag des Bürgers, bei Kindern, die in Adoptivpflege gegeben worden sind (Adoptionssperre), bei Personen, die von Amts wegen vor Ausforschung zu schützen sind (Amtssperre) und bei Betroffenen, die auf Grund § 14 Abs. 2 Berliner Datenschutzgesetz die Sperrung ihrer Daten bewirkt haben. Bis auf die sehr sichere Amtssperre bedeutete eine Auskunftssperre nur eine Beschränkung der Auskunft nach § 17a Meldegesetz, aber keine Einschränkung des Zugriffs für den großen Benutzerkreis. Dies hatte zur Folge, daß in einzelnen Fällen Durchbrechungen der Auskunftssperre, namentlich der Adoptionssperre bekannt wurden (vgl. 2.6). Darüber hinaus waren andere Durchbrechungen zu befürchten, da innerhalb des Kreises der Personen, denen ein Zugriff ermöglicht wird, auch Personen waren, denen gegenüber z. B. das Adoptionsgeheimnis nach § 1758 Bürgerliches Gesetzbuch zu schützen war.

Der Polizeipräsident in Berlin hat das Verfahren des Zugriffs auf die Daten, die einer Sperre unterliegen, programmtechnisch grundlegend geändert. Jetzt können gesperrte Daten nur noch von besonders privilegierten und verantwortlichen Bediensteten, deren Berechtigung im Rahmen der technischen Zugriffskontrolle vom Informationssystem Einwohnerwesen geprüft wird, abgerufen werden. Damit wurde eine Lösung gefunden, die den inneren Dienstbetrieb der Meldebehörden nicht unzumutbar belastet. Darüber hinaus wird der Zugriff auf gesperrte Daten automatisch protokolliert.

Informationssystem Verbrechensbekämpfung

Auf dem Gebiet der Strafverfolgung konnte die von mir im Jahresbericht 1982 angekündigte Überprüfung des Informationssystems Verbrechensbekämpfung aus den obengenannten Gründen zwar begonnen, nicht aber zu Ende geführt werden. Sie wird im kommenden Jahr fortgeführt.

Auf Grund von Eingaben, die sich gegen die Nutzung dieses Systems richten, sind zwei Fallgruppen besonders bemerkenswert, die große Ähnlichkeit mit bereits dargestellten Problemen des Zugriffs auf das Einwohnermelderegister aufweisen.

Mehrfach mußte festgestellt werden, daß Polizeibeamte außerhalb ihrer Zuständigkeit entweder selbst auf personenbezogene Daten im ISVB zugreifen oder aber durch die Einschaltung berechtigter Beamter (z. B. durch Anrufe) sich Kenntnis aus dem ISVB verschaffen.

An der Aufklärung derartiger Fälle des unzulässigen Abrufs ist der Polizeipräsident selbst sehr interessiert und ergreift auch hier harte disziplinarische Maßnahmen, wenn ihm mißbräuchliche Abrufe bekannt werden; in einem Fall ist es zu einem Strafverfahren gekommen, bei dem der Angeklagte zwar freigesprochen wurde, die Problematik der Strafbarkeit des Abrufs aus Dateien (§ 28 Berliner Datenschutzgesetz) aber nicht mit der wünschenswerten Deutlichkeit zum Ausdruck gebracht wurde.

Zum einen bedarf es hier neben den im Rahmen der kommenden Überprüfungen zu diskutierenden Zugriffsbeschränkungen einer verstärkten und kontinuierlichen Aufklärung der Polizeibeamten über ihre Pflichten bei der Nutzung dieses äußerst sensiblen Systems, zum anderen muß sichergestellt werden, daß im Rahmen interner Schulung und Ausbildung beispielhaft nicht auf Echtdaten Zugriff genommen wird, sondern zu diesem Zweck ein eigener Datenbestand mit fiktiven Daten erstellt wird.

Schwierigkeiten bei der datenschutzrechtlichen Aufklärung derartiger Mißbrauchsfälle zeigen sich immer dann, wenn der Petent - obwohl auf diesen Umstand hingewiesen - mir ausdrücklich aufgibt, den Namen des betreffenden Polizeibeamten gegenüber der Polizeibehörde nicht zu nennen. Darüber hinaus kann in solchen Einzelfällen dem Polizeipräsidenten auch die Möglichkeit zu einer gezielten disziplinarischen und strafrechtlichen Verfolgung genommen sein. Dennoch muß sich der Petent auch hier auf die zugesicherte Vertraulichkeit verlassen können, anderenfalls meine gesetzlich verankerte Unabhängigkeit und damit die vom Gesetzgeber gewollte besondere Vertrauensstellung zum Bürger gefährdet würde. Jedoch empfehle ich dem Petenten, sich selbst an den Polizeipräsidenten zu wenden, um die innerorganisatorischen Regelungen wirksam werden zu lassen, da eine vollkommene technische Vorbeugung nicht möglich ist.

Probleme ergeben sich naturgemäß auch aus dem Umstand, daß das ISVB neben nachgewiesenen Daten auch unbestätigte, ja möglicherweise durch das anschließende Gerichtsverfahren widerlegte, aber auch veraltete und im Bundeszentralregister getilgte Daten enthält.

Im Jahresbericht 1982 hatte ich bereits gefordert, durch die Einrichtung entsprechender *Rückmeldungen von den Justizbehörden* an die Polizei wenigstens in den Fällen eine Verbesserung zu erreichen, in denen entsprechende Entscheidungen der Staatsanwaltschaft oder der Gerichte vorliegen. Die Einführung entsprechender, von den Richtlinien für die Führung Kriminalpolizeilicher personenbezogener Sammlungen (KpS) im übrigen vorgeschriebener Verfahren wird bisher von den beteiligten Stellen abgelehnt. In seiner Sitzung vom 1. Juni 1983 hat sich der Unterausschuß „Berliner Datenschutzgesetz" des Ausschusses für Inneres, Sicherheit und Ordnung auch dieses Problems angenommen[19].

Der Unterausschuß hatte übereinstimmend eine zügige Berichtigung dieser Daten für erforderlich gehalten und mich gebeten, im Jahresbericht 1983 auf den Sachstand einzugehen.

Da das Problem bundesweit besteht, wird es notwendig sein, daß sowohl einheitliche Regelungen gefertigt werden als auch ein einheitliches Formular von den Ländern erarbeitet wird.

Die Justiz- und Innenverwaltungen von Bund und Ländern haben inzwischen die Angelegenheit aufgegriffen und befassen sich derzeit mit den Möglichkeiten einer Verbesserung der Unterrichtung der Polizeibehörden über Ausgänge von Strafverfahren.

So ist insbesondere an eine Neufassung der Nr. 11, 12 der Anordnung über Mitteilungen in Strafsachen (MiStra) und an die Ausarbeitung eines differenzierten Formblattes für die Rückmeldungen der Justizbehörden gedacht.

Eine entsprechende Überarbeitung der MiStra hat der Justizminister des Landes Nordrhein-Westfalen übernommen, parallel dazu hat der Arbeitskreis II der Innenministerkonferenz auf seiner Sitzung am 26./27. September 1983 einen ad-hoc-Ausschuß unter dem Vorsitz des Innenministers des Landes Nordrhein-Westfalen mit der Erarbeitung eines Rückmeldeformulars beauftragt.

Die Speicherung personenbezogener Daten, die sich auf Vorgänge beziehen, die im Bundeszentralregister bereits getilgt sind, wird zwar für zulässig gehalten. Die KpS-Richtlinien sehen jedoch auch hier nach dem Ablauf bestimmter Fristen die *Löschung* vor. Mir sind wiederum eine Reihe von Fällen bekannt geworden, in denen trotz der bereits fälligen Löschung derartige Daten an andere Behörden (z. B. zu Einstellungszwecken) weitergegeben wurden.

Im erforderlichen Rahmen ist eine Zusammenarbeit zwischen dem Polizeipräsidenten und dem *Landesamt für Verfassungsschutz* vorgeschrieben. So ist der Polizeipräsident gehalten, bei Ereignissen, bei denen Bestrebungen gegen die freiheitlich demokratische Grundordnung erkennbar sind, das Landesamt für Verfassungsschutz zu informieren. Eine Beschwerde zeigte, daß hierbei nicht immer mit der erforderlichen Präzision vorgegangen wird. So wurde in einem Fall mitgeteilt, eine Personenfeststellung sei „anläßlich gewalttätiger Ausschreitungen in Berlin-Kreuzberg" vorgenommen worden. Tatsächlich war die Identitätsfeststellung Stunden nach der Demonstration in einem Lokal vorgenommen worden, von dem die Polizeibeamten nur vermuteten, daß sich dort Gewalttäter aufhalten könnten. Auf Grund der Mitteilung mußte jedoch angenommen werden, daß gegen den Be-

[19] Vgl. Jahresbericht 1982, S. 12

troffenen bereits ein konkreter Verdacht bestehe. Dies wiederum führte dann bei einer Bewerbung in einen sicherheitsempfindlichen Bereich der öffentlichen Verwaltung dazu, daß ein Petent abgelehnt wurde.

Nachdem ich die Angelegenheit aufgegriffen hatte, hat mir der Polizeipräsident zugesagt, daß man in Zukunft bei entsprechenden Mitteilungen an das Landesamt für Verfassungsschutz auf eine unmißverständliche Darstellung des Sachverhalts achten werde. Im konkreten Fall wurde die negative Entscheidung dadurch korrigiert, daß dem Petenten mitgeteilt wurde, von sofort an stehe einer Bewerbung nichts entgegen.

2.6 Risiken für das Adoptionsgeheimnis

Der Senator für Schulwesen, Jugend und Sport hatte mich auf Grund von Hinweisen auf Verletzungen des Adoptionsgeheimnisses gem. § 1758 Bürgerliches Gesetzbuch gebeten, die Datenflüsse des Adoptionsverfahrens auf Risiken für das Adoptionsgeheimnis zu untersuchen. Dabei kam es auf jene Bereiche des Verfahrens an, in denen die Einwohnerdatenbank des Polizeipräsidenten in Berlin eine Rolle spielt. Meine Untersuchung hatte im wesentlichen folgendes Ergebnis:

Wenn ein Kind, welches in Berlin gemeldet ist, in Adoptionspflege gegeben wird, wird auf Antrag beim Einwohnermeldeamt eine Auskunftssperre für den Datensatz des Kindes gesetzt. Dies bedeutet, daß Benutzer der Datenbank bei Abruf dieses Datensatzes auf die Sperre hingewiesen wurden, der Datensatz jedoch auf dem Bildschirm erschienen ist. Das Vormundschaftsgericht, welches schließlich die Annahme an Kindes Statt ausspricht, meldet diese Entscheidung an das Standesamt, das die Geburt des Kindes beurkundet hat. Das Standesamt trägt den Annahmebeschluß und die Namensänderung als Randvermerk in das Geburtenbuch ein und meldet nach Abschluß des Vorgangs die Änderung des Geburteneintrags an eine für das Standesamt zuständige Meldestelle des Polizeipräsidenten in Berlin. Die Meldestelle ruft dann in der Einwohnerdatenbank ein Programm auf, das die Legitimation des Kindes auf die Datenbank abbildet, insbesondere den Namen des Kindes ändert, alle Bezüge zu den leiblichen Eltern löscht und die Adoptiveltern als neue leibliche Eltern behandelt. Darüber hinaus wird die Adoptionssperre mangels weiterer Erforderlichkeit aufgehoben.

Die geringsten Risiken für das Adoptionsgeheimnis sind dann gegeben, wenn die Eintragung der neuen Kindesadresse und die Eintragung der Adoptionssperre in die Einwohnerdatenbank gleichzeitig erfolgen, wenn die gesperrten Daten in der Zeit der Adoptionssperre nur privilegierten Benutzern zugänglich sind und wenn der Zeitraum zwischen der Gerichtsentscheidung über die Adoption und der datenmäßigen Legitimation des Kindes in der Meldestelle möglichst kurz ist.

Diesen Anforderungen entspricht das bisherige Verfahren nicht in vollem Umfang. Da die Ummeldung des Kindes durch die Adoptionspflegeeltern in der Regel früher geschah als die Sperre auf Antrag der zentralen Adoptionsvermittlung, war daher die Adoptionssperre im Datensatz des Kindes für eine gewisse Zeit meistens nicht gesetzt. Dies stellt ein besonderes Risiko dar, weil Außenstehende mit Kenntnissen behördlicher Arbeitsabläufe diese Schwachstelle ausrechnen und bewußt zur Durchbrechung des Adoptionsgeheimnisses ausnutzen können.

Ich habe daher empfohlen, ein Meldeverfahren einzurichten, bei dem der Eintrag der zu schützenden Daten in die Einwohnerdatenbank und die Verfügung der Sperre gleichzeitig erfolgen. Dies könnte durch ein besonderes zwischen der zentralen Adoptionsvermittlung und dem Einwohnermeldeamt koordiniertes Anmeldeverfahren bei Adoptivkindern geschehen. Mir wurde signalisiert, daß grundsätzliche Bedenken gegen dieses Verfahren nicht bestehen, eine Umsetzung ist jedoch bisher nicht erfolgt.

Die Gefahren versehentlicher Auskunftserteilung über gesperrte Daten, die dadurch groß waren, weil die gesperrten Daten dennoch auf dem Bildschirm für jeden Sachbearbeiter in den Meldestellen sichtbar wurden, ist dadurch gebannt worden, daß der Umgang mit gesperrten Daten in der Einwohnerdatenbank grundsätzlich geändert worden ist. Hierauf bin ich in Abschnitt 2.5 näher eingegangen. Der Polizeipräsident in Berlin hat mir ferner zugesagt, daß die Mitarbeiter der Meldestellen und des Einwohnermeldeamtes besondere Sorgfalt walten lassen, wenn Auskünfte mit Merkmalen, die den früheren Eltern noch bekannt sein können, über Personen erbeten werden.

Ich habe ferner festgestellt, daß der Zeitraum zwischen der Gerichtsentscheidung über eine Adoption und der datenmäßigen Legitimation in der Einwohnerdatenbank sehr lang sein kann, so daß die größtmögliche Sicherheit für das Adoptionsgeheimnis lange Zeit nicht erreicht wird. Ich habe den Polizeipräsidenten in Berlin, die Aufsichtsbehörde für die Standesämter beim Senator für Inneres und den Senator für Justiz gebeten, zu prüfen, welche Möglichkeiten gesehen werden, den Meldeweg zwischen den Vormundschaftsgerichten und den Meldestellen nach Rechtskraft der Adoption zu verkürzen. Die mir bisher vorliegenden Stellungnahmen lassen nicht erkennen, daß organisatorische Änderungen unverzüglich vorgenommen werden. Jedoch hat der Senator für Inneres als Aufsichtsbehörde der Standesämter mein Anliegen an die Standesämter von Berlin weiter vermittelt und um die beschleunigte Abwicklung aller Adoptionsvorgänge gebeten.

Obwohl meine Vorschläge bisher nicht vollständig aufgenommen worden sind, haben sich Risiken für das Adoptionsgeheimnis doch entscheidend verringert, insbesondere weil der Polizeipräsident in Berlin im Bereich des Meldewesens die möglichen Verbesserungen fortschreitend einführt.

2.7 Sozialwesen

Auch 1983 bestätigte sich, daß die neuen Bestimmungen zum Datenschutz im *Sozialgesetzbuch X* nicht ohne Schwierigkeiten vollzogen werden können. Viele teilweise gravierende Probleme waren Gegenstand von Beschwerden und Beratungsvorgängen, aber auch von Fortbildungsveranstaltungen und Koordinierungstreffen, auf denen Lösungsvorschläge im Kontakt mit den Behördenmitarbeitern erarbeitet werden konnten.

Grenzen der Offenbarung

Als zentrales Problem erwies sich dabei häufig die allgemeine Frage, auf welcher *Organisationsebene* die besonderen Bestimmungen des SGB X greifen: Wie die Gemeinden in den anderen Ländern nehmen in Berlin die Bezirksämter eine Vielzahl von Aufgaben nach dem Sozialgesetzbuch wahr, die sowohl von ihrer Zielsetzung als auch vom erforderlichen Datenumfang her erheblich voneinander abweichen. Die gelegentlich vertretene Auffassung, daß ungeachtet dieses Umstands das Bezirksamt als eine speichernde Stelle anzusehen sei und daher die innerhalb des Bezirksamts laufenden Datenflüsse von den Bestimmungen des SGB X nicht tangiert werden, führt zu keiner angemessenen Lösung. Das SGB X zielt gerade darauf ab, die funktionsgerechte Verwertung von Daten, die beim Betroffenen oder bei einem Dritten für einen bestimmten Zweck erhoben worden sind, zu gewährleisten. Zweckentfremdungen sollen nur zulässig sein, wenn dies für die Erfüllung von Aufgaben, die im Sozialgesetzbuch festgesetzt sind, erforderlich ist (§ 69 SGB X) oder der Gesetzgeber dies in einem abgeschlossenen Katalog von weiteren Offenbarungstatbeständen festgelegt hat (§§ 70 ff SGB X). Eine solche Zweckentfremdung liegt aber auch dann vor, wenn innerhalb eines Bezirksamtes personenbezogene Daten von einer Stelle, die eine bestimmte Aufgabe erfüllt, an eine Stelle mit einer anderen Aufgabenstellung weitergegeben werden. Eine Offenbarung im Sinne des SGB X ist daher dann anzunehmen, wenn eine Ungleichheit bei der Aufgabenstellung der betroffenen Stellen vorliegt.

Es ist sicherlich schwierig, die organisatorischen Einheiten festzulegen, innerhalb derer bei einer internen Weitergabe eine solche Aufgabenänderung nicht vorliegt. Da einer Stelle häufig mehrere Aufgaben zugewiesen sind, ist eine Bündelung von Aufgaben nicht immer zu vermeiden. Ein Blick auf das (einheitliche) Organisationsschema der Bezirksämter zeigt, daß diese Voraussetzungen am ehesten auf der Ebene der Ämter vorliegen. Die Folge ist, daß eine Offenbarung von Sozialdaten (nur) dann vorliegt, wenn Daten von einem Amt an ein anderes weitergegeben werden. Darüber hinaus können die Offenbarungsvorschriften auch Konsequenzen für die Organisation der Ämter haben: Die Aufgaben sollten so gebündelt werden, daß innerhalb der Ämter kein Konflikt mit den Offenbarungsvorschriften entstehen kann.

Schwerwiegende Probleme wirft unter diesem Aspekt die *Aktenführung* insbesondere der Stellen auf, bei denen traditionsgemäß eine Vielzahl von Unterlagen aus verschiedenen Aufgabenbereichen urschriftlich, häufig aber auch in Form von Durchschlägen zusammenlaufen. So werden in den Ämtern für Familienfürsorge Akten geführt, die die verschiedensten Lebensbereiche der Betroffenen berühren können (z. B. über wirtschaftliche Hilfen ebenso wie über strafbares Verhalten oder Ehescheidungs-und Sorgerechtsangelegenheiten). Soweit es überhaupt erforderlich ist, derartig umfassende Akten zu führen (dies wäre ebenfalls grundsätzlich zu überprüfen), muß die Aktenführung es ermöglichen, bei einer erforderlichen Weitergabe von Akten diejenigen Aktenbestandteile auszusondern, die für die Aufgabenstellung der anfragenden Stelle nicht erforderlich sind.

Ein weiteres Problem ist der Umstand, daß diese Akten nicht nur personenbezogene Daten der direkt betroffenen Beteiligten enthalten, sondern auch von Personen, die zu deren sozialen Umfeld gehören (z. B. Familie, Freunde, Nachbarn). Hier macht auch die Gewährleistung der datenschutzrechtlichen Ansprüche der Beteiligten Schwierigkeiten: Das Akteneinsichtsrecht des einen Beteiligten beeinträchtigt unter Umständen die Persönlichkeitsrechte eines anderen, auch die Übermittlung im nach dem SGB X zulässigen Rahmen kann die Interessen Dritter berühren.

Vom Senator für Schulwesen, Jugend und Sport ging eine Initiative aus, in einer Projektgruppe unter Beteiligung von Sozialarbeitern aus der Familienfürsorge Verbesserungsmöglichkeiten zu entwickeln. Einer meiner Mitarbeiter hat an dieser Arbeitsgruppe regelmäßig teilgenommen. Ich unterstütze den Versuch, eine Vermittlung zwischen den praktischen Erfordernissen und den datenschutzrechtlichen Anforderungen herbeizuführen. Es wird eine der dringlichen Aufgaben für die beteiligten Senatsverwaltungen sowie die Fachabteilungen der Bezirksämter sein müssen, hierzu einheitliche Grundsätze zu entwickeln und durchzusetzen.

Über die allgemeinen Fragen hinaus stellte sich eine Vielzahl von Einzelproblemen. Einige wichtige Aspekte sollen im folgenden angesprochen werden:

Erhebung und Speicherung

Die Erhebung und Speicherung personenbezogener Daten ist auch im Sozialbereich an der Erforderlichkeit für die Aufgabenstellung zu messen (§ 9 Bundesdatenschutzgesetz). Die herkömmlichen Verfahren berücksichtigen diesen Aspekt nicht immer hinreichend.

Ein Arbeitgeber beschwerte sich über den Inhalt der Formulare, mit denen der Träger der Sozialhilfe gem. § 116 Abs. 2 Bundessozialhilfegesetz vom Arbeitgeber *Auskünfte über das Arbeitsentgelt* einholen kann. In den Formularen wurde auch nach der Steuerklasse, nach zusätzlichen Forderungen und Pfändungen, sowie nach der Krankenkasse des Betroffenen gefragt. Dies geht über den erforderlichen Umfang hinaus. Von der Senatsverwaltung wurde eine Überarbeitung der Formulare zugesichert.

Ein Versicherungsnehmer der Landesversicherungsanstalt Berlin beschwerte sich über die formularmäßige Anforderung des Urteils des Vormundschaftsgerichts zum Nachweis eines Adoptionsverhältnisses. Für den *Nachweis des Kindschaftsverhältnisses* reicht die Vorlage der Geburtsurkunde aus, da diese die Vaterschaft des Adoptivvaters ausweist, ohne einen eindeutigen Hinweis auf das Adoptionsverhältnis zu geben. Dem Adoptionsgeheimnis und damit der Geheimhaltung der leiblichen Eltern kommt ein hoher Stellenwert zu. Die Anforderung der vormundschaftsgerichtlichen Entscheidung berücksichtigt dies nicht, da sie im Gegensatz zur Geburtsurkunde personenbezogene Daten der leiblichen Eltern offenbart.

Häufig werden personenbezogene Daten in einem das erforderliche Ausmaß überschreitenden Umfang erhoben, um ohne Rücksicht auf die Sensibilität der Daten Entscheidungen zusätzlich abzusichern.

Gemäß §§ 39, 40 Bundessozialhilfegesetz übernimmt der Träger der Sozialhilfe im Rahmen der Behindertenhilfe des Kinder- und Jugendpsychiatrischen Dienstes bestimmte Therapiekosten. Hierbei hat die Behörde ähnlich einer Krankenkasse die Therapiebedürftigkeit zu prüfen, um danach die Kostenübernahme zu bewilligen. Während beispielsweise der AOK hierfür ausreicht, daß der Psychotherapeut nur das Ergebnis der Begutachtung und die voraussichtliche Dauer und Art der Therapiebedürftigkeit mitteilt, verlangen die Jugendämter den vollen Wortlaut eines *Kosten- und Behandlungsplanes,* der vom Gesundheitsamt oder einem Therapeuten zu erstellen ist. Abgesehen davon, daß die Erforderlichkeit schon deswegen fragwürdig ist, weil andere Stellen mit vergleichbaren Aufgaben ohne diese Unterlagen auskommen, schreibt § 126 Bundessozialhilfegesetz vor, daß Kosten- und Behandlungspläne nur mit ausdrücklich erklärter Zustimmung des Antragstellers vom Gesundheitsamt an das Jugendamt weitergeleitet werden dürfen. Dieses Erfordernis entspricht den Einschränkungen, die § 76 Abs. 2 SGB X für besonders schutzwürdige personenbezogene Daten enthält. Auch hierüber setzen sich die Jugendämter hinweg, indem sie ihre Leistungen von der entsprechenden Zustimmung des Betreuten abhängig machen. Dies entspricht nicht der Intention des Gesetzgebers. Hätte er dies gewollt, hätte er eine gesetzliche Offenbarungspflicht gegenüber dem Jugendamt geschaffen. Vielmehr ist der Umfang der von den Jugendämtern zu erhebenden Daten auf den zur Aufgabenerfüllung erforderlichen und ohne Einwilligung offenbarungsfähigen Umfang zu reduzieren. Der gesamte Kosten- und Behandlungsplan entspricht dieser Anforderung nicht.

Trotz meiner gegenteiligen Empfehlung ist es in einem Bezirksamt sogar zur Ablehnung eines Leistungsantrages gekommen, der allein mit der verweigerten Zustimmung eines Elternteils zur Übermittlung des Kosten- und Behandlungsplanes an das Jugendamt begründet wurde. Der Bescheid wurde jedoch inzwischen wieder aufgehoben.

Derzeit dauern noch Gespräche mit den zuständigen Verwaltungen an, die auf eine Änderung der Praxis abzielen.

Offenbarung für die Erfüllung sozialer Aufgaben

Abgesehen von der Einwilligung des Betroffenen ist eine Offenbarung von Sozialdaten nur dann zulässig, wenn eine der in den §§ 69 ff SGB X aufgenommenen Tatbestände vorliegt (§§ 35 SGB I, 67 SGB X). Dabei kommt es entscheidend darauf an, ob die Offenbarung zur Erfüllung von Aufgaben nach dem Sozialgesetzbuch erforderlich ist (§ 69 SGB X) oder die Offenbarung einem anderweitigen Zweck dient.

Die Privilegierung der Offenbarung für Zwecke der Sozialverwaltung besteht nicht ohne Einschränkungen: Insbesondere können die Berufsgeheimnisse, denen u. a. Ärzte und staatlich anerkannte Sozialarbeiter unterworfen sind (vgl. § 203 Abs. 1 Ziff. 5 Strafgesetzbuch), auch dann einer Offenbarung entgegenstehen, wenn diese von Sozialbehörden für erforderlich gehalten wird.

Dieses Problem wurde z. B. im Bereich der *Jugendgerichtshilfe* relevant. Die Jugendgerichtshilfe ist als Aufgabe nach dem Sozialgesetzbuch den Jugendämtern zugewiesen (§§ 38 Jugendgerichtgesetz, 27 SBG I) und wird in Berlin von den Ämtern für Familienfürsorge bei den Bezirksämtern wahrgenommen. Nach Ziff. 32 der Anordnung über Mitteilungen in Strafsachen (MiStra) erhält die Jugendgerichtshilfe bei Strafverfahren gegen Jugendliche den polizeilichen Schlußbericht zur Kenntnisnahme. Dies ist zur rechtmäßigen Aufgabenerfüllung der Jugendgerichtshilfe erforderlich. Ein derartiger Schlußbericht wurde in einem Bezirksamt an die Abteilung Sozialwesen weitergeleitet, damit diese überprüfen konnte, ob einem der beteiligten Jugendlichen weiterhin in der bisherigen Höhe Behindertenhilfe gezahlt werden könne.

Das Bezirksamt hielt die Weitergabe wegen § 69 SGB X für zulässig. Dem habe ich widersprochen. Es ist davon auszugehen, daß die im polizeilichen Schlußbericht enthaltenen Angaben persönliche Geheimnisse darstellen und dem in der Jugendgerichtshilfe tätigen Sozialarbeiter dienstlich anvertraut wurden. § 203 Abs. 1 Strafgesetzbuch läßt die Offenbarung nur zu, wenn eine ausdrückliche Befugnisnorm dies vorsieht. Die Befugnisnorm des § 69 Abs. 1 Ziff. 1 SGB X kann diese Funktion nicht übernehmen, da die Daten ausschließlich zu einem bestimmten Zweck, nicht aber generell zur Wahrnehmung von Aufgaben der Sozialverwaltung an den Sozialleistungsträger übermittelt wurden. Der polizeiliche Schlußbericht dient aber ausschließlich Zwecken der Jugendgerichtshilfe (vgl. auch den Wortlaut von Ziff. 32 MiStra).

§69 Abs. 2 bindet eine Reihe von Behörden und anderen Stellen, die dem SGB X verwandte Aufgaben wahrnehmen, aus bestimmten Gründen aber formell nicht Sozialleistungsträger sind, in den Kreis der nach dem SGB X berechtigten und verpflichteten Stellen ein. Hierzu zählen z. B. die Stellen, die Leistungen nach dem Beamtenversorgungsgesetz zu erbringen haben. Als Ausnahmevorschrift ist diese Bestimmung eng auszulegen. So kann eine Analogie zwischen den Stellen, die Leistungen nach dem Beamtenversorgungsgesetz erbringen, zu den Stellen, die über die *Beihilfe* entscheiden (§44 Landesbeamtengesetz), nicht gezogen werden. Aus diesem Grunde mußte beanstandet werden, daß sich das in Berlin für die Beihilfezahlungen einer Reihe von Behörden zuständige Landesverwaltungsamt unmittelbar an die Allgemeine Ortskrankenkasse gewandt hatte, um von dort Angaben zum Beihilfeantrag eines Bediensteten zu erhalten. Hierzu wäre vielmehr die Einwilligung des Betroffenen erforderlich gewesen.

Offenbarung für die Durchführung eines Strafverfahrens

Starkes Interesse in der Öffentlichkeit fand auch in diesem Jahr die Frage, unter welchen Voraussetzungen Sozialleistungsträger Sozialdaten an die Polizei zu Zwecken der Strafverfolgung offenbaren dürfen. Zu berücksichtigen wird hierbei künftig das letztinstanzliche Urteil des Kammergerichts zu einem Fall sein, den ich bereits im Jahresbericht 1982[20] dargestellt hatte. Ein Angestellter eines Arbeitsamtes hatte der Polizei auf deren Anfrage hin mitgeteilt, ein gesuchter Arbeitsloser befinde sich gerade im Dienstgebäude. Da die Polizei keine richterliche Anordnung vorweisen konnte, hielt ein Mitarbeiter diese Mitteilung für unzulässig und schickte den Arbeitslosen weg.

Im Ergebnis wurde der Angeklagte ebenso wie von der Vorinstanz freigesprochen. In der datenschutzrechtlichen Bewertung weicht das Kammergericht jedoch erheblich von der Vorinstanz ab. Insbesondere ist das Gericht der Auffassung, daß neben der speziellen Offenbarungsvorschrift für Strafverfolgungsbehörden (§73 SGB X) diesen Stellen auch die allgemeinen Offenbarungsbefugnisse im Rahmen der *Amtshilfe* zur Verfügung stehen (§68 SGB X). Diese ursprünglich vom Bundesbeauftragten für den Datenschutz ebenso wie von mir wegen der Spezialität des §73 SGB X abgelehnte Deutung muß nunmehr zwar hingenommen werden. Zu beachten ist jedoch, daß nach §68 Abs. 1 SGB X die Amtshilfe durch Sozialleistungsträger nur zulässig ist, wenn die ersuchende Stelle die Angaben nicht auf andere Weise beschaffen kann und wenn durch die Offenbarung schutzwürdige Belange des Betroffenen nicht beeinträchtigt werden. Ferner setzt die Offenbarung nach §68 Abs. 2 SGB X eine Entscheidung des Leiters der ersuchten Stelle, seines allgemeinen Stellvertreters oder eines besonders bevollmächtigten Bediensteten voraus.

Das Kammergericht führt weiter aus: „Mithin umfaßt der Begriff der derzeitigen Anschrift gewissermaßen als Minus auch den gegenwärtigen Aufenthalt". Inwieweit diese Deutung des Begriffs „Anschrift" (§68 SGB X) auf andere Fälle übertragen werden kann, muß sehr sorgfältig geprüft werden. Denn das Kammergericht legt auch dar, daß im vorliegenden Fall eine vom Gesetzgeber nicht gewollte Umfunktionierung der Sozialleistungsträger zur „Ersatzmeldebehörde" nicht vorliege.

Damit wird auch vom Kammergericht an der Grundintention des Sozialgesetzbuches festgehalten, daß die Berechtigten Leistungen frei von der Erwartung entgegennehmen sollen, daß die Entgegennahme der Leistung zum Anlaß für staatliche Maßnahmen dritter Stellen gemacht wird.

Auf keinen Fall läßt sich die vom Kammergericht in einem außergewöhnlichen Fall vorgenommene extensive Auslegung des Begriffs der Anschrift dahingehend verallgemeinern, daß Sozialleistungsträger zunehmend bei Nachforschungen über den Aufenthalt von Sozialleistungsempfängern durch beliebige Behörden herangezogen werden können. Dies würde zu einem Widerspruch zu den eigentlichen Aufgaben von Sozialbehörden führen, deren Funktion nur bei Aufrechterhaltung des Vertrauensverhältnisses zwischen Bürger und Behörde gewährleistet ist. Dieses ist aufgrund des Sozialstaatsgebots verfassungsrechtlich geschützt.

[20] S. 14

Aus der Sicht des Datenschutzes bedeutet dies:

1. Bei der Übertragung des Urteils des Kammergerichts auf andere Fälle muß die einzigartige Ausgestaltung des dem Urteil zugrundeliegenden Falles berücksichtigt werden.
2. In jedem Fall muß bei der Ermittlung des tatsächlichen Aufenthaltes berücksichtigt werden, daß das Sozialgesetzbuch ein Vertrauensverhältnis zwischen Bürger und Sozialleistungsträgern zugrundelegt.
3. Nach wie vor sollte der Weg, den §73 SGB X für Strafverfolgungsbehörden vorsieht, dem einfachen Amtshilfeersuchen nach §68 SGB X vorgezogen werden (wobei die Erleichterungen, die §73 SGB X enthält, nicht außer Acht bleiben sollten!).

Ich habe mehrfach meine Bereitschaft erklärt, an der Erarbeitung praktikabler Lösungen mitzuwirken, die einen vernünftigen Interessenausgleich zwischen Polizei und Sozialbehörden ermöglichen und werde weiterhin auf einen derartigen Ausgleich hinwirken.

Offenbarung an die Ausländerbehörde

Ein verwandtes Problem stellt die Zusammenarbeit zwischen Sozialbehörden und Ausländerbehörden dar. Zwar ist §71 SGB X durch den Bundesgesetzgeber dahingehend geändert worden, daß unter bestimmten Voraussetzungen Ausländer, die ihren Lebensunterhalt nicht selbst bestreiten können, der Ausländerbehörde zu melden sind. Hierzu ist aber vom Senator für Gesundheit, Soziales und Familie eine Verwaltungsrichtlinie erlassen worden, die den Rahmen der geregelten gesetzlichen Übermittlungsbefugnisse durch die Schaffung zusätzlicher Tatbestände überschreitet.

So ermöglicht §10 Abs. 1 Nr. 10 Ausländergesetz die Ausweisung nur dann, wenn ein Ausländer den Lebensunterhalt nicht bestreiten kann. Der Begriff des „Lebensunterhaltes" ist in §11 Abs. 1 Satz 1 Bundessozialhilfegesetz definiert und umfaßt die „notwendigen Bedürfnisse des täglichen Lebens". Hiervon zu unterscheiden ist der Begriff der „Hilfe in besonderen Lebenslagen", der die Hilfe für qualifizierte Bedarfssituationen betrifft. Daraus ist abzuleiten, daß der Begriff Lebensunterhalt im Sinne des §11 Bundessozialhilfegesetz auszulegen ist und §71 Abs. 2 Satz 2 SGB X nur dann eine Offenbarungsbefugnis schafft, wenn Sozialhilfe in der Form der Hilfe zum Lebensunterhalt gewährt wird. Die Verwaltungsvorschriften dehnen die Mitteilungspflichten jedoch auch auf die Hilfe in besonderen Lebenslagen aus.

Ebenfalls nicht in Übereinstimmung mit dem Gesetz befindet sich eine weitere Vorschrift, nach der entsprechende Mitteilungen auch bei Ausländern zu machen sind, bei denen ausländerrechtliche Maßnahmen wegen bestehender internationaler Fürsorgeabkommen nicht ergriffen werden können. In diesen Fällen wird das pflichtgemäße Ermessen der Sozialleistungsträger einer Offenbarung stets entgegenstehen.

Eine Stellungnahme des Senators für Gesundheit, Soziales und Familie zu meiner mit dem 21. Juni 1983 ausgesprochenen Beanstandung ist bisher nicht eingegangen.

Wahrung der Vertraulichkeit

Eine Offenbarung kann auch darin liegen, daß Leistungsempfänger bei der Antragsstellung oder Beratung in den Diensträumen der Behörden gehalten sind, persönliche Angaben in Anwesenheit Dritter zu machen. Dieses Mithören von Unbeteiligten ist nur dann zulässig, wenn der Leistungsempfänger hiermit einverstanden ist. Zunehmend kritisieren Bürger, daß diese Voraussetzungen nicht gewährleistet sind.

Auf meine Bitten hin hat der Senator für Gesundheit, Soziales und Familie die zuständigen Stellen auf die Problematik hingewiesen und gebeten, bei Zweifeln den Sozialhilfeberechtigten unter Hinweis auf die räumliche Situation besonders auf die Freiwilligkeit der Auskunftserteilung bei Anwesenheit Dritter aufmerksam zu machen und - falls er es wünscht - ihm eine Einzelberatung zu ermöglichen. Außerdem wurde um Überprüfung gebeten, ob durch vertretbare organisatorische Maßnahmen auch

bei künftigen Baumaßnahmen Sachbearbeiter mit Publikumsverkehr so untergebracht werden könnten, daß eine Einzelberatung von Antragstellern zunehmend möglich würde.

Diese Bitte hat in den Bezirksämtern zu teilweise heftigen Reaktionen geführt, angesichts derer sich der Senator für Gesundheit, Soziales und Familie zu weiteren Maßnahmen außerstande erklärte.

Auf Grund dieser Situation muß ich nochmals darauf hinweisen, daß die Sozialleistungsträger verpflichtet sind, den Leistungsempfängern zumindest auf Wunsch eine Einzelberatung zu ermöglichen. Anläßlich einzelner Überprüfungen habe ich im übrigen feststellen können, daß bei neuen Baumaßnahmen diesem Bedürfnis Rechnung getragen wurde. Zu überprüfen wäre, inwieweit die zuständigen Genehmigungsbehörden bei künftigen Baumaßnahmen bereits auch datenschutzrechtliche Gesichtspunkte berücksichtigen können. Im übrigen sollte von jeder Stelle geprüft werden, ob nicht durch organisatorische Maßnahmen in Verbindung mit geringfügigen baulichen Vorkehrungen eine Verbesserung des Persönlichkeitsschutzes erreicht werden kann.

Datenschutzbeauftragte nach dem Sozialgesetzbuch

Um die Einhaltung der Vorschriften über den Schutz von Sozialdaten sicherzustellen, enthält das Sozialgesetzbuch im Unterschied zum Berliner Datenschutzgesetz die Verpflichtung, daß jeder Sozialleistungsträger speziell für den Bereich des Sozialgesetzbuches formell Beauftragte für den Datenschutz (DSB SGB) benennt. Zwar ist dies inzwischen durchweg geschehen. Es muß jedoch festgestellt werden, daß dem DSB SGB insbesondere in den Bezirksämtern bislang keine hinreichenden Möglichkeiten zur Wahrnehmung ihrer gesetzlich festgelegten Aufgaben eingeräumt wurden.

Ein Seminar in der Verwaltungsakademie, das unter der Leitung meines Vertreters stand, gab Gelegenheit, die Probleme anhand der §§ 28, 29 Bundesdatenschutzgesetz zu analysieren. Die Teilnehmer haben zur Verbesserung ihrer Arbeitsmöglichkeiten einen Forderungskatalog erstellt.

Dem Erfahrungsaustausch dienten auch regelmäßige Sitzungen der DSB SGB, an denen mein zuständiger Mitarbeiter teilgenommen hat. Ziel dieser Kooperation ist es, eine einheitliche Praxis in Berlin zu erreichen.

2.8 Universitätsklinikum Steglitz der Freien Universität Berlin

Die Überprüfung der Einhaltung der datenschutzrechtlichen Vorschriften im Universitätsklinikum Steglitz der Freien Universität Berlin erfaßte insoweit

- die Feststellung grundsätzlicher datenschutzrechtlicher Probleme;
- die datenschutzrechtliche Beurteilung von Forschungsvorhaben, bei denen patientenbezogene Daten an andere Stellen, z. T. auch ins Ausland übermittelt werden;
- die Erfüllung der Anforderungen an technische und organisatorische Maßnahmen zum Datenschutz bei den zentralen und dezentralen Anwendungen elektronischer Datenverarbeitung;
- den Umgang mit papierenen oder mikroverfilmten patientenbezogenen ärztlichen Unterlagen (z. B. Karteien, Belegsammlungen, Patientenakten).

Geprüft wurden die meisten zentralen und alle wissenschaftlichen Einrichtungen des Universitätsklinikums Steglitz.

Ich gehe davon aus, daß die festgestellten Probleme auch für andere Krankenhäuser Bedeutung haben.

Neben den Datenschutzgesetzen sind für die datenschutzrechtliche Bewertung des Umgangs mit patientenbezogenen medizinischen Daten die Regelungen zur ärztlichen Schweigepflicht (§203 Strafgesetzbuch, §§ 2, 7 Berufsordnung der Ärztekammer Berlin) maßgebend.

Die wichtigsten Ergebnisse der Überprüfung des Universitätsklinikums Steglitz lassen sich wie folgt zusammenfassen:

Unterschiedliche Auffassungen zwischen mir und den Universitätskliniken bestehen über die *Einordnung der Kliniken* nach § 1 Berliner Datenschutzgesetz. Die Kliniken vertreten die Auffassung, daß sie - wie auch die übrigen öffentlichen Krankenhäuser - als öffentlich-rechtliche Unternehmen, die am Wettbewerb teilnehmen, anzusehen sind und damit an Stelle einiger strengerer Vorschriften des Berliner Datenschutzgesetzes Vorschriften des Bundesdatenschutzgesetzes zu beachten hätten. Insbesondere würde diese Einordnung nur die Meldepflicht zum vereinfachten und nicht-öffentlichen Besonderen Dateienregister zur Folge haben und eine Veröffentlichungspflicht der Dateien im Amtsblatt für Berlin entfiele ganz.

Ich kann mich dieser Auffassung nicht anschließen. Unabhängig vom tatsächlichen Raum, den die Krankenversorgung im Universitätsklinikum Steglitz einnimmt, hat sich das Klinikum vor allem der Forschung und Lehre zu widmen (§ 4 Abs. 1 Hochschulgesetz). Insoweit befindet sich das Universitätsklinikum Steglitz keinesfalls im Wettbewerb, sondern nimmt eine wesentlich dem Staat zugeordnete Aufgabe wahr. Die Aufgabe des Universitätsklinikums, Forschung und Lehre zu betreiben, prägt auch tatsächlich den Einsatz der automatisierten Datenverarbeitung und den Umgang mit patientenbezogenen medizinischen Unterlagen in wesentlichem Maße und im Unterschied zu den normalen öffentlichen Krankenhäusern. Es entstehen viele zusätzliche Risiken für die Wahrung des Patientengeheimnisses dadurch, daß patientenbezogene medizinische Daten für wesentlich mehr Zwekke und von einem wesentlich erweiterten, sehr heterogenen Personenkreis ausgewertet werden können. Diese zusätzlichen Risiken erfordern einerseits besondere Sorgfalt bei technischen und organisatorischen Maßnahmen und bei der Regelung der Daten- und Belegflüsse und führen andererseits zu völlig anderen Rahmenbedingungen der Verarbeitung und des Umgangs mit patientenbezogenen medizinischen Daten im Vergleich zu den übrigen öffentlichen Krankenhäusern.

Die *Übermittlung* patientenbezogener medizinischer Daten führt wegen der besonderen Rechtslage zu speziellen Problemen:

- Da es zu den Aufgaben eines Universitätsklinikums zählt zu forschen und zu lehren, bedarf die Verwertung patientenbezogener Daten zu diesen Zwecken wohl einer Aufklärung, jedoch keiner besonderen Einwilligung des Patienten, sofern dieser in einer Rechtsbeziehung zum Universitätsklinikum steht. Die im Rahmen der privaten ärztlichen Behandlung von reinen Konsiliarpatienten entstehenden Daten jedoch werden zwar ohne Rechtsbeziehung des Patienten zum Universitätsklinikum Steglitz im räumlichen Bereich des Klinikums Steglitz erfaßt, die Nutzung der Daten zu Zwecken von Forschung und Lehre im Klinikum Steglitz bedeutet jedoch eine Übermittlung an das Klinikum und erfordert nach § 2 Abs. 7 der Berufsordnung der Ärztekammer Berlin eine ausdrückliche Einwilligung des Patienten.
- Im Rahmen der Zusammenarbeit mit verschiedenen Forschungsinstitutionen werden patientenbezogene medizinische Daten an andere Stellen übermittelt. Diese Übermittlung macht auf Grund § 2 Abs. 7 der Berufsordnung der Ärztekammer Berlin entweder die ausdrückliche Einwilligung oder die vollständige Anonymisierung der Daten erforderlich. Eine Anonymisierung, die patientenbeschreibende Merkmale (z. B. Geburtsdatum, Teile von Vor- und Nachnamen usw.) zur Differenzierung einsetzt, ist nicht ausreichend.
- Im Universitätsklinikum Steglitz wird in verschiedenen Zusammenhängen die Verarbeitung patientenbezogener medizinischer Daten auftragsweise durch Fremdrechenzentren (Zentraleinrichtung Datenverarbeitung der Freien Universität Berlin, Bundesgesundheitsamt, Gesellschaft für Systemforschung und Dienstleistungen im Gesundheitswesen mbH Berlin) durchgeführt, wobei man sich meist des On-line-Zugriffs über Wähl- oder Standleitungen bedient. Diese Auftragsdatenverarbeitung, die bei nicht-medizinischen Daten datenschutzrechtlich in der Regel unproblematisch wäre, stellt wegen der ärztlichen Schweigepflicht ein besonderes Problem dar. Die Voraussetzungen, unter denen medizinische Daten an andere Stellen weitergegeben werden

dürfen, regeln sich nach § 2 der Berufsordnung der Ärztekammer Berlin. Eine Weitergabe von Daten, die der ärztlichen Schweigepflicht unterliegen, an Service-Rechenzentren ist also nur möglich, soweit die Mitarbeiter dieser Rechenzentren, die mit den Daten in Berührung kommen können, als ärztliche Gehilfen angesehen werden. Das wäre jedoch bei externen Rechenzentren eine nicht akzeptable Ausweitung des Begriffs der ärztlichen Gehilfen. Soweit nicht eine grundsätzliche Umorganisation des ADV-Einsatzes am Klinikum Steglitz stattfindet, habe ich empfohlen, die zu Zwekken der Auftragsdatenverarbeitung zu übermittelnden Daten entweder vollständig zu anonymisieren oder Methoden der kryptographischen Verschlüsselung anzuwenden.

Eines von den bereits oben angedeuteten besonderen Risiken für das Arztgeheimnis in Universitätskliniken stellt das *Ablichten* von patientenbezogenen Unterlagen für Lehr- und Forschungszwecke dar. Diese Praxis kann nicht gänzlich unterbunden werden, ohne die Erfüllung des Forschungs- und Ausbildungsauftrags unangemessen zu gefährden. Ich habe dem Universitätsklinikum Steglitz daher Vorschläge zur Kontrolle und angemessenen Beschränkung des Ablichtens solcher Unterlagen unterbreitet.

Im Universitätsklinikum Steglitz werden mit der Führung von Karteien, Belegsammlungen, Patientenakten, Befundsammlungen, Berichten, Mikrofilmsammlungen und anderen ärztlichen Aufzeichnungen in starkem Maße Datenhaltung und -verarbeitung in nicht-automatisierten Verfahren durchgeführt. Bei diesen *manuellen Datensammlungen* habe ich meine Prüfung auf die Sicherung dieser Sammlungen vor unbefugtem Zugriff beschränkt. Soweit die manuellen Datensammlungen den Dateibegriff des § 4 Abs. 3 Nr. 3 Berliner Datenschutzgesetz erfüllen, sind sie aufgrund § 5 Abs. 1 Berliner Datenschutzgesetz vor unbefugtem Zugriff zu sichern. Ansonsten ergibt sich aus der ärztlichen Schweigepflicht nicht nur das Verbot der unbefugten Weitergabe, sondern auch das Gebot der sicheren Verwahrung solcher Unterlagen zum Schutz davor, daß Unbefugte zufällig oder vorsätzlich in Kenntnis dieser Informationen gelangen können. Ich gehe dabei von folgenden Anforderungen aus:

- Manuelle Datensammlungen sind so zu verwahren, daß sie jederzeit entweder durch Sicherheitsverschluß von Schränken oder Räumen oder durch wirksame Aufsicht vor unbefugtem Zugriff geschützt werden.
- Sind die Datensammlungen auf Grund ihres besonderen Inhaltes (z. B. patientenbezogene Unterlagen über Krankheiten, die aufgrund allgemeiner Vorurteile als diskriminierend empfunden werden, etwa psychische Erkrankungen, Geschlechtskrankheiten) oder auf Grund ihres besonderen Umfangs (z. B. Zentralarchiv) mögliche Ziele von Einbruchsversuchen, so sind zusätzliche Sicherungsmaßnahmen vorzusehen.

Dies bedeutet: In allen Bereichen, in denen sich nicht zum Zugriff berechtigte Personen (z.B. Patienten) unbeaufsichtigt aufhalten können, sind die zu schützenden Unterlagen in Schränken mit Sicherheitsschlössern aufzubewahren. Dies gilt auch für die Räume, die ohne Aufsicht durch Zugriffsbefugte vom Reinigungspersonal betreten werden können. Nur wenn dieses ausgeschlossen ist, reicht der Raumverschluß mit Sicherheitsschlössern außerhalb der Anwesenheitszeit des befugten Personals aus.

Im Bereich des Universitätsklinikums Steglitz werden diese Anforderungen überwiegend nicht erfüllt. Insbesondere gilt dies für die Unterbringung von Patientenakten im Bereich der meisten Polikliniken.

Bei der *automatisierten Datenverarbeitung* im Klinikum Steglitz war die Durchführung technisch-organisatorischer Maßnahmen zum Datenschutz gem. § 11 Abs. 5 Berufsordnung der Ärztekammer Berlin und § 5 Abs. 1 Berliner Datenschutzgesetz Schwerpunkt der datenschutzrechtlichen Überprüfung. Außerdem wurde geprüft, inwieweit die ordnungsgemäße Anwendung der Datenverarbeitungsprogramme, mit deren Hilfe personenbezogene Daten verarbeitet werden sollen, überwachbar ist (§ 16 Berliner Datenschutzgesetz).

Die Anwendung der automatisierten Datenverarbeitung im Klinikum Steglitz wird in sehr vielfältiger Weise durchgeführt:

- Einsatz des Rechenzentrums des Klinikums Steglitz für administrative Aufgaben und zu Forschungszwecken,
- Verwendung isolierter Anwendungssysteme mit unterschiedlichen Betriebsformen zu Zwecken der medizinischen Patientenversorgung und Forschung, in geringem Umfang auch zu administrativen Zwecken,
- Auftragsdatenverarbeitung mit externen Rechnern zu administrativen Zwecken, zu Zwecken der medizinischen Patientenversorgung und zur Forschung (vgl. oben).

Die verschiedenen Betriebsformen der automatisierten Datenverarbeitungssysteme können wegen der Vielfalt der Anwendungen und Problemstellungen sinnvoll sein. Bei der Prüfung wurde jedoch der Eindruck gewonnen, daß die Entwicklung der ADV-Anwendungen im Klinikum Steglitz weniger Ergebnis eines planvollen Aufbaus ist, als vielmehr eine nicht abgestimmte Aneinanderreihung individueller Problemlösungen, deren Ursache weniger von sachlicher Zweckmäßigkeit als vielmehr vom Bemühen geprägt ist, trotz der veralteten und den Anforderungen nicht mehr gewachsenen zentralen ADV-Versorgung die Vorzüge moderner Dialogverfahren in Anspruch zu nehmen.

Die Uneinheitlichkeit der ADV-Anwendungen im Klinikum Steglitz wirkt sich für den Datenschutz überwiegend negativ aus:

- Die Sicherstellung des Datenschutzes, insbesondere die Überwachbarkeit der ordnungsgemäßen Programmanwendung wird erheblich erschwert. Die Dokumentation der Programme und Verfahren als Voraussetzung zur Erfüllung von § 16 Satz 2 Nr. 2 Berliner Datenschutzgesetz wird - wenn überhaupt - nach Belieben des jeweiligen Programmierers durchgeführt.
- Eine datenschutzgerechte Organisation des Rechenbetriebes ist mit Einschränkungen nur im Rechenzentrum feststellbar. Ansonsten wird der Rechenbetrieb nach individuellen Konzepten durchgeführt, die Erfüllung der Anforderungen der Anlage zu § 5 Abs. 1 Berliner Datenschutzgesetz erfolgt - wenn überhaupt - entweder zufällig auf Grund anderer Sicherheitsbestimmungen (Strahlenschutz) oder unvollständig unter Bevorzugung einzelner bei gleichzeitiger Vernachlässigung anderer Kontrollanforderungen.
- Die Kontrolle des Datenschutzes durch interne und externe Instanzen wird erheblich erschwert. Eine vollständige interne Kontrolle darüber, inwieweit datenschutzrechtliche Zulässigkeitskriterien für Verarbeitungs- und Übermittlungsvorgänge bei ADV-Projekten erfüllt sind, ist so erschwert, daß sie kaum durchgeführt wird.

Neben diesen grundsätzlichen Feststellungen wurden diverse Mängel hinsichtlich der sich aus der Anlage zu § 5 Abs. 1 Berliner Datenschutzgesetz ergebenden Kontrollanforderungen aufgefunden. Zahlreiche Dateien waren noch nicht zum Dateienregister gemeldet. Eine interne Dateienübersicht gemäß § 16 Satz 2 Nr. 1 Berliner Datenschutzgesetz konnte mir nicht vorgelegt werden.

3. Weitere Feststellungen und Fragen aus der Kontroll- und Beratungspraxis

3.1 Allgemeine Fragen zu technischen und organisatorischen Maßnahmen

Datenschutz bei der Verfahrensentwicklung

Je früher mir ein Projekt bekannt wird und je kontinuierlicher ich über den Fortgang einer Verfahrensentwicklung informiert werde[21], desto geringer ist der Aufwand für eine datenschutzgerechte Gestaltung und desto größer ist die Akzeptanz meiner Einwände bei den Systementwicklern.

Bereits während der Verfahrensentwicklung können Prüfungen vor Ort erforderlich sein. So mußte ich wiederum feststellen, daß bereits in der Testphase datenschutzrechtliche Mängel auftreten, weil unzulässigerweise mit Echtdaten getestet wurde. Auf meinen Jahresbericht 1982 (S. 18) nehme ich insoweit Bezug.

[21] Vgl. dazu Rundschreiben des Senators für Inneres über die rechtzeitige Information und Beteiligung des Berliner Datenschutzbeauftragten vom 17. März 1981, Dienstblatt Teil I, S. 30

Ordnungsmäßigkeit und Transparenz der Datenverarbeitung

Wiederholt bin ich gefragt worden, welches Interesse der Datenschutzbeauftragte an der Überprüfung der Ordnungsmäßigkeit der Datenverarbeitung hat. Gelegentlich wurde sogar behauptet, daß ausführliche Dokumentationen bezüglich des Datenschutzes schädlich seien, da es sich dabei wiederum um Unterlagen handelt, die eines besonderen Schutzes bedürften und deren Preisgabe zu besonderen Risiken für den Datenschutz führen würde.

Diese Auffassung ist unrichtig. Selbstverständlich sind Dokumentationsmaterialien in besonderer Weise zu sichern, aber sie sind für die datenschutzgerechte Datenverarbeitung unentbehrlich. §16 Berliner Datenschutzgesetz ordnet den speichernden Stellen die Verantwortung für die Durchführung des Datenschutzes in ihrem Hause zu. Dieser Aufgabe können sie nur gerecht werden, wenn sie die explizit in der Vorschrift genannten Aufgaben, nämlich die Führung der internen Dateienübersicht und die Überwachung der ordnungsgemäßen Anwendung der Datenverarbeitungsprogramme ernst nehmen und darüber hinaus interne organisatorische Vorkehrungen treffen, die sicherstellen, daß sich jemand um diese gesetzliche Aufgabe kümmert.

Die Transparenz der Datenverarbeitung ist notwendige Voraussetzung dafür, daß eine speichernde Stelle ihre Aufgabe wahrnehmen kann, die Ordnungsmäßigkeit der Programmanwendung zu überprüfen. Ein wichtiges Prüfziel ist also im Zusammenhang mit der Dokumentation stets die Nachvollziehbarkeit und damit Kontrollierbarkeit der Datenverarbeitungsprozesse. Hinzu kommt mein Interesse, bei Bedarf selbst bestimmte Programmfunktionen analysieren zu können.

Die Führung einer Dateienübersicht ist ebenfalls eine Maßnahme, die sowohl der Durchführung der Maßnahmen zur internen Datenschutzkontrolle dient, wie sie auch Grundvoraussetzung für die effektive Datenschutzkontrolle durch mich ist. Stellen, die eine derartige Dateienübersicht nicht führen, können den Datenschutz im eigenen Hause nicht sicherstellen, da ihnen zentral gar nicht bekannt ist, welche Schutzgegenstände es in der Organisation überhaupt gibt. Auch die interne Dateienübersicht ist also eine unverzichtbare Maßnahme zur Herstellung der Transparenz der Datenverarbeitung im eigenen Hause. Bei vielen Überprüfungen habe ich eine interne Dateienübersicht nicht vorgefunden.

Weiter achte ich bei meinen Prüfungen darauf, daß die internen Abläufe bei der Datenverarbeitung und die Zuständigkeiten innerhalb der Datenverarbeitungsorganisation einer speichernden Stelle klar und unmißverständlich geregelt sind.

Funktionentrennung im Sicherheitsbereich eines Rechenzentrums

Der Sicherheitsbereich eines großen Rechenzentrums besteht in der Regel aus den Funktionsbereichen Rechnerraum, Arbeitsvor- und -nachbereitung und Datenträgerarchiv. Optimale Bedingungen für datenschutzgerechte Arbeitsabläufe in den Funktionsbereichen ergeben sich, wenn folgende Voraussetzungen erfüllt werden:

- Die Funktionsbereiche sind baulich voneinander getrennt (räumliche Funktionentrennung).
- Der regelmäßige Zugang zu den einzelnen Funktionsbereichen wird nur jenen Personen während ihrer Dienstzeit gestattet, die dort ihren Arbeitsplatz haben (personelle Funktionentrennung).
- Mitarbeiter, die im Sicherheitsbereich ihren Arbeitsplatz haben, sind aufgabenmäßig nur einem Funktionsbereich zugeordnet.
- Der unregelmäßige Zugang von Personen, die nicht ständig im Funktionsbereich zu tun haben, wird auf das notwendige Maß beschränkt und in jedem Falle protokolliert.
- Das Zusammenwirken der einzelnen Funktionsbereiche wird sichergestellt, ohne daß der gegenseitige Zutritt erforderlich ist (Schleusen, Durchreichen usw.).
- Die Maßnahmen zur Funktionentrennung und die Aufgabenteilung sind durch Dienstanweisungen festgelegt. Für die regelmäßig im Sicherheitsbereich Beschäftigten liegt ein Schichtplan vor, der nach Funktionsbereichen differenziert ist.

Ich bin mir bewußt, daß die genannten Bedingungen ein Optimalziel darstellen, welches in der Regel aus verschiedenen Gründen nicht immer erreichbar sein wird. In kleineren Rechenzentren mit wenigen Beschäftigten läßt sich insbesondere eine personelle Funktionentrennung nicht immer realisieren. In größeren, stetig gewachsenen Rechenzentren stehen häufig bauliche Gegebenheiten einer exakten räumlichen Funktionentrennung entgegen. Jedoch darf erwartet werden, daß die vorhandenen Spielräume in angemessener Weise (§5 Abs. 1 Satz 2 Berliner Datenschutzgesetz) genutzt werden, um die gravierendsten Abweichungen von den Anforderungen zu beseitigen.

Die Funktionentrennung fördert die Transparenz der Arbeitsabläufe in Rechenzentren in entscheidendem Maße, sie reduziert den Umlauf von Datenträgern außerhalb des Archivs auf das erforderliche Mindestmaß und beschränkt den Kreis der Zutrittsberechtigten zu den Funktionsbereichen. Sie wirkt daher positiv auf die Ordnungsmäßigkeit der Arbeitsabläufe, die Wirksamkeit der Zugangskontrolle bezogen auf die einzelnen Funktionsbereiche, der Organisationskontrolle und insbesondere der Abgangskontrolle.

Datenschutz bei isolierten Rechnern

In diesem Jahr sind von mir Grundsätze für die organisatorischen und technischen Maßnahmen beim Einsatz isolierter ADV-Systeme erarbeitet worden. Sie sind diesem Bericht als Anlage 2 beigefügt. Erläuterungen zu diesen Grundsätzen sind ebenfalls bei mir erhältlich. Bei der Formulierung der Grundsätze sind Anregungen anderer Landesdatenschutzbeauftragter mit berücksichtigt worden.

Die Grundsätze betreffen die Anwendung von Systemen mit besonders vereinfachter Einsatzorganisation, wie sie z.B. für Kleinrechner mit kleinem Benutzerkreis und engem Aufgabenspektrum typisch ist. Solche Anwendungsformen sind bereits relativ häufig in der Berliner Verwaltung anzutreffen.

Der Sinn solcher Grundsätze kann nicht sein, neue Normen zu schaffen, die verbindlich zu befolgen sind. Es steht vielmehr die Absicht dahinter, dem Betreiber und Benutzer solcher Systeme Hinweise zur Hand zu geben, die es ihm ermöglichen, den Einsatz so zu gestalten, daß er den Anforderungen auch des Datenschutzes entspricht. Dieses ist erforderlich, weil sich der Einsatz der automatisierten Datenverarbeitung durch die Kostengünstigkeit kleiner, aber leistungsfähiger ADV-Systeme, die Benutzer- und Anwenderfreundlichkeit, die Miniaturisierung der Systeme und durch weitere Entwicklungsrichtungen weiter ausbreitet und von der Inanspruchnahme von Spezialisten zunehmend unabhängiger wird.

Die Grundsätze sind bewußt als Rahmen gehalten. Welche konkreten Maßnahmen hier zu treffen sind, um den in den Grundsätzen genannten Zielen gerecht zu werden, hängt stark von den Verhältnissen im Einzelfall ab. Sie werden jedoch als Richtschnur für Kontrollmaßnahmen zum Datenschutz verwendet werden.

Datenschutz bei manuellen Datensammlungen

Trotz der Ausweitung des Einsatzes automatisierter Datenverarbeitung in allen Bereichen der öffentlichen Verwaltung behält die traditionelle Datenverarbeitung mit Karteien, Belegsammlungen und Akten ihre Bedeutung. Gem. §3 Abs. 2 i. V. m. §4 Abs. 3 Nr. 3 Berliner Datenschutzgesetz fallen Akten und Aktensammlungen, soweit sie nicht durch automatisierte Verfahren umgeordnet und ausgewertet werden können, aus dem Schutzbereich des Berliner Datenschutzgesetzes heraus. Somit ist §5 Abs. 1 Berliner Datenschutzgesetz nicht als Rechtsgrundlage für die sichere Unterbringung von Akten anwendbar. Andere gesetzliche Vorschriften, die etwas zur sicheren Unterbringung von Akten direkt aussagen, gibt es nicht. Falls es jedoch materielle Geheimhaltungsvorschriften gibt (wie z. B. §35 SGB I

bei Sozialdaten oder § 2 Berufsordnung der Ärztekammer Berlin bzw. § 203 Strafgesetzbuch bei medizinischen Daten), ergibt sich daraus die Pflicht, die Akten so zu sichern, daß ein Verstoß gegen die Geheimhaltungsvorschriften ausgeschlossen ist. Eine Offenbarung von Geheimnissen liegt nicht nur bei aktivem Handeln vor, sondern auch dann, wenn versäumt wird, die Daten vor unbefugter Offenbarung zu schützen. Für Akten, die keiner speziellen Geheimhaltungspflicht unterliegen, erfordert § 30 Verwaltungsverfahrensgesetz ebenfalls angemessene Sicherungsmaßnahmen.

Die zu treffenden Maßnahmen liegen im Ermessen der Behörde. Dabei ist ähnlich wie bei § 5 Abs. 1 Satz 2 Berliner Datenschutzgesetz die Verhältnismäßigkeit zwischen Aufwand und Schutzzweck zu beachten. Der Schutzzweck ergibt sich, soweit nicht besondere Geheimhaltungsregeln gelten, aus dem Ausmaß der Verletzung schutzwürdiger Belange der Betroffenen bei unbefugter Offenbarung bzw. aus der Bedeutung möglicherweise vorhandener Motive Dritter, unbefugt in Kenntnis dieser Daten zu gelangen.

Um im Einzelfall die Überprüfung überflüssig zu machen, inwieweit materielle Geheimhaltungsvorschriften gelten oder nicht, kann die Unterbringung von Akten in Verwaltungsvorschriften geregelt werden. Dies ist in § 77 GGO I geschehen, wonach Akten und Schriftstücke möglichst so aufzubewahren sind, daß sie nicht entwendet oder unbefugt eingesehen werden können.

Grundsätzlich empfehle ich, personenbezogene Datensammlungen in Räumen unterzubringen, die mit Sicherheitsschlössern ausgestattet sind. Innerhalb solcher Räume sind sie in Schränken unterzubringen, die ebenfalls mit Sicherheitsschlössern ausgestattet sein sollen, damit die Daten außerhalb der Dienstzeit so gesichert sind, daß Personen, die zwar befugt sind, die Diensträume zu betreten, dennoch nicht unbefugt in die Datensammlungen Einsicht nehmen können (z. B. Reinigungskräfte, Pförtner, Sicherheitskräfte usw.). Ich verweise in diesem Zusammenhang auf meine Ausführung zur Überprüfung des Universitätsklinikums Steglitz (Abschnitt 2.8 dieses Jahresberichtes).

Die genannten Maßstäbe werden bei technisch-organisatorischen Überprüfungen von mir angelegt. Abweichungen werden bemängelt, sofern nicht durch andere Maßnahmen ein gleichwertiger Schutz erreicht worden ist. Im Einzelfall ist durch die Analyse der Sensitivität der Daten zu prüfen, ob nicht höhere Sicherheitsanforderungen an die Akten- und Karteienunterbringung zu erfüllen sind (vgl. auch Anlage 2 zum Jahresbericht 1982).

Vernichtung von Adrema-Platten

Adrema-Adreßplatten stellen eine Datei i. S. von § 4 Abs. 3 Nr. 3 Berliner Datenschutzgesetz dar. Wenn ihre Verwendung wegen des Einsatzes moderner Adressierungstechniken nicht mehr vorgesehen ist, dann sind diese Platten zu vernichten. Ich bin von einigen Stellen um Rat gebeten worden, wie eine solche datenschutzgerechte Vernichtung der aus einer Zinklegierung bestehenden Platten vorgenommen werden kann. Zunächst bietet sich die Verbrennung kleinerer Mengen in der Müllverbrennungsanlage Ruhleben der Berliner Stadtreinigungs-Betriebe an. Jedoch bedeutet dieses die Vernichtung wertvoller Rohstoffe. Umfragen haben ergeben, daß es Firmen gibt, die bereit sind, die Adrema-Platten entgegenzunehmen und durch Einschmelzung sowohl datenschutzgerecht zu vernichten als auch die Rohstoffe einer weiteren Verwendung zuzuführen. Dieses Verfahren habe ich bei Anfragen empfohlen. Der Senator für Stadtentwicklung und Umweltschutz hat sich bereiterklärt, die Empfehlungen in geeigneter Weise zu publizieren.

3.2 Stellungnahmen zu neuen Verfahren

Auch in diesem Jahr habe ich in mehreren Fällen Gelegenheit erhalten, mich zu geplanten ADV-Verfahren zu äußern, zu denen mir Planungsunterlagen (Untersuchungsberichte, Projektdefinitionen usw.) zugesandt wurden. Darüber hinaus wurden von mir Stellungnahmen zu technischen und organisatorischen Einzelfragen sowie zur datenschutzgerechten Organisation des Rechenbetriebes bei kleineren Rechenstellen und zur datenschutzgerechten Unterbringung von papierenen Unterlagen erbeten.

Meine Aussagen zu wichtigen Problemen der Verfahrensentwicklung, die nicht nur bei erbetenen Stellungnahmen, sondern auch im Rahmen meiner durch Eingaben oder von Amts wegen veranlaßten Überprüfungen aufgeworfen wurden, habe ich zusammengefaßt. Ich beschränke daher meinen Bericht hier auf wenige Fälle, die repräsentativ oder von besonderer datenschutzrechtlicher Bedeutung sind.

Automation eines Geschäftsverteilungsplanes

Der Senator für Arbeit und Betriebe informierte mich über seine Absicht, die für die Erstellung des Geschäftsverteilungsplanes erforderlichen Angaben in einer Datei auf einem Kleinrechner zu speichern. Dabei beabsichtigte er, die Datei über die Daten hinaus, die zu einem Geschäftsverteilungsplan gehören, mit weiteren Daten zu ergänzen, die lediglich für die interne Organisation des Hauses von Bedeutung sind. An der Zulässigkeit der geplanten Datei im Rahmen des § 9 Abs. 1 Berliner Datenschutzgesetz habe ich keine Zweifel. Da jedoch der Geschäftsverteilungsplan in Listenform an andere öffentliche Stellen übermittelt wird, habe ich gefordert, daß durch programmtechnische Maßnahmen sichergestellt wird, daß die Daten, die zwar in einer Datei gespeichert sind, nicht jedoch zum Geschäftsverteilungsplan gehören, im Rahmen dieser regelmäßigen Übermittlung nicht mit übermittelt werden, da § 10 Abs. 1 Berliner Datenschutzgesetz die Übermittlung nicht erforderlicher Daten nicht deckt. Allgemein ist zu sagen, daß der Einsatz von Kleinrechnern und Textsystemen für vielerlei der internen Organisation dienenden Listen sich mit Dateien realisieren läßt, die die Gesamtheit aller dafür erforderlichen Daten enthalten. Es ist jedoch darauf zu achten, daß die Verwendung der Dateien für einen bestimmten Zweck sich auf die Felder des Datensatzes zu beschränken hat, die für diesen Zweck benötigt werden.

Zentrale Anschriftenspeicherung

Die Technische Universität Berlin bat mich um Stellungnahme zum Aufbau eines Adressensatzes für die diversen festen Adressatenkreise für Schreiben, Publikationen und Einladungen der Technischen Universität Berlin. An der Zulässigkeit des Aufbaus einer solchen Datei habe ich keinen Zweifel, da ich davon ausgehe, daß es zu den Aufgaben der Technischen Universität gehört, gezielt Öffentlichkeitsarbeit zu leisten. Ein Problem stellt dagegen die Übermittlung dieser Daten an verschiedene öffentliche und private Stellen dar. Da die Präsidialverwaltung der Technischen Universität speichernde Stelle des Adressensatzes ist, ist die Übermittlung dieser Adressen an die Wissenschaftlichen Einrichtungen der Technischen Universität nach § 10 Berliner Datenschutzgesetz zu bewerten. Die Übermittlung dieser Adressen an private Stellen, z.B. an wissenschaftliche Gesellschaften, Standesorganisationen usw. regelt sich dagegen nach § 11 Berliner Datenschutzgesetz, setzt also die Einwilligung der Betroffenen voraus. Dieses gilt auch dann, wenn ein Mitglied der Universität unter dem Briefkopf einer solchen privaten Organisation tätig wird.

Amts- und Staatsanwaltschaften

Der Senator für Justiz entwickelt derzeit in Zusammenarbeit mit dem Landesamt für Elektronische Datenverarbeitung das ADV-Verfahren Amts- und Staatsanwaltschaften (ASTA). Dieses Verfahren soll die Verbrechensbekämpfung durch die aktuelle und fehlerfreie Auskunft über alle anhängigen und anhängig gewesenen Verfahren gegen Beschuldigte und die jeweiligen Verfahrensstände bei der Amts- und Staatsanwaltschaft verbessern. Es soll ferner die Arbeitsmittel der Geschäftsleitung, der Geschäftsstellen, der zentralen Schreibstelle und insbesondere der zentralen Namenskartei der Staatsanwaltschaft am Landgericht rationalisieren. Darüber hinaus wird eine Verbesserung des Informationsaustausches zwischen der Polizei und den Amts- und Staatsanwaltschaften durch Datenträgeraustausch mit dem polizeilichen Informationssystem (ISVB) angestrebt.

Ich habe zu dem geplanten Verfahren ASTA folgende Bedenken geäußert:

Der Ausgang des staatsanwaltschaftlichen Verfahrens wird als Ergebnis des Verfahrens in ASTA eingetragen. Führt ein Verfahren zu einer Anklageerhebung durch die Staatsanwaltschaft, so

wird jedoch das Ergebnis des darauffolgenden Gerichtsverfahrens nicht eingetragen. Zumindest dann, wenn das Gerichtsurteil von der staatsanwaltschaftlichen Bewertung abweicht, gibt der Inhalt der ASTA-Datei ein falsches Bild von dem Beschuldigten wieder. Durch das Fehlen dieser Angabe im Datenbestand ist die dem Benutzer vermittelte Information unvollständig und nicht mit der Realität übereinstimmend, also unrichtig. Unrichtige personenbezogene Daten sind gem. §14 Abs. 1 Berliner Datenschutzgesetz zu löschen, sie dürfen nicht in Kenntnis ihrer Unrichtigkeit gespeichert werden. Ich habe daher empfohlen, Daten über den Stand bzw. über das Ergebnis gerichtlicher Verfahren in die ASTA-Datei aufzunehmen.

Der Senator für Justiz ist meinem Einwand nicht gefolgt, da nach seiner Auffassung die vorgeschlagene Erweiterung des Verfahrens um Urteilsdaten ein auf Berliner Verurteilungen bezogenes Strafregister darstellen würde, was nach dem Bundeszentralregistergesetz nicht zulässig wäre. Zwar bin ich auch der Auffassung, daß durch ASTA kein Berliner Zentralregister geschaffen werden soll, jedoch meine ich, daß die geplante ASTA-Datei aufgrund der Angabe von Tatverdächtigen, Straftatbeständen, Tatzeiten usw. durchaus Parallelen zum Bundeszentralregister aufweist. Ziel meiner Empfehlung ist es in erster Linie nicht, daß alle Ausgänge von Gerichtsverfahren einbezogen werden. Es kommt vielmehr darauf an, daß der durch das staatsanwaltschaftliche Ermittlungsergebnis entstandene, von der folgenden gerichtlichen Entscheidung nicht bestätigte Eindruck korrigiert wird. Zumindest Freisprüche oder zu Gunsten des Beklagten von dem staatsanwaltschaftlichen Ermittlungsergebnis abweichende Gerichtsurteile sollten der ASTA-Datei mitgeteilt werden (vgl. auch oben 2.5).

Der geplante On-line-Anschluß des Generalstaatsanwalts bei dem Kammergericht an das ASTA-Verfahren stellt nach der gegenwärtigen Rechtslage eine Übermittlung aller über die Verbindung zugänglichen Daten dar. Nach meiner Auffassung ist für die Erfüllung der Aufgaben der Staatsanwaltschaft am Kammergericht die Übermittlung aller Daten aus ASTA nicht erforderlich. Ein On-line-Anschluß ist daher unzulässig. Ich habe empfohlen, die On-line-Verbindung zur Staatsanwaltschaft des Kammergerichts durch geeignete programmtechnische Maßnahmen auf den Zugriff auf diejenigen Vorgangsdaten zu beschränken, mit denen die Staatsanwaltschaft des Kammergerichts befaßt ist. Aus der Befugnis der ersten Beamten der Staatsanwaltschaft, sich jederzeit in die Tätigkeit der Staatsanwaltschaft einschalten zu können, leitet jedoch der Senator für Justiz ab, daß die Staatsanwaltschaft am Kammergericht einen uneingeschränkten On-line-Zugriff auf ASTA erhalten darf. Da dies nach meiner Einschätzung aus praktischen Gründen nur dann geschieht, wenn die Staatsanwaltschaft am Kammergericht einen bestimmten Anlaß dafür sieht, rechtfertigt diese Argumentation zwar durchaus die Einzelfallübermittlung, nicht aber den unbeschränkten Zugriff durch einen On-line-Anschluß, über den die vorgesetzte Staatsanwaltschaft künftig beliebig und unbemerkt Daten jedes Verfahrens einsehen könnte.

Im Soll-Konzept für ASTA wird zu recht darauf verwiesen, daß die Behörden der Staatsanwaltschaft gem. §13 Abs. 2 Berliner Datenschutzgesetz nicht verpflichtet sind, Auskunft an Betroffene zu geben. Sie können jedoch nach eigenem pflichtgemäßen Ermessen entscheiden, ob sie im Einzelfall dennoch Auskunft geben wollen. Ich empfahl daher den Behörden der Staatsanwaltschaft, dem Vorbild der Polizeibehörden zu folgen, die in gleicher Weise privilegiert sind und sich dennoch in den Richtlinien über Kriminalpolizeiliche personenbezogene Sammlungen selbst verpflichtet hatten, bei Auskunftsbegehren nach wohlwollendem pflichtgemäßen Ermessen zu entscheiden. Zumindest sollte die Programmausstattung von ASTA geeignet sein, Auskunftsbegehren zu befriedigen. Der Senator für Justiz hat dazu erklärt, daß Auskünfte aus der ASTA-Datei im ASTA-Verfahren sichergestellt sind. Nach Prüfung des Einzelfalls würde die Erteilung von Auskünften außerhalb des ADV-Verfahrens stattfinden können. Zu einer expliziten Selbstverpflichtung hat sich der Senator für Justiz nicht geäußert.

Im Rahmen diverser Funktionen können in die Datensätze Bemerkungen in freier Textauswahl eingegeben werden. Ich habe empfohlen, von einer freien Wählbarkeit des Feldinhaltes abzusehen und stattdessen einen verbindlichen Katalog zulässiger Eintragungen in dieses Datenfeld aufzustellen. Es sollten klare Regelungen vorgesehen werden, die festlegen, unter welchen Voraussetzungen ein Katalogbegriff im Datenfeld "Bemerkungen" eingetragen werden kann. Eintragungen, die dem Katalog nicht entsprechen, sollten programmtechnisch erkannt und zurückgewiesen werden.

Der Senator für Justiz will weiterhin nicht formatierten Text eingeben. Allerdings will er versuchen, meiner Empfehlung auf Katalogisierung des Feldinhaltes weitestgehend zu folgen und nach Erstellung eines Kataloges diesen in eine Dienstanweisung aufzunehmen. Die technische Zurückweisung unzulässiger Bemerkungen wird bisher nicht ins Auge gefaßt.

Einen fest vorgegebenen Merkmalskatalog habe ich auch für das Feld „Merkmale" vorgeschlagen, welches für Zählungen und statistische Auswertung von Verfahren im ASTA-Verfahren eingesetzt werden soll. Ferner bin ich der Auffassung, daß diese Eintragung nur zulässig sein kann, wenn ihre Auswertung in einer konkret definierten, zeitlich begrenzten Untersuchung vorgesehen ist. Eine Datenvorratshaltung für unbestimmte Zwecke halte ich für unzulässig. Der Senator für Justiz beabsichtigt, die statistischen Merkmale nach Fristablauf bzw. Jahresende und statistischem Ausdruck im System zu löschen. Ich habe gegen diese Vorgehensweise keine Bedenken.

3.3 Einzelergebnisse weiterer technisch-organisatorischer Überprüfungen

Die im Vorjahr begonnenen systematischen Überprüfungen von öffentlichen Stellen hinsichtlich der technischen und organisatorischen Maßnahmen zum Datenschutz habe ich in diesem Jahr fortgesetzt. Über die oben dargestellten Überprüfungen hinaus wurden

- die Senatsverwaltung für Bau- und Wohnungswesen
- die Bezirksämter Neukölln und Tempelhof von Berlin

überprüft.

Darüber hinaus wurden zu speziellen Themen bzw. auf besonderen Anlaß oder auf Wunsch der speichernden Stellen hin diverse kleinere Überprüfungen in technischen organisatorischen Fragen durchgeführt, z.B. beim Krankenhaus Neukölln, beim Statistischen Landesamt, an der Einwohnerdatenbank des Polizeipräsidenten in Berlin, bei der Allgemeinen Ortskrankenkasse und bei der Untersuchungshaft- und Aufnahmeanstalt Moabit.

Die Auswertungen der Prüfung beim Bezirksamt Neukölln von Berlin ist zur Zeit der Berichterstattung noch nicht abgeschlossen. Dafür beziehe ich die Ende letzten Jahres durchgeführte Überprüfung des Bezirksamtes Zehlendorf von Berlin in meine Ausführungen ein.

Die Prüfungsergebnisse in meinen Überprüfungsschwerpunkten Eigenbetriebe, kulturelle Einrichtungen und Klinikum Steglitz habe ich oben ausführlich dargestellt (unter 2.3, 2.4 und 2.6).

Folgende, zum Teil häufiger wiederkehrende Mängel habe ich festgestellt:

- Organisatorische Vorkehrungen, die sicherstellen, daß Betroffenen auf Antrag die Empfänger von Übermittlungen der letzten zwei Jahre mitgeteilt werden können, wurden unzureichend getroffen.
- Die Befugnisse, die dem internen Datenschutzbeauftragten eingeräumt wurden, waren nicht ausreichend, um die Einhaltung der Datenschutzbestimmungen in seinem Hause sicherzustellen.
- In einer Arbeitsanweisung für ein ADV-Verfahren wurden echte Daten vorgefunden.
- Protokollisten der Datenerfassung im Personalbezugsverfahren wurden länger aufbewahrt als nach den Zahlungsbestimmungen für Personalbezüge mit Datenverarbeitung (ZPD) festgesetzt ist.
- Unterbringung der Sicherungsbänder und Zugangskontrolle bei der Datenerfassung waren unzureichend.

- Schlüsselbretter wurden nicht in ausreichender Weise beaufsichtigt; auf diese Weise kann nicht verhindert werden, daß Unbefugte sich die Schlüssel aneignen und so unter Umständen Zugang zu Räumen erhalten, in denen Daten gesammelt sind.
- In einem Bezirksamt war die bauliche Sicherung der Poststelle unzureichend.
- Die Einwohnermeldekartei war entgegen einer Anweisung des Senators für Inneres noch nicht vernichtet.
- Karteien wurden vorgefunden, deren Erforderlichkeit mir zweifelhaft erscheint; so z. B. die sogenannte Grundstückskartei des Bezirkseinwohneramtes und die Kartei der Leserverpflichtungskarten in einer Stadtbücherei.

Bei allen geprüften Stellen habe ich in mehr oder weniger großem Ausmaß Mängel hinsichtlich der sicheren Unterbringung manueller Datenträger festgestellt. Schwerwiegend war in einem Fall die mangelhafte Unterbringung von Vormundschaftsakten. Ich verweise in diesem Zusammenhang auf meine Ausführungen in Abschnitt 3.1.

Es wurden ferner in Einzelfällen Mängel hinsichtlich der Erfüllung formeller Pflichten, so etwa Meldungen zum Dateienregister und Veröffentlichungen im Amtsblatt für Berlin festgestellt.

Der Senator für Bau- und Wohnungswesen und das Bezirksamt Zehlendorf von Berlin haben mittlerweile Stellung zu meinen Mängelfeststellungen bezogen. Beide Stellen sind in vollem Umfang meinen Empfehlungen gefolgt und haben so den Datenschutz in ihrem Hause wesentlich verbessern können. Die Stellungnahme des Bezirksamts Tempelhof von Berlin wird derzeit ausgewertet.

Im Krankenhaus Neukölln hatte ich im Jahre 1982 ein Informationsbesuch durchgeführt, bei dem ich einige Mängel feststellte, die ich der Verwaltungsleitung mitteilte. Ich habe später überprüft, inwieweit die mir zugesagten Maßnahmen aufgrund meiner Empfehlungen durchgeführt worden waren. Dabei mußte ich feststellen, daß die Maßnahmen nicht durchgeführt worden waren. Ich habe dies gegenüber dem Bezirksamt Neukölln formell beanstanden müssen. Der Stellungnahme zu der Beanstandung entnehme ich, daß hinsichtlich der beanstandeten Mängel bei der Unterbringung von Patientenunterlagen nunmehr die erforderlichen Maßnahmen getroffen werden.

3.4 Einzelne datenschutzrechtliche Problemfälle

Beschwerden und Beratungsersuchen deckten auch in diesem Jahr datenschutzrechtliche Probleme auf oder bestätigten solche Probleme, die aus dem Gesetz heraus nur schwer lösbar sind und daher von der Verwaltung eine klare Entscheidung zu Gunsten datenschutzfreundlicher Lösungen verlangen. Die folgenden Beispiele zeigen, daß diesem Anliegen in unterschiedlichem Maße nachgekommen wird.

Datenschutz und Forschung

Insbesondere wegen der durch das Grundgesetz vorgesehenen Privilegierung der Forschung stellt der Bedarf der Wissenschaft, aber auch der planenden Verwaltung an personenbezogenen Daten ein Problem dar, das von den geltenden Datenschutzgesetzen und spezialgesetzlichen Regelungen nur unvollkommen gelöst wird.

Gleichwohl muß eine Behebung dieses Rechtsdefizites sehr behutsam angegangen werden. Ein von der baden-württembergischen Landesregierung vorgelegter Novellierungsvorschlag zum Landesdatenschutzgesetz, der inzwischen zurückgezogen worden ist, zeigt, daß die angemessene Wahrung der schutzwürdigen Belange von Personen, die Forschungsgegenstand sind, insbesondere im Bereich medizinischer Forschung allzu leicht den Interessen der Forscher nachgeordnet werden.

Um der Berliner Verwaltung, aber auch den Forschern die Orientierung bei den schwierigen Problemen zu erleichtern, habe ich eine Informationsschrift erarbeitet, die dem Leser anhand einer Checkliste die wesentlichen Datenschutzprobleme des Forschungsvorhabens vor Augen führt und Hilfen für die Lösung der Fragen anbietet. Die Schrift, die ich insbesondere den Hochschulen zur Verfügung gestellt habe, soll fortlaufend verbessert werden.

Bei vielen Forschungsvorhaben wird inzwischen erfreulicherweise vor Beginn der Durchführungsphase mein Rat eingeholt. Auf diese Weise konnten in den meisten Fällen Lösungen gefunden werden, die die Interessen der Forscher und die datenschutzrechtlichen Belange in Übereinstimmung brachten.

Auf andere Vorhaben wurde ich durch Presseveröffentlichungen aufmerksam; aber auch in diesen Fällen sind wesentliche Beanstandungspunkte nicht aufgetreten.

So war dem Senat von der Presse vorgeworfen worden, er habe im Rahmen eines wissenschaftlichen Forschungsprogramms über Meinungen und Tendenzen in der türkischen Bevölkerung „indiskrete" Fragen an Türken in Berlin gestellt. Eine Überprüfung des Sachverhalts hat folgendes ergeben:

Die Verantwortlichkeit für die inhaltliche Ausgestaltung der Fragen sowie die Verwertung der Daten lag auf seiten des Landes Berlin in den Händen der Ausländerbeauftragten beim Senator für Gesundheit, Soziales und Familie. Das Forschungsprogramm soll in zwei Phasen ablaufen. In jeder Phase werden fünfhundert türkische Staatsangehörige über ihre Einstellung insbesondere zu politischen und familiensoziologischen Themen befragt. Die Interviewpartner werden im sogenannten "Random-route-Verfahren" gewonnen (die Interviewer gingen von der niedrigsten Hausnummer einer benannten Straße aus und befragten jeweils in der 7. Wohnung den Haushaltsvorstand). Name und Adresse werden erhoben, jedoch getrennt von den erfragten Daten aufbewahrt. Die Auswertung der Daten erfolgt aufgrund mehrerer Strukturfragen (Alter, Geschlecht, Schulbildung, Berufstätigkeit, Berufsgruppe, Haushaltsnettoeinkommen, Religion, Aufenthaltsdauer in Deutschland, Haushaltsgröße).

Den Interviews, die vertragsgemäß von der Firma Emnid GmbH & Co., Bielefeld, durchgeführt werden, liegt eine türkische Übersetzung des Fragebogens zugrunde. Ein begleitendes Informationsblatt - ebenfalls in türkischer Sprache - informiert die Interviewpartner nicht über den Zweck der Umfrage, wohl aber über die beabsichtigte Verarbeitung der Daten (Weiterversand der Fragebögen an Emnid, getrennte Erfassung von Name und Adresse, Auswertung der Umfrage durch einen Computer, Zusicherung, daß keine Daten an andere Ämter oder Personen weitergegeben werden, Verschwiegenheitspflicht der Mitarbeiter). Ein besonderer Hinweis auf die Freiwilligkeit erfolgt nicht. Bei der datenschutzrechtlichen Beurteilung war die unterschiedliche Stellung der Beteiligten zu berücksichtigen. Da sich der zwischen dem Land Berlin und Emnid geschlossene Vertrag nicht auf genau definierte Datenverarbeitungsvorgänge beschränkt, sondern auch die Erarbeitung der Fragenprogramme, die Erstellung der Stichproben, die Durchführung der Interviews sowie die Auswertung umfaßt, handelt es sich in datenschutzrechtlichem Sinne nicht um Datenverarbeitung im Auftrag (mit der Folge, daß auch den von Emnid durchgeführten Phasen der Datenverarbeitung das Berliner Datenschutzgesetz zugrundezulegen wäre, § 2 Abs. 1 Berliner Datenschutzgesetz), sondern auf Seiten von Emnid um Verarbeitung personenbezogener Daten zum Zwecke der Übermittlung in anonymisierter Form (§ 36 Bundesdatenschutzgesetz). Das Berliner Datenschutzgesetz greift demnach erst bei der Frage ein, welche Daten von Emnid der Ausländerbeauftragten zur Verfügung gestellt und dort aufbewahrt (gespeichert) werden. Darüber hinaus ist jedoch nicht zu verkennen, daß bei Forschungsaufträgen, die öffentliche Stellen vergeben, eine Verantwortung hinsichtlich der Verarbeitung personenbezogener Daten durch das beauftragte Institut besteht. Die datenschutzrechtlichen Verpflichtungen, denen öffentliche Stellen unterworfen sind, können nicht durch die Beauftragung einer privaten Stelle unterlaufen werden. In den Vereinbarungen mit dem Auftragnehmer ist daher ein Datenschutzstandard festzuschreiben, der den Vorschriften für die öffentliche Stelle entspricht. Dies sollte vorzugsweise durch eine entsprechende Klausel im Vertrag geschehen.

Für die Erhebung der Daten selbst, insbesondere für die Gestaltung der einzelnen Fragen enthalten die Datenschutzgesetze keine inhaltlichen Kriterien. Allerdings zieht das Grundgesetz

selbst Grenzen für die Zulässigkeit von Fragen, soweit sie von einer öffentlichen Stelle gestellt werden. So hält das Bundesverfassungsgericht eine statistische Befragung über Personen dort für „entwürdigend und eine Bedrohung des Selbstbestimmungsrechtes ..., wo sie den Bereich menschlichen Eigenlebens erfaßt, der von Natur aus Geheimnischarakter hat, und damit auch diesen inneren Bezirk zu statistisch erschließbarem und erschliessungsbedürftigem Material erklärt[22]". Ein Indiz für die Rechtswidrigkeit der Fragen im vorliegenden Fall war jedoch nicht ersichtlich.

Die Teilnahme an derartigen Forschungsprogrammen ist freiwillig, die auf die Erhebung der Daten folgende Verarbeitung ist daher nur mit Einwilligung der Betroffenen zulässig. Bei der Erteilung der Einwilligung muß dem Betroffenen hinreichend viel Information über die geplanten Verarbeitungsschritte gegeben werden. Das von Emnid verwendete Anschreiben enthält hierzu einige Punkte. Ein ausdrücklicher Hinweis auf die Freiwilligkeit sowie eine bessere Aufklärung über den Zweck der Untersuchung wäre jedoch wünschenswert gewesen. Als Anhaltspunkt habe ich auf die Empfehlungen verwiesen, die ich in meinem Jahresbericht 1980[23] veröffentlicht habe.

Auf Grund meiner Kontaktaufnahme mit dem für die Aufsicht über private Einrichtungen zuständigen Regierungspräsidenten Arnsberg hat dieser mir inzwischen mitgeteilt, daß das Emnid-Institut ihm die notarielle Urkunde vorgelegt hat, nach der die Adressenabschnitte aus der Befragung unter notarieller Aufsicht vernichtet worden sind.

Ein Verstoß gegen datenschutzrechtliche Bestimmungen konnte nicht festgestellt werden.

Zur Sicherstellung und Verbesserung des Datenschutzes bei den künftigen Verfahrensschritten, insbesondere bei der zweiten Repräsentativbefragung im Herbst, habe ich folgendes empfohlen:

Bei erneuten Befragungen sollte die Aufklärung der befragten Personen verbessert werden (etwa unter Berücksichtigung der von mir aufgestellten Grundsätze).

Durch zusätzliche Vereinbarung sollte sichergestellt werden, daß die Ausländerbeauftragte von Emnid keine personenbezogenen Daten erhält und die bei Emnid weiterhin aufbewahrten Daten (vgl. § 6 des Vertrages) nach Auswertung keinen Personenbezug mehr aufweisen. Bei neuen Verträgen sollte sichergestellt werden, daß sich der Auftragnehmer an die Bestimmungen des Berliner Datenschutzgesetzes bindet.

Die Ausländerbeauftragte ist der Empfehlung durch eine Ergänzung der Vereinbarung mit Emnid nachgekommen.

Datenschutz in der Schule

Datenschutzprobleme sind wiederum aus dem Schulbereich an mich herangetragen worden. Auch hier tauchen Fragen im Zusammenhang mit Forschungsvorhaben auf.

So wurde von der Senatsverwaltung für Schulwesen, Jugend und Sport eine Forschungsarbeit zur Integration ausländischer Schüler in Auftrag gegeben. Im Verlauf mehrerer Gespräche mit Vertretern der Verwaltung und der Auftragnehmerin des Forschungsvertrages ist es gelungen, eine Konzeption zu entwickeln, welche die Interessen des Forschungsinstitutes an einer unbeeinflußten Materialerhebung, des Auftraggebers an einer relativ zuverlässigen Forschungsaussage und der Betroffenen an einer ausreichenden Beachtung des Persönlichkeitsrechtes berücksichtigt. Ausgangspunkt war dabei die in § 3 Abs. 1 Berliner Schulgesetz normierte Verpflichtung, von Kindern und Erziehungsberechtigten an einem Schulversuch mit den dazu notwendigerweise gehörigen wissenschaftlichen Begleituntersuchungen teilzunehmen, wenn sie bei der Aufnahme in eine entsprechende Versuchsschule ihr Einverständnis erklärt haben. Die erstmalige Erklärung des Einverständnisses habe ich für ausreichend angesehen, um an allen späteren Phasen der Begleitforschung die Teilnahmeverpflichtung zu begründen. Ich gehe davon aus, daß die Einverständniserklärung ein öffentlich-rechtlicher Vertrag ist, der beide Parteien verpflichtet, im Sinne einer seriösen Forschung und Unterrichtsgestaltung an den erforderlichen Maßnahmen mitzuwirken. Allerdings habe ich für die Schulverwaltung die Verpflichtung hervorgehoben, die Eltern von Anfang an über den absehbaren Verlauf des Projektes zu informieren. Sie sind darauf hinzuweisen, daß und in welchem Umfang Daten erhoben werden, zu welchen Zwecken sie verarbeitet und wann sie wieder vernichtet werden. Die hierbei entstehende personenbezogene Schülerdatei ist bei mir zum Dateienregister anzumelden. Eine spätere Überprüfung habe ich mir vorbehalten.

Auf Grund meiner Empfehlung hat die Senatsverwaltung ein Informationsschreiben für die Eltern entworfen, welches die von mir geltendgemachten Forderungen berücksichtigt.

Vom Landeselternausschuß Berlin wurde an mich die Frage herangetragen, ob in Schulklassen Listen mit Namen und Anschriften aller Schüler erstellt werden dürften, die allen Eltern der Klasse ausgehändigt werden. Angesichts der im Schulverfassungsgesetz verankerten Rechtsstellung der Elternvertretungen im Schulbetrieb habe ich keine Bedenken dagegen gehabt, daß die Herausgabe von Adressen an Mitglieder der Elternvertretungen im Rahmen ihrer jeweiligen Aufgaben erfolgt. Anders ist allerdings die Herausgabe von Adressen an Eltern zu beurteilen, die nicht einem derartigen Gremium angehören. Sie werden dann wie jede andere Privatperson behandelt und die Herausgabe von personenbezogenen Informationen an sie ist nur unter den Voraussetzungen des § 11 Berliner Datenschutzgesetz, d.h. mit Einwilligung der Betroffenen zulässig. Diese Einwilligung kann nicht durch den Beschluß eines Elterngremiums ersetzt werden.

Daher können auch keine Abiturientennamen durch Berliner Schulen an Berliner Zeitungen verteilt werden. Wenn gleichwohl ein Bedürfnis für die Veröffentlichung von Schülernamen in den Zeitungen nach bestandenem Abitur besteht, muß dafür die Einwilligung der betroffenen Schüler eingeholt werden.

In einem anderen Fall habe ich jedoch die Herausgabe einer Schüler- bzw. Elternanschrift an den Vater eines anderen Schülers für zulässig gehalten. § 11 Abs. 1 Berliner Datenschutzgesetz mußte in diesem Fall zurücktreten, da durch die im Schulbereich speziell geltende Vorschrift des § 10 Abs. 3 Schulverfassungsgesetz die Aufsichts- und Fürsorgepflicht des Lehrers über die ihm anvertrauten Schüler eine andere Verfahrensweise gebot. Mein Petent stützte sein Interesse darauf, daß sein eigener Sohn von Mitschülern schwerstens bedroht worden war.

Zu einem sehr empfindlichen Bereich im Verhältnis zwischen Schule, Eltern und Kindern zählt auch die Arbeit des Schulpsychologischen Dienstes. Die Ausführungsvorschriften vom 1. April 1974 sind außer Kraft getreten, so daß eine Neufassung erforderlich wurde. Schon im Februar 1981 lag mir eine erste Neufassung vor, die mittlerweile in verschiedenen Punkten abgeändert wurde. Das Mitzeichnungsverfahren ist jedoch noch immer nicht abgeschlossen. Ich habe meine datenschutzrechtlichen Empfehlungen wiederholt vorgetragen. Insbesondere habe ich darum gebeten, bis zur endgültigen Formulierung und Verabschiedung der neuen Bestimmungen das Recht auf Akteneinsicht in schulpsychologische Unterlagen den Forderungen des Bundesverfassungsgerichts entsprechend zu handhaben. Das Bundesverfassungsgericht bejaht den Anspruch auf Akteneinsicht[24]. Es setzt sich jedoch auch mit dem Schutzbedürfnis des Schülers, welches er mitunter auch vor seinen Eltern haben kann, auseinander und bejaht das Recht des Schülers, eine Einsichtnahme durch seine Erziehungsberechtigten zu verwehren. Ich meine, daß alle Schulen verpflichtet sind, auch ohne ausdrückliche Verabschiedung einer entsprechenden Ausführungsvorschrift den Schülern bzw. ihren Eltern diese Rechte einzuräumen. Das Verfahren zur Verabschiedung der neuen Ausführungsvorschrift sollte gleichwohl energisch vorangetrieben werden, da es sich hier um einen sehr kritischen Bereich der Begegnung zwischen privaten Grundrechten und staatlicher Gewalt handelt.

Als ein weiteres nicht das Verhältnis zwischen Schule und Schülern bzw. deren Eltern betreffendes Problem stellte sich die Existenz einer Lehrerindividualdatei beim Senator für Schulwesen, Jugend und Sport heraus. Die Zulässigkeit dieser Datei ist rechtlich völlig ungeklärt. Die Rechtslage nach dem Allgemeinen

[22] BVerfGE 27, 7
[23] S. 6
[24] Urteil vom 9. Februar 1982 (AZ: 1 BvR 845/79)

Zuständigkeitsgesetz (AZG) bzw. der Durchführungsverordnung zum AZG läßt keinen eindeutigen Schluß darauf zu, für welche Aufgaben die Bezirksverwaltungen und für welche Aufgaben die Senatsverwaltung für Schulwesen, Jugend und Sport letztlich zuständig sein sollen. Eine ausreichende Rechtsgrundlage, die entweder die Bezirke oder die Senatsverwaltung für Schulwesen als befugte speichernde Stelle einer Lehrerindividualdatei ausweist, ist weder in Art. 7 der Verfassung von Berlin noch in § 3 Landesbeamtengesetz (LBG), § 5 Schulgesetz und § 9 Schulverfassungsgesetz vorhanden. Nach § 9 Berliner Datenschutzgesetz ist jedoch Voraussetzung für die Zulässigkeit einer Datenspeicherung, daß die in einer Datei enthaltenen Daten zur Erfüllung konkret bestimmter Aufgaben der speichernden Stelle erforderlich sind. Ich habe der Schulverwaltung empfohlen, hier klärende Maßnahmen zu treffen.

Ein ungewöhnliches Problem, das aber Gegenstand mehrerer Beschwerden war, ist die Frage, inwieweit auch Unterrichtsinhalte auf den Datenschutz Rücksicht nehmen müssen.

Mehrfach hatten sich Eltern darüber beschwert, daß ihr schulpflichtiges Kind in einer Hausaufgabe detailliert häusliche Verhältnisse darstellen soll. Die Eltern befürchteten, daß sich der Lehrer auf diese Weise Informationen über das Elternhaus verschaffen könnte.

Um Befürchtungen von Eltern von vornherein zu begegnen, empfehle ich eine gewisse Zurückhaltung. Gegebenenfalls könnte mit den Kindern sogar auf einfache Weise die Problematik derartiger Beschreibungen diskutiert werden. Schließlich könnte man daran denken, ein unverfänglicheres Thema als Alternative anzubieten, so daß Schüler, die ihre häusliche Sphäre nicht weiter offenbaren wollen, auf ein anderes Thema ausweichen können.

Selbstverständlich kann nicht Ziel des Datenschutzes sein, die Familie zum Tabu zu erklären. Mir schiene es aber ein sehr lohnenswertes pädagogisches Ziel, wenn die Erhebung derartiger Daten im Rahmen von Schulübungen mit einer entsprechenden Diskussion über Persönlichkeitsrechte und ihre Bedeutung verbunden werden könnte. Die Senatorin für Schulwesen, Jugend und Sport hat eine Überprüfung zugesagt.

Zusammenarbeit zwischen Lohnsteuerstellen und Ausländerbehörde

Nach wie vor besteht auf dem Berliner Arbeitsmarkt eine angespannte Situation, die auf konjunkturellen Bedingungen beruht und zusätzlich durch Schwarzarbeit und illegale Beschäftigung negativ beeinflußt wird. Vor diesem Hintergrund erging eine Anweisung des Senators für Inneres an die bezirklichen Lohnsteuerstellen, wonach diese die Ausstellung einer Lohnsteuerkarte an Ausländer weitermelden sollen. Damit soll ein Beitrag zur Bekämpfung illegaler Praktiken auf dem Arbeitsmarkt geleistet werden.

Beim Senator für Inneres bestanden - ebenso wie beim Senator für Finanzen - bei der Planung des Verfahrens Zweifel, ob die Übermittlungen mit dem Steuergeheimnis zu vereinbaren seien. Nach einem Schriftwechsel mit dem Bundesminister für Finanzen teilte dieser dem Senator für Inneres im Juni 1983 mit, daß aus steuerlicher Sicht keine Bedenken gegen eine Mitteilung an die Ausländerbehörde bestünde. Ich habe den Senator für Inneres darauf hingewiesen, daß bei der vom Bundesminister für Finanzen gebilligten Verfahrensweise das Steuergeheimnis des § 31 a Abgabenordnung (AO) nicht gewahrt ist.

Nach § 31 a Abs. 1 Satz 1 AO ist die Offenbarung der nach § 30 AO (Steuergeheimnis) geschützten Verhältnisse des Betroffenen zulässig, soweit sie der Bekämpfung der Schwarzarbeit dient und der Betroffene seine steuerlichen Pflichten verletzt hat. Nach Satz 2 dieser Vorschrift gilt gleiches, wenn ein Arbeitnehmer ohne die erforderliche Erlaubnis nach § 19 Abs. 1 des Arbeitsförderungsgesetzes (Arbeitserlaubnis für Ausländer) beschäftigt oder tätig wird. Ganz offensichtlich wäre die Übermittlung mit § 31 a Abs. 1 Satz 1 AO nicht vereinbar, denn die Ausländer zeigen, indem sie eine Lohnsteuerkarte beantragen, daß sie ihre Steuerpflichten gerade nicht verletzen wollen. Als Rechtfertigung für die Übermittlung beruft sich der Senator für Inneres daher auf § 31 a Abs. 1 Satz 2 AO, denn dort ist nur davon die Rede, daß eine Offenbarung zulässig sei, falls ein Ausländer keine Arbeitserlaubnis hat.

Allein das Abstellen auf den Wortlaut der Vorschrift reicht jedoch nicht. Die Abgabenordnung regelt das Steuerrecht, nicht jedoch das Ausländerrecht. Allein eine Verletzung der ausländerrechtlichen Vorschriften kann daher nicht zu einer zulässigen Offenbarung führen. Vielmehr muß auch in der zweiten Alternative eine Verletzung steuerlicher Pflichten vorliegen, um eine Offenbarung zu ermöglichen.

Es kommt hinzu, daß das Gesetz gegen illegale Beschäftigungen in Art. 1 Ziff. 4 eine Regelung getroffen hat, auf welche Weise die Ausländerbehörde ggf. über illegale Beschäftigungen unterrichtet werden soll. Danach soll die Bundesanstalt für Arbeit, sofern sie bei der Durchführung des Arbeitnehmerüberlassungsgesetzes konkrete Anhaltspunkte für Verstöße gegen § 19 Arbeitsförderungsgesetz erhält, die Ausländerbehörden unterrichten. Eine direkte Information der Ausländerbehörde durch die Finanzämter ist durch die abschließende Regelung ausgeschlossen worden.

Ein Einvernehmen konnte mit dem Senator für Inneres bisher nicht hergestellt werden. Da auch der Bundesminister für Finanzen betroffen ist, habe ich mich mit dem Bundesbeauftragten für den Datenschutz in Verbindung gesetzt, um eine Klärung zu erreichen.

Zugriff auf die Kaufpreissammlung nach dem Bundesbaugesetz

Der beim Senator für Bau- und Wohnungswesen bestehende Gutachterausschuß hat nach §§ 136 ff. Bundesbaugesetz (BBauG) u. a. die Aufgabe, Wertgutachten für Grundstücke zu erstellen. Grundlage für seine Beurteilung bildet dabei die Kaufpreissammlung, in der sämtliche Käufe mit Angaben über Grundstücksart, -größe, -kaufpreis und -lage erfaßt werden. Bei der Vorbereitung der Gutachten wirken nach § 7 Abs. 3 DVO-BBauG die bezirklichen Vermessungsämter mit. Es ist geplant, daß alle Bezirke über einen On-line-Anschluß auf den gesamten Berliner Datenbestand der Kaufpreissammlung zugriffsberechtigt sein sollen, um Bewertungsmaterial für die Gutachten zu erlangen.

Ein derartiges Verfahren wäre mit §§ 136 ff. BBauG unvereinbar, da nach diesen Vorschriften die Kaufpreissammlung nur dem Gutachterausschuß selbst und den Finanzämtern zur Verfügung steht. Demgegenüber vertrat der Senator für Bau- und Wohnungswesen die Auffassung, daß die zulässige Mitwirkung der Bezirke auch das unbeschränkte Zugriffsrecht auf die Kaufpreissammlung beinhalte. Diese Ansicht verkennt, daß eine Durchführungsverordnung nicht mehr Rechte einräumen kann, als die Ermächtigungsnorm, hier das Bundesbaugesetz, erlaubt.

Dennoch habe ich mich dem Anliegen des Senators für Bau- und Wohnungswesen, der darauf hinwies, daß bei einer völligen Sperrung des Zugangs auf die Kaufpreissammlung für die Bezirke eine Vorbereitung von Gutachten nicht mehr möglich sei, nicht verschlossen. Gemeinsam wurde eine Lösung gefunden, die den Zugriff der Bezirke auf das Erforderliche beschränkt, so daß künftig in jedem Einzelfall vorab geprüft werden wird, inwieweit ein beschränkter Zugriff auf die Daten der Kaufpreissammlung für die Vorbereitung des Gutachtens ausreicht. Entsprechende Änderungen der Verwaltungsanweisungen und des § 7 Abs. 3 DVO-BBauG werden vorbereitet.

4. Nachtrag zu Feststellungen aus den Vorjahren

Kriminalpolizeiliche personenbezogene Sammlungen (KpS) (Jahresbericht 1982, S. 11)

Im Gegensatz zu anderen Bundesländern war in Berlin bisher nicht vorgesehen, daß die Errichtung automatisierter und manueller Dateien zu Zwecken der Strafverfolgung in einem formellen Verfahren geregelt und festgeschrieben wird. Mit Erlaß vom 11. August 1983 hat der Senator für Inneres nunmehr bestimmt, daß in automatisierten Verfahren geführte Dateien nur mit Zustimmung des Senators für Inneres errichtet werden dürfen; die Errichtung von manuell geführten Dateien bedarf in Zukunft in jedem Einzelfall der besonderen Anordnung durch den Landeskriminaldirektor; dabei sind der Zweck der Kartei, die Rechtsgrundlage, der betroffene Personenkreis, die Arten der zu erfassenden personenbezogenen Daten, die karteiführende Stelle,

die Anlieferung bzw. Ursprung der Daten, die Benutzer der Kartei, die voraussichtliche Dauer der Karteiführung und die Behandlung ausgesonderter Unterlagen festzustellen. Mit dem Erlaß verbunden ist die Anordnung, die bereits bestehenden manuellen Datensammlungen festzustellen. Dies entspricht meinen Empfehlungen.

Kriminalpolizeiliche personenbezogene Sammlungen im Zusammenhang mit Hausbesetzungen (Jahresbericht 1982, S. 12)

In Gesprächen mit dem Senator für Inneres sowie dem Polizeipräsidenten in Berlin wurde in Aussicht gestellt, daß die wesentlichen von mir angesprochenen Probleme dadurch gelöst werden, daß die damals erhobenen Daten in relativ kurzer Frist gelöscht werden („Datenamnestie"). Ich werde darauf hinwirken, daß diese Löschung auch bei den Stellen nachvollzogen wird, an die aufgrund der entsprechenden Vorgänge personenbezogene Daten übermittelt wurden.

Angabe des Überweisungsgrundes auf Überweisungsträgern (Jahresbericht 1981, S. 12, Jahresbericht 1982, S. 13)

Auf Überweisungsträgern,mit denen Sozialleistungen angewiesen werden, sollten keine Angaben über den Grund der Überweisung enthalten sein, da die damit verbundene Offenbarung gegenüber der Bank über das erforderliche Ausmaß hinausgeht. Ausreichend ist, wenn auf dem Überweisungsträger auf den Bescheid Bezug genommen wird. Dieses bisher aufgrund praktischer Erwägungen abgelehnte Verfahren ist jetzt erleichtert, da seit August 1983 aufgrund der Automatisierung des Verfahrens in jedem Fall an die Leistungsempfänger schriftliche Bescheide verschickt werden. Der Senator für Gesundheit, Soziales und Familie hat die Bezirksämter aufgefordert, bei den Überweisungen nur noch auf diesen Bescheid Bezug zu nehmen.

Wohnungsbau-Rechenzentrum (WBRZ) (Jahresbericht 1982, S. 17)

Die von mir vertretene Auffassung, angesichts der Schachtelbeteiligung des Landes Berlin am Wohnungsbau-Rechenzentrum stehe mir wegen §2 Abs. 3 Berliner Datenschutzgesetz eine unmittelbare Kontrollbefugnis zu, schloß sich auch im Berichtsjahr das Wohnungsbau-Rechenzentrum nicht an, obwohl der Unterausschuß Berliner Datenschutzgesetz des Ausschusses für Inneres, Sicherheit und Ordnung meine Meinung teilte. Praktisch wird das Problem dadurch gelöst, daß sich das Wohnungsbau-Rechenzentrum in einer vertraglichen Vereinbarung dem Berliner Datenschutzgesetz und der Kontrolle des Berliner Datenschutzbeauftragten unterwirft.

Schülerdaten (Jahresbericht 1980, S. 13, Jahresbericht 1981, S. 11 f., Jahresbericht 1982, S. 19 f.)

Der Senator für Schulwesen, Jugend und Sport hat in der Zwischenzeit Entwürfe einer Allgemeinen Verwaltungsvorschrift über Schülerakten in der Berliner Schule vorgelegt. Ich habe hierzu eine Stellungnahme erarbeitet.

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

Der Senator für Inneres hat in einem Rundschreiben empfohlen, die Einholung unbeschränkter Auskünfte aus dem Bundeszentralregister einzuschränken. Für den eigenen Geschäftsbereich erging eine entsprechende Anweisung. Ich werde überprüfen, ob den Empfehlungen von allen Stellen gefolgt wird.

Verordnung über Führung, Inhalt und Aufbewahrung von Krankengeschichten in Krankenhäusern - Krankengeschichtenverordnung - (Jahresbericht 1981, S. 6, Jahresbericht 1982, S. 20)

Mir ist ein Entwurf der Verordnung vorgelegt worden, der allerdings ein wesentliches Anliegen nicht berücksichtigt: Jede Vorschrift über die Führung personenbezogener Akten sollte Bestimmungen darüber enthalten, in welchem Umfang und auf welche Weise Akteneinsicht zu gewähren ist. Dem kommt gerade im Gesundheitsbereich große Bedeutung zu (vgl. oben). Ich werde weiter auf die Aufnahme entsprechender Regelungen hinwirken.

Telefondatenerfassung (Jahresbericht 1981, S. 17)

Die Freie Universität Berlin hat ihr Verfahren zur automatischen Erfassung von Telefondaten inzwischen so geändert, daß die Speicherung von Zielnummern bei privaten Ferngesprächen nicht mehr erfolgt. Der Unterausschuß Berliner Datenschutzgesetz des Ausschusses für Inneres, Sicherheit und Ordnung des Abgeordnetenhauses hat mich gebeten, auf eine einheitlich rechtmäßige Handhabung in Berlin hinzuwirken. Ich habe mich daraufhin über die Verfahrensweise in allen Hochschulen, bei den Eigenbetrieben und bei den meisten anderen Körperschaften und Anstalten des öffentlichen Rechts informiert. Ich habe dabei festgestellt, daß in keinem Fall eine rechtswidrige Speicherung der Zielnummer von privaten Ferngesprächen erfolgt. Da jedoch auf Grund der technischen Entwicklung die breite Einführung moderner Telefondatenerfassungssysteme zu erwarten ist, habe ich die öffentlichen Stellen vorsorglich von meiner Rechtsauffassung informiert.

5. Zusammenarbeit mit anderen Stellen

5.1 Datenschutzbeauftragte des Bundes und der Länder

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat in vier Sitzungen unter dem Vorsitz des Landesbeauftragten für den Datenschutz der Freien Hansestadt Bremen beraten.

Die wichtigsten Ergebnisse lassen sich wie folgt zusammenfassen:

14. Konferenz am 21. März 1983

- Beschluß zur Volkszählung 1983, der insbesondere die Forderungen der Datenschutzbeauftragten zur Volkszählung enthält (vgl. Anlage 3).
- Beschluß über die Kontrollrechte der Datenschutzbeauftragten und Geheimhaltungsvorschriften. Mit dem Beschluß unterstützt die Konferenz die Auffassung des Bundesbeauftragten, daß seine Prüfungskompetenz im Hinblick auf die anderen Vorschriften über den Datenschutz im Sinne des §19 Abs. 1 Bundesdatenschutzgesetz auch für Kontrollen bezüglich der Einhaltung besonderer Geheimhaltungsvorschriften (z. B. ärztliche Schweigepflicht) besteht.
- Beschluß über den Umfang der Prüfungskompetenz beim Verfassungsschutz.

15. Konferenz am 6. Juni 1983

- Im Zusammenhang mit der Einführung der fälschungssicheren Personalausweise wurde diskutiert, inwieweit dem Junktimbeschluß des Bundestages (Bundestagsdrucksache 8/3498) im Bund und den Ländern Rechnung getragen worden sei, und welche Konsequenzen dies für die datenschutzrechtliche Beurteilung der Personalausweise habe. Es wurde eine Arbeitsgruppe eingesetzt, die die datenschutzrechtlichen Anforderungen formuliert.
- Zur Übernahme des Btx-Staatsvertrages wurden die Anforderungen an die Übernahmegesetze festgelegt.

16. Konferenz am 13. September 1983

- Beschluß über den Datenschutz bei den Personalausweisen (vgl. Anlage 4).

17. Konferenz am 3. November 1983

- Beschluß zur Novellierung des Bundesdatenschutzgesetzes.

Der Vorsitz auf der Konferenz wird mit dem Jahreswechsel turnusgemäß auf den Hamburgischen Datenschutzbeauftragten übergehen.

5.2 Aufsichtsbehörde für nicht-öffentliche Stellen, andere Kontrollbehörden

In den turnusmäßigen Sitzungen mit dem Senator für Inneres als Aufsichtsbehörde für den Datenschutz wurden zahlreiche Grundsatz- und Einzelfragen behandelt: Unter anderem Probleme des §11 Berliner Datenschutzgesetz, Namensveröffentlichungen von Mitarbeitern im Landespressedienst, das Verhältnis Sozialgesetzbuch - Strafverfolgung, der Entwurf des Btx-

Staatsvertrages, Neufassung der GGO I, Fragen der privatärztlichen Behandlung in öffentlichen Krankenhäusern sowie die Probleme bei der Erhebung personenbezogener Daten insbesondere über die Einkommensverhältnisse der Ehegatten beim Vollzug des Bundeskindergeldgesetzes.

Kontaktgespräche mit einzelnen Datenschutzbeauftragten der Religionsgemeinschaften habe ich in diesem Jahr fortgeführt. In mehreren Fällen sind bei mir Eingaben über die Kirchensteuerstellen eingegangen. Diese mußte ich an die zuständigen Datenschutzbeauftragten der Religionsgemeinschaften weitergeben. Wegen der verfassungsrechtlich garantierten Autonomie der Kirchen stehen mir insoweit keine Kontrollbefugnisse zu.

5.3 Berliner Verwaltung

Zusammenarbeit

In der Zusammenarbeit mit den meisten Berliner Verwaltungsstellen ist inzwischen eine gewisse Normalität eingetreten, da sich diese Stellen in der Regel an die Existenz des Datenschutzbeauftragten gewöhnt haben und in wachsender Zahl auch gewisse Vorteile darin erkennen, ihre Arbeitsweise auf die Datenschutzbestimmungen einzustellen, um von vornherein Angriffen von dieser Seite vorzubeugen. Dem gegenseitigen Verständnis förderlich ist es ferner, daß die Dienststelle des Datenschutzbeauftragten als Ausbildungsstation dient, die seit 1980 bereits 28 Nachwuchskräfte durchlaufen haben.

Dateienregister

Nachdem ich bei verschiedenen öffentlichen Stellen die Abgabe der Anmeldung der automatisierten Dateien zu dem bei mir geführten Register angemahnt hatte, hat sich die Zahl der Dateimeldungen von 474 im Vorjahr auf 895 in diesem Jahr nahezu verdoppelt. Es ist davon auszugehen, daß im Laufe des kommenden Jahres endlich ein vollständiger Überblick über die von öffentlichen Berliner Stellen geführten Dateien vorliegt.

5.4 Abgeordnetenhaus

Auf Grund meiner Hilfsfunktion für das Parlament bestehen vielfältige Beziehungen zu den Fraktionen und Abgeordneten. U. a. habe ich zu folgenden Problemen Stellung genommen:

Für den *Hauptausschuß* habe ich auf dessen Wunsch im September 1983 einen Erfahrungsbericht über meine bisherige Tätigkeit erstellt. Im *Ausschuß für Inneres, Sicherheit und Ordnung* habe ich schriftlich und mündlich zum Entwurf des Landesmeldegesetzes und zu dem Entwurf einer Änderung des 11 Berliner Datenschutzgesetz Stellung genommen. Im *Ausschuß für Kulturelle Angelegenheiten* hatte ich Gelegenheit zur Stellungnahme zum Btx-Staatsvertrag und zum Zustimmungsgesetz. Mit dem *Petitionsausschuß* bestehen naturgemäß Berührungspunkte. So habe ich auf Bitten des Vorsitzenden eine Stellungnahme abgegeben, daß sich Verwaltungen gegenüber dem Petitionsausschuß nicht unter Hinweis auf das Sozialgesetzbuch weigern können, Daten an den Petitionsausschuß herauszugeben. Schließlich sind vom Vorsitzenden des *Ersten Untersuchungsausschusses* (Verfahrensweise der Ausländerbehörde) zwei Stellungnahmen zu der Frage erbeten worden, unter welchen Umständen sich Zeugen und Dienststellen gegenüber diesem Ausschuß auf das Sozialgeheimnis berufen können.

Die guten Kontakte zu allen Parteien im Abgeordnetenhaus stellen eine wichtige Grundlage für die Verwirklichung des Datenschutzes dar.

6. Aufgaben des Berliner Datenschutzbeauftragten

6.1 Im Berichtsjahr 1983

Anrufungen durch jedermann

Die Zahl der schriftlichen Eingaben ist nach den großen Zuwachsraten der Vorjahre nicht weiter angestiegen. Dabei war die interessante Entwicklung zu beobachten, daß einfache Eingaben zurückgegangen sind. Dies dürfte nicht zuletzt auf die Öffentlichkeitsarbeit und das gestiegene Problembewußtsein zurückzuführen sein. Dagegen ist die Zahl komplizierter Fälle beachtlich angestiegen.

Die Verteilung der Eingaben auf die einzelnen Verwaltungsbereiche hat sich gegenüber dem Vorjahr nicht wesentlich geändert. Sie entfallen nach der Häufigkeit geordnet insbesondere auf folgende Gebiete:

1. Öffentliche Sicherheit und Ordnung
2. Gesundheit und Soziales
3. Wirtschaftsverwaltung
4. Justiz
5. Finanzen
6. Kultur

In gut 50 % aller Eingaben haben sich Mängel herausgestellt.

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

Beratung und Kontrolle

Bei den Beratungsersuchen (§ 21 Abs. 1 letzter Satz Berliner Datenschutzgesetz) ist eine ähnliche Entwicklung zu beobachten wie bei den Anrufungen.

In vielen Fällen wenden sich öffentliche Stellen mit der Bitte um Beratung an mich. Dies begrüße ich ausdrücklich, da sich so häufig die Beachtung der Datenschutzvorschriften von vornherein sicherstellen und damit nachträgliche Kritik vermeiden läßt.

Durch die Beratung soll sichergestellt werden, daß insbesondere Erfahrungen aus der Prüfungspraxis anderen Stellen nutzbar gemacht werden.

Die Beratung bedeutet jedoch keine „Unbedenklichkeitsbescheinigung" für ein Projekt, da

- das Projekt nach der Beratung noch verändert werden kann (es entspricht der praktischen Erfahrung, daß dies sogar recht häufig geschieht),
- die praktische Durchführung eines rechtlich einwandfrei konzipierten Projektes durchaus Datenschutzmängel aufweisen kann,
- sich das Datenschutzrecht fortentwickelt (z. B. zwischenzeitlich Grundsatzentscheidungen der Gerichte getroffen werden) und diese Fortentwicklung bei einer späteren Kontrolle berücksichtigt werden muß.

Nach alledem bleibt festzustellen, daß von einer Beratung durch den Datenschutzbeauftragten für diesen keine Bindungswirkungen im Hinblick auf eine spätere Kontrolle ausgehen.

Bereits aus diesen Gründen verbietet es sich, bei Vorhaben ohne mein vorheriges Einverständnis mit der Beteiligung des Datenschutzbeauftragten zu werben.

Vor allem sollte - um späterer Kritik vorzubeugen - in Fällen, in denen der Datenschutzbeauftragte einmal beteiligt worden ist, nicht vergessen werden, ihn auch über Veränderungen zu unterrichten. Dazu gehören z. B. Konkretisierungen wie das Erstellen von Anschreiben und Fragebogen bei Befragungen von bestimmten Bürgern etc.

Öffentlichkeitsarbeit

Der gute Kontakt zur Bevölkerung und zu den Medien konnte ausgebaut werden. So hat der SFB im Frühjahr ca. eine Dreiviertelstunde über meine Tätigkeit berichtet[25]. Ferner habe ich an einer einstündigen Diskussionsrunde des NDR-Fernsehens über die Volkszählung teilgenommen. Daneben berichteten Presse, Rundfunk und Fernsehen sehr umfangreich über die Volkszählung. Meine Mitarbeiter und ich haben ca. 40 Veranstaltungen anläßlich der Volkszählung in Berlin besucht.

Um den Kontakt zur Verwaltung zu vertiefen, habe ich eine Schrift herausgegeben, die sich an die Verwaltungsmitarbeiter richtet und ihnen helfen soll, sich bei Datenanforderungen von Seiten der Forschung und Planung richtig zu verhalten. Daneben

[25] Interessenten kann eine Aufzeichnung zur Verfügung gestellt werden

habe ich an Aus- und Fortbildungsveranstaltungen an der Freien Universität, der Verwaltungsakademie und im Bereich der Lehrerfortbildung teilgenommen.

Für das Museum für Verkehr und Technik habe ich an der Konzeption einer Datenschutzwand für die Ausstellung „Rechen-, Speicher- und Datentechnik" mitgewirkt. Die 3 mal 5 m große Tonbildwand zum Thema Datenschutz soll die Spannweite der Datenverarbeitung und ihre Auswirkung auf den einzelnen Menschen verdeutlichen. Dem Zuschauer soll anhand von sechs typischen Lebenssituationen (z.B. Geburt, Schule, Verkehr mit einem Kreditinstitut) bewußt werden, daß viele Handlungen einen „Datenschatten" werfen. Beispiele, die echten ADV-Verfahren entsprechen, werden in der Wand eingeblendet. Anhand zweier Entscheidungssituationen, Bewerbung um einen Arbeitsplatz und Kreditantrag, wird jeweils verdeutlicht, wie die Entscheidung ausfiele, wenn es keinen Datenschutz gäbe und wenn der Datenschutz beachtet wird. Dem Zuschauer wird dabei optisch angezeigt, auf welche Daten im letzten Fall zugegriffen werden darf und welche tabu sind. Zum Schluß soll dem Zuschauer verdeutlicht werden, welche Mittel die Einhaltung des Datenschutzes garantieren und wohin er sich im Zweifel wenden kann.

Auf besonderes Interesse auch im internationalen Bereich stoßen vor allem die Neuen Medien. So fand anläßlich der Internationalen Funkausstellung 1983 eine Sondersitzung der Arbeitsgruppe Datenschutz bei Massenmedien (Working Group on Mass Media) der internationalen Datenschutzbeauftragten unter Vorsitz Norwegens in Berlin statt.

Schließlich haben meine Mitarbeiter und ich auf Einladung zahlreicher Verbände und Parteien bei Veranstaltungen über Datenschutzthemen gesprochen. Im Haus der Kirche fand eine öffentliche Diskussion über Fragen des Melderechts und des maschinenlesbaren Personalausweises statt.

Räumliche Unterbringung der Dienststelle

Mit Unterstützung durch alle im Parlament vertretenen Fraktionen wurde es möglich, meine Dienststelle endgültig in der Hildegardstraße 29/30 in 1000 Berlin 31 (nahe Bundesplatz) einzurichten. In diesen Räumen war zuvor die Projektgruppe Einwohnerwesen untergebracht. Die freiwerdenden Räume im Europa-Center hat der Senator für Kulturelle Angelegenheiten Berlin übernommen. Durch diesen Ringtausch ist eine funktionsgerechte und dauerhafte Unterbringung erreicht.

6.2 Voraussichtliche Schwerpunkte der künftigen Arbeit

Auf Grund der bisherigen Erfahrungen ergeben sich folgende Schwerpunkte für das Jahr 1984:

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

   Ich sehe es nach wie vor für meine wesentliche Aufgabe an, diese Eingaben möglichst zügig zu erledigen.

b) Überprüfung von Amts wegen und Beratung
   - Sozialleistungsträger
   - „Wettbewerbsunternehmen" i.S. §1 Abs.2 Berliner Datenschutzgesetz
   - Öffentliche Sicherheit und Strafverfolgung
   - Neue Medien (insbesondere Kabelpilotprojekt)
   - Fortsetzung der Überprüfungen im bezirklichen Bereich.

6.3 Absehbare Entwicklungen

Novellierung des Bundesdatenschutzgesetzes

Nachdem sich die neue Bundesregierung in den Koalitionsvereinbarungen auf eine Weiterentwicklung des Datenschutzrechts festgelegt hatte, wurde erneut ein Referentenentwurf vorgelegt. Einige wesentliche Verbesserungen, die in dem im vergangenen Jahr vorgelegten Referentenentwurf enthalten waren, sind nicht mehr aufgenommen worden. Ohne die Berechtigung einzelner Vorschläge bestreiten zu wollen, erscheinen mir die beabsichtigten Änderungen derart marginal, daß sie eine Novellierung des Bundesdatenschutzgesetzes zu diesem Zeitpunkt nicht rechtfertigen. Ich bin überzeugt, daß es für alle Beteiligten und Betroffenen besser wäre, weiter praktische Erfahrungen zu sammeln, die Entwicklung der Rechtsprechung abzuwarten und das Datenschutzrecht in den Nachbarstaaten zu beobachten, ehe man an eine Neuregelung des Datenschutzes herangeht.

Ich vertrete darüberhinaus auch die Meinung, daß eine Änderung des Berliner Datenschutzgesetzes zur Zeit nicht erforderlich ist. Da das Berliner Datenschutzgesetz zu den neueren Datenschutzgesetzen zählt, enthält es ohnehin einige Regelungen, die in das Bundesdatenschutzgesetz erst eingefügt werden sollen.

Es mehren sich die Stimmen, die bei dieser Gelegenheit auch die Aufnahme entsprechender verfassungsrechtlicher Bestimmungen fordern. Meine Skepsis derartigen Bemühungen gegenüber habe ich bereits in dem Bericht über die Aufnahme meiner Tätigkeit Ausdruck verliehen[26]. Diese Zurückhaltung wird auch vom Wissenschaftlichen Dienst des Abgeordnetenhauses geteilt, der auf Antrag der F.D.P.-Fraktion zu dieser Frage ein wissenschaftliches Gutachten erstellt hat. Die Auswertung des Urteils des Bundesverfassungsgerichts zum Volkszählungsgesetz 1983 vom 15. Dezember 1983 wird zeigen, ob die Bestätigung des „informationellen Selbstbestimmungsrechts" durch das Gericht eine Kodifizierung erforderlich macht oder ob diese von mir seit jeher vertretene Position[27] auch ohne Änderung des Grundgesetzes umgesetzt werden kann.

Der Berliner Gesetzgeber wird sich mit mehreren spezialgesetzlichen Regelungen zum Datenschutz beschäftigen müssen.

Im Berichtsjahr eingebracht wurde ein Gesetzentwurf der CDU-Fraktion des Abgeordnetenhauses, mit dem das unabdingbare Einwilligungserfordernis des §11 Berliner Datenschutzgesetz abgeschafft und die Bestimmung an die Regelung des Bundesdatenschutzgesetzes angepaßt werden sollte. Ich habe mich einer Lösung nicht verschlossen, die bei Beibehaltung des grundsätzlichen Erfordernisses der Einwilligung des Betroffenen bei der Übermittlung von Daten an nicht-öffentliche Stellen dennoch in Konfliktfällen Abhilfe schafft.

Das im August vorgelegte Gesetz für psychisch Kranke enthält zum derzeitigen Stand noch keinerlei datenschutzrechtliche Regelungen. Angesichts der Sensitivität der Daten, die gerade bei psychiatrischen Behandlungen entstehen, sind hier Bestimmungen erforderlich, die die Speicherung sowie die zulässigen Offenbarungen entsprechender Daten auf das unerläßliche Ausmaß beschränken. Auch der Umfang des Einsichtsrechtes nach Abschluß der Behandlung sollte hier geregelt werden.

Das umfangreichste Gesetzgebungsverfahren, zu dem bereits intensive Verhandlungen im Innenausschuß des Abgeordnetenhauses angelaufen sind, wird das neue Gesetz über das Meldewesen sein. Meine Auffassung zu den vorgesehen Bestimmungen habe ich bereits ausführlich im Jahresbericht 1982 dargelegt.

Berlin, 29. Dezember 1983

Der Berliner Datenschutzbeauftragte

Dr. Kerkau

[26] Mitteilungen des Präsidenten - Nr. 40 -, Drs 8/277 vom 22. Januar 1980, S. 6
[27] ebenda, S.3

Anlage 1

Übersicht zum Btx-Staatsvertrag über die Forderung der Gutachter und ihrer Verwirklichung im Staatsvertrag

Begleitforschung Berlin (Drucksache des Abgeordnetenhauses 9/1095 vom 5. April 1983)	Gesetz zum Staatsvertrag über Bildschirmtext vom 23. Juni 1983 (GVBl. S. 971)	Begleitforschung Düsseldorf (Vorlage Landtag NW 9/1157)	Grundsätze der Datenschutzbeauftragten für den Datenschutz bei den Neuen Medien vom 11. Dezember 1980 (Drucksache des Abgeordnetenhauses 9/248 vom 29. Dezember 1981)
Forderung nach Btx-spezifischer Datenschutzregelung mit rechtstheoretischer Begründung wegen des allgemeinen Gefährdungsrisikos (insbesondere S. 37, 56)	Vgl. Art. 9, 10, 11 und §§ 3, 4 Übernahmegesetz	Vgl. Begleitforschung S. 45	Vgl. Vorbemerkung und Ziff. 2.2
Btx-spezifische Datenschutzregelung für – Betreiber – Anbieter (vgl. insbesondere S. 59, 62)	Vgl. Art. 9 Abs. 3; Art. 10 Vgl. Art. 9 Abs. 5, 6; Art. 11	Vgl. Begleitforschung S. 27 ff., 46 ff.	Vgl. entsprechende Grundsätze in Ziff. 1.1 bis 6
Nutzungsneutrale Speicherung von Abrechnungsdaten und Gebühren als Regelfall (insbesondere S. 60, 66)	Vgl. Art. 9 Abs. 3 Satz 1	Vgl. Begleitforschung S. 44, 71 bis 73, 90, 108	Richtlinien Ziff. 1.5
Gestuftes Inkassoverfahren bei der Entgeltabrechnung durch den Betreiber, wenn nutzungsneutrale Abrechnung problematisch ist (vgl. insbesondere S. 66 ff.)	Übermittlung von Nutzungsdaten an Anbieter nur auf Antrag des Betroffenen (vgl. Art. 9 Abs. 3 Satz 1 Halbs. 3) und nach erfolgloser Mahnung (Satz 2)	Nutzungsneutrale personenbezogene Abrechnung nur auf Antrag des Betroffenen; Übermittlung dieser Daten nur auf Grund zusätzlicher Einwilligungserklärung des Betroffenen (vgl. S. 44, 71 bis 73, 90, 108)	Ziff. 1.5 (nutzungsneutrale Abrechnung)
Weitere Datenübermittlung nur auf Grund einer Rechtsvorschrift, die den Art. 9 konkret benennt (S. 61)	Weitere Übermittlung nur auf Grund von „besonderen Rechtsvorschriften" (vgl. Art. 9 Abs. 3 Satz 2)	–	
Trennung von Betreiber- und Anbieterfunktionen (S. 62)	–	–	–
Beschränkungen für das Medienprivileg in Anbieterprogrammen (S. 64, 71, 72 ff.)	Geltung der Datenschutzgesetze auch für Programminhalte (Art. 9 Abs. 5), jedoch keine Beschränkung des Medienprivilegs	Erörterung des Rechtscharakters von Bildschirmtext als Datenfernverarbeitungssystem (S. 50 ff.)	Fortschreibung des Medienprivilegs (Ziff. 5)
Zweckbindung als Maßstab für die Zulässigkeit der Datenabfrage und Datenerhebung, keine Ausforschung von Betroffenen durch Anbieter (S. 62, 63)	Verbot der Datenerhebung über den „erforderlichen" Umfang einer Zweckbestimmung hinaus (Ausnahme: Kreditgeschäfte) gem. Art. 9 Abs. 6 Satz 1	Kritik am Begriff Zweckbestimmung und am Begriff der „Erforderlichkeit"; stattdessen Anknüpfung am Begriff der „rechtlichen Unerläßlichkeit" empfohlen (S. 37 ff.)	Datenerhebung nur im Rahmen der „Erforderlichkeit" (Ziff. 1.4), völliges Verbot von Abstimmungen und Umfragen (Ziff. 4.3)
–	Verbot personenbezogener Umfragen (Art. 11 Abs. 2)	Hinweis auf die Gefährdung (S. 42) auch Dritter	
Verengung des Selbstbestimmungsrechts der Betroffenen: keine leichtfertige Preisgabe personenbezogener Daten auf Grund von Einwilligungserklärungen, S. 64 ff.	Kein Junktim zwischen bestimmten Leistungen und weitergehenden Einwilligungserklärungen zu zweckfremder Datenverarbeitung (Art. 9 Abs. 6 Satz 4)	Einwilligung zu weitergehender Datenverarbeitung kann nur in Schriftform gegeben werden (S. 135)	Keine Einwilligungsverarbeitung (Ziff. 3)
Schaffung eines Btx-spezifischen Datengeheimnisses (S. 52 f., 76)	Art. 10	Vgl. Begleitforschung S. 59	Ziff. 6
Anpassung der Betroffenenrechte im Btx-System an Auskunfts- und Berichtigungs-, Löschungs- und Sperrungsansprüche des allgemeinen Datenschutzrechts (S. 75, 76)	Vgl. Art. 9 Abs. 7	Vgl. Begleitforschung S. 36, 59	Vgl. Ziff. 2
Die Fremdkontrolle ist nach Möglichkeit in einer Hand zu konzentrieren (S. 78)	§3 Abs. 3 erweitert die Kontrollmöglichkeiten des Berliner Datenschutzbeauftragten	Kontrollkompetenz der Datenschutzbeauftragten hinsichtlich aller Daten die in der Bildschirmtextzentrale verarbeitet werden (S. 59)	Ziff. 7.1
Technisch-organisatorische Sicherheitsmaßnahmen des allgemeinen Datenschutzrechts müssen auch für Bildschirmtext fortgeschrieben werden	Vgl. Art. 9 Abs. 8	Vgl. Begleitforschung S. 17	Ziff. 7.2

Anlage 2

Grundsätze für die organisatorischen und technischen Maßnahmen beim Einsatz isolierter ADV-Systeme

1. **Geltungsbereich**

1.1 Diese Grundsätze betreffen den Einsatz isolierter ADV-Systeme zur Verarbeitung personenbezogener Daten im Sinne von § 2 Abs. 1 Bundesdatenschutzgesetz (§ 4 Abs. 1 Berliner Datenschutzgesetz).

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

1.3 Isolierte ADV-Systeme im Sinne dieser Grundsätze sind ADV-Systeme, die überwiegend folgende Merkmale aufweisen:

a) Der Einsatz des Systems erfolgt nicht in einem arbeitsteilig organisierten Rechenzentrumsbetrieb.

b) Die Maschinenbedienung erfolgt durch den Benutzer selbst.

c) Über selbsttätige Einrichtungen außerhalb des isolierten Bereiches kann auf das isolierte ADV-System nicht zugegriffen werden, wenn der Zugriff nicht vom Benutzer des isolierten Systems veranlaßt wird.

d) Schnittstellen zur interaktiven Nutzung des isolierten ADV-Systems befinden sich im gleichen isolierten Bereich wie das System selbst.

e) Soweit mehrere Benutzer gleichzeitig mit dem isolierten ADV-System interagieren, arbeiten sie im Rahmen des gleichen ADV-Verfahrens (Teilhaberbetrieb).

f) Datenträger, die personenbezogene Daten enthalten, werden ausschließlich vom berechtigten Benutzer verwaltet.

Weiteres, bei den meisten Anwendungen geltendes Merkmal ist:

g) Das System wird für die Erfüllung einer oder weniger Aufgaben eingesetzt (Dedicated System).

2. **Allgemeine Grundsätze**

2.1 Der Grad der Schutzbedürftigkeit personenbezogener Daten ergibt sich insbesondere aus ihrer Natur und aus dem Zusammenhang, in dem sie verwendet werden. Die Art der eingesetzten ADV-Anlage und ihre Einsatzform spielen daher bezüglich der Anforderungen an den Datenschutz eine geringe Rolle. Daten dürfen nicht deshalb schlechter geschützt sein, weil sie auf einem isolierten Rechner verarbeitet werden.

2.2 Der für den technischen und organisatorischen Datenschutz betriebene Aufwand hat in einem angemessenen Verhältnis zum Schutzzweck und zum Aufwand für das ADV-System zu erfolgen. Auf die Erzielung der in 2.1 umschriebenen Wirkung ist zu achten.

2.3 Bei isolierten ADV-Systemen kann ein wirksamer organisatorischer und technischer Datenschutz in der Regel mit relativ geringen Mitteln erreicht werden. Deshalb eignen sich isolierte ADV-Systeme u. U. für besonders sensible Verfahren.

2.4 Es sind soweit möglich technische Einrichtungen einzusetzen, die die Maßnahmen zur Durchführung des Datenschutzes unterstützen.

2.5 Die mit dem Einsatz eines isolierten ADV-Systems befaßten Personen lassen sich ihrer Funktion nach als Betreiber, als Anwender und als Benutzer einordnen.

(1) **Betreiber** sind jene Personen oder Instanzen, die die Verfügungsgewalt über das isolierte ADV-System ausüben.

(2) **Anwender** sind jene Personen oder Instanzen, die das isolierte ADV-System für ihre Aufgaben einsetzen.

(3) **Benutzer** sind jene Personen, die ADV-Prozesse auf dem isolierten ADV-System durchführen.

Häufig werden zwei oder gar drei dieser Funktionen von einer Person wahrgenommen. Diese hat dann die Grundsätze für alle wahrzunehmenden Funktionen zu beachten.

3. **Grundsätze für den Betreiber**

3.1 Der Betreiber ist verantwortlich für die Ausstattung des ADV-Systems hinsichtlich Hardware, System- und Unterstützungssoftware, Organisationsmittel, Einbindung des Systembetriebes in die Aufbau- und Ablauforganisation des Gesamtbetriebes.

3.2 Der Betreiber stellt den Schutz der Anlage samt der verfügbaren Schnittstellen an das System durch geeignete bauliche Maßnahmen sicher.

3.3 Der Betreiber organisiert den Betrieb des isolierten ADV-Systems. Zur Organisation des Betriebs bestellt er eine möglichst DV-fachlich kompetente Person als Systemverwalter. Er regelt ferner die Vertretung. Der Systemverwalter hat folgende Aufgaben:

(1) Vergabe von Rechenzeit und Rechenterminen auf Antrag der Benutzer;

(2) Kontrolle der Zulässigkeit der beantragten Datenverarbeitung i. S. von § 3 BDSG (§ 6 BlnDSG);

(3) Kontrolle, ob der verfügbare oder erreichbare Standard der technischen und organisatorischen Maßnahmen zum Datenschutz hinsichtlich der Sensitivität der bei der beantragten Datenverarbeitung verwendeten Daten angemessen ist;

(4) Sicherstellung der erforderlichen technischen und organisatorischen Maßnahmen zum Datenschutz (§ 6 BDSG, § 5 BlnDSG), soweit sie im Rahmen des Grundsatzes 3.1 im Verantwortungsbereich des Betreibers liegen;

(5) Aufbewahrung und Verwaltung der Schlüssel oder maschinenlesbaren Ausweise zum Betreten des isolierten Bereiches, zur Benutzung von Schnittstellen, zum Zugang zu Datenträgern mit personenbezogenen Daten, zur Benutzung von Datenfernübertragungseinrichtungen sowie allen anderen Betriebsmitteln, deren differenzierte Verwendung aus Gründen des Datenschutzes angebracht ist;

(6) Führung eines Benutzerbuches für die isolierte ADV-Anlage, welche für jede Benutzung folgende Angaben enthalten soll:

- Name und ggf. Andresse des Anwenders
- Namen der Benutzer, die in den isolierten Bereich gelangen
- Datum und Uhrzeit vom Anfang und Ende der Benutzung
- Art der Anwendung (u. U. Angabe der zur Verfügung gestellten Anwendungssoftware)
- Name der benutzten personenbezogenen Dateien
- Informationen zu ggf. beabsichtigten Datenfernübertragungen (Adressat, Absender);

(7) Verwaltung, Ausgabe und Rücknahme von Datenträgern, die dem Anwender bzw. Benutzer verfügbar gemacht werden sollen;

(8) Kontrolle der maschinell erstellten Protokolle;

(9) Stichprobenhafte Kontrolle, daß der Anwender bei der Benutzung des isolierten ADV-Systems nur Datenverarbeitung im Rahmen seines bewilligten Antrags durchführt;

(10) Beratung bei der Benutzung des isolierten ADV-Systems.

3.4 Der Betreiber überwacht die ordnungsgemäße Anwendung der von ihm zur Verfügung zu stellenden Programme (Systemprogramme, Programme aus einer von ihm betriebenen Programmbibliothek). Er ist verantwortlich für die ordnungsgemäße Führung einer vollständigen Dokumentation seiner Programme.

4. **Grundsätze für den Anwender**

4.1 Der Anwender ist als speichernde Stelle im Sinne der Datenschutzgesetze (§ 2 Abs. 3 Nr. 1 BDSG, § 4 Abs. 3 Nr. 1 BlnDSG) verantwortlich für den Datenschutz im Rahmen seiner Anwendung. Er ist verantwortlich für die von ihm genutzten Anwendungsprogramme und Anwendungsdaten.

4.2 Der Anwender ist verpflichtet, den Anordnungen des Betreibers im Hinblick auf die in Ziff. 3 enthaltenen Grundsätze Folge zu leisten.

4.3 Dem Anwender obliegen die in den Datenschutzgesetzen definierten formalen Pflichten einer speichernden Stelle.

4.4 Der Anwender überwacht die ordnungsgemäße Anwendung der von ihm zu stellenden Programme, mit denen personenbezogene Daten verarbeitet werden sollen. Er ist verantwortlich für die ordnungsgemäße Führung einer vollständigen und aktuellen Dokumentation seiner Programme.

4.5 Der Anwender stellt die erforderlichen technischen und organisatorischen Maßnahmen zum Datenschutz (§ 6 BDSG, § 5 BlnDSG) sicher, die gem. Grundsatz 4.1 in seinem Verantwortungsbereich liegen.

Er hat insbesondere für die dem Schutzzweck der Daten angemessene Aufbewahrung der Datenträger mit personenbezogenen Daten Sorge zu tragen.

4.6 Der Anwender hat den von ihm beauftragten Benutzern Weisungen zu geben, die die datenschutzgerechte Verarbeitung der Daten zum Ziel haben. Er hat die Befolgung seiner Weisungen zu kontrollieren.

4.7 Der Anwender hat dafür zu sorgen, daß die vom Betreiber zur Verfügung gestellte Ausstattung bestmöglich genutzt wird, um zu verhindern, daß Unbefugte personenbezogene Daten zur Kenntnis nehmen oder mißbräuchlich verwenden können. Er hat ferner zu prüfen, ob die vom Betreiber zur Verfügung gestellte Ausstattung jenen Sicherheitsgrad ermöglicht, der dem Schutzzweck der Daten entspricht.

5. **Grundsätze für den Benutzer**

5.1 Der Benutzer ist verantwortlich für die datenschutzgerechte und ordnungsgemäße Durchführung der Datenverarbeitung an isolierten ADV-Systemen. Er ist gebunden an die Weisungen von Betreiber und Anwender, insbesondere soweit sie die Grundsätze für Betreiber und Anwender ausführen.

Arbeiten mehrere Benutzer gleichzeitig im Teilhaberbetrieb am isolierten ADV-System [vgl. Grundsatz 1.3 e)], so ist vom Anwender ein verantwortlicher Benutzer zu benennen.

5.2 Der Benutzer nutzt die vorhandenen Einrichtungen zur Durchführung des technischen und organisatorischen Datenschutzes in sorgfältiger Weise. Insbesondere

- führt er alle vorgesehenen Protokollierungen, besonders zur Zu- und Abgangskontrolle, Eingabekontrolle und Übermittlungskontrolle, durch, sofern diese nicht automatisiert durchgeführt werden;
- achtet er darauf, daß während seines Aufenthaltes im isolierten Bereich keine Unbefugten den Bereich betreten;
- achtet der verantwortliche Benutzer darauf, daß Datenträger mit personenbezogenen Daten nur im Zusammenhang mit ihrem unmittelbaren Gebrauch offen zugänglich sind.

Anlage 3

Forderungen des Berliner Datenschutzbeauftragten zur Volkszählung

Gewährleistung des Datenschutzes bei der Volkszählung in Berlin

Forderungen des Berliner Datenschutzbeauftragten

Bei der Durchführung der Volkszählung 1983 ist aus datenschutzrechtlicher Sicht folgendes zu gewährleisten:

I.

Verbot von Maßnahmen gegen den Betroffenen (§ 9 Abs. 1 Satz 2, Abs. 2 Satz 3, Abs. 3 Satz 3 Volkszählungsgesetz)

- Wegen eines Verstoßes gegen das Meldegesetz oder andere Rechtsvorschriften wird ein Bußgeld nicht verhängt.
- Aufgrund von Erkenntnissen aus der Volkszählung werden Strafverfahren gegen die Betroffenen nicht eingeleitet.
- Aufgrund von Erkenntnissen aus der Volkszählung werden staatliche Leistungen nicht rückwirkend zurückgefordert.

II.

Melderegisterabgleich (§ 9 Abs. 1 Volkszählungsgesetz)

- Der Melderegisterabgleich erfolgt nicht mit Hilfe der Erhebungsbogen, sondern mit Hilfe gesonderter Aufstellungen, die von der Meldebehörde erstellt werden („Begleitlisten"); die Erhebungsbogen werden nicht an die Meldebehörde ausgehändigt.
- Die Berichtigung des Melderegisters erfolgt erst nach Benachrichtigung der Betroffenen; diese erhalten die Möglichkeit, Stellung zu nehmen.
- Eine gesonderte Zusammenstellung der berichtigten Daten erfolgt nicht.
- Auskunft über die berichtigten Daten wird nicht von Amts wegen gesondert aus Anlaß der Berichtigung erteilt, sondern nur im Rahmen der üblichen regelmäßigen Datenübermittlungen.

III.

Offenbarung von Einzelangaben (§ 9 Abs. 2 ff Volkszählungsgesetz)

- Das Statistikgeheimnis (§ 11 Bundesstatistikgesetz) gilt für alle Stellen und Personen, die mit der Volkszählung befaßt sind oder denen Einzelangaben zugeleitet werden.
- Eine Weitergabe von Einzelangaben an oberste Bundes- oder Landesbehörden und den von diesen bestimmten Stellen ist nur zu statistischen Zwecken zulässig; für Berlin gilt, daß statistische Auswertungen ausschließlich vom Statistischen Landesamt vorgenommen werden.
- Soweit darüber hinaus Offenbarungen zulässig sind (z.B. für wissenschaftliche Zwecke), wird eine strenge Prüfung der Erforderlichkeit (insbesondere im Hinblick auf die Größe der geographischen Zuordnungsmerkmale) vorgenommen; der Berliner Datenschutzbeauftragte wird vor der Übermittlung benachrichtigt.

IV.

Trennung und Löschung der zur Identifizierung der Betroffenen dienenden Daten (§ 11 Abs. 7 Bundesstatistikgesetz)

- Eine Eingabe des Namens auf die zur Weiterverarbeitung bestimmter Datenträger erfolgt nicht.
- Die Erhebungsbogen und andere Unterlagen zur Volkszählung werden in jeder Phase so transportiert und gelagert, daß Unbefugte nicht Einblick nehmen können.
- Eine Zusammenführung von codierten Einzelangaben mit den Namen mit Hilfe technischer Auswertungsverfahren (z.B. durch die Auswertung der Zählerlisten) findet nicht statt.
- Erhebungsbogen und Zählerliste werden unmittelbar nach Abschluß der Auswertung vernichtet.

V.

Zählerorganisation

- Angaben, die ausschließlich der Organisation dienen (insbesondere Telefon-Nr.), werden weder gespeichert noch weitergegeben.
- Die Betroffenen werden auf die Freiwilligkeit der Angabe der Telefon-Nr. hingewiesen.
- Es muß die Möglichkeit bestehen, dem Zähler den Erhebungsbogen im verschlossenen Umschlag zu überreichen (z.B. wenn der Betroffene aufgrund persönlicher Bekanntschaft dem Zähler seine Daten nicht offenbaren will).
- Die Zähler werden darüber aufgeklärt, daß sie auch hinsichtlich aller Wahrnehmungen im Rahmen der Zählertätigkeit der Geheimhaltungspflicht unterliegen und Verstöße strafrechtlich geahndet werden können.
- Die Zähler werden nicht in ihrer Nachbarschaft eingesetzt.
- Für das Auffinden nicht gemeldeter Personen wird ein besonderes Entgelt an die Zähler nicht gezahlt.

(Stand: 28. Februar 1983)

Die Konferenz der Datenschutzbeauftragten zur Volkszählung 83:

I.

Die Konferenz beobachtet die wachsende Unruhe in der Bevölkerung über die bevorstehende Volkszählung 83. Die Datenschutzbeauftragten haben Verständnis für die Sorgen der Bürger. Die anhängigen Verfassungsbeschwerden geben Gelegenheit, die Verfassungsmäßigkeit der Volkszählung zu prüfen.

Das Volkszählungsgesetz weist einige Unklarheiten und Schwachstellen auf. Die Konferenz erinnert deshalb an die schon 1979 von Datenschutzbeauftragten im Laufe des Gesetzgebungsverfahrens vorgebrachten Bedenken. Diese richteten sich vornehmlich gegen die Durchbrechung des Prinzips der Trennung von Statistik und Verwaltungsvollzug, insbesondere

- gegen die Verbindung einer statistischen Erhebung mit der Aktualisierung der Melderegister
- gegen die Übermittlung nicht anonymisierter Volkszählungsdaten durch die Statistischen Landesämter an Dritte
- gegen die unklare Reichweite des Benachteiligungsverbotes.

Die Konferenz stellt fest, daß die Volkszählungserhebungsbogen den Bestimmungen des Volkszählungsgesetzes, des Bundesstatistikgesetzes und der Datenschutzgesetze nicht in allen Punkten entsprechen, und zwar weil

- nicht darauf hingewiesen wird, daß jeder Auskunftspflichtige einen eigenen Haushalts- und Wohnungsbogen ausfüllen kann, damit er nicht anderen Auskunftspflichtigen seine personenbezogenen Daten offenbaren muß
- der Hinweis auf das Verbot von Maßnahmen gegen den Auskunftspflichtigen mißverständlich ist, da nicht jeglicher Nachteil für den Betroffenen ausgeschlossen werden kann
- der Namensteil von den sonstigen Daten nicht abgetrennt werden kann
- nicht auf die Freiwilligkeit derjenigen Angaben hingewiesen wird, zu deren Beantwortung keine Verpflichtung besteht.

II.

Die Datenschutzbeauftragten haben sich seit langem bei den für die Durchführung der Volkszählung zuständigen öffentlichen Stellen für die Gewährleistung datenschutzrechtlicher Anforderungen eingesetzt. Die Konferenz begrüßt, daß entsprechende Maßnahmen in einem Teil der Länder bereits vorgesehen sind. Soweit die nachstehenden Anforderungen nicht bereits berücksichtigt sind, fordert die Konferenz:

- Zähler dürfen nicht in unmittelbarer Nähe ihres Wohngebietes eingesetzt werden,
- auf den Einsatz von Zählern, bei denen im Hinblick auf ihre dienstliche Tätigkeit Interessenkonflikte nicht auszuschließen sind, sollte verzichtet werden,
- der Bürger muß auf sein Recht hingewiesen werden, den Volkszählungsbogen der Erhebungsstelle im verschlossenen Umschlag direkt zuzuleiten oder dort abzugeben, wenn er nicht wünscht, daß der Zähler von den Angaben Kenntnis erhält,
- die Bürger sind darüber aufzuklären, daß niemand verpflichtet ist, seine Daten einem anderen Auskunftspflichtigen zu offenbaren; daher ist jedem Auskunftspflichtigen, sofern er dies verlangt, ein eigener Bogen auszuhändigen,
- die Bürger müssen darauf hingewiesen werden, daß die Beantwortung der nachstehend genannten Fragen freiwillig ist
  - Telefonnummer
  - Fragen an Diplomaten und Angehörige ausländischer Streitkräfte, soweit sie über die diesbezügliche Zugehörigkeit hinausgehen
  - Gründe für die Nichtzahlung von Löhnen und Gehältern (Arbeitsstättenbogen)
- den Meldebehörden dürfen nur die zum Melderegistervergleich erforderlichen Daten zur Verfügung gestellt werden; es ist unzulässig, den Meldebehörden den kompletten Erhebungsbogen zugänglich zu machen,
- eine Berichtigung des Melderegisters darf erst nach einem förmlichen melderechtlichen Verfahren erfolgen, in dem der Bürger Gelegenheit zur Äußerung erhält,
- die Bürger müssen darüber aufgeklärt werden, daß das Verbot von Maßnahmen gegen den Betroffenen beim Melderegistervergleich kein striktes Verwertungsverbot darstellt, das jegliche Benachteiligung des Betroffenen nach Berichtigung des Melderegisters ausschließt,
- außer für den Melderegistervergleich dürfen Gemeinden die Einzelangaben aus den Erhebungsbogen nicht für eigene Zwecke verwenden,
- eine Datenübermittlung im Rahmen des § 9 Abs. 2 bis 4 VZG darf nur im Rahmen des Erforderlichen stattfinden. In aller Regel dürfen nur statistische Ergebnisse übermittelt werden. Eine Übermittlung von Einzelangaben, insbesondere von Straße und Hausnummer, ist ausgeschlossen, wenn die Übermittlung aggregierter Daten ausreicht.
- Im Rahmen von § 9 Abs. 2 VZG dürfen Einzelangaben nur für statistische und planerische Zwecke übermittelt werden. Deshalb läßt das VZG nicht zu, daß z.B. Polizei, Verfassungsschutz, Sozialbehörden und Finanzämter Einzelangaben erhalten.
- Im Rahmen von § 9 Abs. 3 VZG dürfen den Gemeinden Einzelangaben nur für eine bestimmte statistische Aufbereitung zur Verfügung gestellt werden. Die Übermittlung muß auf die für die jeweilige statistische Aufbereitung erforderlichen Angaben beschränkt werden; dazu gehört in keinem Fall der Name.
- Die Statistischen Landesämter haben in jedem Einzelfall zu prüfen, ob die angeforderten Daten zur Erfüllung des angegebenen und zulässigen Zwecks erforderlich sind.
- Der zuständige Datenschutzbeauftragte ist über alle Übermittlungen von Einzelangaben aus der Volkszählung durch die Statistischen Ämter des Bundes und der Länder zu unterrichten.
- Die Erhebungsunterlagen sind nach Übernahme der Daten auf elektronische Datenträger, spätestens jedoch Ende 1984 zu vernichten. Gleichzeitig sind Kennummer und Zählerlistennummer zu löschen.

III.

Die Datenschutzbeauftragten werden verstärkte Kontrollen bei der Ausführung des VZG durchführen. Sie werden dabei insbesondere

- die Erhebung der Daten,
- das Verfahren des Melderegistervergleichs,
- die Aufbewahrung, Auswertung und Vernichtung der Erhebungsunterlagen bei den Statistischen Landesämtern sowie die Übermittlung statistischer Einzelangaben und ihre Verwendung beim Empfänger

prüfen und die Öffentlichkeit über die Ergebnisse der Prüfungen unterrichten.

Wird diesen Forderungen der Datenschutzbeauftragten Rechnung getragen, so sind nach ihrer Überzeugung die Sorgen der Bürger im wesentlichen unbegründet.

(Stand: 22. März 1983)

Anlage 4

Datenschutzrechtliche Anforderungen an den fälschungssicheren und maschinenlesbaren Personalausweis bzw. Paß

Die Datenschutzbeauftragten in Bund und Ländern weisen darauf hin, daß sie bereits im November 1979 datenschutzrechtliche Anforderungen an die Einführung des fälschungssicheren und maschinenlesbaren Personalausweises gestellt haben. In das Bundespersonalausweisgesetz sind daraufhin entscheidende datenschutzrechtliche Regelungen aufgenommen worden.

Die Datenschutzbeauftragten betonten jedoch seinerzeit, daß ein maschinenlesbarer Personalausweis nur in Verbindung mit einem datenschutzgerechten Melderecht und bereichsspezifischen Datenschutzregelungen für den Sicherheitsbereich hinnehmbar ist. Anknüpfend an diese Forderungen nahm der Deutsche Bundestag bei der Verabschiedung des Personalausweisgesetzes am 17. Januar 1980 den nachstehenden Entschließungsantrag an (vgl. BT-Drs 8/3498):

„Der Deutsche Bundestag ist der Auffassung, daß angesichts der raschen Fortentwicklung der automatischen Datenverarbeitung und deren Einsatz in der öffentlichen Verwaltung über die Verabschiedung des Gesetzes zur Änderung des Gesetzes über Personalausweise hinaus weitere Maßnahmen erforderlich sind, um einen ausreichenden Schutz der Persönlichkeitsrechte der Bürger gegen mißbräuchliche Verwendung ihrer persönlichen Daten zu gewährleisten.

Die Bundesregierung wird deshalb ersucht,

1. den Entwurf eines datenschutzgerechten Melderechtsrahmengesetzes einzubringen und
2. die Arbeiten zur Entwicklung bereichsspezifischer Datenschutzregelungen für die Sicherheitsbehörden nachdrücklich fortzusetzen."

Die Anwendung moderner Informationstechnologien hat inzwischen zunehmend zur Kombination und Integration neuer und vorhandener Informationssysteme geführt. Die Entwicklung der Informationstechnologie ist gekennzeichnet durch die Verknüpfung von Daten, Text, Sprache, Schriftzügen und Bildern, die eine umfangreiche Darstellung und Überprüfung von Personen möglich machen können. Die Einführung des maschinenlesbaren Personalausweises bzw. Passes muß im Zusammenhang mit dieser Entwicklung gesehen werden. Die Aussage, daß ein maschinenlesbarer Personalausweis unter Datenschutzgesichtspunkten hinnehmbar ist, kann nur dann aufrechterhalten werden, wenn die bereits 1979 erhobenen Forderungen in ausreichendem Maße erfüllt werden und auch im übrigen bei der Ausführung des Personalausweisgesetzes den Datenschutzbelangen Rechnung getragen wird. Das bedeutet, daß weitere Regelungen getroffen werden müssen, um inzwischen zu Tage getretene Unklarheiten und Mißverständnisse auszuräumen und eine datenschutzgerechte Anwendung des Gesetzes sicherzustellen.

A) Zum Personalausweisgesetz

1. Soweit bei polizeilichen Personenkontrollen Anfragen in polizeilichen Informationssystemen vorgenommen werden, dürfen diese Anfragen nicht personenbezogen protokolliert werden, damit insbesondere keine Bewegungsbilder entstehen können. Da solche Protokollierungen, die als „Einrichtung von Dateien" anzusehen sind, nicht Zwecken der Grenzkontrolle und der Fahndung im Sinne des § 3 Abs. 5 Satz 2 Personalausweisgesetz dienen, sind sie nach § 3 Abs. 5 Satz 1 Personalausweisgesetz unzulässig. Im übrigen läßt sich aus der Entstehungsgeschichte dieser Vorschrift ableiten, daß der Gesetzgeber eine Verwendung des Ausweises zur automatischen Einrichtung von Dateien grundsätzlich nicht gestatten wollte.
2. Die Datenschutzbeauftragten gehen davon aus, daß die Nutzung des Personalausweises durch die Polizei nach § 3 Abs. 5 Satz 2 Personalausweisgesetz nicht auch die Verwendung der Seriennummer einschließt; hierfür ist § 3 Abs. 4 Personalausweisgesetz die Spezialvorschrift.
3. Die unterschiedliche Formulierung in §§ 3 Abs. 5 Satz 1 und 4 Satz 2 Personalausweisgesetz gibt zu Mißverständnissen Anlaß. Die Regelung in § 4 muß deshalb der in § 3 angeglichen werden.
4. Die internationale Lesbarkeit des Personalausweises erfordert für deutsche Staatsangehörige die gleiche Schutzintensität auch im grenzüberschreitenden Reiseverkehr. Die Konferenz bittet daher die Bundesregierung, sich dafür einzusetzen, daß die datenschutzrechtlichen Anforderungen an die innerstaatliche Verwendung des Ausweises auch im internationalen Bereich umgesetzt werden.

B) Zu den Ausführungsvorschriften der Länder

1. Im Ausführungsgesetz oder in den Verwaltungsvorschriften muß festgelegt werden, daß ein Personenfeststellungsverfahren nur durchzuführen ist, wenn Zweifel an der Identität des Ausweisbewerbers nicht ausgeräumt werden können, und daß in diesem Verfahren erkennungsdienstliche Maßnahmen nur als letztes Mittel zulässig sind. Eine Weiterleitung dieser Unterlagen an das Bundeskriminalamt darf nur für den Vergleich mit anderen Unterlagen zugelassen werden.
2. Im Ausführungsgesetz muß bestimmt werden, daß die erkennungsdienstlichen Unterlagen zu vernichten sind, sobald die Identität festgestellt ist.
3. In das Personalausweisregister dürfen nur die im Personalausweis enthaltenen personenbezogenen Daten (§ 1 Abs. 2 Personalausweisgesetz) sowie Vermerke über Anordnungen nach § 2 Abs. 2 Personalausweisgesetz aufgenommen werden. Von der Aufnahme der Angabe „unveränderliche Kennzeichen" (§ 11 Abs. 2 Nr. 6 des Formulierungsvorschlags) muß abgesehen werden.
4. Der Zweck des Personalausweisregisters ist im Landesgesetz selbst festzulegen. Hierbei ist zu berücksichtigen, daß es nicht Aufgabe dieses Registers sein kann, eine weitere umfassende Identifizierungsdatei neben dem Melderegister zu eröffnen, zumal dadurch weitere Daten (Lichtbild und Unterschrift) mit den Meldedaten verknüpft werden können. Datenübermittlungen an andere öffentliche Stellen und an Private sind auszuschließen. Eine Ausnahme darf nur für Übermittlungen an die Polizei zugelassen werden, wenn es im Einzelfall für deren Aufgabenerfüllung erforderlich ist.
5. Spätestens fünf Jahre nach Ablauf der Gültigkeit des Personalausweises sind die Daten im Personalausweisregister ohne Einschränkung zu löschen.

   Für die Ausstellung eines vorläufigen Personalausweises reicht eine kürzere Aufbewahrungsdauer aus. Entsprechend § 10 Abs. 4 des Entwurfs des Niedersächsischen Ausweisgesetzes sollten die Daten höchstens bis zu einem Jahr nach Ablauf des Jahres der Gültigkeitsdauer aufbewahrt werden.
6. Für Daten der Personen, die im Fall der Entmündigung, wegen Geisteskrankheit oder im Fall dauernder Anstaltsunterbringung von der Ausweispflicht befreit worden sind, ist wegen der damit gegebenen Sonderstellung eine strenge Verwendungsbeschränkung vorzusehen.
7. In den Verwaltungsvorschriften zum Ausführungsgesetz der Länder müssen das Verfahren bei Mitteilungen über den Verlust des Personalausweises geregelt und das Formular festgelegt werden.

C) Zu bereichsspezifischen Datenschutzregelungen

1. Soweit die Regelungen in den Meldegesetzen der Länder dem Melderechtsrahmengesetz entsprechen, sind die datenschutzrechtlichen Anforderungen erfüllt. Die Speicherung der Seriennummer, die in einigen Landesmeldegesetzen in den Datenkatalog aufgenommen wurde, widerspricht dem in § 3 Abs. 4 Satz 1 Personalausweisgesetz festgelegten Nutzungsverbot, erhöht die mit der Maschinenlesbarkeit des Personalausweises verbundenen Gefahren und ist überdies im Hinblick auf die Fälschungssicherheit des Ausweises überflüssig.
2. Durch die Maschinenlesbarkeit des Ausweises werden die nachfolgend aufgeführten datenschutzrechtlichen Probleme verschärft, deren Lösung die Datenschutzbeauftragten von Bund und Ländern bereits früher gefordert haben, die aber durch die bisher erlassenen polizeilichen Richtlinien (insbesondere KpS- und Dateienrichtlinien sowie die Regelung über die Amtshilfe zwischen Bundesgrenzschutz und Nachrichtendiensten) noch nicht erreicht ist.

2.1 Im Polizeirecht des Bundes und der Länder und im Strafverfahrensrecht sind gesetzliche Grundlagen für die Informationsverarbeitung der Polizei, insbesondere für die polizeiliche Beobachtung und die Identitätsfeststellung zu schaffen. Ziel dieser Regelung muß es auch sein, den Umfang der Personenkontrollen im Hinblick auf die Nutzung des maschinenlesbaren Ausweises zu begrenzen.

2.2 Zulässigkeit und Grenzen des Informationsaustausches zwischen Polizei und den Nachrichtendiensten sind gesetzlich zu regeln.

2.3 Der Beschluß der Innenministerkonferenz vom 2. September 1977, der vorsieht, daß alle Personen, die der Polizei bei der Erfüllung ihrer Aufgaben bekannt werden, durch Abfrage in der Personenfahndungsdatei überprüft werden, muß aufgehoben werden. Die vorhandenen Rechtsgrundlagen lassen eine derart umfassende Überprüfung nicht zu. Das gleiche gilt für einen routinemäßigen Abgleich mit den Fahndungsdateien im Rahmen von Verkehrskontrollen.

2.4 Eine Rechtsgrundlage für den Anschluß der Länderpolizeien an die zollrechtliche Überwachung ist nicht ersichtlich. Dieser Anschluß ist zu lösen.

3. Für die Praxis der Polizeikontrollen, insbesondere unter Verwendung des maschinenlesbaren Personalausweises, sind Richtlinien zu erlassen, die den Grundsatz der Verhältnismäßigkeit konkretisieren.

D) Zum Entwurf eines Paßgesetzes

Die gleichen datenschutzrechtlichen Forderungen gelten für die mit dem Entwurf eines Paßgesetzes vorgesehene Einführung eines maschinenlesbaren Passes.

Darüber hinaus behält sich die Konferenz weitere Forderungen zum Paßgesetz vor.

Anlage 5

Stichwortverzeichnis zu den seit 1979 erschienenen Jahresberichten

Zitierweise: **Jahr**, Seite **79**, 14 = 1979, S. 14