Abgeordnetenhaus von Berlin

Drucksache 12 / 1219

12. Wahlperiode

Bericht

des Berliner Datenschutzbeauftragten
zum 31. Dezember 1991

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

Vorlage - zur Kenntnisnahme -

Bericht des Berliner Datenschutzbeauftragten zum 31. Dezember 1991

Der Berliner Datenschutzbeauftragte hat dem Abgeordnetenhaus und dem Regierenden Bürgermeister jährlich einen Bericht über das Ergebnis seiner Tätigkeit vorzulegen (§ 29 Berliner Datenschutzgesetz - BlnDSG -). Der vorliegende Bericht schließt an den am 6. März 1991 vorgelegten Jahresbericht 1990 an und deckt entsprechend der Intention des Gesetzgebers den Zeitraum zwischen 1. Januar und 31. Dezember 1991 ab.

Wir kommen damit zugleich den Pflichten nach § 3 Abs. 3 Gesetz zum Staatsvertrag über Bildschirmtext sowie § 55 Abs. 1 Kabelpilotprojektgesetz nach.[1]

Inhaltsverzeichnis

1. Rahmenbedingungen für Berlin

1.1 Datenschutzrecht in Deutschland und Europa
1.2 Entwicklung der Informationstechnik

2. Datenschutz in Berlin

2.1 Die Datenverarbeitung in Berlin - demnächst ohne gesetzliche Grundlage?
2.2 Erbe der DDR
2.3 Medien und Telekommunikation
2.4 Personalwesen
2.5 Technik und Organisation
2.5.1 Umsetzung formaler Vorschriften des Berliner Datenschutzgesetzes
2.5.2 Vom unsicheren Umgang mit Bürgerdaten
2.5.3 Angelegenheiten der Geschäftsordnung: Formularwesen und Postverkehr

3. Berichte aus den Geschäftsbereichen

3.1 Bau- und Wohnungswesen
3.2 Finanzen
3.3 Gesundheit
3.4 Inneres
3.4.1 Polizei
3.4.2 Verfassungsschutz
3.4.3 Ausländer
3.4.4 Statistik
3.5 Jugend und Familie
3.6 Justiz
3.7 Kulturelle Angelegenheiten
3.8 Schule, Berufsbildung und Sport
3.9 Soziales
3.10 Stadtentwicklung und Umweltschutz
3.11 Wissenschaft und Forschung

4. Aus der Arbeit der Dienststelle

[1] vgl. 2.3

Anlagen

1. Rede des Berliner Datenschutzbeauftragten vor dem Berliner Abgeordnetenhaus am 13. Juni 1991
2. Entschließungen der Konferenz der Datenschutzbeauftragten des Bundes und der Länder
2.1 Beschluß der Sonderkonferenz am 29. Januar 1991 zum Vorschlag der EG-Kommission für eine Richtlinie zum Schutz von Personen bei der Verarbeitung personenbezogener Daten
2.2 Beschluß der 41. Konferenz am 8. März 1991 zu Telekommunikation und Datenschutz
2.3 Entschließung der Konferenz vom 25. Juni 1991 - gegen die Stimme Bayerns - zum Bundesratsentwurf eines Gesetzes zur Bekämpfung des illegalen Rauschgifthandels und anderer Erscheinungsformen der Organisierten Kriminalität
2.4 Entschließung der 42. Konferenz am 26./27. September 1991 zum Datenschutz im Recht des öffentlichen Dienstes
3. Bericht der Arbeitsgruppe Telekommunikation und Medien der Internationalen Datenschutzkonferenz über Probleme des Telemarketing, der Kartentelefone und der elektronischen Directories und
   Beschluß der 13. Internationalen Konferenz der Datenschutzbeauftragten am 4. Oktober 1991
4. Merkblatt des Berliner Datenschutzbeauftragten zu den Aufgaben eines behördlichen Datenschutzbeauftragten (behDSB)

1. Rahmenbedingungen für Berlin

1.1 Datenschutzrecht in Deutschland und Europa

Die Entscheidung des Deutschen Bundestages vom 21. Juni 1991, die Bundeshauptstadt Berlin auch zum *Sitz von Parlament und Regierung* zu machen, erhöht die Bedeutung, die den bundesrechtlichen Vorgaben für die Landesverwaltung zukommt. Mehr als zuvor wird Berlin nicht mehr nur dem Bundesrecht unterworfen sein - auch die letzten, gerade im Bereich des Datenschutzes bedeutsamen Vorbehalte wie etwa beim Post- und Fernmeldegeheimnis sind gefallen -; das Augenmerk der anderen Länder wird sich vielmehr erheblich stärker darauf richten, wie das Land Berlin diese Vorgaben umsetzt. Die Leitfunktion, die unserem Land damit zukommt, muß gerade bei den strukturellen Fragestellungen unserer Gesellschaft in die Zukunft weisen. Die Gewährleistung der informationellen Selbstbestimmung gehört hierzu.

Dies betrifft auch das Verhältnis *zu Europa*. Die Staaten Osteuropas einschließlich der Nachfolgestaaten der Sowjetunion haben sich gerade im vergangenen Jahr faktisch in einer Weise dem Westen geöffnet, wie dies zuvor noch unvorstellbar schien. Ihre formale Einbindung in die Europäische Gemeinschaft ist nur noch eine Frage der Zeit. Nicht nur wegen seiner geographischen Lage, sondern auch auf dem Hintergrund der geschichtlichen Bindungen wird Berlin bei diesem Prozeß eine hervorragende Rolle zukommen. Da sich bereits jetzt abzeichnet, daß bei der Entwicklung dieser Staaten der Informationstechnik eine ganz besondere Rolle zukommen wird, ist es selbstverständlich, daß dem Berliner Datenschutzbeauftragten die Entwicklung der informationellen Selbstbestimmung in der Europäischen Gemeinschaft und in den osteuropäischen Ländern ein wichtiges Anliegen ist.

Informationelle Selbstbestimung ist ein Grundrecht

Der umfassende Einsatz der Informationstechnik wird in der Literatur bereits jetzt als das Charakteristikum der heutigen Gesellschaft angesehen, die häufig bereits als *„Informationsgesellschaft"* bezeichnet wird; die „Informationsweise" einer Gesellschaft beschreibe deren Entwicklungsstand erheblich besser als die klassische Kategorie der „Produktionsweise".

Trifft dies zu, ist es nur konsequent, dem *Grundrecht auf informationelle Selbstbestimmung* auch in den Verfassungstexten Ausdruck zu verleihen. Dies ist in der Vergangenheit in einer Reihe europäischer Staaten auch geschehen (z. B. in Österreich, Spanien und Portugal). Einige Bundesländer sind dem Vorbild des Landes Nordrhein-Westfalen gefolgt und haben entsprechende Bestimmungen in die Landesverfassungen aufgenommen - auch in der nunmehr für die ganze Stadt geltenden Berliner Verfassung ist ein Grundrecht auf Datenschutz aufgenommen worden, das allerdings nicht so ausgearbeitet ist wie die entsprechende Bestimmung der Verfassung der Stadtverordnetenversammlung vom 23. Juli 1990.

Es ist zwingend, daß auch das Grundgesetz der informationellen Selbstbestimmung ausdrücklich den Rang eines *Grundrechts* zuweist - das Bundesverfassungsgericht hat dies in seiner Rechtsprechung bereits vorweggenommen. Die Berliner Mitglieder des gemeinsamen Verfassungsrates des Bundestages und des Bundesrates zur Reform des Grundgesetzes sind aufgefordert, dies zu unterstützen.

Dabei ist zu erwägen, ob nicht dem Grundrecht auf informationelle Selbstbestimmung ein entsprechendes *Grundrecht auf Informationsfreiheit* zur Seite gestellt werden sollte. Nur vordergründig besteht zwischen beiden Rechten ein Widerspruch - tatsächlich ist gerade die Transparenz staatlichen Handelns, besonders wenn es sich der Informationstechnik bedient, eine Voraussetzung für die Geltendmachung des individuellen Rechts auf Datenschutz. Der Entwurf für die Brandenburgische Verfassung, der derzeit im dortigen Landtag diskutiert wird, gesteht den Bürgern ein Grundrecht auf Akteneinsicht zu, ohne daß ein berechtigtes Interesse glaubhaft gemacht werden müßte - selbstverständlich findet die Informationsfreiheit ihre Grenze im Persönlichkeitsrecht Dritter oder einem überwiegenden Allgemeininteresse, das der Gesetzgeber zu präzisieren hat.

Bundesgesetzgebung

Das neu gefaßte *Bundesdatenschutzgesetz* vom 20. Dezember 1990[2] ist am 1. Juni 1991 in Kraft getreten. Dieses Gesetz hat vielfältige Auswirkungen auf die Verarbeitung personenbezogener Daten nicht nur der Wirschaftsunternehmen des Landes, sondern auch von Sozial- und Personaldaten durch öffentliche Stellen des Landes Berlin. Allerdings bleibt das neue Bundesdatenschutzgesetz deutlich hinter dem Datenschutzniveau des Berliner Datenschutzgesetzes zurück. Nach wie vor besteht ein erhebliches „Gefälle" zwischen dem Datenschutz im öffentlichen Bereich und in der privaten Wirtschaft, das vor dem Hintergrund der neueren Rechtsprechung des Bundesverfassungsgerichts zur Geltung des Grundrechts auf Datenschutz im Privatrechtsverkehr[3] sehr problematisch ist. Dies wird besonders deutlich, wenn man berücksichtigt, daß der Bürger als Arbeitnehmer, Mieter oder Bankkunde in aller Regel einem übermächtigen Vertragspartner gegenübersteht, dessen Forderungen zur Offenbarung personenbezogener Daten er sich auch dann praktisch nicht entziehen kann, wenn diese Daten für den Vertragsabschluß oder die Durchführung nicht erforderlich sind.

Mit dem Inkrafttreten des neuen Bundesdatenschutzgesetzes haben die Bürger Berlins erstmals die Möglichkeit, der Kontrolle des Berliner Datenschutzbeauftragten bei der Verarbeitung von Patienten- und Personaldaten zu widersprechen. Diese Widerspruchsklausel schränkt die verfassungsrechtlich gebotene unabhängige Datenschutzkontrolle gravierend ein[4]. Um zu verhindern, daß die Kontrolltätigkeit des Datenschutzbeauftragten durch eine falsche Auslegung der mißverständlich formulierten Bestimmungen des Bundesdatenschutzgesetzes noch zusätzlich erschwert wird, haben wir darauf gedrungen, daß die Bürger sowohl im Bereich der Krankenhäuser, Seniorenheime und Krankenkassen als auch alle Bediensteten des Landes Berlin auf dieses Widerspruchsrecht hingewiesen werden. Die Berliner Krankenhausgesellschaft und die Allgemeine Ortskrankenkasse haben für eine entsprechende Aufklärung gesorgt. Dies hat allerdings dazu geführt, daß z. B. in zwei Nervenkliniken die Patienten formularmäßig auf ihr Widerspruchsrecht hingewiesen und ihnen gleichzeitig - mit Hilfe eines entsprechenden Vordrucks - der Widerspruch „nahegelegt" wurde. Dementsprechend sind aus diesen beiden Krankenhäusern bisher auch die meisten Widersprüche bei uns eingegangen. Wir nehmen diese Widersprüche ernst und werden sie bei unserer Kontrolltätigkeit berücksichtigen. Die Vermutung liegt allerdings nahe, daß viele von denjenigen, die Widerspruch eingelegt haben, sich nicht dessen bewußt sind, daß sie damit nicht so sehr im eigenen Interesse als vielmehr im Interesse des Krankenhauses gehandelt haben, das ihre Daten verarbeitet und sich der Kontrolle durch den Datenschutzbeauftragten umso effektiver entziehen kann, je mehr Patienten dieser Kontrolle widersprechen. Wir haben aus diesem Grunde die beiden Krankenhäuser gebeten, ihre Patienten darauf hinzuweisen, daß der Berliner Datenschutzbeauftragte als vom Parlament gewählte unabhängige Kontrollinstanz gerade die Aufgabe hat, die Daten der Patienten vor unbefugtem Zugriff und Zweckentfremdung zu schützen.

Im Bereich der Personaldatenverarbeitung haben wir der Senatsverwaltung für Inneres Vorschläge für eine entsprechende Information aller öffentlich Bediensteten über ihr Widerspruchsrecht gemacht, die nach dem Berichtszeitraum umgesetzt wurden. Es kam dabei entscheidend darauf an, den Betroffenen deutlich zu machen, daß der Datenschutzbeauftragte den gesetzlichen Auftrag hat, den Umgang mit Personaldaten im Interesse der Betroffenen zu kontrollieren. Nur wer dies weiß, kann einer solchen Kontrolle auch wirksam widersprechen. Der Widerspruch ist gegenüber dem Berliner Datenschutzbeauftragten zu erklären und kann jederzeit widerrufen werden.

Von besonderer - auch datenschutzrechtlicher - Bedeutung ist das am 1. Januar 1992 in Kraft getretene *Stasi-Unterlagen-Gesetz*[5]. Mit diesem Gesetz wird eine zentrale Forderung der Bürgerbewegung der ehemaligen DDR verwirklicht, indem die Bespitzelten das Recht erhalten, Einsicht in die über sie angelegten Akten der Staatssicherheit zu nehmen. Wir haben die Schaffung dieses Einsichtsrechts von Anfang an unterstützt und sehen darin - trotz aller damit verbundenen schmerzlichen Erkenntnisse und menschlichen Probleme - die Verwirklichung des informationellen Selbstbestimmungsrechts für die Bürger eines Staates, der dieses Recht systematisch mit Füßen getreten hat. Ob die betroffenen Bürger von ihrem Akteneinsichtsrecht Gebrauch machen, muß jeder einzelne nach reiflicher Überlegung selbst entscheiden. Wer sich dafür entscheidet, in seine Akten Einsicht zu nehmen, kann dies jetzt oder - je nach Dringlichkeit - innerhalb absehbarer Zeit tun. Dies ist ein entscheidender Durchbruch auch für den Datenschutz. Die Belange Dritter sind durch die recht komplizierten Bestimmungen des Stasi-Unterlagen-Gesetzes hinreichend geschützt.

Der Berliner Datenschutzbeauftragte hat an Anhörungen des Rechtsausschusses des Deutsches Bundestages am 28. August 1991 und des Gemeinsamen Ausschusses der neuen Bundesländer zum Entwurf des Stasi-Unterlagen-Gesetzes am 16. September 1991 teilgenommen. Dabei hat er sich insbesondere dafür eingesetzt, daß der Bundesgesetzgeber die Einrichtung von *Landesbeauftragten für die Stasi-Unterlagen* in Berlin und den neuen Bundesländern ermöglicht, die eine Reihe von länderspezifischen Aufgaben im Zusammenhang mit den vom Bundesbeauftragten für die Unterlagen des Ministeriums für Staatssicherheit erteilten Auskünften wahrnehmen sollten. Dazu zählen landeseinheitliche Richtlinien über den Umgang, die Verwendung und die Aufbewahrungsdauer von Auskünften aus den Stasi-Unterlagen bei öffentlichen Stellen der Länder. Aber auch die Beratung der Betroffenen und der Behörden, denen Auskünfte erteilt werden, bei der Bewertung dieser Auskünfte könnte durch die Landesbeauftragten für die Stasi-Unterlagen erfolgen. Eines der größten

[2] BGBl. I, S. 2954 ff.
[3] s. dazu 1.1
[4] vgl. Jahresbericht 1990, 1.2
[5] BGBl. 1991 I, S. 2272

Probleme im Umgang mit diesen Unterlagen besteht gerade darin, daß die Stasi-Akten Informationen enthalten, die durch Einsichtnahme oder Auskunftsgewährung weitergegeben werden, über deren Bedeutung aber Unsicherheit herrscht. Eine sachkundige Stelle, bei der Menschen tätig sind, die möglichst aus eigener Erfahrung etwas über die örtlichen Strukturen und Arbeitsweise der Staatssicherheit wissen, könnte diese Unsicherheit verringern helfen. Der Bundesgesetzgeber ist unseren Vorschlägen gefolgt. Der Landesgesetzgeber muß nun auch in Berlin regeln, unter welchen Voraussetzungen Dienstbehörden Anfragen an den Bundesbeauftragten für die Stasi-Unterlagen richten dürfen. Das Stasi-Unterlagen-Gesetz des Bundes regelt lediglich die Frage, wem und für welche Zwecke der Bundesbeauftragte Auskünfte erteilen und Akteneinsicht gewähren darf.

Die Verabschiedung des Stasi-Unterlagen-Gesetzes, die den Betroffenen erstmals den Zugang zu ihren Unterlagen eröffnet, ist zugleich ein wichtiger Schritt in Richtung auf eine *allgemeine Informationsfreiheitsgesetzgebung.* Das Stasi-Unterlagen-Gesetz darf nicht in der Weise mißverstanden werden, daß Akteneinsichts- und Informationszugangsrechte nur in einer so außergewöhnlichen Situation und gegenüber einer totalitären Überwachungsbürokratie geschaffen werden dürfen. Vielmehr bleiben der Bundesgesetzgeber, aber auch der Berliner Landesgesetzgeber aufgefordert, ein Informationsfreiheitsgesetz zu schaffen, wie es in Berlin 1990 bereits kurz vor der Verabschiedung stand[6].

Der Bundesumweltminister hat seine Absicht erklärt, zur Umsetzung der entsprechenden EG-Richtlinie bis Ende 1992 ein *Umwelt-Informations-Gesetz* in Kraft zu setzen. Einen entsprechenden Arbeitsentwurf hat uns die Senatsverwaltung für Stadtentwicklung und Umweltschutz bereits zugeleitet. Dies ist ein weiterer wichtiger Schritt zu einem allgemeinen Informationsfreiheitsgesetz. Es sollte nicht der letzte sein.

Für eine Reihe von Verwaltungsbereichen wurde neues Bundesrecht geschaffen (z. B. Telekommunikation, Kinder- und Jugendhilfe) oder weiterberaten (z. B. Justiz), das gerade den Datenschutz neu regelt. Auf die Einzelheiten wird im Zusammenhang mit den jeweiligen Geschäftsbereichen eingegangen.

Europäisches Informationsrecht

Das von der EG-Kommission am 27. Juli 1990 vorgeschlagene *„Datenschutz-Paket"*, das u. a. zwei Richtlinienvorschläge zur Harmonisierung der allgemeinen Datenschutzgesetzgebung und zum Datenschutz in digitalen Telekommunikationsnetzen enthält[6a] ist im Berichtszeitraum sehr kontrovers diskutiert worden und seiner Verabschiedung nur wenig näher gekommen. Nur ein Vorschlag aus diesem Paket für einen Ratsbeschluß auf dem Gebiet der Informationssicherheit (INFOSEC) hat bisher die Zustimmung aller Mitgliedsländer gefunden. Dagegen erscheint es jetzt ausgeschlossen, daß - entsprechend der ursprünglichen Absicht der Kommission - die beiden vorgeschlagenen Richtlinien bis zum Beginn des Europäischen Binnenmarktes am 1. Januar 1993 bereits in das innerstaatliche Recht der Mitgliedstaaten umgesetzt worden sind. Im günstigsten Falle werden die Richtlinien bis zu diesem Zeitpunkt vom Ministerrat verabschiedet, aber selbst dies erscheint jetzt ungewiß.

Die *Richtlinie zur Harmonisierung der allgemeinen Datenschutzgesetzgebung* befindet sich - ebenso wie die Richtlinie zum Datenschutz in digitalen Telekommunikationsnetzen - noch in der Phase der ersten Lesung, in der sich sowohl das Europäische Parlament als auch eine Arbeitsgruppe des Ministerrats mit diesen Vorschlägen befassen. Sobald die Stellungnahme des Parlaments vorliegt, will die Kommission einen neuen Vorschlag erarbeiten.

Die allgemeine Datenschutzrichtlinie soll ein möglichst hohes gleichwertiges Datenschutzniveau in allen Mitgliedstaaten sicherstellen, damit nach ihrer Umsetzung der Datenaustausch zwischen den Mitgliedstaaten nicht mehr unter Hinweis auf fehlende Datenschutzregelungen verhindert werden kann.

Die Kommission hat ausdrücklich betont, daß die Angleichung der Rechtsvorschriften in den Mitgliedstaaten nicht zu einer Verringerung des national garantierten Datenschutzes führen darf, sondern darauf abzielen muß, in der Gemeinschaft ein hohes Schutzniveau sicherzustellen. Diese Festlegung ist deshalb außerordentlich wichtig, weil die Harmonisierung auf Gemeinschaftsebene nicht dazu führen darf, das verhältnismäßig weit entwickelte Datenschutzrecht in der Bundesrepublik Deutschland dem Rechtszustand in anderen Mitgliedstaaten anzupassen und dabei das Schutzniveau in der Bundesrepublik abzusenken. Ziel der Richtlinie sollte es deshalb sein, einen möglichst hohen Mindeststandard für den gemeinschaftsweiten Datenschutz festzulegen, von dem die nationalen Gesetzgeber jedoch auch zugunsten der Bürger durch Erlaß strikterer Datenschutzregelungen abweichen können. Tun sie dies, so dürfen allerdings grenzüberschreitende Datenübermittlungen nicht unter Hinweis darauf beschränkt werden, daß im Empfängerland lediglich der gemeinschaftsrechtliche Mindeststandard eingehalten wird.

Der Vorschlag der Kommission für eine allgemeine Datenschutzrichtlinie kombiniert Elemente aus den nationalen Datenschutzsystemen einzelner Mitgliedstaaten, insbesondere aus dem deutschen und dem französischen Datenschutzrecht. Eine entsprechende Richtlinie des Ministerrats würde vor allem diejenigen Mitgliedstaaten zu einschneidenden Änderungen ihres Rechtssystems zwingen, die bisher keine Datenschutzgesetzgebung haben (Belgien, Griechenland, Italien und Spanien). Zwar ist die Richtlinie zunächst an die Mitgliedstaaten gerichtet, für die sie nach dem EWG-Vertrag (Artikel 189) hinsichtlich des zu erreichenden Ziels verbindlich ist, überläßt jedoch den innerstaatlichen Stellen die Wahl der Form und der Mittel zur Umsetzung. Dazu wird den Mitgliedstaaten eine bestimmte Übergangsfrist eingeräumt. Der Europäische Gerichtshof hat jedoch bereits in der Vergangenheit mehrfach Richtlinien unter bestimmten Voraussetzungen dann für unmittelbar anwendbar erklärt, wenn die Mitgliedstaaten die Anpassungsfrist ungenutzt verstreichen lassen. Überdies kann die Kommission in einem solchen Fall Verfahren gegen die betreffenden Mitgliedstaaten wegen Verstoßes gegen den EWG-Vertrag vor dem Europäischen Gerichtshof einleiten.

Diese einschneidenden rechtlichen Folgen der Datenschutzrichtlinie erklären zum Teil die Heftigkeit, mit der über den Vorschlag der Kommission diskutiert wird. Vor allem die Wirtschaft - insbesondere der Adressenhandel - haben den Entwurf als zu weitgehend und das angestrebte Datenschutzniveau als zu hoch kritisiert. Diese Kritik wird nicht nur von europäischen Wirtschaftsverbänden und Interessengruppen, sondern mit auffallender Intensität auch von entsprechenden Verbänden aus den Vereinigten Staaten vorgetragen. Da es in den Vereinigten Staaten bisher keine Datenschutzgesetzgebung auf Bundesebene gibt, sieht die amerikanische Wirtschaft in einem einheitlichen europäischen Datenschutzstandard ein mögliches Handelshemmnis zwischen der Gemeinschaft und den USA. Andererseits gibt es in jüngster Zeit verstärkt Stimmen im amerikanischen Kongreß, die auch in den Vereinigten Staaten die Verabschiedung eines allgemeinen Datenschutzgesetzes fordern. Sie erhoffen sich von den Harmonisierungsbestrebungen der Europäischen Gemeinschaft eine zusätzliche Schubwirkung.

Der Bundesrat hat leider mit der Stimme Berlins in seiner Stellungnahme zur EG-Datenschutzrichtlinie die Kompetenz des Ministerrats zur Verabschiedung einer solchen Richtlinie nach dem EWG-Vertrag bezweifelt, soweit der Richtlinienvorschlag den öffentlichen Bereich betrifft. Im privaten Bereich hält der Bundesrat die Vorschläge der Kommission - ähnlich wie die Wirtschaft - für zu weitgehend.

Demgegenüber hat die Konferenz der Datenschutzbeauftragten des Bundes und der Länder in ihrem Beschluß vom 29. Januar 1991 den Kommissionsvorschlag begrüßt und gegen die Kritik der privaten Datenverarbeiter und des Bundesrates verteidigt[7]. Allerdings hat die Datenschutzkonferenz auch darauf hingewiesen, daß der Richtlinienentwurf - jedenfalls für den öffentlichen Bereich - in mehreren Punkten hinter dem novellierten Bundesdatenschutzgesetz zurückbleibt. Der Anwendungsbereich der Richtlinie ist auf die Verarbeitung personenbezogener Daten in Dateien beschränkt, und der Zweckbindungsgrundsatz soll gegenüber dem deutschen Recht abgeschwächt werden. Auch

6) vgl. Jahresbericht 1990, 1.2
6a) vgl. Jahresbericht 1990, 1.2

7) vgl. Anlage 2.1

sind zu viele Ausnahmefälle für den Auskunftsanspruch des Betroffenen vorgesehen. Von entscheidender Bedeutung ist die Schaffung einer unabhängigen Datenschutzinstanz auf der Ebene der Europäischen Gemeinschaft, die die Einhaltung und einheitliche Anwendung der Datenschutzrichtlinie überwacht. Diese Instanz sollte von der EG-Kommission unabhängig sein und dem Europäischen Parlament zugeordnet werden. Auch sollte der allgemeine Richtlinienentwurf durch Regelungen insbesondere für den Arbeitnehmer- und Sozialdatenschutz ergänzt werden.

Mit ihrem gleichzeitig vorgelegten *Richtlinienvorschlag zum Datenschutz in digitalen Kommunikationsnetzen* hat die EG-Kommission ausdrücklich eine Forderung der Datenschutzbeauftragten aufgegriffen, die bereits auf ihrer 11. Internationalen Konferenz in Berlin im August 1989 die Notwendigkeit von Datenschutzregeln für das grenzüberschreitende ISDN betont hatten[8]. Der Kommissionsvorschlag enthält eine erste bereichsspezifische Regelung für den Telekommunikationssektor. Dies ist um so bemerkenswerter, als in diesem Bereich die nationale Rechtsetzung in den meisten Mitgliedstaaten bisher unterentwickelt ist und weit hinter der technischen Entwicklung zurückbleibt. Mit ihrem Vorschlag hat die Kommission - möglicherweise etwas verspätet - zu erkennen gegeben, daß auch sie in einem hohen einheitlichen Schutzniveau kein Hindernis, sondern im Gegenteil eine notwendige Bedingung für den einheitlichen europäischen Telekommunikations-Binnenmarkt ab Ende 1992 und für den entstehenden Europäischen Wirtschaftsraum (EWR) sieht.

Die europäischen Datenschutzbeauftragten in der Arbeitsgruppe Telekommunikation und Medien der Internationalen Datenschutzkonferenz haben unter dem Vorsitz des Berliner Datenschutzbeauftragten Veränderungen des Richtlinienentwurfs zur weiteren Verbesserung des Datenschutzes angeregt.[9]

Auch wenn die beiden Richtlinien nicht mehr rechtzeitig zum Beginn des Europäischen Binnenmarktes am 31. Dezember 1992 in Kraft gesetzt werden, kann doch kein Zweifel daran bestehen, daß sie zu einem wichtigen Baustein des Grundrechtsschutzes in der bis zum Ende des Jahrtausends entstehenden Europäischen Union werden[9a].

Rechtsprechung

Einer der großen Streitpunkte war bisher, ob das *Grundrecht* des Bürger *auf informationelle Selbstbestimmung* auch zwischen Privatpersonen gilt[10]. Das hat das *Bundesverfassungsgericht* jetzt entschieden. Ein Vermieter hatte einem wegen Geistesschwäche Entmündigten eine Wohnung vermietet, wobei sowohl dieser als auch sein Vormund den Mietvertrag unterschrieben hatten. Später kündigte der Vermieter den Vertrag mit der Begründung, die Entmündigung sei ihm verschwiegen worden, und erhob Räumungsklage. Die Zivilgerichte gaben dem Vermieter Recht. Auf die Verfassungsbeschwerde des Mieters hin stellte jedoch das Bundesverfassungsgericht fest, daß der Mieter durch die Verpflichtung zur Offenbarung seiner Entmündigung in seinem allgemeinen Persönlichkeitsrecht verletzt würde. Das Bundesverfassungsgericht betonte in diesem Zusammenhang, daß die Offenbarung der Entmündigung die Gefahr der sozialen Abstempelung in sich birgt und die am Sozialstaatsprinzip orientierten Hilfsmaßnahmen zur sozialen Wiedereingliederung erschweren kann. Ein Entmündigter ist also beim Abschluß von privatrechtlichen Verträgen nicht stets dazu verpflichtet, dem Vertragspartner seine Entmündigung zu offenbaren, sondern nur dann, wenn dieser ein schützenswertes Interesse an der Offenlegung hat. Vor dem Hintergrund dieser Rechtsprechung ist es um so unverständlicher, daß das neue Bundesdatenschutzgesetz das Datenschutzgefälle zwischen dem öffentlichen Bereich und dem privaten Bereich zu Lasten des Bürgers aufrecht erhält. Für den Bürger kann es mindestens ebenso beeinträchtigend sein, wenn ein privater Datenverarbeiter unrichtige Daten über ihn in seinen Akten verarbeitet, wie wenn dies eine Behörde tut.

In einer Entscheidung von weitreichender Bedeutung[11] hat das Bundesverfassungsgericht sich zum *Schutz des gesprochenen Wortes beim Telefonieren* geäußert. Ein Journalist hatte von seinem dienstlichen Telefon aus mit einem Kollegen telefoniert. Bei diesem Gespräch äußerte er sich beleidigend über seinen Chefredakteur, der selbst dieses Gespräch von einem anderen Apparat der Nebenstellenanlage aus mithörte und dem Journalisten daraufhin fristlos kündigte. Das Landesarbeitsgericht München wies die Kündigungsschutzklage des Journalisten mit dem Hinweis darauf ab, daß er die technische Möglichkeit des jederzeitigen Mithörens bei Benutzung der dienstlichen Telefonanlage gekannt habe. Er habe sich aus diesem Grund ein zusätzliches privates Telefon in sein Arbeitszimmer legen lassen. Gegen die Entscheidung erhob der Journalist Verfassungsbeschwerde. Der Berliner Datenschutzbeauftragte hatte im Jahre 1986[12] Stellung genommen. Das Bundesverfassungsgericht hat jetzt - in Übereinstimmung mit unserer Auffassung - festgestellt, daß die Entscheidung des Landesarbeitsgerichts München das Recht am gesprochenen Wort als Konkretisierung des allgemeinen Persönlichkeitsrechts verletzt. Dabei betont das Bundesverfassungsgericht die Befugnis des Menschen, selbst zu bestimmen, ob seine Worte einzig seinem Gesprächspartner, einem bestimmten Kreis oder der Öffentlichkeit zugänglich sein sollen. Dies gilt auch für Telefonate, die Arbeitnehmer von Dienstapparaten aus führen. Auch die Kenntnis einer bloßen Mithörmöglichkeit läßt nicht den Schluß zu, der Arbeitnehmer willige pauschal darin ein, daß der Arbeitgeber vom Inhalt seiner dienstlichen Telefongespräche erfahre. Das Landesarbeitsgericht München hatte die Verwertung der rechtswidrig mitgehörten Beleidigung als Kündigungsgrund zugelassen, ohne zwischen dem Recht des Journalisten am eigenen Wort und dem Interesse des Chefredakteurs abzuwägen. Hierin sieht das Bundesverfassungsgericht einen Eingriff in das allgemeine Persönlichkeitsrecht und die Menschenwürde. Diese Entscheidung dürfte weitreichende Bedeutung auch für den Betrieb von Nebenstellenanlagen durch private und öffentliche Arbeitgeber haben. Der Berliner Datenschutzbeauftragte hat seit längerem die Forderung erhoben, daß das Mithören von Telefongesprächen durch Dritte den beiden Gesprächspartnern technisch (z. B. durch einen Signalton) rechtzeitig signalisiert werden muß, damit sie entscheiden können, ob sie das Gespräch unter dieser Voraussetzung weiterführen wollen. Zugleich müßten die Gesprächsteilnehmer auch darüber informiert werden, wer ihr Gespräch mithören will.

In seiner Entscheidung zur *Besteuerung von Einkünften aus Kapitalvermögen*[13] hat das Bundesverfassungsgericht die Verpflichtung des Gesetzgebers betont, die Steuerehrlichkeit durch hinreichende, die steuerliche Belastungsgleichheit gewährleistende Kontrollmöglichkeiten abzustützen. Diese Entscheidung ist in der öffentlichen Diskussion ausführlich erörtert worden. Weniger bekannt ist jedoch, daß das Bundesverfassungsgericht in diesem Urteil erstmals ausdrücklich von einem „Grundrecht auf Datenschutz" gesprochen hat. Dieses Grundrecht ist zwar nach Auffassung der Datenschutzbeauftragten schon im Volkszählungsurteil von 1983 formuliert worden, seine Existenz wurde aber in der juristischen Literatur vereinzelt bestritten. In seinem Zinsurteil betont das Bundesverfassungsgericht, daß steuerliche Kontrollmitteilungen und Auskunftspflichten mit den Grundrechten der Banken und der Bankkunden vereinbar seien. Jedenfalls rechtfertige das überwiegende Allgemeininteresse an der Offenlegung steuerlich erheblicher Angaben diesen Informationseingriff und beschränke insoweit das Grundrecht auf Datenschutz[14]. Eine verfassungskonforme Alternative zu Kontrollmitteilungen ist nach dieser Entscheidung auch die Besteuerung von Zinseinkünften an der Quelle ein Weg, den der Bundesgesetzgeber jetzt offenbar gehen will.

In einer weiteren Entscheidung[15] hat das Bundesverfassungsgericht zum *Verhältnis von Persönlichkeitsrecht und Meinungsfreiheit* bei der Veröffentlichung eines Briefes Stellung genommen. Eine Bürgervereinigung hatte einen Brief veröffentlicht, den der Chefarzt eines Krankenhauses an den Bürgermeister der Gemeinde gerichtet hatte und in dem er einen Arzt als möglicherweise geistesgestört bezeichnet. Mit der Veröffentlichung war nur der kritisierte Arzt einverstanden, nicht aber sein Verfasser.

---

8) vgl. Jahresbericht 1989, Anlage 2.4
9) siehe dazu 2.3
9a) vgl. den Vertrag von Maastricht, Bulletin der Bundesregierung Nr. 17/S. 113 v. 12. 2. 1992
10) BVerfG NJW 1991, S. 2411 ff.
11) Beschluß vom 19. 12. 1991 - 1 BvR 382/85 -
12) vgl. Jahresbericht 1986, S. 5
13) BVerfG NJW 1991, S. 2129 ff.
14) BVerfGE, a.a.O., S. 2132
15) BVerfG NJW 1991, S. 2339 f.

Dieser setzte vor den Zivilgerichten ein Veröffentlichungsverbot durch, das wiederum vom Bundesverfassungsgericht als unzulässiger Eingriff in die Meinungsfreiheit bezeichnet wurde. Zwar betont das Bundesverfassungsgericht, auch die Veröffentlichung eines teilweise schon bekannten Briefes könne gegen das Persönlichkeitsrecht des Verfassers verstoßen. Wenn der Autor den Brief nicht zur Veröffentlichung bestimmt habe, stelle nicht nur die erstmalige, sondern auch die wiederholte Publikation eine - wenn auch möglicherweise abgeschwächte - Beeinträchtigung des Persönlichkeitsrechts dar. Bei der Entscheidung, ob der Kläger diese Veröffentlichung zivilrechtlich untersagen könne, müsse jedoch berücksichtigt werden, daß die Bürgervereinigung den Brief nicht in Verfolgung privater Interessen, sondern im Rahmen einer Kritik an öffentlichen Mißständen in dem Krankenhaus wiedergeben wollte und dafür den Schutz der Meinungsfreiheit in erhöhtem Maße genoß. Zudem habe der Verfasser des Briefes diesen nicht in seiner Eigenschaft als Privatmann, sondern in amtlicher Funktion geschrieben und ihn zudem an einen Amtsträger gerichtet.

Erstmals hat sich der *Bundesgerichtshof* im vergangenen Jahr mit dem Problem auseinandergesetzt, unter welchen Voraussetzungen ein Arzt *Patientendaten* einer gewerblichen Verrechnungsstelle zum Zwecke der Rechnungserstellung und Einziehung des ärztlichen Honorars offenbaren darf. Beim sogenannten Factoring verkauft der Arzt seine Honorarforderungen gegen die Patienten an eine private Verrechnungsstelle. Geschieht dies ohne Einwilligung der Patienten, so sieht der Bundesgerichtshof darin einen Verstoß gegen die ärztliche Schweigepflicht, die auch den Forderungsverkauf nichtig macht[16]. Die Ausführungen in der Urteilsbegründung machen deutlich, welch hohen Stellenwert der Bundesgerichtshof der ärztlichen Schweigepflicht beimißt. Das Gericht betont, daß die häufig über intimste Dinge des Patienten genaue Auskunft gebenden Abrechnungsunterlagen einen besonders wirksamen Schutz verdienen. Dieser sei grundsätzlich nur gewährleistet, wenn die Honorarabrechnung in einem für den Patienten überschaubaren Bereich erfolgt; das aber sei in aller Regel allein die Praxis des behandelnden Arztes einschließlich der für die Abrechnung zuständigen Mitarbeiter. Jedes Überschreiten der Grenzen dieses Bereichs stelle ein Offenbaren des dem Arzt anvertrauten Patientengeheimnisses dar, wobei es ohne Bedeutung ist, ob der Mitteilungsempfänger seinerseits - etwa als Arzt oder privatärztliche Verrechnungsstelle - der Schweigepflicht unterliegt. Zwar hatte der Bundesgerichtshof in diesem Fall nicht darüber zu entscheiden, unter welchen Voraussetzungen ein Arzt Honorarforderungen von einer privaten Verrechnungsstelle lediglich abrechnen lassen darf, ohne sie dieser zu verkaufen. Die Urteilsbegründung läßt aber keinen Zweifel daran, daß auch dies nur mit ausdrücklicher schriftlicher Einwilligung das Patienten zulässig ist. Der allgemeine Hinweis z. B. auf einem Schild im Wartezimmer, das der Arzt eine private Verrechnungsstelle zur Abrechnung der Honorarforderungen einschaltet, reicht dafür nicht aus. Dies sollten die niedergelassenen Ärzte berücksichtigen, um das Risiko einer strafbaren Verletzung der ärztlichen Schweigepflicht von vornherein auszuschließen.

Das *Bundesarbeitsgericht* hat in mehreren Entscheidungen vom 15. Mai 1991[17] seine bisherige Rechtsprechung bekräftigt, daß der Einsatz eines elektronischen Überwachungsprogramms mit *verdeckten Videokameras*, die jederzeit eingeschaltet werden können, ohne daß der Arbeitnehmer davon erfährt, zu einem unzulässigen Eingriff in das allgemeine Persönlichkeitsrecht der Arbeitnehmer führt. Dies gilt selbst dann, wenn der Betriebs- oder Personalrat einem solchen Vorgehen zugestimmt hat, denn die Regelungsbefugnis der Betriebsparteien findet ihre Grenze im Persönlichkeitsschutz des Arbeitnehmers. Soweit der Arbeitgeber keine konkret überwiegenden schutzwürdigen Interessen darlegt, die einen so weitgehenden Eingriff in das Persönlichkeitsrecht rechtfertigen, hat der einzelne Arbeitnehmer einen Anspruch auf Unterlassung gegen den Arbeitgeber.

Auch in der Bundesrepublik greifen private Unternehmen immer stärker zum Mittel der *Telefonwerbung (Telemarketing)*, um den Absatz ihrer Produkte zu steigern. In einem Urteil vom 9. Oktober 1991[18] hat sich das *Oberlandesgericht Karlsruhe* mit dieser Praxis und der zusätzlichen „Nachbearbeitung" von Kunden beschäftigt. Die Vertreterin eines Lexikon-Verlages hatte eine Kundin angerufen und um einen Besprechungstermin in deren Wohnung gebeten, um ihr ein Lexikon anzubieten. Bei diesem Gespräch bestellte die Kundin zunächst das Lexikon, widerrief diese Bestellung allerdings anschließend. Daraufhin wurde sie von einem Mitarbeiter des Verlages in ihrer Wohnung aufgesucht, der sich nach den Gründen des Widerrufs erkundigte. Auf die Klage des Verbraucherschutzvereins hin hat das Oberlandesgericht Karlsruhe sowohl den Telefonanruf für Werbezwecke als auch die persönliche „Nachbearbeitung" nach dem Widerruf der Bestellung als wettbewerbswidrig verboten.

Bereits der Bundesgerichtshof hat in mehreren Entscheidungen ausgeführt, daß der Telefoninhaber mit der Bekanntgabe seiner Anschlußnummer in den Telefonbüchern nicht seine Bereitschaft erklärt, mit jedermann Kontakt aufnehmen zu wollen. Wer deshalb im geschäftlichen Verkehr zu Werbezwecken mit dem privaten Endverbraucher telefonischen Kontakt aufnehmen möchte, muß zuvor dessen Einverständnis einholen, auf diese Art beworben zu werden. Dieses Einverständnis kann entweder ausdrücklich erklärt werden, etwa wenn der Kunde selbst um einen Telefonanruf gebeten oder bei der Aufnahme des Geschäfskontakts erklärt hat, mit einer „telefonischen Betreuung" einverstanden zu sein. Das Einverständnis kann auch durch schlüssiges Handeln erklärt werden, insbesondere wenn der Kunde neben seiner Adresse auch seine Telefonnumer in der Erkenntnis mitteilt, diese werde von dem werbenden Unternehmen zur Fortführung des geschäftlichen Kontakts genutzt. Diese Voraussetzungen der zulässigen Telefonwerbung waren in dem zugrunde liegenden Fall nicht erfüllt. Auch der Besuch eines Mitarbeiters des Lexikon-Verlages nach dem Widerruf der Bestellung war rechtswidrig, weil die Kundin dadurch gezwungen wurde, ihren Widerruf nachträglich zu rechtfertigen, obwohl sie dazu rechtlich nicht verpflichtet war.

1.2 Entwicklung der Informationstechnik

Datensicherheit für die informationelle Selbstbestimmung

Das Begriffspaar *„Datenschutz" und „Datensicherheit"* wird regelmäßig in der Weise gebraucht, daß die Datensicherheit der Beitrag der Techniker und Organisatoren zum Gesamtziel Datenschutz ist. Daß dies zu einfach ist, zeigt zum Beispiel, daß sich der Datenschutz nur auf personenbezogene Daten bezieht, die Datensicherheit jedoch auch für andere schützenswerte Daten verlangt wird.

Gleichwohl erfolgt die Sicherstellung der informationellen Selbstbestimmung auch durch technische und organisatorische Maßnahmen für den Schutz der Vertraulichkeit und Integrität der Daten, wie sie zum Beispiel im § 5 Berliner Datenschutzgesetz verlangt werden. Man kann hier vom technischen und organisatorischen Datenschutz sprechen, um damit deutlich zu machen, welchen Zielen die Schutzmaßnahmen vor allem zu dienen haben, nämlich sicherzustellen, daß nicht durch den Zugriff Unbefugter auf persönliche Daten die informationelle Selbstbestimmung verletzt wird.

Ein Teilaspekt des technischen Datenschutzes ist die *Sicherheit der Informationstechnik* (IT-Sicherheit). Sie ist der Beitrag der Systemhersteller zur Sicherstellung der Verfügbarkeit und Integrität von Systemen, Programmen und Daten sowie der Vertraulichkeit der Daten und Programme. Sie ist dort von besonderer Bedeutung, wo Angriffe auf die Sicherheit mit ausgefeilten technischen Mitteln und hohem Sachverstand auf Anwendungen der automatisierten Datenverarbeitung zu befürchten sind, obwohl bereits hinreichende Schutzmaßnahmen getroffen wurden. Wenn die Organisation der Datenverarbeitung, die Entwicklung der Anwendungsprogramme und die tägliche Arbeit mit den Systemen und mit Datenträgern nicht ebenfalls vom Sicherheitsverständnis geprägt sind, spielt die IT-Sicherheit bei der Gesamtbewertung des technischen und organisatorischen Datenschutzes nur eine untergeordnete Rolle.

Andererseits hat die datenverarbeitende Stelle außer bei der Auswahl der Systeme keine Einflußmöglichkeiten auf die IT-Sicherheit. Vielmehr hat sie darauf zu achten, daß in Pflichtenheften sowohl für die Hardware wie für die System- und Anwen-

[16] BGH NJW 1991, S. 2955 ff.
[17] Z. B. 5 AZR 115/90
[18] AZ 6 U 46/91

dungssoftware die für die Sicherheit des ADV-Einsatzes notwendigen Anforderungen berücksichtigt werden, daß Sicherheitsregeln für die Organisation vorgegeben werden und in der täglichen Anwendung akzeptiert und vollzogen werden. Zu den Aufgaben der Datenschutzbeauftragten gehört es, die Organisationen dabei zu unterstützen.

Sie wären aber hoffnungslos überfordert, würde man von ihnen erwarten, sie könnten alleine die in ihrem Zuständigkeitsbereich eingesetzten informationstechnischen Systeme hinsichtlich der IT-Sicherheit untersuchen und bewerten. Es ist deswegen zu begrüßen, daß sich seit dem 1. Januar 1991 das *Bundesamt für Sicherheit der Informationstechnik (BSI)* auf der Grundlage eines Errichtungsgesetzes (BSI-Gesetz)[19] mit diesen Aufgaben befaßt, indem es Betriebssysteme, Datenbanksysteme und spezielle Sicherheitssysteme auf ihre Funktionalitäten und die dabei erreichten Qualitätsstufen untersucht und in einer nachvollziehbaren Skala einstuft.

Die IT-Sicherheitskriterien - eine Meßlatte für sicherheitsbewußte Systemgestaltung

Grundlage dafür sind die *„IT-Sicherheitskriterien"*, die das BSI veröffentlicht hat. Sie sind aus ähnlichen Kriterien im sog. *„Orange Book"* hervorgegangen, die schon vor längerer Zeit vom amerikanischen Verteidigungsministerium entwickelt worden sind. Die deutsche - und in Folge auch eine europäische - Meßskala nimmt für sich in Anspruch, differenzierter und im zivilen Sektor brauchbarer zu sein. Die deutschen IT-Sicherheitskriterien kennen sechs hierarchisch aufeinanderfolgende Funktionalitätsklassen F0 - F5, die die Funktionen aufzählen, die ein System leisten muß, um in die jeweilige Klasse aufgenommen zu werden. Sie kennen ferner sieben Qualitätsklassen Q0 - Q6, die die Qualität, mit denen die Funktionen mindestens erfüllt werden müssen, beschreiben.

Die Datenschutzbeauftragten gingen bei erster Betrachtung der IT- Sicherheitskriterien davon aus, daß ADV-Systeme, die in der öffentlichen Verwaltung zur Verarbeitung personenbezogener Daten eingesetzt werden, mit F2 und Q3 von der BSI evaluiert werden sollten. Mittlerweile müssen diese Anforderungen insoweit relativiert werden, als sie nur als mittelfristig generell anzustrebende Zielsetzung angesehen werden können, weil es kaum Systeme auf dem Markt gibt, die diesen Anforderungen entsprechen.

Die Hersteller sind allerdings der Verantwortung, Systeme zu entwickeln, die vom BSI hochrangig evaluiert werden, bisher nicht ausreichend nachgekommen: Unsichere Standard-Betriebssysteme UNIX und MS-DOS beherrschen die Welt der Anwendungen am Arbeitsplatz, Sicherheitsmängel von Betriebs- und Datenbanksystemen waren u. a. Ursachen spektakulärer Hackerfälle, der Befall von IT-Systemen mit Computerviren machte nachhaltig Schlagzeilen. Kurzum: Die IT-Sicherheit gehörte bis vor kurzem zu den vernachlässigten Gestaltungszielen bei der Entwicklung von Informationstechnik.

Das Umdenken hat aber bereits angefangen. Hersteller legen jetzt mehr Wert darauf, Systeme zu entwickeln, die den offiziellen Sicherheitskriterien des BSI oder des „Orange Book" genügen. Es gibt Aussagen von Analytikern, wonach die Sicherheit der IT neuerdings alle anderen Gestaltungsziele hinsichtlich ihrer Priorität übertroffen haben.

Ein Beispiel für die Bemühungen heute einerseits und für Versäumnisse in der Vergangenheit andererseits ist die Entwicklung der neuesten Version (Vers. 10) des *Betriebssystems BS 2000* der Firma Siemens-Nixdorf, die die höhere Sicherheit zum vorrangigen Ziel hatte und von der BSI mit hohem Aufwand entwicklungsbegleitend evaluiert wurde. Die erheblichen Verbesserungen dieses auch in früheren Versionen als relativ sicher geltenden Betriebssystems führten zu einer Evaluation nach der Funktionalitätsklasse 2 und der Qualitätsstufe 3 (F2, Q3), eine Bewertung, die - wie oben bereits erwähnt - für personenbezogene Anwendungen als generell anzustreben gilt, den Einsatz bei besonders riskanten Anwendungen ohne zusätzliche Verbesserungen aber eigentlich ausschließt.

[19] BGBl. I 1990, S. 2834

Es ergibt sich daraus die Empfehlung für die zahlreichen BS-2000-Anwender, insbesondere auch für das Landesamt für Informationstechnik, möglichst umgehend auf die sicherheitstechnisch optimierte neue Betriebssystem-Version umzustellen.

„IT-Sicherheitshandbuch" - ein Rückfall

Zur weiteren Verbesserung des Sicherheitsniveaus beim Einsatz der Informationstechnik soll ein *„IT-Sicherheitshandbuch"* führen, welches von der BSI entwickelt wurde. Da das IT-Sicherheitshandbuch verbindlich nur in der Bundesverwaltung für die Durchführung von Risikoanalysen und zur Entwicklung von Sicherheitskonzepten herangezogen werden soll, gegebenenfalls bei entsprechender Tauglichkeit auch im privaten Bereich Einfluß nehmen soll, nicht jedoch die Landesverwaltungen binden kann, hat man auch seitens des Bundes von einer Unterrichtung der Landesdatenschutzbeauftragten abgesehen. Dieses ist vermutlich eine Fehleinschätzung. Was im Bundesbereich verbindlich einzusetzen ist und im privaten Bereich Erfolg haben soll, wird seine Wirkung auf die Länder und Gemeinden kaum verfehlen. Die Mitwirkung des Bereichsleiters für Technik und Organisation im Präsidiumsarbeitsbereich „Datenschutz und Sicherheit" der Gesellschaft für Informatik gab uns daher eine willkommene Gelegenheit, uns mit dem Papier zu befassen.

Der vorliegende Entwurf beschreibt die Ansprüche des IT-Sicherheitshandbuchs allumfassend:

- Es will eine Methode sowie Vorgaben und praktische Anleitungen zur Feststellung der Schutzbedürftigkeit, zur Durchführung von Bedrohungs- und Risikoanalysen und zur Erstellung von IT-Sicherheitskonzepten liefern.
- Es richtet sich an das Management von Unternehmen und Verwaltungen, damit sie sich der Risiken des IT-Einsatzes bewußt werden, Kostenbewußtsein für Maßnahmen entwickeln und sich rechtzeitig für Sicherheitsmaßnahmen entscheiden können und an die für die Sicherheit der IT Verantwortlichen als Hilfestellung zur Wahrnehmung ihrer Aufgaben, darüber hinaus an alle Personen, die mit dem IT-Einsatz direkt oder indirekt befaßt sind, unabhängig von der Branche oder Behörde.
- Es soll für fast alle Arten und Größen von IT-Systemen verwendbar sein.
- Es soll sowohl im Planungsprozeß als auch bei vorhandenen und im Einsatz befindlichen IT-Systemen (im Rahmen von Revisionsprozessen) angewendet werden können.
- Darüber hinaus soll es datenschutzrelevante Daten und Verschlußsachen gleichermaßen erfassen, technische und nichttechnische Aspekte der IT-Sicherheit berühren und die Wirtschaftlichkeit und Angemessenheit berücksichtigen.

Diesen Ansprüchen kann der Entwurf des IT-Sicherheitshandbuchs nicht genügen. Viele Abschnitte können weder inhaltlich noch nach der Ausdrucksweise und Darstellung den üblichen fachlichen Ansprüchen standhalten. Die Methode zur Analyse der Risiken und zur Entwicklung von IT-Sicherheitskonzepten krankt u. a. an folgenden Mängeln:

- Das Verfahren verzichtet auf eine ganzheitliche Betrachtung der Organisationen, die sich der Informationstechnik bedienen, um ihre Leistungen zu erbringen. Damit werden Ursachen wie Mängel übergeordneter Organisationsstrukturen, Interessengegensätze, Führungsmängel und mangelhafte Planung der Informationsflüsse aus der Risikoanalyse ausgeblendet.
- Die Risikobewertung und -ermittlung erfolgt an einer pauschalisierenden numerischen Werteskala, die mit ihrer Pseudomathematik Objektivität und Unangreifbarkeit vortäuscht, jedoch nicht nachvollziehbar ist und bei Risiken, die mehr ideeler Natur sind (z. B. die Wahrung der informationellen Selbstbestimmung), ungeeignet ist.
- Die Wahrung der informationellen Selbstbestimmung, die Beachtung bestimmter besonderer gesetzlicher Rahmenbedingungen, die den Wert einer Anwendung beeinflussen, werden zwar pauschal erwähnt, werden bei dem Verfahren zur Ermittlung der Schutzbedürftigkeit jedoch nicht beachtet.

- Ein Konzept für die Aktualisierung und Fortschreibung der Ergebnisse der Risikoanalyse und des IT-Sicherheitskonzeptes wird nicht mitgeliefert. Die organisatorische Installation eines Sicherheitsmanagements wird nicht explizit unterstützt.
- Der zeitliche und personelle Aufwand für die Anwendung des Sicherheitshandbuches verletzt bei kleineren IT-Anwendungen die Grundsätze der Verhältnismäßigkeit und Wirtschaftlichkeit. Gerade angesichts der Änderungshäufigkeit bei Hard- und Softwarekomponenten ist zu erwarten, daß die Analysen von sicherheitsrelevanten Änderungen der Konfigurationen überholt werden.

Eine Befassung mit den Details des Entwurfs des IT-Sicherheitshandbuchs, z. B. bei den Anforderungen an sichere IT-Anwendungen im PC-Bereich oder bei Mehrplatzsystemen, zeigt bald, daß die längst veröffentlichten und größtenteils auch akzeptierten Anforderungen der Datenschutzbeauftragten und auch anderer Fachleute bei weitem nicht erreicht werden.

Angesichts der uns bekannt gewordenen Absicht, trotz der warnenden Stellungnahmen das IT-Sicherheitshandbuch zumindest erprobungshalber für eine bestimmte Frist für die Bundesverwaltung verbindlich zu machen, warnen wir davor, daß sich die Berliner Landesverwaltung einer solchen Vorgehensweise bei der Erstellung von Sicherheitskonzepten anschließt, solange das Handbuch nicht wesentlich verbessert wird.

Trends der informationstechnischen Entwicklung

Um rechtzeitig mit Empfehlungen und Hinweisen den Beratungsbedarf der Verwaltung und der Gesetzgeber befriedigen zu können, ist es für Datenschutzbeauftragte unerläßlich, sich frühzeitig mit informationstechnischen Entwicklungstendenzen auseinanderzusetzen. Was heute in den Labors entwickelt wird, kann morgen Gegenstand einer öffentlichen Beschaffungsmaßnahme sein und übermorgen Risiken für die informationelle Selbstbestimmung hervorrufen, die durch gesetzliche Regelungen und technische und organisatorische Maßnahmen gebändigt werden müssen.

Die bekannten Entwicklungstrends in der Informationstechnik sind nach wie vor aktuell. Die Entwicklungsgeschwindigkeit hat an Rasanz nichts eingebüßt:

Der Trend zur Miniaturisierung der Hardware hält an. Tragbare Computer (Laptops) erreichen atemberaubende Leistungsdaten, die noch vor wenigen Jahren Großrechnern vorbehalten waren. Notebook-Computer ermöglichen die Mitnahme automatisierter Datenbanken in der Hand- oder Jackentasche. Individuelle automatisierte Datenverarbeitung ist damit längst nicht mehr ortsgebunden. Dieser Komfort ist aber auch mit neuen Gefahren für den Datenschutz und die Sicherheit der Datenverarbeitung verbunden.[20]

Das Preis-/Leistungsverhältnis wird weiterhin immer günstiger. Beinahe jeder ist heute finanziell in der Lage, sich erstaunlich leistungsfähige Computer zu kaufen.

Deshalb sind Computer bereits heute in vielen Privathaushalten anzutreffen. Aber wie zu beobachten ist, bleibt es nicht dabei, die Computer dort für die private Lebensführung oder zum Spielen zu verwenden. Auch öffentlich Bedienstete verlagern Teile ihrer dienstlichen Arbeit an ihren häuslichen PC und entziehen sich damit einer effektiven Kontrolle durch Dienstbehörde oder Datenschutzbeauftragte[21].

Die Systeme folgen zunehmend internationalen Industriestandards. Die meisten Personalcomputer arbeiten mit dem Betriebssystem MS-DOS, so daß weltweit kompatible Software nach einheitlichen Bedingungen eingesetzt werden kann. Damit wird auch Standard-Software relativ billig, weil sie einen hohen Verbreitungsgrad erreichen kann. Aber auch hier gibt es Wermutstropfen: MS-DOS enthält keine Sicherheitsfunktionalitäten. Sicherheit muß teuer hinzugekauft werden. Dies geschieht aber nur dann, wenn auch das nötige Sicherheitsbewußtsein die Notwendigkeit solcher präventiver Maßnahmen einsichtig macht. Die weltweite Verbreitung kompatibler Systeme fördert auch die weltweite Verbreitung kompatibler Schadprogramme wie Viren, Würmer und Trojanische Pferde.

Rechner werden zunehmend vernetzt. Sie werden zu lokalen Netzen (LAN) zusammengeschaltet, um gemeinsame Ressourcen zu nutzen, um Ausfälle auszugleichen oder Kommunikation zu ermöglichen. Lokale Netze werden über große Entfernungen hinweg zu Weitbereichsnetzen (WAN) verknüpft. Die Verwaltungen großer Metropolen vernetzen sich über „Metropolitan Area Networks" (MAN) - wie es auch in Berlin geplant ist. Die Zusammenführung aller Netze zu einem weltumspannenden „Global Area Network" (GAN) ist kaum noch Utopie, wenn man bedenkt, daß für die Verbindungen im Netz ISDN als weltweiter Standard zur Verfügung steht.

Mit der Ausbreitung solcher Netze und der zunehmenden Abhängigkeit von ihrer Verfügbarkeit und Integrität entstehen existenzielle Risiken für Menschen und ihre Organisationen. Die Sicherheit der Systeme gewinnt angesichts der Risiken der Verletzlichkeit der Gesellschaft an Bedeutung[22].

Software wird heute mit leistungsfähigen Generierungs-Werkzeugen und neuartigen Programmiersprachen (objektorientierte Programmierung) erstellt, die es ermöglichen, immer komplexere Programme zu erstellen, die die schnelleren Rechengeschwindigkeiten und fast unbegrenzten Speicherkapazitäten für neue Anwendungen erschließen können. Wissensbasierte Expertensysteme, komplexe Simulationen, hochauflösende, schnell bewegte Graphikpräsentationen werden möglich.

Die Verknüpfung technischer Präsentations- und Simulationstechniken mit menschlichem Empfindungsvermögen eröffnet eine neue Gefahrendimension für die informationelle Selbstbestimmung, die unter dem Stichwort „Cyberspace" im Berichtsjahr ins öffentliche Bewußtsein trat.

2. Datenschutz in Berlin

2.1 Die Datenverarbeitung in Berlin - demnächst ohne gesetzliche Grundlage?

Das neue *Berliner Datenschutzgesetz* (BlnDSG) vom 17. Dezember 1990[23] enthält die deutliche Aufforderung an den Landesgesetzgeber, die von diesem Gesetz vorausgesetzten bereichsspezifischen Verarbeitungsbefugnisse für den Umgang mit personenbezogenen Daten innerhalb einer Frist von einem Jahr zu schaffen. Es ist vielleicht nicht verwunderlich, daß diese Frist nicht eingehalten werden konnte. Zugleich ist es aber auch bezeichnend, daß das einzige Landesgesetz mit datenschutzrechtlichem Bezug, das im Berichtszeitraum verabschiedet wurde, das Erste Gesetz zur Änderung des Berliner Datenschutzgesetzes war[24], mit dem die Übergangsfrist des § 34 BlnDSG um weitere drei Monate verlängert wurde.

Dies geschah vor allem, um genügend Zeit für eine intensive parlamentarische Beratung des *Entwurfs für ein novelliertes Allgemeines Sicherheits- und Ordnungsgesetz (ASOG)* zu haben, der am 21. November 1991 ins Abgeordnetenhaus eingebracht wurde und die seit dem Volkszählungsurteil von 1983 überfälligen gesetzlichen Grundlagen für die polizeiliche Datenverarbeitung schaffen soll[25]. Gleichzeitig mit dem ASOG-Entwurf wurden Entwürfe für ein *Ausführungsgesetz zum Gerichtsverfassungsgesetz*[26] und - mittlerweile zu dritten Mal - für ein *Landesstatistikgesetz*[27] in das Parlament eingebracht. Nicht einmal dies wäre vermutlich geschehen, hätte nicht das Berliner Datenschutzgesetz von 1990 mit seiner einjährigen Übergangsfrist eine strikte zeitliche Vorgabe enthalten. Es bleibt abzuwarten, ob die verlängerte Übergangsfrist ausreichen wird, die erforderlichen bereichsspezifischen Regelungen zu verabschieden. Bereits im Vorjahr wurde darauf hingewiesen, daß es dem Landesgesetzgeber nicht freisteht, diese Übergangsfrist beliebig zu verlängern, da der vom Bundesverfassungsgericht eingeräumte Übergangsbonus seinerseits bereits Ende 1990 abgelaufen ist[28].

---

20) Ausführliches dazu und zu Empfehlungen im Jahresbericht 1990, 2.4 ff.
21) siehe dazu 3.8
22) siehe dazu 1.2
23) GVBl. 1991, S. 16
24) GVBl. 1991, S. 281
25) vgl. dazu bei 3.4.1
26) dazu 3.6
27) dazu 3.4.4
28) vgl. Jahresbericht 1990, 1.2

Gesetz über die Schaffung bereichsspezifischer Regelungen für die Verarbeitung personenbezogener Daten

Schon zu Beginn des Jahres hatten wir vorgeschlagen, die notwendigen bereichsspezifischen Gesetze zur Umsetzung des novellierten Berliner Datenschutzgesetzes in einem *Artikelgesetz* zusammenzufassen, in das alle Senatsverwaltungen ihre Vorschläge für die erforderlichen bereichsspezifischen Rechtsgrundlagen hätten einstellen können. Die Senatsverwaltung für Inneres hat diesen Vorschlag aufgegriffen und die Federführung für das Artikelgesetz übernommen. Der Senat hat allerdings erst am 10. Dezember 1991 endgültig über den Entwurf eines entsprechenden Gesetzes über die Schaffung bereichsspezifischer Regelungen für die Verarbeitung personenbezogener Daten beschlossen, der jetzt im Abgeordnetenhaus eingebracht worden ist (Drs. 12/1029) und noch vor Ablauf der verlängerten Übergangsfrist am 31. März 1992 verabschiedet werden muß.

Zweck des Artikelgesetzes ist es zunächst, das Berliner Datenschutzgesetz an das novellierte, am 1. Juni 1991 in Kraft getretene Bundesdatenschutzgesetz insoweit anzupassen, als es selbst Verweisungen auf das Bundesgesetz enthält. Der Senat hat hinsichtlich dieser Anpassung unsere Empfehlungen im Entwurf zum großen Teil aufgegriffen.

Die zentrale Aufgabe des Artikelgesetzes ist es jedoch, die bereichsspezifischen Gesetzgebungsvorhaben zu bündeln, die die erforderlichen Verarbeitungsbefugnisse nach dem Berliner Datenschutzgesetz schaffen sollen. Die Senatsverwaltung für Inneres hat hierzu eine Umfrage unter den übrigen Senatsverwaltungen gemacht, welche Gesetzgebungsvorhaben für erforderlich gehalten werden. Das Ergebnis dieser Umfrage zeigt, daß die Tragweite des Berliner Datenschutzgesetzes und des mit ihm verbundenen Regelungsbedarfs weitgehend noch nicht erkannt worden ist. Vielen Verwaltungen ist offenbar bisher nicht hinreichend verdeutlicht worden, daß das neue (im Gegensatz zum alten) Berliner Datenschutzgesetz selbst - bis auf wenige Ausnahmen - keine eigenen Rechtsgrundlagen für die Verarbeitung personenbezogener Daten enthält, sondern daß es diese Rechtsgrundlagen vielmehr voraussetzt. Sind sie nicht vorhanden oder werden sie nicht mehr rechtzeitig geschaffen, so dürfen personenbezogene Daten von Bürgern nur noch mit deren Einwilligung verarbeitet werden. Spätestens seit dem Inkrafttreten des Berliner Datenschutzgesetzes von 1990 kann die Verwaltung ihre Befugnis zur Verarbeitung personenbezogener Daten auch nicht mehr aus der Aufgabe ableiten, die ihr der Gesetzgeber zugewiesen hat. Erst recht gilt dies, wo sogar die gesetzliche Aufgabenzuweisung fehlt (z. B. im Archivwesen).

Der Entwurf des Artikelgesetzes enthält nur einen Bruchteil der erforderlichen bereichsspezifischen Regelungen und kann daher nur als erster Schritt zur Umsetzung des Berliner Datenschutzgesetzes angesehen werden. Während einige Senatsverwaltungen den Regelungsbedarf durchaus erkannt haben, jedoch sich zu einer gesonderten Novellierung - z. B. des Landeskrankenhausgesetzes, des Berliner Meldegesetzes und des Allgemeinen Sicherheits- und Ordnungsgesetzes - entschlossen haben, sahen andere Senatsverwaltungen zunächst überhaupt keinen Bedarf für bereichsspezifische Regelungen zur Datenverarbeitung.

Der Artikelgesetzentwurf ist auch aus einem anderen Grund lückenhaft: Überall dort, wo Berliner öffentliche Stellen *Bundesgesetze* auszuführen haben, die ihrerseits keine hinreichenden Regelungen über die Verarbeitung personenbezogener Daten enthalten[29], ist der Landesgesetzgeber nach dem Berliner Datenschutzgesetz gehalten, ergänzend die erforderlichen Verarbeitungsregeln zu schaffen. Dies geschieht zweckmäßigerweise in Ausführungsgesetzen zu den entsprechenden Bundesgesetzen. Der Senat hat dementsprechend den Entwurf eines Ausführungsgesetzes zum Gerichtsverfassungsgesetz auf Vorschlag der Senatsverwaltung für Justiz in das Parlament eingebracht[30]. Demgegenüber vertritt die Senatsverwaltung für Inneres die Auffassung, es sei nicht Aufgabe des Landesgesetzgebers, Ausführungsgesetze zu Bundesgesetzen zu beschließen, weil damit die Bundeskompetenz berührt werde. Dabei wird jedoch die Kompetenzordnung nach dem Grundgesetz verkannt. Im Bereich der konkurrierenden Gesetzgebung haben die Länder die Befugnis zur Gesetzgebung, solange und soweit der Bund von seiner Kompetenz keinen Gebrauch macht (Art. 72 Abs. 1 GG). Auch haben die Länder die Einrichtung der Behörden und das Verwaltungsverfahren dann zu regeln, sofern sie - wie dies zumeist geschieht - die Bundesgesetze als eigene Angelegenheit ausführen.

Verarbeiten öffentliche Stellen personenbezogene Daten der Bürger, so greifen sie in deren Grundrecht auf informationelle Selbstbestimmung ein. Deshalb ist es nur konsequent, wenn das Berliner Datenschutzgesetz für jede Verarbeitung personenbezogener Daten ohne Einwilligung der Betroffenen eine bereichsspezifische gesetzliche Grundlage fordert. Dabei handelt es sich nicht lediglich um eine formale Legalisierung der gegenwärtigen Verwaltungspraxis. Vielmehr sichert der Vorbehalt der bereichsspezifischen gesetzlichen Verarbeitungsbefugnis den Grundrechtsschutz des einzelnen Bürgers. Der Gesetzgeber muß sich deshalb kritisch mit den *Informationsinteressen der Verwaltung* auseinandersetzen und kann sich nicht damit begnügen, den öffentlichen Stellen Blankett-Ermächtigungen zur Verarbeitung personenbezogener Daten zu erteilen.

Vor diesem Hintergrund erscheint der Entwurf des Artikelgesetzes nicht nur lückenhaft, sondern auch in sich widersprüchlich. Während die Senatsverwaltung für Bau- und Wohnungswesen anstrebt - wenngleich nicht immer mit der erforderlichen Normenklarheit -, die Art der zu verarbeitenden personenbezogenen Daten zu benennen, begnügt sich die Senatsverwaltung für Finanzen damit, daß das Verarbeiten personenbezogener Daten zulässig sein soll, wenn ihre Kenntnis für die rechtmäßige Erfüllung der in der Zuständigkeit der datenverarbeitenden Stelle liegenden Aufgaben und für den jeweils damit verbundenen Zweck erforderlich ist. Eine derartige Blankett-Ermächtigung zur Verarbeitung personenbezogener Daten entspricht zwar dem Rechtszustand nach dem alten Berliner Datenschutzgesetz. Dieser war jedoch seit dem Volkszählungsurteil des Bundesverfassungsgerichts von 1983 mit dem Grundgesetz nicht mehr vereinbar, weil der Bürger - aufgrund einer so allgemeinen gesetzlichen Regelung - gerade nicht erkennen kann, welche Informationen über ihn die Verwaltung für erforderlich hält und was sie infolgedessen wann und bei welcher Gelegenheit über ihn weiß. Wollte man es zulassen, daß zur Umsetzung des novellierten Berliner Datenschutzgesetzes in alle bereichsspezifischen Gesetze die Klausel aufgenommen wird: „die zur Erfüllung der jeweiligen gesetzlichen Aufgabe erforderlichen personenbezogenen Daten dürfen von der zuständigen Stelle verarbeitet werden", so würde die verfassungsrechtlich gebotene und mit dem neuen Berliner Datenschutzgesetz begonnene Weiterentwicklung des Datenschutzrechts vereitelt und auf einem Umweg der alte verfassungswidrige Zustand wiederhergestellt.

Im Gegensatz zu vielen anderen Bundesländern verfügt Berlin nicht über ein Organisations- oder Datenverarbeitungsgesetz, mit dem geregelt wird, wie der Einsatz der Informationstechnik im Lande organisiert werden soll. Weder gibt es gesetzliche Aufgabenzuweisungen für die daran zentral oder koordinierend beteiligten Instanzen noch gibt es gesetzliche Regelungen zur Durchführung von ADV-Projekten. Anstelle eines entsprechenden Gesetzes wurden ADV-Grundsätze aus dem Jahre 1984 angewendet, die in Teilen sehr bald wieder außer Kraft gesetzt wurden, weil sie einerseits ADV-politischen Vorstellungen nicht mehr entsprachen, andererseits gerade für die Projekte zur dezentralen Datenverarbeitung vom Aufwand her nicht mehr als angemessen angesehen worden waren. Zwischendurch wurde der Versuch unternommen, mit Grundsätzen für die Informations- und Kommunikationstechnologie (IuK-Grundsätze) Regelungen zu entwickeln, die den neueren technischen Entwicklungen, z. B. dem Zusammenwachsen zwischen automatisierter Datenverarbeitung und Telekommunikation, gerecht werden sollten. Dieser Ansatz ist nicht zu Ende geführt worden.

Im Jahre 1988[31] haben wir im Zusammenhang mit den damaligen - bisher aber nicht weiterverfolgten - Plänen für ein Senatsinformationssystem als berlinweit vernetztes System von Bürokommunikationssystemen gefordert, daß dafür eine rechtliche Grundlage geschaffen werden müsse. Da hierüber Konsens mit der Ver-

[29] s. hierzu 3.4.3
[30] s. hierzu 3.6

[31] Jahresbericht 1988, 4.1

waltung bestand, wurde von der Senatsverwaltung für Inneres 1989 ein erster Versuch unternommen, in einem *„Gesetz über den Einsatz der Informations- und Kommunikationstechnik im Lande Berlin" (IuK-Gesetz)* den Regelungsbedarf zu befriedigen. Wir hatten bereits im letzten Jahr[32] darauf hingewiesen, daß das Interesse in der Innenverwaltung an dem Entwurf stark erlahmte.

Erst im Frühsommer 1991 wurde der Entwurf als *„Gesetz über den Einsatz der Informationstechnik im Lande Berlin" (IT-Gesetz)* erneut wieder aufgegriffen. Mittlerweile waren viele datenschutzfreundliche Regelungen entfallen oder verwässert worden und wichtige Regelungsbereiche ganz entfallen (etwa besondere Vorschriften für den Einsatz dezentraler Systeme, für IuK-Netze, Bürokommunikationssysteme, digitale TelekommunikationsNebenstellenanlagen, für den Schutz von Dienstkräften vor ergonomischen Gefahren und vor der Verletzung ihres informationellen Selbstbestimmungsrechts), weil ein Konsens innerhalb der Verwaltung nicht zu erzielen war. Auch dieser Entwurf wurde nicht realisiert.

Wegen des nahenden Ablaufs des Übergangsbonus beschränkt sich die Innenverwaltung vielmehr darauf, in einem Entwurf eines *„Gesetzes über die Verarbeitung personenbezogener Daten bei der allgemeinen Verwaltungstätigkeit in den Behörden Berlins (AllgVTG)"* die nach § 6 Abs. 1 BlnDSG erforderlichen rechtlichen Grundlagen für die Verarbeitung personenbezogener Daten bei der allgemeinen, also in bereichsspezifischen Vorschriften nicht faßbaren, Vorgangsbearbeitung zu schaffen. Dem haben wir unter den Voraussetzungen zugestimmt, daß die definitorische Abgrenzung allgemeiner und bereichsspezifischer Vorgangsbearbeitung gelingt. Bereichsspezifisch zu regelnde Vorgänge sollten von den pauschalen, an der geringeren Sensibilität allgemeiner Vorgangsbearbeitung orientierten Regelungen auch bei weitester Auslegung nicht erfaßt werden. Im Gesetzgebungsverfahren sollte klargestellt werden, daß die übrigen in den früheren Entwürfen als regelungsbedürftig erkannten Gegenstandsbereiche des IT-Einsatzes ebenfalls einer gesetzlichen Regelung zugeführt werden.

Mit der Verlängerung der Frist wurde der Versuch unternommen, das Minimalgesetz AllgVTG wieder mit weiteren Regelungen anzureichern. Notwendig sind nach unserer Auffassung vor allem:

- Rechtsgrundlagen für die allgemeine Vorgangsbearbeitung (im Sinne des Entwurfs des AllgVTG);
- Rechtsgrundlagen für die fachübergreifenden und landesweiten IuK-Infrastrukturen wie das existierende und auszubauende Abgeordnetenhaus-Dokumentations- und Informationssystem, das geplante Senatsinformationssystem und die geplante neue Telekommunikationsinfrastruktur der Berliner Verwaltung;
- gesetzliche Aufgabenzuweisungen für das Landesamt für Informationstechnik (LIT) und andere mit der Bereitstellung von IuK-Dienstleistungen betrauten Behörden;
- Rechtsgrundlagen für die Verarbeitung personenbezogener Daten für Zwecke der IuK-Dienstleistung, z. B. für die im LIT für eigene organisatorische Zwecke zu verarbeitenden Daten;
- Organisation von IuK-Projekten;
- Regelung des Einsatzes von digitalen Nebenstellenanlagen für die Sprach- und Datenkommunikation sowie Rechtsgrundlagen für die Verarbeitung personenbezogener Daten im Rahmen dieser Systeme.

Diese Hinweise wurden in dem endgültigen Senatsbeschluß nur zu einem geringen Teil berücksichtigt. Das Ergebnis der Erweiterung des Entwurfes des AllgVTG war der Entwurf eines *„Gesetzes über die Informationsverarbeitung bei der allgemeinen Verwaltungstätigkeit (Informationsverarbeitungsgesetz)" (IVG)*[33], wobei der bisherige Entwurf des AllgVTG lediglich durch eine gesetzliche Ermächtigung für das Abgeordnetenhaus-Dokumentations- und Informationssystem ergänzt wurde.

In einem Punkt ist ein besonderes *Vollzugsdefizit des Berliner Datenschutzgesetzes* festzustellen: Seit einem Jahr gilt die Forderung des Gesetzgebers, daß *jede* Vorlage für einen neuen Gesetzentwurf Angaben über die Daten, die für den Vollzug des Gesetzes mit Datenverarbeitungsanlagen erforderlich sind, und über die Form der vorgesehenen Datenverarbeitung enthalten muß. Diese gesetzliche Verpflichtung wurde offenbar bisher nicht zur Kenntnis genommen.

Zusammenarbeit mit dem Land Brandenburg

Aus naheliegenden Gründen kommt es in vielen Bereichen zu einer immer stärkeren Zusammenarbeit zwischen der Bundeshauptstadt Berlin und dem Land Brandenburg. Zu diesem Zweck werden gegenwärtig zahlreiche Staatsverträge ausgehandelt, etwa im Bereich des Rundfunks oder bei der Gründung einer Akademie der Wissenschaften zu Berlin-Brandenburg. In allen diesen Fällen sind Regelungen darüber notwendig, welches Datenschutzrecht auf die von den beiden Ländern gebildeten neuen Einrichtungen anzuwenden ist. Soweit diese Einrichtungen - wie z. B. die Medienanstalt oder die Akademie der Wissenschaften - ihren Sitz in Berlin haben, sollte nach dem Grundsatz der Belegenheit das Berliner Datenschutzgesetz Anwendung finden[34]. In den Entwurf eines Rundfunkstaatsvertrages mit Brandenburg ist aufgrund unseres Hinweises eine entsprechende Klarstellung aufgenommen worden. Außerdem wurde die Datenschutzkontrolle in einer Weise geregelt, die für die Zusammenarbeit mit dem Brandenburgischen Landesbeauftragten für den Datenschutz richtungweisend sein könnte. Danach wird der Berliner Datenschutzbeauftragte - wenn der Staatsvertrag in Kraft treten sollte - im Einvernehmen mit dem Datenschutzbeauftragten des Landes Brandenburg die Einhaltung der Datenschutzbestimmungen im Anwendungsbereich des Staatsvertrages überwachen.

2.2 Erbe der DDR

Mit dem Zusammentritt des neuen Abgeordnetenhauses zu Beginn des Jahres begann auch für die Berliner Verwaltung eine neue Epoche. Aus den bisher nach der deutschen Vereinigung noch getrennten Verwaltungseinheiten im West- und im Ostteil Berlins wurde eine einheitliche Organisation. Dies bedeutete, daß die im Ostteil der Stadt vorhandenen Datensammlungen eingebracht werden mußten in Abläufe, die sich an der Grundentscheidung des Einigungsvertrages orientieren, auch in den östlichen Bezirken im wesentlichen die bundesrechtlichen Strukturen einzuführen. Die rechtliche Grundlage wurde hierfür durch die beiden *Mantelgesetze* gelegt, durch die nahezu das gesamte Recht des Westens auf den Osten erstreckt wurde.

Auch ist die Vereinigung der zentralen behördlichen Datenverarbeitungsinstitutionen der beiden Stadthälften bemerkenswert reibungslos verlaufen. Das vom früheren Landesamt für elektronische Datenverarbeitung übernommene Magistratsrechenzentrum wurde „abgewickelt". Diese informationstechnische Vereinigung der Stadt dokumentiert sich auch durch die Namensänderung des LED in *„Landesamt für Informationstechnik"*. Alte DDR-Informationstechnik findet sich im Großrechnerbereich nicht mehr, hier und da findet man noch Personalcomputer der Fa. Robotron, deren Ersatz aber bevorsteht.

Daß hierbei Schwierigkeiten auftreten würden, lag angesichts der fundamentalen Unterschiede der Staatsauffassungen auf der Hand. Eine flächendeckende Überprüfung war nicht möglich und nicht nötig: Allerorten war das Bemühen spürbar, trotz der vielfach unzureichenden Möglichkeiten angemessene Lösungen zu finden, auch wenn das Verständnis für die Grundgedanken des Datenschutzes mitunter Mühe bereitete. Einige Beispiele sollen die Schwierigkeiten beleuchten.

Unsere Prüfpraxis ging davon aus, daß denjenigen, die den Aufbau der neuen Verwaltungsstrukturen zu bewerkstelligen hatten, eine faire Chance eingeräumt werden muß, ordnungsgemäße Abläufe herzustellen. Intensive oder gar überraschende Überprüfungen in derartigen Aufbausituationen sind zwar mitunter erforderlich, müssen aber behutsam eingesetzt werden.

[32] Jahresbericht 1990, 1.2
[33] Drs. 12/1103
[34] vgl. Jahresbericht 1990, 2.1

Datensammlungen der Polizei

Großes Augenmerk war naturgemäß auf die Frage zu richten, auf welche Weise die Datenbestände der Polizei übernommen wurden, die sich auf Einwohner des Ostteils der Stadt bezogen.

Es handelte sich dabei in erster Linie um die Daten des *„Dialog-orientierten Recherche- und Auskunftssystems"* des Zentralen Kriminalamts der ehemaligen DDR (DORA), das auch von den Bezirkskriminalämtern und den Kreiskriminalämtern benutzt wurde. In DORA konnten bei geringfügigen Straftaten, Straftaten ohne überregionale Bedeutung und bei Ersttätern Meldedaten, der Urteilsspruch, Angaben aus dem Strafvollzug, Hinweise auf erkennungsdienstliche Maßnahmen und Straftaten gespeichert werden. Bei Straftaten von erheblicher Bedeutung kamen weitere Daten hinzu, wie z. B. Daten zur Personenbeschreibung, zum Tathergang und zur polizeilichen Beobachtung, Angaben über Arbeitsstellen und Daten über Fahrerlaubnisse. Darüber hinaus konnten Daten von Personen gespeichert werden, die der Republikflucht verdächtigt wurden.

Nach der Vereinigung der beiden deutschen Staaten wurde das Zentrale Kriminalamt als *Gemeinsames Landeskriminalamt (GLKA)* der neuen Bundesländer weitergeführt[35]. Dies gilt nach dem Einigungsvertrag solange und soweit die neuen Bundesländer keine Landeskriminalämter eingerichtet haben. In Berlin nimmt diese Aufgabe der Polizeipräsident wahr. Im Gegensatz zu den anderen Ländern hat Berlin sich von vornherein nicht am GLKA beteiligt.

Der Polizeipräsident in Berlin hat vielmehr die DORA-Datenbestände, für die er zuständig ist, sofort übernommen. Vor der Übernahme fand eine Teilbereinigung statt. Gelöscht waren Daten über Personen, die wegen Sachverhalten gespeichert waren, die nach dem bundesdeutschen Recht kein strafbares Verhalten darstellen. So waren Datenspeicherungen wegen „Republikflucht" oder ähnlicher Straftaten zum Zeitpunkt der Übernahme bereits gelöscht. Nach Übernahme der DORA-Daten durch die Berliner Polizei wurden auch diese Datenbestände im laufenden DORA-Verfahren gelöscht. Die Ost-Berliner Datenbestände sind jedoch weiterhin im GLKA auf Datenträgern archiviert.

Dies ist problematisch. Für die Verarbeitung übernommener polizeilicher Datenbestände ist ausschließlich der Polizeipräsident in Berlin zuständig. Er hat zu entscheiden, welche Daten nach den bereits genannten Grundsätzen übernommen werden und auch, inwieweit eine bundesweite Speicherung einzelner Datenbestände im INPOL-System erforderlich ist. Damit sind auch die Archivbestände zu übernehmen - was angesichts der anstehenden Auflösung des GLKA ohnehin ansteht.

Neben DORA verfügte die ehemalige Volkspolizei auch über *regionale Sammlungen,* deren Berliner Bestände ebenfalls vom Polizeipräsidenten übernommen wurden. Darunter befanden sich neben Sammlungen, die in ähnlicher Form auch beim Polizeipräsidenten geführt werden (z. B. Kriminalakten, Bezirksspeicher Daktyloskopie, Täterlichtbildkartei, Personenfahndungskartei) auch recht eigenwillige Bestände, wie z. B. eine Spitznamenkartei, eine Kartei „Faschos, Skinheads und Sympathisanten" oder gar eine Ohrenabdruckspuren-Sammlung. Diese Datensammlungen wurden, soweit sie für die Arbeit der Polizei weiterhin erforderlich sind, in die bestehenden Bestände integriert. Im übrigen war darüber zu entscheiden, ob sie weiterhin aufbewahrt oder vernichtet werden sollten.

Bei der Vernichtung der Daten war zu berücksichtigen, daß nach § 17 Abs. 3 Satz 3 BlnDSG vor der Löschung personenbezogener Daten die Betroffenen zu hören sind. Allerdings hatte der Polizeipräsident eine Reihe der übernommenen Karteien und einzelne Teile der Aktensammlungen offenbar bald nach deren Auffinden vernichtet. Auf unsere Intervention nach Inkrafttreten des neuen Berliner Datenschutzgesetzes wurden weitere Vernichtungen gestoppt.

Die Senatsverwaltung für Inneres hat in Abstimmung mit uns den Polizeipräsidenten gebeten, die Akten und Datensammlungen bis zum 31. Dezember 1996 gesichert aufzubewahren und sicherzustellen, daß sie nur für Auskünfte an Betroffene und mit Einverständnis der Betroffenen zu deren Rehabilitation genutzt werden.

Etwaige Betroffene sollen durch wiederholte öffentliche Bekanntmachung darüber informiert werden, welche Datensammlungen im einzelnen übernommen wurden und wann die Vernichtung erfolgen soll, damit sie Gelegenheit zur Geltendmachung ihrer schutzwürdigen Belange erhalten.

Gesamtberliner Meldewesen

Bereits im Vorjahr wurde die zentrale Speicherung der Einwohnerdaten der DDR in einer Personendatenbank - nach der Wende in *Zentrales Einwohnerregister* (ZER) umbenannt - beschrieben[36]. Die Überführung dieser Daten in ein einheitliches Melderegister war eine wesentliche Voraussetzung für den Aufbau der Verwaltung.

Eine Projektgruppe im Landeseinwohneramt, bestehend aus Angehörigen der Senatsverwaltung für Inneres, des (damals noch existierenden) Ministeriums des Innern der DDR, der ehemaligen Magistratsverwaltung für Inneres, der Volkspolizei und des Landeseinwohneramtes (LEA) wurde Mitte 1990 ins Leben gerufen, um Konzepte zur *Übernahme* der für ein *einheitliches Meldewesen* notwendigen Daten aus dem Zentralen Einwohnerregister (ZER) zu erarbeiten. Geplant wurde, bis zum April 1991 diese Übernahme zu vollziehen und in der Folgezeit die Vereinheitlichung des Berliner Meldewesens zu realisieren. Dieses anspruchsvolle Vorhaben soll bis zum Ende des Jahres 1992 abgeschlossen sein.

Ursprünglich war angedacht, die Daten der Bürger aus dem Ostteil der Stadt mit bereits vorhandenen DV-Programmen eines Dialogverfahrens zu übernehmen, um eine korrekte Fortschreibung des Datenbestandes zu gewährleisten. Dieser Weg erwies sich jedoch als nicht gangbar. So wurde aus dem im ZER gehaltenen, nach der Wende bereinigten und den Vorschriften des Melderechtsrahmengesetzes angepaßten Datenbestand ein Auszug auf Magnetband erstellt, der die Daten aller Personen beinhaltete, die auf irgendeine Weise mit Berlin zu tun haben bzw. hatten. Diese Auszugsdatei wurde danach in eine Datei überführt, deren Aufbau dem ADV-Verfahren für das Einwohnerwesen des LEA (EWW) entsprach. Mit Hilfe dieser Datei wurde zunächst eine Datenbank eingerichtet, die ausschließlich Daten von Bürgern aus dem Ostteil der Stadt enthielt. Dieser Datenbestand wurde auch gesondert behandelt, da z. B. die Lohnsteuermerkmale über die Bezirkseinwohnerämter zu ergänzen waren und die Änderungen, die sich aus dem normalen Meldestellenbetrieb ergeben, in einer „Zentralen Änderungsstelle" des LEA bearbeitet und in die Datenbank eingegeben werden mußten. Bis Ende 1991 sollte diese Sonderbehandlung beendet sein und die Bestände beider Datenbanken zusammengeführt werden.

Bei einer Überprüfung, die im vergangenen Jahr nicht abgeschlossen werden konnte, wurden einige Mängel im Zusammenhang mit der Überführung der Bestände festgestellt.

Nach der Übernahme der Daten gibt es im vom ZER genutzten Rechenzentrum immer noch denselben als *„inaktiv" deklarierten Datenbestand.* Diese Doppelspeicherung von personenbezogenen Daten ist für die Aufgabenerfüllung nicht erforderlich, eine künftig notwendige Rechtsgrundlage auch für die Speicherung von Daten aus „verarbeitungstechnischen Gründen" liegt ohnehin nicht vor. Sie widerspricht zudem der Aussage des Senats in seiner Stellungnahme zu unserem Jahresbericht 1990.

In den Meldestellen der östlichen Bezirke wird noch mit den alten *Meldekarteikarten* gearbeitet. Auf diesen Karten sind nach den jetzt geltenden Rechtsnormen unzulässige Daten eingetragen. Über diese Datei und über Verknüpfungen zu anderen noch bestehenden Karteien oder Dateien (z. B. mit Hilfe der verfassungswidrigen Personenkennzahl) sind rechtswidrige Nutzungen möglich. Diese Karteien sind in einigen Meldestellen noch bis 1993 erforderlich, da die Einrichtung der notwendigen EDV-Geräte vorher nicht möglich ist. Die unzulässigen Eintragungen sind daher unkenntlich zu machen.

[35] vgl. Vertrag über die Herstellung der Einheit Deutschlands Anlage I B Kap. II, Abschnitt III Ziff. 2

[36] Jahresbericht 1990, 2.1

Das LEA hat vom ZER Daten von *allen Personen* übernommen, die *jemals in Berlin wohnhaft* waren oder eine Arbeitstätte hier hatten. Vom LEA wird dies mit Auskunftsersuchen von Betroffenen zu Rentenzeiten oder ähnlichem begründet. Für diese Datenerhebung gibt es jedoch keine rechtliche Grundlage. Grundsätzlich gilt, daß in der aktuellen Einwohnerdatei nur die z. Z. in Berlin lebenden Personen erfaßt werden dürfen (§§ 1 und 2 MeldeG).

Hausbücher

Von verschiedenen Seiten sind wir auf den Verbleib der in der ehemaligen DDR geführten Hausbücher angesprochen worden. Diese Datensammlungen, in denen akribisch der Ein- und Auszug der Bewohner und die Besucher der Mieter festgehalten wurden, haben die jeweiligen Hausbuchbeauftragten geführt.

Der Innenminster der DDR hatte im September 1990 angeordnet, daß sämtliche Hausbücher zu vernichten seien. Die Einziehung der Bücher sollte durch die zuständigen Meldestellen erfolgen. In Berlin hat sich ein ehemaliger Oberstleutnant der Nationalen Volksarmee mit diesem Thema beschäftigt, der noch zu DDR-Zeiten die Meldestellen aus dem Polizeibereich löste und eine Struktur entsprechend dem Landeseinwohneramt mit den verschiedenen Meldestellen schuf. Weiterhin schrieb er die Hausbuchbeauftragten an und bat darum, die Hausbücher den Meldestellen zu übergeben.

Eine Überwachung der Rückgabe wurde jedoch nicht durchgeführt. Weil zwischenzeitlich - z. T. bereits vor dem 3. Oktober 1990 - in Teilbereichen die Kartei der Hausbuchbeauftragten und auch zurückgegebene Hausbücher vernichtet wurden, war eine Rücklaufkontrolle auch nachträglich nicht mehr möglich.

Das Landeseinwohneramt hat uns erklärt, daß ca. 86 000 Hausbücher in Umlauf waren, von denen ca. 11 000 bei den Meldestellen einschließlich Landeseinwohneramt lagerten. Der Verbleib der restlichen Unterlagen war nicht mehr zu klären.

Auch die abgegebenen Hausbücher sind zwischenzeitlich vernichtet worden. Eine Anhörung der Betroffenen vor der Vernichtung (§ 17 Abs. 3 BlnDSG) erschien nicht erforderlich, da die Eintragungen in den Hausbüchern allen Beteiligten bekannt waren und die Verletzung schutzwürdiger Belange ausschied.

Datenspeicher Wohnungspolitik

Durch die Vereinigung war dem Land Berlin der „Datenspeicher Wohnungspolitik" mit über 630 000 Datensätzen mit sehr detaillierten personenbezogenen Wohnungsdaten der Bevölkerung des Ostteils Berlins zugefallen. Die Senatsverwaltung für Bau- und Wohnungswesen bat uns um datenschutzrechtliche Bewertung, inwieweit diese Datei noch genutzt werden könne. Zu diesem Zeitpunkt hatte die Senatsbauverwaltung bereits einen Abzug des Datenbestandes zu Zwecken der Durchführung des Wohnungsbindungsgesetzes und des Gesetzes zum Abbau der Fehlbelegung im Wohnungswesen erstellt, sich dabei jedoch auf die Daten beschränkt, die ausschließlich für diese Aufgaben erforderlich waren. Neben dem Wunsch der Senatsbauverwaltung, die vorhandenen Daten für Zwecke der Stadtplanung zu nutzen, lagen darüber hinaus Anträge auch vom Bundesministerium für Raumordnung, Bauwesen und Städtebau sowie der Senatsverwaltung für Stadtentwicklung und Umweltschutz vor. Ein privates Unternehmen bat um Nutzung der Daten für die Erstellung eines Energiekonzeptes für die Bezirke Pankow, Köpenick und Treptow, das sie im Auftrag des Bundes und des Berliner Senats zu erarbeiten hatte. In ihrem Antrag hatte sie darauf verwiesen, daß ihre Arbeit entscheidend von der Bereitstellung territorialer Ausgangsdaten abhänge. Der Datenspeicher Wohnungspolitik sei die Basis des Auftrags, weil er hausbezogene Daten enthalte, die unter Verwendung des territorialen Grundschlüssels angelegt und bis Mai 1990 geführt worden sei.

Dem Datenspeicher Wohnungspolitik lagen zwar in der ehemaligen DDR das Gesetz über die örtlichen Volksvertretungen in der Deutschen Demokratischen Republik sowie die Wohnraumlenkungsverordnung zugrunde, so daß die Daten bis zum 2. Oktober 1990 auch rechtmäßig gespeichert waren. Der Einigungsvertrag enthält allerdings keine besondere Bestimmung für fortgeltendes Recht der DDR - auch nicht als Landesrecht -, die den Bestand und die Nutzung des Datenspeichers Wohnungspolitik rechtfertigen würde. Damit hat der Datenspeicher *insgesamt* seit dem 3. Oktober 1990 keine Rechtsgrundlage mehr. Nach § 6 i. V. m. 10 und 11 BlnDSG wäre damit jede weitere Speicherung unzulässig und die Daten wären zu sperren bzw. zu löschen.

Ergänzend war zu prüfen, ob eine weitere Nutzung *einzelner* Datensätze durch fortgeltende Rechtsgrundlagen der früheren DDR abgedeckt sein könnten. Hier kommen über Art. 9 Einigungsvertrag die statistischen Daten des territorialen Grundschlüssels (TGS) über das Statistikgesetz der DDR vom 20. Juli 1990 in Betracht, soweit sie vergleichbar sind mit den Statistikdaten des Regionalen Bezugssystems. Jedoch müßten bei einer Weitergabe solcher Daten auf jeden Fall dieselben vertraglichen Absicherungen wie bei der Weitergabe der Daten aus dem Regionalen Bezugssystem vorgenommen werden.

Ob darüber hinaus auf spezialrechtlicher Grundlage oder gar auf dem Weg des Übergangsbonus nach § 34 Abs. 1 BlnDSG auch diejenigen Einzeldaten, die für die Erfüllung rechtmäßiger Aufgaben erforderlich sind, weiterhin gespeichert und verwendet werden können, wird noch geprüft. Dies setzt eine genaue Analyse voraus, welche der übernommenen Daten für welche gesetzlichen Aufgaben unerläßlich sind. Dabei ist selbstverständlich die Verwendung bestimmter Daten, wie der Personenkennzahl, ausgeschlossen.

Zum Beispiel scheinen die §§ 138 ff Baugesetzbuch (BauGB) für die festgesetzten *Sanierungsgebiete* als Rechtsgrundlage für eine weitere Verwendung einzelner Daten geeignet zu sein. Jedoch ist auch hier zu bedenken, daß die Daten ursprünglich hinter dem Rücken der Betroffenen und nicht bei den Betroffenen erhoben wurden. Dies könnte dadurch geheilt werden, daß die Betroffenen über die bisherige Speicherung informiert werden und unter Hinweis auf § 138 BauGB gleichzeitig nach der Richtigkeit derjenigen Informationen befragt werden, die auch nach dieser Vorschrift beim Betroffenen hätten erhoben werden dürfen. Diese Überlegung gilt auch bei anderen Gesetzen, die als Grundlage für die weitere Verwendung einzelner Daten herangezogen werden sollen.

Denkbar ist ferner, die Daten in anonymisierter und aggregierter Form entweder bei der Senatsverwaltung für Bau- und Wohnungswesen fortzuführen oder dem Statistischen Landesamt für deren Zwecke zu überlassen. Dies würde allerdings zur Vermeidung einer Deanonymisierung eine hinreichende Aggregation voraussetzen.

Der Verdacht, daß der vom Magistratsrechenzentrum übernommene Datenspeicher auch Gegenstand *rechtswidriger Datenübermittlungen* war, wurde durch einen Hinweis der Senatsbauverwaltung genährt, daß ihr ein Verkaufsangebot einer privaten Firma vorliege, mit dem Daten aus Gebäudedateien des Gebietes der ehemaligen DDR zum Verkauf angeboten werden. Diese Firma hatte als ehemalige öffentliche Stelle der DDR Daten im Auftrag des Magistrats von Ostberlin verarbeitet. Ein Ergebnis der von uns bei der zuständigen Senatsverwaltung für Inneres angeregten Überprüfung steht noch aus.

Gesundheitswesen

Als besonders problematisch stellt sich der Umgang mit den personenbezogenen Daten sowohl der Patienten als auch des ehemaligen Personals bei der „Abwicklung" bzw. Privatisierung von Einrichtungen des Gesundheitswesens der ehemaligen DDR im Ostteil Berlins dar.

Es besteht der Eindruck, daß man sich des hohen Risikos, das bei der Auflösung vollständiger Gesundheitseinrichtungen hinsichtlich des angesammelten Datenmaterials besteht, nicht oder zumindest nur unvollkommen bewußt ist. Beispielsweise sind allein im Bezirksamt Mitte noch ca. 500 000 Patientenakten und 2 400 Personalakten aufzuarbeiten. Der Schriftwechsel zwischen den Beteiligten ist rege, jedoch Aktionen, die einer Lösung dienen, fehlen aus unserer Sicht weitgehend. Hinzu kommt in einzelnen Fällen ein erhebliches Kompetenzgerangel.

Ein besonders gravierender Fall ist die „Abwicklung" des ehemaligen *Regierungs- und Diplomatenkrankenhauses* in der Scharnhorststraße. Ohne daß es zu einer abschließenden Klä-

rung hinsichtlich der Abwicklungszuständigkeit zwischen den Bundes- und Landesbehörden einschließlich der neuen Länder gekommen war, beschloß die Gesamtberliner Landesregierung im Dezember 1990, die Senatsverwaltung für Wissenschaft und Forschung mit der „Abwicklung" des umstrittenen Krankenhauses zu betrauen. Man ging zu diesem Zeitpunkt davon aus, daß zum einen kein Bedarf zur Weiterführung des Krankenhausbetriebes mehr bestand und zum ande ren die Gebäude und Einrichtungen der Charité zur weiteren Nutzung übergeben werden sollten. So führten auch zwei von der Charité übernommene ehemalige Mitarbeiter nach der endgültigen Einstellung der Krankenhausaktivitäten im März 1991 die Registratur stundenweise weiter, um ehemalige Patienten mit Kopien aus ihren Akten zu versorgen, die für ihre weitere Behandlung benötigt wurden.

Mittlerweile sind offenbar zumindest die Eigentumsverhältnisse hinsichtlich der Liegenschaft dergestalt geklärt, daß aus dem ehemaligen Reichsvermögen Bundesvermögen wurde. Da der Bund im Zuge des teilweisen Umzuges seiner Verwaltungen nach Berlin verständlicherweise Eigenbedarf anmeldete, war an eine Übernahme des ehemaligen Krankenhauses durch die Charité natürlich nicht mehr zu denken. Was jedoch sollte aus dem sicher nicht unerheblichen Inventar und den besonders sensiblen Datensammlungen in den Archiven, Registraturen (die ja vermutlich Akten über die gesamte DDR-Prominenz enthalten) und der Personalverwaltung werden? Im September veranlaßte die Senatsverwaltung für Wissenschaft und Forschung eine Bestandsaufnahme hinsichtlich des Umfanges des in dem Krankenhausareal gelagerten Aktenmaterials. Von diesem Zeitpunkt an wurde wieder um die Zuordnung der Verantwortlichkeit für die Aufarbeitung der Unterlagen innerhalb des Senates gerungen. Daß inzwischen die mit der Schaffung von Baufreiheit in einem Teil des Gebäudekomplexes beauftragte OFD Berlin nicht inaktiv blieb und versuchte, die belegten Räume von den brisanten Akten zu befreien, kann eigentlich nicht verwundern - allerdings bedurfte es erst des energischen Eingreifens des Leitenden Amtsarztes des Bezirksamts Mitte, damit die Verlagerung der Bestände unter der fachlichen Aufsicht stattfand, die im Hinblick auf die ärztliche Schweigepflicht geboten ist. Der Senat hat zwischenzeitlich beschlossen, die Zuständigkeit ganz in die Hände der Gesundheitsverwaltung zu legen.

Diese hat nun die gewaltige Aufgabe, gemeinsam mit den für die Gesundheitsaufsicht zuständigen Bezirken nach Lösungen für die endgültige Lagerung aller Akten zu suchen. Erforderlich ist dabei eine Lagerung, die die Nutzung für künftige Krankheitsfälle der Patienten ermöglicht.

Probleme bestehen im übrigen auch bei den *fortgeführten* Einrichtungen des Gesundheitswesens. Einige stichprobenartige Besichtigungen haben ergeben, daß teilweise katastrophale Zustände hinsichtlich der zu gewährleistenden Datensicherheit zu vermerken sind. So fehlt es am notwendigsten, wie verschließbare Aktenschränke, Ausstattung der Schränke mit Sicherheitsschlössern. In einem Fall ergab die Besichtigung einer ärztlichen Dienststelle, daß Patientenunterlagen in einem unabgeschlossenen Raum zum Treppenhaus gelagert wurden und dieser Raum zusätzlich noch als Durchgangsraum zu den anderen Diensträumen benutzt wurde.

Flächendeckende Beanstandungen sind in diesem Fall nicht angebracht: Ein Vorwurf kann angesichts der Mangellage auch in personeller und finanzieller Hinsicht kaum erhoben werden, zumal von einer mitunter beeindruckenden Lernbereitschaft und Veränderungswilligkeit der Mitarbeiter ausgegangen werden kann. Gleichzeitig fehlt es jedoch noch an Wissen über die rechtlichen Rahmenbedingungen und über die technisch-organisatorischen Möglichkeiten, wie diese Zustände auch mit unkonventionellen Möglichkeiten schnellstmöglich verbessert werden können. Deswegen hat der Schwerpunkt unserer Tätigkeit bei der datenschutzrechtlichen Beratung gelegen.

Das *Krebsregister* der ehemaligen DDR soll nunmehr bis zum Inkrafttreten des Krebsregister-Sicherungsgesetzes (längstens bis zum 31. Dezember 1992) vom Bundesgesundheitsamt im Wege der Organleihe als Organ der neuen Bundesländer und Berlins verwaltet werden. Zu diesem Zweck ist ein Verwaltungsabkommen am 1. Januar 1992 zwischen den beteiligten Ländern und dem Bund in Kraft getreten.

Entgegen den Forderungen der Datenschutzbeauftragten verwaltet das Bundesgesundheitsamt nicht nur treuhänderisch den personenbezogenen Teil des Krebsregisters, der von den übrigen - für die wissenschaftliche Nutzung ausschließlich interessanten - Daten zu trennen ist, sondern alle Unterlagen des „Nationalen Krebsregisters" der ehemaligen DDR, die personenbezogene Daten enthalten. Das Bundesgesundheitsamt hat lediglich die Aufgabe, diese Unterlagen zu verwahren und sie gegen unbefugten Zugriff zu sichern. Dies gilt auch für die ab dem 1. Januar 1992 auf freiwilliger Grundlage erstatteten ärztlichen Meldungen.

Das Verwaltungsabkommen sieht außerdem vor, daß für diese Datensammlung das Datenschutzrecht des Landes gilt, aus dem die jeweilige Meldung stammt. Daraus folgt, daß das Bundesgesundheitsamt den vorhandenen Datenbestand nach Herkunftsländern getrennt verwahren muß, zumal die Datenschutzgesetze der Länder, aus denen die Meldungen stammen, zum Teil stark voneinander abweichen. Für eine wissenschaftliche Nutzung des Krebsregisters enthält das Verwaltungsabkommen ohnehin nicht die erforderliche gesetzliche Grundlage. Es ist dringend erforderlich, daß dieses datenschutzrechtlich völlig unzureichende Provisorium alsbald abgelöst wird durch eine gesetzliche Regelung, die das informationelle Selbstbestimmungsrecht der Krebskranken im östlichen Teil Berlins und in den neuen Bundesländern respektiert.

Riskante Telefonnebenstellenanlagen

Die Telefonnebenstellenanlagen in den öffentlichen Stellen der östlichen Bezirke Berlins entsprechen in aller Regel nicht dem technischen Stand, der im Westen Berlins trotz der auch dort zögerlichen Modernisierung Standard ist. Darüber hinaus gab es besondere Probleme:

Aufgeschreckt durch die Enthüllungen über die weitreichende Abhörtätigkeit der Staatssicherheit, wandte sich der Personalrat eines Bezirksamtes mit einem Problem an uns, das sicher auch andere Stellen im östlichen Berlin betrifft: Schon das Abnehmen des Telefonhörers genügte, um ungewollt Teilhaber eines telefonischen Dialoges zu sein. Auch während des Wählens einer Rufnummer stellte sich der gleiche Effekt ein, obwohl der Wahlvorgang noch gar nicht abgeschlossen war. Diese Umstände führten zu der Schlußfolgerung, daß es den Mitgliedern des Personalrates umgekehrt ähnlich widerfahren könnte, wenn sie ihrerseits miteinander telefonierten, zumal nicht eindeutig nachgewiesen werden konnte, ob es sich bei den Telefonaten, zu deren unfreiwilligem Mithörer man werden konnte, um Gespräche innerhalb des Hausnetzes handelte, oder ob die Fehlschaltungen auf das allgemeine Telefonnetz der damaligen Deutschen Post zurückzuführen seien.

Nachfragen bei der für die Wartung der Telefonanlage des Bezirksamtes zuständigen Stelle ergaben, daß die Anlage nach der Installation mit Fehlern übergeben und abgenommen wurde. Die „Unzulänglichkeiten" sollten im Laufe der Zeit beseitigt werden, was sich jedoch als kaum realisierbar herausstellte.

In einem Gespräch mit dem Bezirksbürgermeister stellte sich heraus, daß auch ihm diese Probleme nicht unbekannt waren und auch bereits Aktivitäten zur Behebung des unbefriedigenden Zustandes eingeleitet worden waren, was wiederum dem Personalrat offensichtlich nicht bekannt war. Trotz der erheblichen finanziellen Hürden wurde letztlich doch noch eine Möglichkeit gefunden, die unzuverlässige Telefonanlage auszutauschen.

Stasi beim Fernsehen

Die menschenrechtswidrigen Datenerhebungen des Staatssicherheitsdienstes sind Legion und auf Grund der aktuellen Debatten auch bekannt. Einem besonders niederträchtigen Datenzugriff beim inzwischen „abgewickelten" Deutschen Fernsehfunk (DFF) kamen wir mit Hilfe eines Dokuments auf die Spur, das uns ein aufmerksamer Bürger zur Verfügung gestellt hatte.

Im Programm des Fernsehens der DDR, der Vorläuferin des DFF, zählte die Sendung PRISMA zu den populärsten Fernsehsendungen vor der Wende. Die Redaktion verstand sich als Sammelstelle für Bürgereingaben, die bisher fruchtlos geblieben waren. Eine Vielzahl von Bürgern versuchte sich hier in einer

Weise kritisch zu äußern, wie dies über andere Medien kaum möglich war. Gerade zu den Unterlagen dieser Sendung, die nach außen ein Bollwerk gegen die Allmacht des Systems schien, verschaffte sich die Stasi einen (wie in diesem bürokratischen Staat üblich) formell geregelten Zugang - und zwar offensichtlich nicht nur zu den entstandenen Dokumenten, sondern auch zu der Informationstechnik, die der Eingabenstelle seit einigen Jahren zur Verfügung stand. Wir versuchten, diesem Zugang auf die Spur zu kommen.

Die vorgefundenen schriftlichen Programm- bzw. Verfahrensdokumentationen erwiesen sich zwar für einen Nachvollzug als unzureichend. Einige noch vorhandene Dateien zeigten jedoch, daß versucht wurde, mit einem auf einer Programmdiskette entdeckten Datenbank-Verfahren, als dessen Hersteller der Rat des Bezirkes Erfurt firmiert, die „Eingaben der Bürger" (so der Name des ADV-Verfahrens) automatisiert zu verarbeiten. Das Hauptmenü enthielt neben weiteren sieben Funktionen auch drei paßwortgeschützte Menüpunkte: Wahlfreie Recherche, Terminkontrolle und Statistik. Bei Versuchen, den Paßwortschutz zu umgehen, stießen wir auf ein Softwareprodukt einer (West-)Berliner Firma zur Verschlüsselung (Kryptographie) von Dateien.

Da bei der Einrichtung der Schlüsselwort-Dateien die Quelldateien nicht gelöscht worden waren, hatten wir die Möglichkeit, das gültige Paßwort für diese konkrete Anwendung beim DFF zu finden und die eigentlich zu schützenden Funktionen des Verfahrens zu testen. So war es möglich, alle unter einem Namen gespeicherten Eingaben aufzulisten. Auch der Beschwerdegrund konnte als Suchbegriff eingesetzt werden. Man kann sich vorstellen, daß dieses Datenbanksystem für die Eingabenbearbeitung hilfreich gewesen sein muß. Dies galt aber nicht nur für diesen eigentlichen Zweck. Auch für diejenigen, die mehr Interesse an Informationen zu bestimmten Personen hatten, bot sich auf diese Weise ein schneller Zugriff auf dieses Datenmaterial.

Da ähnliche Informationsspeicher über Bürgereingaben bei anderen Dienststellen (Eingabenstellen des Staatsrates, des Ministerrates, des Ministeriums für Handel und Versorgung, der Räte der Kreise bzw. in Berlin der Räte der Stadtbezirke) existierten, versuchten wir Querverbindungen und Analogien zur PRISMA-Eingabenstelle zu finden. Wir stießen bei entsprechenden Befragungen tatsächlich auf das gleiche Erfurter Datenbankverfahren, das offensichtlich in unterschiedlichem Maße über die damalige Magistratsverwaltung bei den ehemaligen Räten der Stadtbezirke eingeführt wurde.

Sowohl aus den letztgenannten Auskünften als auch aus den in der PRISMA-Redaktion erzielten Prüfungsergebnissen läßt sich kein eindeutiger Schluß auf die Art und Weise des Stasi-Zugriffs auf die von den DDR-Bürgern vertrauensvoll übergebenen personenbezogenen Informationen ziehen. Es ist mithin nicht gesichert, ob die Datenübermittlung entsprechend den konkreten Begehrlichkeiten des MfS durch persönliche Einsichtnahme vor Ort erfolgte oder ob regelmäßig Kopien der Datenbank auf Disketten übergeben wurden bzw. sich eine derartige Übergabe erst im Stadium der Vorbereitung befand. Vielleicht ergibt sich ja aus der nun möglichen Einsichtnahme von Betroffenen in die über sie von der Staatssicherheit gesammelten Akten eine endgültige Aufklärung dieses Sachverhalts.

Prüfung der Verfassungstreue oder Zwang zur Selbstbezichtigung?

Die Übernahme von Mitarbeiterinnen und Mitarbeitern von Dienststellen der DDR in den öffentlichen Dienst bereitet eine Vielzahl von Schwierigkeiten; hierzu gehört vor allem auch die Überprüfung von Bewerberinnen und Bewerbern daraufhin, ob ihre Übernahme aufgrund ihrer früheren Tätigkeiten zumutbar ist - und zwar nicht nur wegen der Zuarbeit zur Staatssicherheit, sondern auch wegen anderweitiger Verstrickungen in menschenverachtende Verhaltensweisen. Über die hierzu vom Land Berlin eingeleiteten Befragungen haben wir im vergangenen Jahr ausführlich berichtet[37].

Überprüfungen bei einigen Verwaltungen haben ergeben, daß in den überwiegenden Fällen nach den Richtlinien der Senatsverwaltung für Inneres verfahren wird, mit denen unsere wesentlichen Forderungen zum Verfahren und zur Verwendung der Daten aus den Fragebögen erfüllt worden waren.

Gleichwohl sind aber noch eine ganze Reihe gewichtiger Probleme offen, der Vollzug im einzelnen warf vielerlei Fragen auf.

Bereits seit längerem hatten die Datenschutzbeauftragten des Bundes und der Länder auf das Erfordernis hingewiesen, die Überprüfung bei der Übernahme in den öffentlichen Dienst auf eine *gesetzliche Grundlage* zu stellen. Zwar enthält der Einigungsvertrag einen außerordentlichen Kündigungsgrund in den Fällen, in denen der Arbeitnehmer gegen die Grundsätze der Menschlichkeit oder Rechtsstaatlichkeit verstoßen hat oder für die Staatssicherheit tätig war und deshalb ein Festhalten am Arbeitsverhältnis unzumutbar erscheint. Eine ausdrückliche Befugnis zur Erhebung entsprechender personenbezogener Daten oder Regeln für die weitere Verwendung dieser Daten enthält der Einigungsvertrag jedoch nicht. Rundschreiben und Verwaltungsvorschriften können *allenfalls übergangsweise* als Basis für die Befragung dienen. Selbst wenn die erforderliche gesetzliche Regelung nicht kurzfristig geschaffen werden kann, muß zumindest sichergestellt werden, daß den Betroffenen keine Fragen gestellt werden, die sie zu einer *verfassungswidrigen Selbstbezichtigung* zwingen. Es wäre zu begrüßen gewesen, wenn sich die Innenminister und -senatoren angesichts der sehr unterschiedlichen Fragepraxis zumindest auf eine Vereinheitlichung der Fragebögen verständigt hätten. Nichts von dem ist geschehen.

Dessen ungeachtet hat die Senatsinnenverwaltung nicht nur das Verfahren für übernommene Mitarbeiter der ehemaligen DDR-Verwaltung auf alle zukünftigen Bewerber für den öffentlichen Dienst ausgeweitet, sondern den Fragenkatalog wieder entscheidend erweitert und den Zwang zur verfassungswidrigen Selbstbezichtigung erneut eingeführt.

Zwar ist eine *Vereinheitlichung des Bewerberverfahrens* und somit auch eine Gleichbehandlung aller zukünftigen Mitarbeiter der Berliner Verwaltung begrüßenswert. Gerade wegen der Erhebung höchst sensitiver Daten kann dies aber ebenfalls nur auf einer bereichsspezifischen Rechtsgrundlage geschehen. Der Verweis des Berliner Datenschutzgesetzes auf das Bundesgesetz, das die Erforderlichkeit „im Rahmen der Zweckbestimmung eines Vertragsverhältnisses" ausreichen läßt, kann die geplanten Befragungen jedenfalls nicht rechtfertigen.

Der im Dezember 1990 vorgesehene *Fragenkatalog* beschränkte sich noch auf Fragen nach einer Funktion in der SED, einer anderen Blockpartei, nach eventuellen Tätigkeiten für das frühere Ministerium für Staatssicherheit, dessen Untergliederungen oder vergleichbare Institutionen und auf die Frage, ob gegen den Befragten der „Vorwurf oder der Verdacht erhoben worden ist, gegen Grundsätze der Menschlichkeit verstoßen zu haben". Dies entsprach dem Erforderlichkeitsprinzip. Die jetzt vorgesehenen Fragen überschreiten den zulässigen Rahmen aber erheblich. So soll erneut gefragt werden, ob der Betroffene „innerhalb seiner beruflichen oder gesellschaftlichen Tätigkeit solche Aufgaben zu erfüllen hatte, die gegen die Grundsätze der Menschlichkeit oder Rechtsstaatlichkeit verstoßen haben". Diese Frage stellt eine unerlaubte Aufforderung zur Selbstbezichtigung dar. Ebenso problematisch ist die Frage nach der Zugehörigkeit zum Nomenklaturkader, die für eine objektive Beurteilung ungeeignet und ebenfalls unzulässig ist.

Beim Vollzug des bisherigen Verfahrens sind ebenfalls noch Fragen offen:

So ist weiterhin ungeregelt die Frage der *Dauer der Aufbewahrung* der Fragebögen (sowie weiterer Protokolle oder Notizen hierzu). Auch wenn diese Unterlagen in geeigneter Weise verschlossen werden, kann die Aufbewahrungsdauer nicht identisch sein mit der der Aufbewahrungsdauer der Personalakte selbst. Bei den Angehörigen der ehemaligen Volkspolizei wurde die Aufbewahrungsdauer auf zehn Jahre begrenzt. Wir halten dies auch allgemein für einen ausreichenden Zeitraum, da sich nach Ablauf dieser Frist die Notwendigkeit erneuter Überprüfungen erübrigt haben dürfte. Vor allem auch im Hinblick auf die möglicherweise in den Antworten enthaltenen Daten über Dritte halten wir eher eine noch kürzere Aufbewahrungsdauer für angemessen.

Es ist nicht hinnehmbar, daß Arbeitnehmer in abgewickelten Einrichtungen, die den Personalbogen ausgefüllt haben, aber

[37] Jahresbericht 1990, 3.5

nicht erneut beim Land Berlin beschäftigt werden, den Fragebogen nur auf Wunsch ausgehändigt bekommen sollen. Dies würde dazu führen, daß Fragebögen solcher Bewerber, die nicht von sich aus die *Aushändigung* wünschen, auf Dauer aufbewahrt werden, obwohl sie noch nicht einmal Bedienstete des Landes Berlin sind.

Bei unseren Überprüfungen vor Ort haben sich einige zusätzliche Aspekte herausgestellt:

Die Zusatzfragen und in diesem Zusammenhang stehende Vorgänge werden in einem verschlossenen und versiegelten Umschlag (in einer Beiakte) zur Personalakte genommen und mit der Aufschrift „Personalvorgänge aus Anlaß der Weiterbeschäftigung nach der Vereinigung. Nur vom Leiter der Personalabteilung oder dem ausdrücklich Bevollmächtigten zu öffnen" versehen. Unklar ist, woran erkennbar ist, wann und zu welchem Zweck der *Umschlag geöffnet* wurde. Es müßte daher auf dem Originalumschlag ein Aufdruck angebracht werden, der entsprechende Hinweise aufnehmen kann; der Umschlag müßte nach der Einsicht wieder versiegelt werden. Zur Kontrolle wäre eine von der Personalakte unabhängige Aufbewahrung der Umschläge günstiger.

Die *Verfügungen zur Weiterbeschäftigung* werden direkt in die Personalakte aufgenommen. Hierbei besteht jedoch die Gefahr, daß jederzeit nachvollziehbar ist, ob eine Anhörung stattgefunden hat (was ja auch Rückschlüsse auf Inhalte des verschlossenen Umschlags zuläßt). Es würde ausreichen, die jeweiligen Verfügungen ebenfalls in den verschlossenen Umfang zu nehmen, weil bereits der Arbeitsvertrag (der in die Personalakte zu nehmen ist) erkennen läßt, daß die Grundlagen für eine Weiterbeschäftigung vorlagen.

Im Zusammenhang mit dem Inkrafttreten des Dritten Gesetzes über die Vereinheitlichung des Berliner Landesrechts[38] (Erstrekkung des Landesbeamtenrechts) trat die Senatsverwaltung für Inneres mit der Frage an uns heran, ob die Fragebögen im Rahmen der *Verfassungstreue-Überprüfung* nach § 9 Abs. 1 Nr. 2 Landesbeamtengesetz (LBG) vor Übernahme von Beschäftigten in das Beamtenverhältnis verwendet werden dürfen. Dies muß verneint werden.

Die Daten sind ausschließlich auf der Grundlage des Einigungsvertrages und der dort festgelegten Zweckbindung erhoben und ausgewertet worden. Zwar ist im Einigungsvertrag geregelt, daß außerordentliche Kündigungsgründe in den Fällen vorliegen, in denen Arbeitnehmer gegen die Grundsätze der Menschlichkeit und Rechtsstaatlichkeit verstoßen haben oder für das frühere MfS tätig waren und deshalb ein Festhalten am Arbeitsverhältnis unzumutbar erscheint. Dies rechtfertigt aber nicht die Verwendung zu einer Verfassungstreueprüfung, die aufgrund einer völlig anderen Rechtsvorschrift erfolgt. Dies gilt auch dann, wenn die Fragebögen von allen Bewerbern ausgefüllt werden sollen.

Ein bezirkliches Schulamt hatte angeordnet, daß Bewerber um ein Lehramt mit dem üblichen Personalfragebogen auch den neuen Zusatzfragebogen ausgefüllt und unterschrieben der Leitung der Schule vorzulegen haben, bei der die Einstellung vorgesehen ist.

Diese Regelung ist unzulässig, da Schulleitungen weder Teil der personalaktenführenden Stelle noch einstellende Dienstbehörde sind. Wegen der besonderen Zweckbindung von Personaldaten sind zugriffsberechtigt nur die Stellen, die selbständig dienst- oder arbeitsrechtliche Verhältnisse begründen, verändern und auflösen dürfen (Dienstvorgesetzte). Für einen Fachvorgesetzten ergibt sich dagegen ein unmittelbares Recht auf Einsicht in Personaldaten nicht, da dieser regelmäßig nicht mit dienstrechtlichen Aufgaben betraut ist[39].

Antragsteller von ABM-Projekten, für die die Koordinierungs- und Abwicklungsstelle der ehemaligen Akademie der Wissenschaften (KAI/AdW) als Träger fungierte, wurden aufgefordert, bereits bei Antragstellung die Personalfragebögen für mögliche spätere *ABM-Kräfte* mit den Zusatzfragen einzureichen, obwohl zu diesem Zeitpunkt noch gar nicht feststand, ob das Projekt überhaupt genehmigt würde. Auch dies war unzulässig: Es bestand kein Erfordernis, die Bewerber bereits zu einem Zeitpunkt zu überprüfen, zu dem die Schaffung der ABM-Stelle noch unsicher war, die Voraussetzungen für ein Beschäftigungsverhältnis also überhaupt noch nicht gegeben waren.

In mehreren überführten Hochschulen wurden zusätzlich zu dem allgemeinen Überprüfungsverfahren *Ehrenausschüsse* mit der Aufgabe eingesetzt, interne Erkenntnisse über frühere Verhaltensweisen von Hochschulmitarbeitern in den Beurteilungsprozeß einzubringen. Dabei war nicht klargestellt, inwieweit ein Austausch von Personaldaten zwischen des Ehrenausschüssen und den Personalstellen erfolgen sollte. In einigen Fällen sollten Mitarbeiter (auch) ihr Einverständnis erklären, daß über sie Auskünfte beim Sonderbeauftragten der Bundesregierung für die personenbezogenen Unterlagen des ehemaligen Staatssicherheitsdienstes eingeholt werden.

Trotz der besonderen Bedeutung der persönlichen Integrität im Bereich von Wissenschaft und Lehre können die Befugnisse derartiger Gremien nicht über das gesetzlich vorgegebene Maß hinausgehen. Die Ermächtigung, Daten im Rahmen eines Dienstverhältnisses zu erheben und zu verarbeiten, berechtigt nur die für die Personalentscheidungen zuständige Stelle; eine Kenntnisnahme durch Dritte - hier durch Mitglieder der Ehrenausschüsse - ist mangels Erforderlichkeit für die Vertragsabwicklung davon nicht gedeckt. Insoweit muß dafür Sorge getragen werden, daß die Ausschüsse gegenüber den Bediensteten keine Befugnis für sich reklamieren, Daten sammeln zu dürfen.

Deshalb darf auch der von den Ausschüssen ausgegebene Antrag auf Überprüfung beim Sonderbeauftragten der Bundesregierung von diesem Gremium nicht einmal entgegengenommen werden. Die Behörde hat vielmehr ein eigenes Antragsrecht und muß den Betroffenen nur informieren. Lediglich bei Neueinstellungen ist die Zustimmung Betroffener zur Auskunftserteilung einzuholen. Es ist daher nicht ersichtlich, weshalb die Bediensteten durch eine solche Aufforderung unnötig unter Druck gesetzt werden. Es könnten allein aus einer solchen Weigerung keine dienstrechtlichen Konsequenzen abgeleitet werden.

Mangels gesetzlicher Befugnis sind die Ehrenausschüsse auch nicht berechtigt, Erklärungen über eventuelle Mitarbeit beim MfS entgegenzunehmen.

Trotz dieser Rechtslage wollen einzelne Hochschulen weiterhin Ehrenausschüsse zur Beratung heranziehen. Dies ist nur unter folgenden Bedingungen möglich:

- Mitgliedern der Ausschüsse bzw. Vertrauensleuten im Rahmen ihrer Mitarbeit werden keine Namen oder sonstigen personenbezogenen Daten mitgeteilt;
- sofern Ehrenausschüssen bereits personenbezogene Daten vorliegen, sind diese unverzüglich den personalentscheidenden Stellen auszuhändigen, da bereits deren Erhebung durch die Ehrenausschüsse unzulässig war;
- sämtliche an die oder über die Ehrenausschüsse eingegangenen Informationen (z. B. Auskünfte der Gauck-Behörde) sind in das ordnungsgemäße Verfahren einzubeziehen;
- die Weigerung Betroffener, sich gegenüber den Ehrenausschüssen zu erklären oder diesen den Antrag auf Überprüfung bei der Gauck-Behörde abzugeben, darf zu keinen nachteiligen Konsequenzen für die Betroffenen führen;
- es dürfen keine personenbezogenen Informationen aus den Überprüfungsverfahren (so auch keine aufgrund von Erkenntnissen der Ehrenausschüsse erlangten Daten) veröffentlicht werden.

Die Bezirksverordneten und Bezirksstadträte eines Bezirks wurden von einem Ausschuß der *Bezirksverordnetenversammlung* zur Abgabe einer „Eidesstattlichen Erklärung" aufgefordert, daß sie weder hauptamtlicher noch informeller Mitarbeiter des ehemaligen Staatssicherheitsdienstes der DDR oder anderer Sicherheitsorgane waren. Diese Erklärung sollte durch Anfrage beim Sonderbeauftragten für die Stasi-Unterlagen überprüft werden.

Die Form dieser „Eidesstattlichen Erklärung" konnte bei juristischen Laien zu der irrigen Vorstellung führen, wer fälschlich eine solche Erklärung abgebe, mache sich strafbar. Weder die Bezirksverordnetenversammlung noch einer ihrer Ausschüsse sind jedoch eine zur Abnahme einer Versicherung an Eides Statt

[38] GVBl. 1991, S. 294 ff.
[39] vgl. Jahresbericht 1986, S. 21

zuständige Behörde im Sinne des Strafrechts. Wir haben die Vorsteherin der Bezirksverordnetenversammlung darauf hingewiesen, daß die Form der Eidesstattlichen Erklärung objektiv ungeeignet war, der Wahrheitsfindung zu dienen, sondern lediglich den unwissenden Bezirksverordneten unter einen gewissen Druck gesetzt hat.

2.3 Medien und Telekommunikation

Datenschutz und Rundfunkfreiheit

Das neue Berliner Datenschutzgesetz sieht in Anlehnung an die Rechtslage in Hessen und Bremen vor, daß auch der *Sender Freies Berlin* der Kontrolle des Berliner Datenschutzbeauftragten unterliegt, soweit er personenbezogene Daten zu anderen als journalistisch-redaktionellen Zwecken verarbeitet. Dies betrifft die Personaldatenverarbeitung, aber auch die Verarbeitung von Bürgerdaten, die etwa bei der Einziehung von Rundfunkgebühren anfallen. Zur Kontrolle der Datenverarbeitung im journalistisch-redaktionellen Bereich bestellt der Sender Freies Berlin einen eigenen Beauftragten für den Datenschutz. Diese gesetzliche Regelung trägt den verfassungsrechtlichen Anforderungen an eine unabhängige Datenschutzkontrolle auch im Rundfunkbereich Rechnung, ohne die ebenfalls verfassungsrechtlich gewährleistete Rundfunkfreiheit zu tangieren. Gleichwohl hat der Sender Freies Berlin Zweifel an der Verfassungsmäßigkeit einer staatlichen unabhängigen Datenschutzkontrolle der nichtjournalistischen Datenverarbeitung geäußert.

Diese Zweifel sind unbegründet. Ebensowenig wie der Forscher sich unter Berufung auf die Wissenschaftsfreiheit über das Persönlichkeitsrecht des Bürgers hinwegsetzen darf, dessen Daten er für seine Untersuchungen braucht, kann der Rundfunk sich unter Hinweis auf die Freiheit der Berichterstattung einer unabhängigen Kontrolle des Persönlichkeitsschutzes durch den Datenschutzbeauftragten entziehen. Dazu besteht auch keine Veranlassung, denn der Datenschutzbeauftragte wird die Rundfunkfreiheit ebenso sorgfältig beachten wie er es bei der Wissenschaftsfreiheit seit jeher getan hat. Weder die Rundfunkberichterstattung noch die Forschung kann er zensieren. Seine Aufgabe ist es, frei von Weisungen die informationelle Selbstbestimmung der Bürger in Abwägung mit den Freiheitsrechten des Rundfunks wie auch der Forschung zu schützen.

Am 1. Januar 1992 ist der *Staatsvertrag über den Rundfunk im vereinten Deutschland* in Kraft getreten, der an die Stelle aller bisher geltenden staatsvertraglichen Regelungen im Rundfunkbereich tritt und die grundlegenden Regelungen für den öffentlich-rechtlichen und den privaten Rundfunk in einem dualen Rundfunksystem der Länder des vereinten Deutschlands enthält[40].

Teil dieses Pakets aus insgesamt sechs Staatsverträgen ist ein *Rundfunkstaatsvertrag*, der erstmals eine bundeseinheitliche Datenschutzvorschrift für den privaten Rundfunk (§ 28) enthält. Diese Vorschrift ist wesentlich geprägt von den Datenschutzregelungen des Berliner Kabel-Pilotprojekt-Gesetzes (KPPG), die im Jahre 1984 in enger Abstimmung mit dem Berliner Datenschutzbeauftragten formuliert worden sind und eine bundesweite Vorreiterfunktion hatten. Kern dieser Regelung ist das Verbot, aus Abrechnungsdaten ein Mediennutzungsprofil des einzelnen Teilnehmers zu erstellen. Zeitpunkt, Dauer, Art, Inhalt und Häufigkeit bestimmter vom einzelnen Teilnehmer in Anspruch genommene Programmangebote dürfen nur erkennbar sein, wenn der Teilnehmer schriftlich eine nach einzelnen Programmangeboten aufgeschlüsselte Entgeltabrechnung beantragt hat.

Der neue *Rundfunkgebührenstaatsvertrag* (Art. 4 des Staatsvertrages über den Rundfunk im vereinten Deutschland) regelt erstmals in datenschutzgerechter Weise, welche Angaben jeder Rundfunkteilnehmer von sich aus gegenüber der jeweiligen Rundfunkanstalt zur Einziehung der Rundfunkgebühr machen muß. Der alte Rundfunkgebührenstaatsvertrag regelte diese Anzeigepflicht nur in einer pauschalen und mit dem Volkszählungsurteil des Bundesverfassungsgerichts nicht zu vereinbarenden Weise. Jetzt ist dies im einzelnen ebenso staatsvertraglich festgelegt wie die Zweckbindung bei der Verarbeitung dieser Daten und eine Benachrichtigungspflicht gegenüber dem Rundfunkteilnehmer bei einer erstmaligen automatisierten Speicherung.

Zum großen Teil greift der neue Rundfunkgebührenstaatsvertrag Forderungen auf, die der Arbeitskreis Medien der Konferenz der Datenschutzbeauftragten unter dem Vorsitz des Berliner Datenschutzbeauftragten erarbeitet hat.

Hinsichtlich der Gebührenbefreiung verpflichtet der Rundfunkgebührenstaatsvertrag diejenigen Länder, in denen nicht die Landesrundfunkanstalt über den Antrag auf Gebührenbefreiung entscheidet, durch Rechtsverordnung zu bestimmen, welche personenbezogenen Daten die für die Entscheidung zuständige Stelle an die Landesrundfunkanstalt zu übermitteln hat[41]. Eine solche Rechtsverordnung muß in Berlin noch erlassen werden. Die inzwischen in Kraft getretene *Verordnung über die Feststellung der Befreiung von der Rundfunkgebührenpflicht*[42] enthält nicht die erforderlichen Regelungen über die Erhebung und Verarbeitung der teilweise sehr sensiblen personenbezogenen Informationen (Sozialhilfebezug, Krankheitsdaten), obwohl wir bereits vor längerer Zeit detaillierte Vorschläge für entsprechende Regelungen gemacht hatten.

Schließlich erlaubt der neue Rundfunkgebührenstaatsvertrag den Landesrundfunkanstalten, die von ihr gespeicherten personenbezogenen Daten der Rundfunkteilnehmer für andere Landesrundfunkanstalten auch im Rahmen eines automatisierten Abrufverfahrens bereitzuhalten, soweit dies zur rechtmäßigen Erfüllung der Aufgaben der beteiligten Landesrundfunkanstalten beim Gebühreneinzug erforderlich ist. Gegen diese Regelung hatten die Datenschutzbeauftragten eingewandt, dadurch würde ein *bundesweites elektronisches Teilnehmerverzeichnis* entstehen, bei dessen Nutzung die Zweckbindung nicht mehr zu kontrollieren sei. Auf Vorschlag der Datenschutzbeauftragten ist deshalb eine strikte Protokollierungspflicht der übermittelnden Landesrundfunkanstalt festgelegt worden, die aufzuzeichnen hat, an welche Stellen, wann und aus welchem Grund welche personenbezogenen Daten übermittelt worden sind[43]. In der Praxis wird sehr sorgfältig anhand dieser Aufzeichnungen zu kontrollieren sein, ob Teilnehmerdaten im gesetzlich zugelassenen Rahmen übermittelt und genutzt werden.

Bildschirmtext und Kabelpilotprojekt

Die Datenschutzbestimmung des alten *Bildschirmtext-Staatsvertrages* hat sich bewährt. Im neuen Bildschirmtext-Staatsvertrag[44] ist diese Regelung deshalb unverändert übernommen worden. Auch das Berliner Zustimmungsgesetz zum Staatsvertrag über den Rundfunk im vereinten Deutschland hat wortgleich die entsprechende Vorschrift im alten Zustimmungsgesetz zum Bildschirmtext-Staatsvertrag übernommen, in der dem Berliner Datenschutzbeauftragten eine besondere Kompetenz zur Beobachtung und Feststellung von Mängeln bei der Einhaltung der Datenschutzvorschriften im Bereich des Bildschirmtextes zugewiesen wurde. Die Senatsverwaltung für Inneres hatte sich anfänglich für eine Streichung dieser Kompetenz ausgesprochen. Es ist zu begrüßen, daß der Gesetzgeber dem nicht gefolgt ist, zumal die Befugnisse und Zuständigkeiten der Senatsverwaltung für Inneres und des Berliner Datenschutzbeauftragten nach dem Bundesdatenschutzgesetz und dem Berliner Datenschutzgesetz unberührt bleiben. Beim Bildschirmtext gab es im Berichtszeitraum keinen Anlaß für datenschutzrechtliche Beanstandungen.

Spätestens am 30. April 1992 tritt das *Kabel-Pilotprojekt-Gesetz* (KPPG) von 1984 außer Kraft. Es muß ersetzt werden durch ein Gesetz, das eine unbefristete allgemeine Regelung für den privaten Rundfunk im Lande Berlin enthält[45]. Diese unbefristete Regelung für den privaten Rundfunk wird entweder durch einen *Staatsvertrag über die Zusammenarbeit zwischen Berlin und Brandenburg* im Bereich des Rundfunks oder durch ein *Berliner Mediengesetz* getroffen werden. In jedem Fall muß der hohe datenschutzrechtliche Standard des bisher geltenden Kabel-Pilotprojekt-Gesetzes aufrechterhalten werden.

[40] GVBl. 1991, S. 309 ff.

[41] § 6 Abs. 4

[42] GVBl. 1992, S. 3 f.

[43] § 8 Abs. 3 Satz 2

[44] Art. 6 des Staatsvertrages über den Rundfunk im vereinten Deutschland

[45] § 7 Satz 2 des Gesetzes zur Überleitung der Versuche mit privatem Rundfunk in Berlin und zur Änderung des KPPG vom 17. Juli 1990 (GVBl. S. 1575)

Telekommunikationsverordnungen des Bundes

Die gerade in Berlin fortschreitende Digitalisierung des Telekommunikationsnetzes gefährdet das *Grundrecht auf unbeobachtbare Kommunikation*[46]. Diese Gefahr besteht nicht - wie viele glauben - erst dann, wenn man einen ISDN-Hauptanschluß beantragt und sich ein modernes Telefon mit Display besorgt. Von den gegenwärtig ca. 1,7 Millionen Telefon-Hauptanschlüssen sind ca. 390 000 an digitalisierte Ortsvermittlungsstellen angeschlossen. Bald werden es alle Telefon-Hauptanschlüsse sein. Auch wer ein altmodisches, vertraut aussehendes Telefon benutzt, das an eine digitalisierte Ortsvermittlungsstelle angeschlossen ist, muß damit rechnen, daß er bald - ohne es zu wissen - zwangsläufig Datenspuren im Netz der TELEKOM hinterläßt.

Gewissermaßen in letzter Minute beschloß die Bundesregierung mit Zustimmung des Infrastrukturrates die Verordnung über den Datenschutz bei Dienstleistungen der Deutschen Bundespost TELEKOM *(TELEKOM-Datenschutzverordnung - TDSV)* vom 24. Juni 1991[47], die am 1. Juli 1991 in Kraft trat und die bisher geltende Telekommunikationsordnung ablöste. Den Auftrag, den der Bundesgesetzgeber im Postverfassungsgesetz von 1989 erteilt hatte, entsprechende Datenschutzregelungen auch für private Teledienstunternehmen (z. B. die Betreiber von Mobilfunknetzen) zu treffen, erfüllte die Bundesregierung mit noch größerer Verspätung, indem sie die Verordnung über den Datenschutz für Unternehmen, die Telekommunikationsdienstleistungen erbringen *(Teledienstunternehmen-Datenschutzverordnung-UDSV)* vom 18. Dezember 1991 mit Zustimmung des Bundesrates beschloß[48]. Die UDSV ist am 29. Dezember 1991 in Kraft getreten. Bereits zum 1. Juli 1991 gelten außerdem eine POSTBANK- und eine POSTDIENST-Datenschutzverordnung[49].

Die ursprünglichen Entwürfe, die der Bundesminister für Post und Telekommunikation zur Regelung des Datenschutzes bei öffentlichen und privaten Anbietern von Telekommunikationsdienstleistungen vorgelegt hatte, waren völlig unzureichend. Dem Telefonteilnehmer sollten sowohl die *langfristige Speicherung seiner Verbindungsdaten* über jedes einzelne Telefongespräch als auch die *Übermittlung seiner Rufnummer an den Angerufenen* vor Herstellung der Verbindung ohne Unterdrückungsmöglichkeit aufgezwungen werden.

Im Rahmen einer Anhörung des Bundestagsausschusses für Post und Telekommunikation am 5. März 1991 hat der Berliner Datenschutzbeauftragte als Vorsitzender des Arbeitskreises Medien der Konferenz der Datenschutzbeauftragten des Bundes und der Länder zu den Verordnungsentwürfen Stellung genommen und betont, daß die Entwürfe das Grundrecht auf informationelle Selbstbestimmung und unbeobachtbare Kommunikation der Teilnehmer nicht hinreichend berücksichtigten. Vielmehr müßten Verbindungsdaten, die für die Gebührenberechnung nicht benötigt werden, sofort gelöscht werden. Es dürfe nicht - wie in den Entwürfen vorgesehen - mindestens bis zur Rechnungserstellung gespeichert bleiben, wer mit wem wann und wie lange telefoniert hat. Soweit ein Teilnehmer einen *Einzelentgeltnachweis* beantragt hat, gebiete das informationelle Selbstbestimmungsrecht des angerufenen Teilnehmers, daß dessen Daten nicht in der Rechnung erscheinen. Außerdem müsse jeder Anrufer die Möglichkeit erhalten, die Anzeige seiner Rufnummer am Telefon des Angerufenen fallweise zu unterdrücken. Dies wurde in den ursprünglichen Verordnungsentwürfen ausdrücklich ausgeschlossen.

Die ursprünglich vorgesehenen Regelungen stellten die betrieblichen Interessen der Deutschen Bundespost TELEKOM sowie ihrer privaten Konkurrenten und die Geschäftsinteressen kommerzieller Teilnehmer (insbesondere des Versandhandels) über die Grundrechte der Betroffenen. In den Vereinigten Staaten werden bereits Rufnummern von Anrufern, die auf dem Display des angerufenen Unternehmens angezeigt werden, mit Hilfe eines angeschlossenen PC's blitzschnell in einem elektronischen Telefonbuch gespeichert und für Zwecke der späteren Telefonwerbung vorgehalten.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat in ihrem Beschluß vom 8. März 1991[50] auf Vorschlag des Arbeitskreises Medien Kritik an den Verordnungsentwürfen geübt.

Diese Kritik - wie auch die deutlichen Einwände der Kirchen, die insbesondere die Notwendigkeit anonymer telefonischer Beratung und Seelsorge unterstrichen - hat immerhin dazu geführt, daß das Bundespostministerium seine ursprünglichen Entwürfe in zwei Punkten modifizieren mußte. Während ursprünglich vorgesehen war, daß die Verbindungsdaten *nach Wahl* des Teilnehmers nach Versendung der Entgeltrechnung entweder unverzüglich gelöscht oder zum Zwecke des Nachweises für weitere 80 Tage vollständig gespeichert werden sollten, sind sie nun spätestens mit Versendung der Entgeltrechnung beim Telefon nach Wahl des entgeltpflichtigen Kunden entweder vollständig zu löschen oder unter Verkürzung der Zielrufnummer um die letzten drei Ziffern zu speichern oder vollständig zu speichern, wenn ein Einzelentgeltnachweis beantragt wurde. Bei allen anderen Telekommunikationsdiensten werden die Verbindungsdaten dagegen vollständig gespeichert[51].

Außerdem muß der Anrufer spätestens ab dem 1. Januar 1994 im Rahmen der Einführung des Europäischen Diensteintegrierenden Digitalen Netzes (Euro-ISDN) die Möglichkeit erhalten, die *Übermittlung seiner Rufnummer* an den Angerufenen im Einzelfall *zu unterdrücken*. Fraglich bleibt allerdings, was mit den ISDN-fähigen Telefonen geschehen soll, die vor diesem Datum installiert werden, ohne über einen Unterdrückungsknopf für die Rufnummernanzeige zu verfügen. Es ist zu befürchten, daß der einzelne Telefonteilnehmer die Kosten für ein datenschutzgerechtes Telefon selbst wird übernehmen müssen. Es wäre zu begrüßen, wenn die Deutsche Bundespost TELEKOM bis zum 1. Januar 1994 auf die Verwirklichung der Rufnummernanzeige im digitalen Telefonnetz verzichten würde. Nur auf diese Weise kann nämlich sichergestellt werden, daß die Rufnummernanzeige in der Zwischenzeit nicht gegen den Willen des Anrufers stattfindet.

Bei den Beratungen der UDSV im Bundesrat wurde eine Forderung der Datenschutzbeauftragten aufgegriffen: für die privaten Teledienstunternehmen ist abschließend festgelegt, welche Verbindungsdaten sie erheben und verarbeiten dürfen. Demgegenüber darf die TELEKOM mit Zustimmung des Bundespostministers darüber hinaus weitere *Verbindungsdaten* erheben und verarbeiten, „soweit es die technische Entwicklung erfordert". Der Infrastrukturrat und der Bundesbeauftragte für den Datenschutz müssen zwar vor der Zustimmung beteiligt werden, können sie aber nicht verhindern. Diese Blankettermächtigung der TELEKOM läßt den Bürger über den Umfang der Datenverarbeitung im Telefonnetz vollends im unklaren. Sie ist mit dem informationellen Selbstbestimmungsrecht nicht zu vereinbaren und sollte gestrichen werden.

In zentralen Punkten lassen beide Datenschutzverordnungen die Forderungen der Datenschutzkonferenz unberücksichtigt und enthalten keine praktikablen Vorkehrungen zur Sicherung der unbeobachtbaren Kommunikation. So werden die Verbindungsdaten, die zwangsläufig durch die computergesteuerte Vermittlungstechnik entstehen, nicht unverzüglich nach dem Ende des Telefongesprächs gelöscht, sondern nur auf Wunsch des Kunden „spätestens mit Versendung der Entgeltrechnung" entweder vollständig gelöscht oder um die letzten drei Ziffern verkürzt gespeichert, wenn der Kunde keinen Einzelentgeltnachweis beantragt hat. Wird ein Einzelentgeltnachweis (detaillierte Telefonrechnung) beantragt, so enthält dieser stets die vollständigen Zielrufnummern und die Verbindungsdaten bleiben vollständig für einen Zeitraum von 80 Tagen nach Versendung der Telefonrechnung gespeichert. Damit wird das informationelle Selbstbestimmungsrecht des angerufenen Teilnehmers pauschal den Interessen des Anrufers untergeordnet. Diese Regelung widerspricht auch dem Vorschlag der EG-Kommission für eine ISDN-Datenschutzrichtlinie, wonach im Einzelentgeltnachweis die Zielruf-

[46] vgl. dazu Jahresbericht 1990, 2.3
[47] BGBl. I, S. 1390 ff.
[48] BGBl. I, S. 2337 ff.
[49] BGBl. I, S. 1387 ff. bzw. 1385 ff.
[50] Anlage 2.2
[51] § 6 Abs. 2 TDSV und UDSV

nummer stets um die letzten vier Ziffern verkürzt werden muß. Diesen Vorschlag hatte die Konferenz der Datenschutzbeauftragten unterstützt. Zumindest wäre es notwendig, dem Angerufenen rechtzeitig mit einem besonderen Signalton zu signalisieren, daß der Anrufer einen Einzelentgeltnachweis beantragt hat und deshalb die vollständige Telefonnummer des Angerufenen auf dieser Rechnung erscheinen wird, damit der Angerufene sich entscheiden kann, ob er unter diesen Voraussetzungen das Telefongespräch führen will.

Der Bundespostminister hat demgegenüber auf seinem Standpunkt beharrt und dafür vordergründige *Gesichtspunkte des Verbraucherschutzes* angeführt. Sicherlich ist es eine zusätzliche Dienstleistung für die Telefonkunden (die sich die TELEKOM auch gesondert bezahlen läßt), wenn die Kunden kontrollieren können, mit wem im Abrechnungszeitraum von ihrem Telefonanschluß aus telefoniert worden ist. Das Interesse des Anrufers als Verbraucher an einer transparenten Telefonabrechnung ließe sich aber ebenso mit verkürzten Zielrufnummern befriedigen, ohne daß Rechte des Angerufenen beeinträchtigt werden. Im übrigen ist es eine Illusion zu glauben, mit Hilfe des Einzelentgeltnachweises könne der Telefonkunde in Zukunft die Richtigkeit der Telefonrechnung zuverlässig überprüfen. Daß dies nicht der Fall ist, zeigen die jüngst bekanntgewordenen Fälle, in denen die TELEKOM nach Pressemeldungen für Anrufe aus den alten Bundesländern in die neuen Bundesländer selbst dann Gebühren berechnet hat, wenn keine Verbindung zustande gekommen ist. Wenn derartige „Fehlversuche" auf einem Einzelentgeltnachweis erscheinen würden, wäre es Sache des anrufenden Telefonkunden zu beweisen, daß in diesen Fällen gar keine Verbindung zustande gekommen ist. Dasselbe gilt, wenn die Verbindungen zwar zustande gekommen sind, aber der Gebührenrechner der TELEKOM - aufgrund eines Programmfehlers - zu hohe Gebühren errechnet hat.

Statt dem informationellen Selbstbestimmungsrecht des angerufenen Telefonkunden durch die Verkürzung seiner Rufnummer in praktikabler Weise Rechnung zu tragen, enthalten die Datenschutzverordnungen komplizierte und unzureichende Regelungen, mit denen die *Anonymität der telefonischen Beratung* sichergestellt werden soll. Hierzu müssen die öffentlichen und privaten Beratungseinrichtungen entsprechende Anträge bei der TELEKOM und privaten Netzbetreibern stellen, damit diese sicherstellen, daß die Rufnummern der Beratungseinrichtungen in den Einzelentgeltnachweisen der Anrufe nicht (auch nicht verkürzt) erscheinen. Um die praktische Bedeutung dieses Problems zu verstehen, muß man sich nur vergegenwärtigen, daß jemand telefonisch einen Beratungstermin bei einer AIDS-Beratungsstelle vereinbaren will, ohne damit rechnen zu müssen, daß dies dem Inhaber des Anschlusses (z. B. den Eltern des Anrufers) auf der detaillierten Telefonrechnung mitgeteilt wird oder zumindest zu Nachfragen Anlaß gibt.

Diese unpraktikable Regelung zur Sicherstellung der anonymen telefonischen Beratung tritt für Festanschlüsse, bei denen die TELEKOM nach wie vor ein Monopol hat, erst dann in Kraft, wenn die zu ihrer Durchführung erforderlichen Datenverarbeitungsprogramme verfügbar sind, spätestens aber am 1. Juli 1992. Die TELEKOM hat sich - auf Druck der Kirchen - bereiterklärt, vor diesem Zeitpunkt von der Erstellung von Einzelentgeltnachweisen ganz abzusehen. Es bleibt abzuwarten, wie die Einzelentgeltnachweise gestaltet sein werden, insbesondere ob durch Leerzeilen oder Differenzen zwischen den Kosten einzelner Gespräche und der Gesamtsumme ein Hinweis auf Telefonate mit schweigepflichtigen Beratungsstellen gegeben wird. Dies würde wiederum zu Nachfragen und Rechtfertigungszwängen innerhalb der Familie führen und die wenig praktikable Regelung der Verordnung vollends ad absurdum führen.

Eine datenschutzgerechte Alternative zu dem komplizierten Antragsverfahren, das die Beratungsstellen durchlaufen müssen, um die Vertraulichkeit der telefonischen Beratung sicherzustellen, wäre die Bereitstellung eines eigenen Nummernblocks (entsprechend dem 0130-Dienst der TELEKOM), der der Telefonnummer der Beratungsstelle voranzustellen wäre und bei dem vom Netzbetreiber sichergestellt würde, daß die Nummer der angewählten Beratungseinrichtung nicht auf der Telefonrechnung erscheint.

Um den *Datenschutz bei telefonischer Beratung* durch öffentliche Stellen des Landes Berlin sicherzustellen, haben wir im November 1991 alle beteiligten Senatsverwaltungen und die Abteilungen Volksbildung, Sozialwesen, Jugend und Sport, Gesundheit und Umweltschutz der Bezirksämter von Berlin sowie den Hauptpersonalrat auf die neue TELEKOM-Datenschutzverordnung hingewiesen. Damit der Bürger, der sich per Telefon an eine Beratungsstelle wendet und aus guten Gründen seine Identität nicht - oder jedenfalls nicht von vornherein - offenlegen will, neben der - ohnehin schon zu weit gehenden - Speicherung von Verbindungsdaten keine zusätzlichen Spuren im Fernmeldenetz hinterlassen muß, haben wir empfohlen, bereits jetzt die erforderlichen Anträge bei der Deutschen Bundespost TELEKOM zu stellen, damit durch technische Vorrichtungen die Beachtung des Beratungsgeheimnisses sichergestellt wird. Antragsberechtigt sind z. B.

- Bürgerberatungsstellen,
- Sozial- und Gesundheitsämter,
- Schwangerschaftsberatungsstellen,
- Drogenberatungsstellen,
- AIDS-Beratungsstellen,
- Frauenhäuser und Beratungsstellen für vergewaltigte oder mißhandelte Frauen,
- Frauenbeauftragte,
- Versorgungsämter,
- Schulpsychologische Dienste,
- Schulärztliche Dienste,
- Erziehungsberatungsstellen,
- Personalräte,
- Jugendgerichtshilfe,
- Telefonseelsorge und Telefon des Vertrauens.

Nur wenn diese Einrichtungen entsprechende Anträge stellen, hat die TELEKOM sicherzustellen, daß ihre Telefonnummern nicht auf detaillierten Telefonrechnungen erscheinen können. Sie hat außerdem auf Antrag die Übermittlung der Rufnummer des anrufenden Anschluß an einen Anschluß in den genannten Beratungsstellen auszuschließen. Schließlich hat die TELEKOM die in dieser Weise geschützten Anschlüsse im nächsten Amtlichen Telefonbuch entsprechend zu kennzeichnen.

Auch der Berliner Datenschutzbeauftragte, der nach § 23 BlnDSG zur besonderen Verschwiegenheit verpflichtet ist, hat bereits entsprechende Anträge bei der Deutschen Bundespost TELEKOM stellen lassen.

Es ist notwendig, diese Maßnahmen bereits jetzt zu ergreifen, obwohl noch nicht alle Ortsvermittlungsstellen im Land Berlin digitalisiert sind und digitalisierte Endgeräte bisher noch wenig verbreitet sind. Denn sobald die TELEKOM *Einzelentgeltnachweise* erstellt (ab dem 1. Juli 1992), können auf diesen auch die Telefonnummern herkömmlicher analoger Telefonanschlüsse erscheinen. Die *Anzeige der Rufnummer* des anrufenden Anschlusses setzt dagegen voraus, daß der Angerufene über ein ISDN-fähiges Telefon mit Display verfügt. Ist das der Fall, so kann technisch auch die Rufnummer eines analogen Anschlusses angezeigt werden, von dem aus angerufen wird. Die Deutsche Bundespost TELEKOM hat zwar zugesichert, daß die Rufnummern analoger Rufnummern nicht angezeigt werden. Dies wird jedoch nur softwaretechnisch realisiert.

Zahlreiche öffentliche Stellen sind unserer Empfehlung gefolgt, die notwendigen Anträge bei der TELEKOM zu stellen. Dies ist auch deshalb wichtig, weil vor der Einführung des Einzelentgeltnachweises in erstem Halbjahr 1992 die nächste Ausgabe (1992/93) des Amtlichen Telefonbuchs erscheinen wird, in dem bereits Hinweise auf bestimmte geschützte Telefonnummern der Beratungseinrichtungen enthalten sein müssen.

Die Telefonkunden erhielten im vergangenen Jahr mit ihrer Gebührenrechnung ein *Informationsblatt der TELEKOM*, in dem

sie nur sehr unzureichend über ihre neuen Rechte nach der TELEKOM-Datenschutzverordnung aufgeklärt wurden. Sie wurden zwar darauf hingewiesen, daß sie neuerdings die Möglichkeit haben, den Umfang der Eintragung ihrer Daten in das Telefonbuch zu beschränken oder der Eintragung ganz zu widersprechen. Dagegen wurden die Kunden nicht darauf hingewiesen, daß sie jetzt der Weitergabe der Nutzung ihrer Daten an die Deutsche Postreklame oder andere Unternehmen zu Werbezwecken widersprechen können. Auch wurden sie nicht über ihr Recht informiert, die gespeicherten Verbindungsdaten über jedes geführte Telefongespräch löschen oder nur verkürzt speichern zu lassen. Statt die Kunden darüber zu informieren, daß die TELEKOM-Datenschutzverordnung ihnen in beschränktem Umfang zusätzliche Rechte zum Schutz ihrer Privatsphäre beim Telefonieren einräumt, wies die TELEKOM ihre Kunden lediglich darauf hin, daß sie der Kontrolle durch den Bundesbeauftragten für den Datenschutz widersprechen können, und zwar in einer Weise, die es den Lesern des Faltblatts nahelegte, möglichst bald Widerspruch einzulegen. Verschwiegen wurde dabei, daß es die Aufgabe der Datenschutzbeauftragten ist, die Persönlichkeitsrechte der Bürger zu schützen und daß zahlreiche Widersprüche eine datenschutzrechtliche Kontrolle der Telefondatenverarbeitung erheblich behindern würde. Der Bundesbeauftragte für den Datenschutz, der Berliner Datenschutzbeauftragte und das für die Deutsche Postreklame als Aufsichtsbehörde zuständige Regierungspräsidium Darmstadt haben die TELEKOM aufgefordert, die Telefonkunden alsbald umfassend über ihre Datenschutzrechte zu informieren.

Der Telefonkunde hat jetzt erstmals das *Recht, der Eintragung seiner Daten in das Telefonbuch* ganz oder teilweise *zu widersprechen.* Darauf muß die TELEKOM ihn hinweisen (§ 10 Abs. 3 TDSV). Dies bedeutet auch, daß der Telefonkunde, der mit einem Abdruck von Name, Anschrift und Telefonnummer im herkömmlichen Telefonbuch einverstanden ist, der Speicherung dieser Daten auf einem elektronischen Datenträger *(CD-ROM* = Compact Disc Read Only Memory) widersprechen kann. Diese Datenträger ermöglichen es, sämtliche Telefonbücher der ganzen Bundesrepublik auf kleinstem Raum zu speichern und automatisiert auszuwerten, etwa auch das Telefonbuch „umzudrehen", so daß man sehr schnell feststellen kann, welchem Teilnehmer eine unbekannte Telefonnummer zuzuordnen ist. Die Deutsche Postreklame beabsichtigt, ein solches bundesweites Telefonverzeichnis auf CD-ROM herauszugeben. Damit würde zum ersten Mal ein *zentrales automatisiertes Einwohnerregister auf Bundesebene* geschaffen, daß das geltende Melderecht gerade ausschließt.

Um so wichtiger ist es, daß der Telefonkunde dieser Art der Verwendung seiner Daten, die er zur Veröffentlichung in einem herkömmlichen Telefonbuch angegeben hat, widersprechen kann. Dies setzt voraus, daß die TELEKOM ihn darüber informiert, daß Telefonbücher über Belegleser (Scanner) in Rechner eingelesen und auf auf CD-ROMs gespeichert werden können. Bisher bestreitet die TELEKOM allerdings sowohl eine Verpflichtung, den Kunden auf diese weitreichenden Verwendungsmöglichkeiten hinzuweisen, als auch ein partielles Widerspruchsrecht des Kunden gegen die Verwendung. Dies ist unverständlich, denn es müßte gerade im Interesse der TELEKOM liegen, dem Kunden ein differenziertes Widerspruchsrecht einzuräumen. In der Vergangenheit war jeder Kunde gezwungen, seine Daten im Telefonbuch abdrucken zu lassen. Warum soll er jetzt nicht die Möglichkeit haben, sich auf diesen Abdruck zu beschränken, aber eine automatisierte Verarbeitung dieser Daten auszuschließen? Bliebe die TELEKOM bei ihrer starren Haltung, so kann man Kunden, die eine Speicherung ihrer Telefondaten auf CD-ROM effektiv ausschließen wollen, nur raten, dem Telefonbucheintrag insgesamt zu widersprechen.

Auch das von den Datenschutzbeauftragten geforderte Verbot der *Erstellung von Kommunikationsprofilen* über das Verhalten der einzelnen Kunden, insbesondere wie häufig und wie lange sie telefonieren und welche anderen Telekommunikationsdienste sie nutzen, ist nicht in die Datenschutzverordnungen aufgenommen worden. Dennoch besteht kein Zweifel daran, daß die Erstellung solcher Profile den Kernbereich des Grundrechts auf unbeobachtbare Kommunikation verletzen würde.

Das *Fernmeldegeheimnis* ist infolge der Digitalisierung neuen Gefährdungen ausgesetzt. Das *Fernmeldeanlagengesetz* (FAG)[52] sieht vor, daß in strafgerichtlichen Untersuchungen der Richter und bei Gefahr im Verzug auch die Staatsanwaltschaft unter bestimmten Voraussetzungen Auskunft über den Fernmeldeverkehr verlangen kann. Diese Voraussetzungen sind sehr viel weiter gefaßt als die Umstände, die eine Überwachung und Aufzeichnung des Fernmeldeverkehrs nach der Strafprozeßordnung[53] ermöglicht. Das Auskunftsrecht des Strafrichters oder Staatsanwalts nach dem FAG, das bisher nur geringe praktische Bedeutung hatte, erhält mit der Digitalisierung des Telefonnetzes eine neue, verfassungsrechtlich nicht mehr hinnehmbare Qualität. Durch die massenhafte Speicherung von Verbindungsdatensätzen, die mit der neuen Technik ermöglicht wird, kann in jedem Strafverfahren (auch wegen Bagatellstraftaten) vollständige Auskunft über die bei der TELEKOM dokumentierte Telefonnutzung sowohl des Beschuldigten als auch Dritter (z. B. Zeugen) verlangt werden.

Die Konferenz der Datenschutzbeauftragten hat daher im März 1991 die rechtsstaatlich gebotene Einschränkung des Auskunftsrechts nach dem FAG gefordert[54].

Auch der Bundesrat hat diese Einschränkung in einer Entschließung bei der Verabschiedung der UDSV ausdrücklich für notwendig erklärt. Diese Entschließung steht allerdings in eklatantem Widerspruch zu dem vom Bundesrat selbst eingebrachten Entwurf für ein Gesetz zur Bekämpfung der Organisierten Kriminalität (OrgKG)[55]. Dieser sieht vor, daß die Überwachung und Aufzeichnung des Fernmeldeverkehrs (also nicht nur die Auskunft über Verbindungsdaten) weitergehend als bisher schon zur Abwehr einer gegenwärtigen Gefahr für Leben, Leib oder Freiheit einer Person angeordnet werden kann. Ob diese Abhörbefugnis für präventive Zwecke überhaupt erforderlich ist, bedarf selbst nach Auffassung der Bundesregierung noch der Prüfung. In jedem Fall ist sie entschieden zu weit gefaßt. Sie muß zumindest an einen eng begrenzten Straftatenkatalog geknüpft und strikter verfahrensrechtlich abgesichert werden.

Wir haben gegenüber dem Bundestagsausschuß für Post und Telekommunikation auch zum Entwurf der *POSTBANK-Datenschutzverordnung (PB-DSV)* Stellung genommen. Dabei hat er kritisiert, daß mit dem Verordnungsentwurf die Gelegenheit versäumt werde, einen ersten Schritt zu einer umfassenden Regelung der wesentlichen Datenschutzprobleme im Bereich der Kreditinstitute zu tun. Diese Probleme sind in den Tätigkeitsberichten der Aufsichtsbehörden eingehend beschrieben worden. Es fehlen insbesondere Bestimmungen zum Datenaustausch mit Kreditinformationssystemen, vor allem der SCHUFA und zur Videoüberwachung. Trotz der Wettbewerbssituation, in der sich das Unternehmen POSTBANK mit anderen privaten Kreditinstituten befindet, die bisher keinen vergleichbaren Regelungen unterliegen, hätte das Bundesministerium für Post und Telekommunikation die Gelegenheit ergreifen sollen, zumindest für die POSTBANK diese Probleme zu regeln und damit dem POSTBANK-Kunden ein Mehr an Datenschutz als die privaten Kreditinstitute anbieten zu können. In der Praxis hat die POSTBANK einen begrüßenswerten Schritt dahin getan, in dem in den Schalterräumen klare Vorkehrungen zur Wahrung der Diskretion getroffen wurden, so daß die Warteschlangen erst mit einem gewissen Abstand zu dem jeweils bedienten Kunden beginnen.

Nach dem Entwurf der POSTBANK-Datenschutzverordnung war vorgesehen, daß die POSTBANK Bestandsdaten ihrer Kunden auch nach Beendigung des Vertragsverhältnisses für Werbezwecke weiter nutzen darf, ohne daß der Kunde dem hätte widersprechen können. Dies hätte der POSTBANK den Handel mit den Adressen ihrer ehemaligen Kunden noch mehr erleichtert, als dies für den privaten Adressenhandel nach dem novellierten Bundesdatenschutzgesetz ohnehin der Fall ist. Die in Kraft gesetzte Verordnung enthält jetzt immerhin ein Widerspruchsrecht der Kunden, allerdings keine Pflicht der POSTBANK, ihre Kunden auf dieses Widerspruchsrecht hinzuweisen. Auch unsere Vorschläge für Regelungen einer Übermittlungsbefugnis der

[52] § 12 FAG
[53] § 100 a StPO
[54] Anlage 2.2
[55] siehe dazu 3.6

POSTBANK an Kreditinformationssysteme und zur Videoüberwachung wurden nicht aufgegriffen.

Telekommunikation in Europa

Auf europäischer Ebene enthält der Vorschlag der EG-Kommission für eine *ISDN-Datenschutzrichtlinie*[56] zahlreiche positive Elemente, die - bei einer unveränderten Verabschiedung der Richtlinie durch den Ministerrat - zu einer datenschutzgerechten Gestaltung des deutschen Telekommunikationsrechts beitragen werden.

Der Richtlinienentwurf sieht die generelle Verkürzung der Zielnummer im Einzelentgeltnachweis des Anrufers um die letzten vier Ziffern vor. Diese datenschutzfreundliche Regelung entspricht einer Forderung der Datenschutzbeauftragten und sollte gegen die Kritik der nationalen Telekommunikationsorganisationen verteidigt werden. Sie ermöglicht auch technisch praktikable Lösungen im Gegensatz etwa zur deutschen Telekommunikations-Datenschutzverordnung.

Auch der Vorschlag der Kommission, dem Anrufer zu signalisieren, wenn die Möglichkeit besteht, daß seine Rufnummer beim Angerufenen angezeigt wird, ist ebenso zu begrüßen wie das prinzipielle Recht des Anrufers, die Rufnummernanzeige im Einzelfall auf Knopfdruck zu unterdrücken. Dies muß auch für grenzüberschreitende Telefonate sichergestellt werden, wie dies France TELECOM bereits praktiziert.

Andererseits sollte der Richtlinienentwurf nach Auffassung der Arbeitsgruppe Telekommunikation und Medien der Internationalen Datenschutzkonferenz anonyme Zahlverfahren (z. B. mittels Chip-Karten) für bestimmte Telekommunikationsdienste wie das Telefon und Datenübertragungsdienste verbindlich vorschlagen. Auch muß die Direktwerbung über Telefon und Telefax weitergehend eingeschränkt werden, als die Kommission dies bisher vorsieht. Ein effektiver Schutz der Privatsphäre ist nur möglich, wenn Telemarketing von der vorherigen schriftlichen Einwilligung des Betroffenen abhängig gemacht wird.

Neben der Schaffung rechtlicher Garantien für die informationelle Selbstbestimmung auf europäischer Ebene muß auch der ständige Prozeß der europa- und weltweiten Standardisierung (Normung) stärker als bisher Belange des Datenschutzes einbeziehen. Dies setzt voraus, daß die Anbieter und Anwender den Datenschutz als zwingenden Bestandteil einer bürgerfreundlichen Technik verstehen und nur datenschutzgerechte Produkte auf den Markt bringen bzw. einsetzen.

Rahmendienstvereinbarung für Berlin

Am 15. August 1991 ist die *Rahmendienstvereinbarung über den Einsatz und den Betrieb von digitalen Telefonnebenstellenanlagen*[57] in Kraft getreten[58]. Diese Vereinbarung schafft im Zusammenhang mit der gleichzeitig geschlossenen konkreten Dienstvereinbarung über ein Gebäude, in dem mehrere Senatsverwaltungen untergebracht sind, erfreulich eindeutige Regelungen über den datenschutzgerechten Umgang mit personenbezogenen Daten bei digitalen Telefonnebenstellenanlagen. Wichtig ist insbesondere die Festlegung, daß Gebührendaten nur auf der Grundlage einer gesetzlichen Regelung gespeichert und verarbeitet werden dürfen (§ 5 Abs. 4 Satz 2 RahmenDV). Damit haben die an dieser Vereinbarung beteiligten Stellen, die Senatsverwaltung für Inneres und der Hauptpersonalrat, die Konsequenz aus dem Berliner Datenschutzgesetz gezogen, das die Verarbeitung personenbezogener Daten ohne Einwilligung der Betroffenen nur aufgrund einer besonderen Rechtsvorschrift zuläßt. Die Verbindungsdaten sind nach der Rahmendienstvereinbarung nach Beendigung der Verbindung zu löschen. Das Mithören von Gesprächen und die Aufschaltung von Dritten ist nur mit Kenntnis und Zustimmung aller Teilnehmer/-innen im Einzelfall zulässig. Dies entspricht der neuesten Rechtsprechung des Bundesverfassungsgerichts[59].

[56] siehe 1.1
[57] Dienstblatt des Senats von Berlin I, S. 305 ff.
[58] Jahresbericht 1990, 2.3
[59] s. o. 1.1

2.4 Öffentlicher Dienst

Gesetzgebung in Sicht

In früheren Jahresberichten[60] hatten wir immer wieder auf die datenschutzrechtlichen Defizite bei der Verarbeitung von Personaldaten im öffentlichen Dienst hingewiesen. Leider ist ein Gesetzentwurf hierzu vom Bundestag nicht mehr verabschiedet worden. Wir gehen aber davon aus, daß die gesetzlichen Grundlagen in absehbarer Zeit vorliegen werden. Auch besteht Anlaß zu der Hoffnung, daß ein Gesetz über den *Arbeitnehmerdatenschutz* vom Bundestag noch im Lauf der 12. Legislaturperiode verabschiedet werden wird. Beide Gesetze würden in einem ganz besonders sensitiven Bereich des Persönlichkeitsrechts den Datenschutz verbessern.

Die Datenschutzbeauftragten der Länder und des Bundes haben Grundsätze zum Datenschutz der Arbeitnehmer im öffentlichen Dienst beschlossen[61]. Diese Grundsätze sollten bei der weiteren Entwicklung des Dienstrechts berücksichtigt werden. Sie sollten aber auch Signalwirkung für die Entwicklung des allgemeinen Arbeitnehmerdatenschutzes haben.

Rahmendienstvereinbarung

Am 8. August 1991 ist eine *Rahmendienstvereinbarung über die Personaldatenverarbeitung* zwischen der Senatsverwaltung für Inneres und dem Hauptpersonalrat in Kraft getreten[62] Gegenstand dieser Dienstvereinbarung ist es,

- einen generellen Rahmen für den Umfang, die Ziele und die Zulässigkeit der Anwendung von Verfahren zur automatisierten Verarbeitung personenbezogener Daten festzulegen, die zur Überwachung von Verhalten oder Leistung der Dienstkraft geeignet sein könnten,
- die Rechte der Dienstkräfte und des Personalrats bei der Personaldatenverarbeitung zu präzisieren und
- Grundsätze für den Datenschutz und die Datensicherung für Einzelverfahren vorzugeben.

Die Rahmendienstvereinbarung erfaßt alle Personalaktendaten und sonstigen personenbezogenen Daten (insbesondere Daten in Prüfungs-, Sicherheits- und Kindergeldakten, Prozeßakten, Vorgängen der Personalplanung, der Stellenausschreibung, des Auswahlverfahrens, der Stellenbewertung und der Geschäftsverteilung) in automatisierten Dateien.

Es ist zwar grundsätzlich zu begrüßen, daß diese Vereinbarung aufgrund einer Initiative des Hauptpersonalrats zustandegekommen ist und jetzt alle öffentlichen Stellen Berlins bereits vor Verabschiedung spezialgesetzlicher Normen im Personaldatenbereich bindet. Allerdings wurden unsere detaillierten Empfehlungen zur Verbesserung des Datenschutzes bei Abschluß dieser Dienstvereinbarung unberücksichtigt gelassen. So wird der Dateibegriff unzulässig eingeschränkt, das Erforderlichkeitsprinzip bei der Verarbeitung personenbezogener Daten nicht hinreichend berücksichtigt, und die Datenverarbeitung wird auch aufgrund dienst- bzw. arbeitsrechtlicher Entscheidungen des Arbeitgebers zugelassen. In diesen Punkten bleibt die Dienstvereinbarung hinter den gesetzlichen Datenschutzbestimmungen zurück.

Dienstvereinbarung gegen den Alkoholmißbrauch

Die Abteilung Personal und Verwaltung und der Personalrat eines Bezirksamts hatten Entwürfe für eine *„Dienstvereinbarung bei Verdacht auf Alkoholabhängigkeit von Mitarbeitern/Mitarbeiterinnen"* erarbeitet. Vorgesehen war, einen Suchtbeauftragten und weitere „interessierte Mitarbeiter" zu einer Arbeitsgruppe zusammenzufassen, die alkoholgefährdeten Bediensteten ihre Beratungsdienste anbieten und gleichzeitig auch Verbindung zu den Personalstellen, zum Personalrat u. a. im konkreten Einzelfall halten sollten. Aufgabe dieser Arbeitsgruppe sollte zum einen die Bekämpfung von Suchtkrankheiten am Arbeitsplatz allgemein, aber auch das konkrete Hilfsangebot an Betroffene zur Vermeidung dienst- bzw. arbeitsrechtlicher Konsequenzen sein.

[60] zuletzt im Jahresbericht 1989, 4.4
[61] Anlage 2.4
[62] Dienstblatt 1991 I, S. 300 ff.

Mangels konkreterer Rechtsnormen im Personaldatenbereich ist jede Form der Verarbeitung von Personaldaten nur im Rahmen der Zweckbestimmung des Dienstverhältnisses zulässig (§ 34 Abs. 2 BlnDSG i. V. m. § 28 Abs. 1 Nr. 1 BDSG).

Zwar ist im Rahmen der *Fürsorgepflicht des Dienstherrn* die Bekämpfung von Suchtkrankheiten am Arbeitsplatz eine wichtige Aufgabe im Rahmen des Arbeitsvertrages bzw. Dienstverhältnisses.

Die Dienstbehörde ist jedoch verpflichtet, den Personenkreis, der mit Personaldaten umgeht oder von ihnen Kenntnis erhält, so eng wie möglich zu begrenzen. Dies muß um so mehr dann gelten, wenn es sich um besonders sensible Krankheitsdaten der Betroffenen handelt. Schon aus diesem Grund begegnet die Datenweitergabe an die Arbeitsgruppe bzw. den Suchtbeauftragten erheblichen datenschutzrechtlichen Bedenken.

Die neu einzurichtende Arbeitsgruppe sollte sich aus einer nicht überschaubaren Anzahl „interessierter Mitarbeiter" zusammensetzen. Gerade weil jederzeit neue Personen hinzutreten oder ehemalige Mitglieder wegfallen könnten, wäre nicht sichergestellt, daß die unbedingt erforderliche Diskretion gewahrt bliebe.

Dagegen wäre die Betätigung der Arbeitsgruppe oder des Suchtbeauftragten im Bereich allgemeiner Schulung, Fortbildung und Warnung vor Alkoholgefahren datenschutzrechtlich nicht zu beanstanden. In diesem Zusammenhang könnten sie den Betroffenen auch Beratung anbieten. Es muß dem Betroffenen dabei aber - ohne Nachteile befürchten zu müssen - freistehen, darüber zu entscheiden, in welchem Umfang - wenn überhaupt - der Arbeitskreis oder der Suchtbeauftragte von seiner Alkoholkrankheit erfahren. Eine Information durch Dienst- oder Fachvorgesetzte „hinter dem Rücken des Betroffenen" wäre unzulässig. Zwar genügt nach § 6 Abs. 1 BlnDSG auch die Einwilligung des Betroffenen, dieser muß die Einwilligung jedoch frei von äußeren Zwängen erteilen. Aufgrund der Abhängigkeiten im Rahmen eines Dienstverhältnisses ist der Betroffene aber nicht frei in seiner Entscheidung, da er regelmäßig mit persönlichen Nachteilen rechnet, wenn er die Einwilligung verweigert. Insoweit bleibt der Beschäftigungsbehörde nur, auf die Möglichkeit des Angebots hinzuweisen, ohne daß sie im konkreten Einzelfall überprüfen dürfte, ob der Betroffene von diesem Angebot Gebrauch macht.

Erklärung zum Ortszuschlag

> Ledige Mütter werden regelmäßig einmal im Jahr von ihrer Personalstelle bei der Senatsverwaltung für Inneres aufgefordert, auf dem Vordruck „Erklärung zum Ortszuschlag . . ." anzugeben, ob sich ihre familiären Verhältnisse geändert haben.

Damit sollen die Frauen nicht ermahnt werden, doch nun endlich ihre familiären Verhältnisse „in geordnete Bahnen" zu lenken - auch wenn einige der Betroffenen diesen Rechtfertigungszwang empfinden. Es handelt sich vielmehr um die Überprüfung, ob der Ortszuschlag gekürzt werden muß. Hierbei wird offenbar den *ledigen Müttern* ein besonderes Mißtrauen entgegengebracht.

Obwohl sich aus den Bestimmungen des § 40 Bundesbesoldungsgesetz bzw. § 29 BAT eine permanente Nachweispflicht ergibt, wird im „Normalfall" auf eine Folgebefragung verzichtet. Da ohnehin alle Ortszuschlagsberechtigten in ihrem ersten Antrag schriftlich erklärt haben, jede in den angegebenen Verhältnissen eintretende Änderung, die sich auf die Höhe der genannten Zuschläge auswirkt, unverzüglich der personalaktenführenden Stelle anzuzeigen, ist es nicht erforderlich, bei Frauen mit nichtehelichen Kindern eine jährliche Zusatzbefragung vorzunehmen. Ungeachtet der Frage der Verhältnismäßigkeit dieser Maßnahme ist dies auch ein diskriminierender Eingriff in die Persönlichkeitsrechte dieser Personengruppe.

Die Senatsverwaltung für Inneres verweist darauf, daß der jährlichen Überprüfung des Fortbestehens der Anspruchsvoraussetzungen nicht nur Mütter nichtehelicher Kinder unterliegen, sondern alle ledigen und alle geschiedenen Beamtinnen und Beamten, die eine andere Person in die Wohnung aufgenommen haben und dieser Person zum Unterhalt gesetzlich oder sittlich verpflichtet sind. Durch die regelmäßige Überprüfung sollen Überzahlungen vermieden werden. Berlin sei an dieses bundeseinheitliche Verfahren gebunden.

Dies überzeugt nicht. Bei anderen Bediensteten wird auf eine Folgebefragung grundsätzlich verzichtet. Weder die bundeseinheitlichen Verfahrensregelungen noch die betreffenden Verwaltungsvorschriften[63] können den Eingriff in die Persönlichkeitsrechte in Form einer Ausgrenzung bestimmter Personengruppen rechtfertigen, zumal alle Ortszuschlagsberechtigten verpflichtet sind, relevante Änderungen im persönlichen Bereich unverzüglich anzuzeigen. Für diese sich wiederholende Datenerhebung fehlt nicht nur die Rechtsgrundlage, sondern auch die Erforderlichkeit. Die Erklärung wird auch nicht freiwillig abgegeben, da es sich um Personaldaten handelt, bei denen eine „echte" Freiwilligkeit der Betroffenen nicht vorausgesetzt werden kann.

Gegen eine regelmäßige Erinnerung an die Mitteilungspflichten durch Merkblätter - möglichst ohne Ausgrenzung bestimmter Personengruppen - gibt es aus datenschutzrechtlicher Sicht nichts einzuwenden. Dies würde auch einen deutlich geringeren Aufwand im Gegensatz zum gegenwärtigen Verfahren bedeuten, da ein Rücklauf nicht besonders beobachtet werden müßte.

Namenslisten mit Fremddaten

> Vom Personalrat der Lehrer und Erzieher eines Bezirksamtes sind wir darauf aufmerksam gemacht worden, daß sich in Personalakten von Lehrern Ausdrucke mit den Namen der gleichzeitig in den Vorbereitungsdienst übernommenen Lehramtsanwärter befinden.

Bereits früher hatten wir[64] im Zusammenhang mit den Friedensdemonstrationen an Berliner Schulen festgestellt, daß sich in Personalakten von Lehrern Listen befanden, aus denen die Namen der Mitglieder des Lehrerkollegiums hervorgingen, denen man Unterrichtsausfälle im genannten Zusammenhang anlastete. Dies ist unzulässig, weil die Aufnahme von Namen anderer Bediensteter eine unverhältnismäßige, für das betreffende Dienstverhältnis nicht erforderliche Speicherung von Fremddaten darstellt. Bei der Einsicht in die eigene Personalakte können Betroffene Informationen über andere Kollegen der Schule erhalten. Dadurch werden Personaldaten unbefugt offenbart.

Unsere Rechtsauffassung wurde in den vorläufigen Verwaltungsvorschriften über die Führung von Personalakten der Dienstkräfte des Landes Berlin vom 3. Dezember 1986[65] berücksichtigt. Zwar läßt sich auf der Grundlage der genannten Verwaltungsvorschriften eine korrekte Handhabung im Land Berlin erreichen. Jedoch werden solche Namenslisten zunehmend auch in Personalakten von Mitarbeitern - insbesondere der Lehramtsberufe - aufgefunden, die im Zusammenhang mit Bewerbungen aus den anderen Bundesländern nach Berlin gelangen. Vor dem Hintergrund, daß einheitliche bereichsspezifische Regelungen noch immer nicht vorhanden sind, haben wir den Datenschutzbeauftragten in den anderen Bundesländern empfohlen, sich der Problematik ebenfalls anzunehmen, um möglichst umgehend eine einheitliche, datenschutzgerechte Praxis zu erreichen.

Weitergabe von Bewerbungen

> Eine Bürgerin beschwerte sich bei uns über den Umgang mit ihren Bewerbungsunterlagen. Sie hatte sich um die Stelle als Angestellte im Vorzimmerdienst eines Senators beworben. Da die Stelle anderweitig vergeben wurde, hatte die Senatsverwaltung die Bewerbungsunterlagen zur Überraschung der Bürgerin an die Leiter nachgeordneter Behörden weitergegeben, ohne zuvor die Einwilligung der Betroffenen einzuholen. Die Dienststelle sah sich hierzu im Rahmen ihrer personalwirtschaftlichen Befugnisse als Hauptverwaltung berechtigt.

Dies ist unzutreffend. Die Weitergabe der Personaldaten hätte der ausdrücklichen Einwilligung der Betroffenen bedurft. Dies

63) Rundschreiben SenInn II Nr. 62/1985
64) Jahresbericht 1984, 4.3
65) Rundschreiben SenInn Nr. 88/1986

gilt insbesondere dann, wenn sich die Bewerbung ausdrücklich auf eine hervorgehobene Stelle bezieht, und nicht nur ganz allgemein eine Beschäftigung bei der ausschreibenden Behörde angestrebt wird. Ist von vornherein beabsichtigt, Bewerbungen auch bei anderen Stellen als der ausgeschriebenen zu berücksichtigen, muß dies bereits in der Ausschreibung zum Ausdruck kommen. Anderenfalls ist das Einverständnis der Betroffenen nachzuholen.

Zwar hatte die Senatsverwaltung im vermeintlichen Interesse der Betroffenen gehandelt, jedoch hatte die Bürgerin gerade die besondere Stelle im Vorzimmer des Senators im Auge und - wie ihre Beschwerde deutlich macht - sich durch die Weitergabe ihrer Bewerbungsunterlagen in ihren schutzwürdigen Belangen beeinträchtigt gefühlt. Die betreffende Senatsverwaltung hat zugesagt, zukünftig in jedem Fall die erforderlichen Einwilligungen vor einer Weitergabe von Bewerbungsunterlagen einzuholen.

Beihilfeheft - Bestandteil der Personalakte?

Ein Referendar hat bei Einsicht in seine Personalakte festgestellt, daß das sogenannte Beihilfeheft, in dem Gesundheitsdaten des Betroffenen enthalten sind, der Personalhauptakte beigefügt war. Uns wurde von der Personalstelle mitgeteilt, daß die gesamte Personalakte, d. h. auch das Beihilfeheft, bei einer Bewerbung der ausschreibenden Stelle mitübersandt werde, soweit der jeweilige Bewerber die Einsicht in seine Personalakte gestattet hat. Das Beihilfeheft sei notwendiger Teil der Personalakte und es stehe dem Beamten frei, Teile der Personalakten von seinem Einverständnis mit der Einsichtnahme durch Dritte auszunehmen.

Die Übermittlung personenbezogener Daten ist nach § 6 Abs. 1 BlnDSG nur aufgrund besonderer gesetzlicher Ermächtigung oder mit ausdrücklicher Einwilligung des Betroffenen zulässig. Eine normenklare gesetzliche Grundlage für die *Übermittlung von Beihilfeakten mit den Personalakten* gibt es nicht. Selbst wenn davon ausgegangen wird, daß §§ 28 ff BDSG i. V. m. § 34 Abs. 2 BlnDSG bis zur Schaffung normenklarer spezialgesetzlicher Regelungen als ausreichende Regelungen herangezogen werden können, weil es sich auch bei Beihilfedaten um Personaldaten handelt, ist deren Übermittlung „am Betroffenen vorbei" unzulässig. Gemäß § 34 Abs. 2 BlnDSG i. V. m. § 28 Abs. 1 Nr. 1 BDSG ist das Erheben und Übermitteln von personenbezogenen Daten nur im Rahmen der Zweckbestimmung des Dienstverhältnisses zulässig. Es ist im Rahmen der Zweckbindung des derzeitigen oder des zukünftigen Dienstverhältnisses nicht erkennbar, warum es erforderlich ist, bereits im Rahmen eines Bewerbungsvorgangs mit der Personalakte auch Beihilfevorgänge an die zukünftige Dienststelle zu übersenden. Beihilfeakten werden nur zum Zweck der Kostenerstattung erhoben und dürfen daher auch nur zu diesem Zweck genutzt werden.

Auch der umfassende *Personalaktenbegriff* ändert an dieser Bewertung nichts. Er resultierte ursprünglich aus der Zielrichtung, den Beamten ein weitgehendes Einsichtsrecht zu ermöglichen. Jedoch sah man damals keine schutzwürdigen Interessen des Beamten an einer Begrenzung[66], da das Recht auf informationelle Selbstbestimmung noch nicht anerkannt war. Aus heutiger Sicht ist zu beachten, daß Beihilfedaten zu den sensibelsten Daten eines Beamten gehören, die zum Schutz des informationellen Selbstbestimmungsrechts des Betroffenen bei einer Weitergabe einer besonders strengen Zweckbindung unterliegen müssen. Diese datenschutzrechtlich gebotene weitgehende Geheimhaltung ist - auch unter Wahrung des genannten umfassenden Personalaktenbegriffs - möglich, indem man die Beihilfedaten in einer getrennten Beiakte führt, die der Personalakte bei einer Übermittlung entnommen wird. Dementsprechend sieht auch die Neufassung der Beihilfevorschriften vor, daß Beihilfedaten geheimzuhalten sind und nur bei gesetzlicher Berechtigung oder mit *ausdrücklichem* Einverständnis des Betroffenen weitergegeben werden dürfen.

Die pauschale Einwilligung in die Weitergabe der Personalakte reicht hierfür nicht aus.

Frauenförderplan

Um einen Frauenförderplan gemäß § 4 Landesantidiskriminierungsgesetz (LADG) entwickeln zu können, verlangte die Frauenbeauftragte einer Fachhochschule einen detaillierten Überblick über die berufliche Situation aller weiblichen Beschäftigten. Hierzu hatte die Frauenbeauftragte einen sehr umfangreichen Fragenkatalog entwickelt, der eine eingehende Auswertung der jeweiligen Personalakten erforderlich gemacht hätte.

Die Erforderlichkeit der Übermittlung im Rahmen des Dienstverhältnisses ist weder nach § 4 LADG noch nach dem Berliner Hochschulgesetz (BerlHG) feststellbar. Gemäß § 59 BerlHG - Stellung und Aufgaben der Frauenvertreterin im Hochschulbereich - hat diese „unter Beachtung datenschutzrechtlicher Belange Akteneinsicht", also nur insofern eine solche zur Aufgabenerfüllung erforderlich ist. Die Entwicklung eines Frauenförderplanes ist jedoch keine der Frauenbeauftragten zugeschriebene Aufgabe. Sie ist hierbei lediglich zu beteiligen. Darüber hinaus reicht zur Erstellung eines Frauenförderplanes die Nutzung anonymisierter Daten aus.

Aufbewahrung personenbezogener Sachakten

Ein Fachschullehrer beklagte sich darüber, daß sein Schulleiter außerhalb der Personalakten in Form einer „Lose-Blatt-Sammlung" weitere persönliche Daten über die Bediensteten aufbewahrt. So waren in dieser Weise zu seiner Person schriftliche Beschwerden von Schülern über seine Unterrichtsführung und sein Verhalten abgeheftet worden.

Bereits früher hatten wir darauf hingewiesen[67], daß es eine Reihe von Vorgängen gibt, die besonderen, von dem Beamten- oder Arbeitsverhältnis sachlich zu trennenden Zwecken dienen. Diese Vorgänge sind in Sachakten einzuordnen, die keine unerlaubte Personalnebenakten darstellen.

Die Schulleitung ist zunächst gehalten, Schülerbeschwerden zum Nachweis des Eingangs (Erteilung einer Eingangsbestätigung, Dokumentation der organisatorischen Maßnahmen) aufzubewahren. Damit werden die Datenschutzrechte der Betroffenen nicht eingeschränkt. So ist Betroffenen entsprechend § 16 Abs. 4 BlnDSG Einsichtnahme zu gewähren bzw. oder Auskunft zu erteilen, wenn die Daten mit Daten Dritter (hier z. B. der Beschwerdeführer) verbunden sind.

Die Vorgänge sind zu vernichten, wenn ihre Kenntnis für die Schulleitung nicht mehr erforderlich ist (§ 17 BlnDSG). Dabei dürfen allerdings schutzwürdige Belange Betroffener - wie hier beim Beschwerdeführer - nicht beeinträchtigt werden. In diesem Fall sind die Vorgänge zu sperren, d. h. sie dürfen ohne Einwilligung der Betroffenen nicht mehr genutzt werden.

Fehlzeitenerfassung

Um Material für die mögliche Kündigung von Bediensteten aufgrund häufiger kurzfristiger Erkrankungen zu erhalten, wurden die Dienststellen der BVG in einer Direktionsverfügung angewiesen, jeden einzelnen Erkrankungsfall aufzuzeichnen. Dabei sollen auch die Folgen (z. B. Störungen im Betriebsablauf, Beschwerden von Kunden, Überlastung der übrigen Mitarbeiter) notiert werden.

Es gibt immer wieder Unsicherheiten, in welcher Weise und in welchem Umfang Fehlzeitenerfassungen zulässig sind. Angesichts der Vielzahl von Zwecken, die der Dienstherr damit verfolgen kann, ist es unmöglich, allgemein festzulegen, welche Daten unter welchen Voraussetzungen verarbeitet werden dürfen. Auszugehen ist allerdings davon, daß eine Fehlzeitenerfassung dem Arbeitgeber oder Dienstherrn nicht grundsätzlich verwehrt werden kann, da diese zu vielfältigen Zwecken unerläßlich ist (Abrechnung, Überwachung von Krankmeldungen, Lohnfortzahlungsfristen).

[66] BVerwGE 15, S. 14 f.

[67] Jahresbericht 1984, 4.3

Folgende allgemeine Grundsätze können festgestellt werden:

- Jeder Fehlzeitenerfassung sollte eine konkrete Zweckbestimmung vorangehen.
- Nur in dem hierzu konkret erforderlichen Umfang dürfen die Daten erfaßt werden, wobei das *Verbot der Vorratsspeicherung* zu beachten ist. Es reicht nicht aus, daß die Daten nur möglicherweise benötigt werden. Sofern beispielsweise Fehlzeiten zur Rechtfertigung späterer krankheitsbedingter Kündigungen herangezogen werden sollen, dürfen nicht etwa sämtliche Zeiten undifferenziert erfaßt werden. Die Speicherung ist vielmehr erst zulässig, wenn eine begründete Vermutung besteht, daß die Fehlzeiten eine spätere krankheitsbedingte Kündigung rechtfertigen können. Dabei müssen auch der Kreis der betroffenen Dienstkräfte (z. B. Ausschluß von unkündbaren Bediensteten beim Zweck „Kündigung") und der Umfang der Daten berücksichtigt werden.
- Es sind Vorkehrungen zu treffen, die gewährleisten, daß die Daten nur für den ursprünglichen Zweck genutzt werden, insbesondere nicht zu Vergleichen zwischen den einzelnen Bediensteten etc. herangezogen werden. Bereits bei der Erfassung sollte deshalb der „ungefährlichere" Datenträger verwendet werden (Beispiel: Listen über kurze Fehlzeiten statt Kartei über alle Arbeitnehmer). Eine automatisierte Datei muß bereits im Programm entsprechende Vorkehrungen (Fristenvormerkungen, Sperren) enthalten, die - auch vom Personalrat - überprüfbar sind.
- Nach § 85 Abs. 1 Nr. 13 Personalvertretungsgesetz ist die Mitbestimmung des Personalrats zu beachten, soweit die Daten automatisiert verarbeitet werden. Für dieses Recht läßt das Bundesarbeitsgericht in ständiger Rechtsprechung die objektive Eignung zur Überwachung genügen, eine subjektive Überwachungsabsicht des Arbeitgebers ist nicht erforderlich.
- Nach dem Volkszählungsurteil ist wesentlicher Inhalt des informationellen Selbstbestimmungsrechts, daß der Betroffene weiß, was über ihn wo gespeichert ist. Die Bediensteten sind deshalb über die jeweiligen Erfassungen zu informieren.
- Zugriffsberechtigt sind im Rahmen ihrer jeweiligen Zuständigkeit im jeweils erforderlichen Umfang ausschließlich Dienstvorgesetzte sowie die mit dienstrechtlichen Aufgaben betrauten Mitarbeiter wie Personalsachbearbeiter und Büroleiter[68]. Eine kurzfristige Aufzeichnungsmöglichkeit für einige Tage durch Fachvorgesetzte, um den ordnungsgemäßen Betriebsablauf und Arbeitseinsatz planen bzw. koordinieren zu können, bleibt hiervon unberührt.

2.5 Technik und Organisation

Zu den technischen und organisatorischen Aspekten des Datenschutzes gehört insbesondere die Schaffung aller Voraussetzungen für die Prüfbarkeit, Durchschaubarkeit und Beherrschbarkeit der Datenverarbeitung. Ohne Transparenz können informationstechnische Systeme nicht verantwortbar eingesetzt werden. Wir haben uns deshalb bei Prüfungen von ADV-Verfahren besonders aufmerksam auch immer der Frage gewidmet, ob die in den Datenschutzgesetzen geforderte Kontrollierbarkeit der ordnungsgemäßen Anwendung der Datenverarbeitungsprogramme sichergestellt ist. In allzu vielen Fällen war diese Frage zu verneinen, weil die Programmdokumentationen unvollständig oder inaktuell waren, weil keine ordnungsgemäße Freigabeerklärung die Übernahme der Verantwortung durch die Anwender dokumentierte, weil keine zuverlässige Datenträgerverwaltung die Vollständigkeit und Authentizität der Datenträger garantierte oder weil nicht einmal eine Übersicht über eingesetzte IuK-Systeme bestand. Die Datenschutzgesetze konkretisieren die Transparenzanforderungen dadurch, daß sie formelle Pflichten vorsehen, die die Datenschutzkontrolle erst ermöglichen. Dazu gehörten schon immer die Meldepflicht zum Dateienregister beim Datenschutzbeauftragten sowie die Führung interner Dateienübersichten bei den verarbeitenden Stellen.

2.5.1 Umsetzung formaler Vorschriften des neuen Berliner Datenschutzgesetzes

Mit dem neuen Datenschutzgesetz sind die formellen Anforderungen an die datenverarbeitenden Stellen erweitert worden, die die Voraussetzungen für interne und externe Kontrollen sowie für die Informationsmöglichkeiten der Betroffenen verbessern sollen:

- Das schon im früheren Berliner Datenschutzgesetz verlangte *interne Verzeichnis der personenbezogenen Dateien* ist in § 19 Abs. 2 BlnDSG inhaltlich konkretisiert und erweitert worden.
- Zusätzlich wird in § 19 Abs. 4 BlnDSG ein *Geräteverzeichnis* verlangt, das ebenfalls inhaltlich konkretisiert wird und in einer Rechtsverordnung näher zu regeln ist.
- Die schon nach bisherigem Gesetz vorgesehene Meldung zum öffentlich zugänglichen *Dateienregister* beim Berliner Datenschutzbeauftragten wird in § 25 BlnDSG sowohl inhaltlich als auch hinsichtlich der meldepflichtigen Dateien durch die Einschränkung von Ausnahmeregelungen wesentlich erweitert.
- Die datenverarbeitenden Stellen haben nach § 19 Abs. 5 BlnDSG *behördliche Datenschutzbeauftragte* formell zu bestellen, deren Aufgaben im Berliner Datenschutzgesetz und aufgrund einer entsprechenden Verweisung im Bundesdatenschutzgesetz (§§ 36, 37) bestimmt sind.

Dateienregisterordnung

Die Umsetzung der §§ 19 Abs. 4 und 25 BlnDSG ist meiner Rechtsverordnung näher zu bestimmen. Da die alte Datenschutzregisterordnung den Anforderungen des neuen Berliner Datenschutzgesetzes nicht mehr genügt, wurde in Abstimmung mit uns eine neue *Dateienregisterordnung* für die Meldungen zum bei uns zu führenden Dateienregister entworfen. Das Dateienregister wird in Zukunft aus dem *Dateien-* und dem *Geräteverzeichnis* bestehen. Zwischen beiden Verzeichnissen besteht eine Beziehung, die den Dateien die Geräte zuordnen, mit denen sie verarbeitet werden. Für das neue Dateienregister waren auch neue Meldeformulare zu entwickeln.

Die Dateienregisterordnung wird voraussichtlich im Frühjahr 1992 in Kraft treten. Dann werden die datenverarbeitenden Stellen Meldeformulare für beide Verzeichnisse beim Landesverwaltungsamt abfordern können. Wegen des größeren Schwierigkeitsgrades beim Ausfüllen der Meldeformulare werden wir eine Ausfüllanleitung an die datenverarbeitenden Stellen verteilen.

Bestellung behördlicher Datenschutzbeauftragter

Mit dem neuen Berliner Datenschutzgesetz wurde den datenverarbeitenden Stellen die Bestellung eines *behördlichen Datenschutzbeauftragten* zwingend vorgeschrieben. Die Aufgaben des behördlichen Datenschutzbeauftragten leiten sich im wesentlichen aus dem Berliner Datenschutzgesetz und dem Bundesdatenschutzgesetz ab:

- Sicherstellung der Ausführung von Datenschutzvorschriften;
- Gewährleistung der ordnungsgemäßen Anwendung der ADV-Programme;
- Schulung der Mitarbeiter in Datenschutzfragen;
- beratende Mitwirkung bei der Personalauswahl;
- Umsetzung der formellen Vorschriften zu internen Übersichten und Meldepflichten;
- Verpflichtungen auf das Datengeheimnis;
- Aufbau einer internen Datenschutzinfrastruktur;
- interne Beratung und Kontrollen;
- Auskunftserteilung und Benachrichtigungen gem. § 16 BlnDSG;
- Kontaktpflege mit externen Kontroll- und Beratungsinstanzen
  - hier speziell mit dem Berliner Datenschutzbeauftragten.

[68] Jahresberichte 1986, 4.3; 1984, 4.3

Wir haben ein Merkblatt entwickelt, in dem die Aufgaben der behördlichen Datenschutzbeauftragten näher beschrieben worden sind (Anlage 4).

Damit behördliche Datenschutzbeauftragte ihren Aufgaben sinnvoll nachgehen können, müssen sie bestimmte *persönliche Voraussetzungen* mitbringen. Gesetzlich wird in § 36 Abs. 2 BDSG verlangt, daß sie die für ihre Aufgaben erforderliche Fachkunde und Zuverlässigkeit aufweisen müssen. Das bedeutet, daß sie im Idealfall Fachkunde in folgenden Gebieten aufweisen sollten:

1. Datenschutzrecht (Berliner Datenschutzgesetz, Bundesdatenschutzgesetz, spezialrechtliche Vorschriften, z. B. Sozialgesetzbuch X);
2. rechtliche Vorschriften für die im Zuständigkeitsbereich des behördlichen Datenschutzbeauftragten zu bearbeitenden Verwaltungsaufgaben;
3. Kenntnisse über die im Zuständigkeitsbereich eingesetzten IuK-Systeme;
4. spezielle Kenntnisse zum ordnungsgemäßen, sicheren und datenschutzgerechten Einsatz von IuK-Technik.

Dieser Idealfall ist in einer Person in der Regel nicht zu vereinigen. Ein behördlicher Datenschutzbeauftragter sollte sich deshalb ausreichende Kenntnisse zum Datenschutzrecht und zum datenschutzgerechten Technikeinsatz aneignen, um seinen routinemäßigen Aufgaben nachgehen zu können. Die übrigen Kenntnisse benötigt er nur von Fall zu Fall. Er sollte sich dann des Sachverstandes der jeweiligen Fachleute im Hause bedienen und entsprechende Ansprechpartner auswählen, mit denen er eine fallbezogene Kooperation eingehen kann.

Es ist selbstverständlich, daß nur persönlich integre Mitarbeiter zum Datenschutzbeauftragten bestellt werden dürfen. Es dürfen also keine Zweifel an der persönlichen Zuverlässigkeit bestehen.

Für die Zuverlässigkeit ist aber auch Voraussetzung, daß keine Interessenkonflikte mit anderen Aufgaben in der Person des behördlichen Datenschutzbeauftragten liegen dürfen. Er soll nicht in die Lage versetzt werden müssen, Dinge zu kontrollieren, die in seinen Verantwortungsbereich in anderer Funktion fallen.

In der Regel (Bezirksämter, Senatsverwaltungen, IuK-intensive Verwaltungen) sollte dieses Problem deshalb nicht auftreten, weil der behördliche Datenschutzbeauftragte aufgrund der Vielfalt seiner Aufgaben, die er verantwortlich wahrzunehmen hat, kein weiteres Amt mehr ausüben kann. In diesem Falle wäre er aus seinem bisherigen Aufgabengebiet auszugliedern und unmittelbar der Behördenleitung (in Bezirksämtern dem Bürgermeister oder besser dem Bezirksamtsgremium) zu unterstellen.

Für den Fall, daß ein behördlicher Datenschutzbeauftragter noch andere organisatorische Aufgaben hat, ist es mit dem Amt als Datenschutzbeauftragter nicht vereinbar, wenn er darüber hinaus ein Amt ausübt, in dem er verantwortlich Sachgebiete leitet, die einer besonderen Aufmerksamkeit des behördlichen Datenschutzbeauftragten bedürften. Dies ist der Fall, wenn er die Verantwortung für die Gestaltung des IuK-Einsatzes, für den Betrieb von Rechenzentren, für personenbezogene Datenbestände größerer Bedeutung trägt. Dies bedeutet, daß

- politische Entscheidungsträger (Senatoren, Staatssekretäre, Bürgermeister, Stadträte),
- Leiter von sonstigen Landesbehörden,
- DV-Leiter und Leiter von Organisationsstellen,
- Leiter von Personalabteilungen, -referaten oder -stellen,
- Leiter von Anwendungsbereichen mit intensiver personenbezogener IuK-Anwendung, z. B. Leiter der Bezirkseinwohnerämter,

nicht zu behördlichen Datenschutzbeauftragten bestellt werden dürfen, wohl aber nichtleitende Mitarbeiter aus diesen Bereichen.

Ferner ist es mit dem Amt als behördlicher Datenschutzbeauftragter nicht vereinbar, wenn er in anderen Rechtsgebieten mit Personenbezug aufgrund seiner Funktion parteilich ist, d. h. auch

- Personalräte,
- Frauenbeauftragte,
- Ausländerbeauftragte

u. ä. sollten nicht zu behördlichen Datenschutzbeauftragten bestellt werden.

Der *Pflicht, behördliche Datenschutzbeauftragte zu ernennen,* ist bisher nur eine Minderheit der Behörden nachgekommen. Bei den großen Verwaltungen gilt dies vor allem für die meisten Bezirksämter, die einerseits wegen der Vielzahl der Rechtsgebiete, die bei ihnen die Verarbeitung personenbezogener Daten erforderlich machen, und andererseits wegen des Umfangs und der Vielfalt von IuK-Systemen nicht darum herumkommen werden, Datenschutzbeauftragte zu bestellen, die sich dieser Aufgabe ausschließlich zu widmen haben. In Gesprächsrunden und Schriftwechseln haben sie immer wieder deutlich gemacht, daß es ihnen ohne Bereitstellung einer gesonderten Stelle nicht möglich sei, eine Benennung vorzunehmen, die den Anforderungen des Berliner Datenschutzgesetzes genügt.

Als ein Bezirksamt ein von uns an den behördlichen Datenschutzbeauftragten gerichtetes Schreiben mit dem Hinweis zurücksandte, daß aufgrund der Unklarheiten über Aufgabenumfang und stellenplanmäßiger Berücksichtigung von der gesetzlich vorgeschriebenen Bestellung eines Datenschutzbeauftragten abgesehen worden sei, haben wir dies zum Anlaß für eine formelle Beanstandung genommen. Die Aufsichtsbehörde unterstützte unser Anliegen, indem sie den Bezirk auf seine gesetzliche Verpflichtung hinwies. Der Bezirk machte deutlich, daß er seinen gesetzlichen Verpflichtungen nachkommen möchte, aufgrund der gegebenen Stellensituation dies aber nur formell, nicht aber mit der auch aus seiner Sicht notwendigen Ausstattung in personeller und sachlicher Hinsicht erfolgen könne. Ein Hinweis auf die bessere Situation der stellenmäßig komfortabler ausgestatteten Senatsverwaltungen fehlte nicht.

Um betroffene Behörden, allen voran die Bezirksämter, bei der Bestellung der behördlichen Datenschutzbeauftragten zu unterstützen, haben wir die für die Stellenplangestaltung zuständige Senatsverwaltung für Inneres gebeten, die Berücksichtigung des behördlichen Datenschutzbeauftragten in den behördlichen Stellenplänen zu prüfen.

Die Senatsverwaltung für Inneres hat eine solche Prüfung abgelehnt. Sie weist zu Recht darauf hin, daß die Verpflichtung zur Durchführung des Berliner Datenschutzgesetzes und damit auch zur Bestellung eines behördlichen Datenschutzbeauftragten für die Behörden unabhängig davon besteht, ob hierfür eine zusätzliche Stelle zur Verfügung gestellt wird. Es sei bei der Vorbereitung des Berliner Datenschutzgesetzes unterstellt worden, daß diese Aufgabe von dem in den Behörden vorhandenen Personal miterledigt werden kann. Die dramatische Verschlechterung der Finanzlage Berlins ließe es jetzt nicht zu, allgemein Stellen für behördliche Datenschutzbeauftragte einzurichten. Die Stellenplanbehörde erwartet daher, daß die angemessene Entlastung des behördlichen Datenschutzbeauftragten durch Aufgabenumverteilung in der jeweiligen Organisationseinheit erfolgt. Die jeweilige Personalwirtschaftstelle müsse zusätzlich bei Bedarf durch Ausschöpfung aller im eigenen Stellenplan vorhandenen Möglichkeiten zur Entlastung des behördlichen Datenschutzbeauftragten beitragen. Erst wenn diese Möglichkeiten ausgeschöpft seien, ohne daß die notwendige Entlastung erreicht sei, sei die Senatsverwaltung für Inneres zu weitergehenden Prüfungen bereit.

2.5.2 Unsicherer Umgang mit Bürgerdaten

Die Prüfungen und Erfahrungen zur Sicherheit der Daten vor unbefugtem Zugriff und zur Ordnungsmäßigkeit der Datenverarbeitung werden im Zusammenhang mit anderen datenschutzbezogenen Fragen behandelt, denn in den meisten Prüf- und Beratungsfällen lassen sich rechtliche, technische und organisatorische Aspekte kaum sinnvoll voneinander trennen. Zwei Beispiele zur fehlenden Sicherheit nichtautomatisierter Datenbestände und zum sorglosen Umgang mit moderner Informationstechnik seien hier gesondert dargestellt:

Aktenlagerung während Renovierungsarbeiten bei einem Tiefbauamt

Aufgrund eines Hinweises einer Fraktion einer Bezirksverordnetenversammlung haben wir die Aktenunterbringung im Tiefbauamt eines Bezirksamtes während Renovierungsarbeiten überprüft. Der Hinweis erwies sich als vollkommen gerechtfertigt:

In einem Flur des Tiefbauamtes lagen Aktenordner, Hefter und Listen offen und für jedermann zugänglich auf Tischen und Konsolen, aber auch in offenen Kartons auf dem Fußboden. Weitere Unterlagen waren in Schränken untergebracht, in deren Schlössern die Schlüssel steckten, so daß Unbefugte ohne große Mühe die dort aufbewahrten Unterlagen hätten lesen, kopieren, verändern oder entfernen können.

Bei Stichproben haben wir u.a. folgende Unterlagen mit personenbezogenen Angaben vorgefunden:

- Eingaben von Bürgern bezüglich der Einrichtung von Rad- und Gehwegen;
- Widersprüche bei Straßenbenennungen (offenbar aus einer Bürgerinitiative, da die Schreiben alle gleichlautenden Text enthielten);
- Schriftverkehr bezüglich des Neubaus einer Straße mit Rechnungen und Abschlagszahlungen.

Wir haben die im Tiefbauamt des Bezirksamtes praktizierte Form der Aufbewahrung personenbezogener Unterlagen während der Renovierungsarbeiten beanstandet. Die ungesicherte Unterbringung der ausgelagerten Datensammlungen auf dem Flur verstieß gegen datenschutzrechtliche Vorschriften, da keine Maßnahmen getroffen worden waren, um den Zugriff Unbefugter zu verhindern (§ 5 Abs. 2 BlnDSG).

Zur Beseitigung der beschriebenen Mängel und zur Verbesserung des Datenschutzes haben wir empfohlen, bei künftigen Umzugs-, Umbau- und Renovierungsmaßnahmen für die Auslagerung von Unterlagen mit personenbezogenen Daten einen Lagerraum vorzusehen, damit dort eine Aufbewahrung unter sicherem Verschluß erfolgen kann. Weiterhin haben wir angeregt, die Aufbewahrungsregelungen für derartige Auslagerungen schutzbedürftiger, weil personenbezogener Unterlagen schriftlich festzulegen und in geeigneter Weise im Hause bekannt zu machen. Das Tiefbauamt hat die sofortige Umsetzung unserer Empfehlungen zugesagt.

Einsatz von Sicherheits-Software

Die bei der *Koordinierungsstelle Verwaltungseinheit (KVE)* eingerichtete *Personalbörse* hat die Aufgabe, Mitarbeiter der Senatsverwaltungen und der Bezirksämter aus dem Westteil der Stadt bei angezeigtem Interesse in entsprechende Positionen bei Bezirksämtern und anderen öffentlichen Stellen im Ostteil der Stadt zu vermitteln. Zu diesem Zweck werden bei der KVE personenbezogene Daten der Interessenten gespeichert wie z. B. Geschlecht, Name, Vorname, Geburtsjahr, Titel, derzeitige Dienstbehörde, private Wohnanschrift, Bearbeiterfunktion im Rahmen der letzten Tätigkeit. Zusätzlich werden weitere Daten wie z. B. Angabe einer Schwerbehinderung, Familienstand, Anzahl der Kinder abgefragt, die jedoch als nicht unbedingt erforderlich für die Vermittlung gekennzeichnet sind.

Diese Daten werden in einem PC-Netz bei der Senatsverwaltung für Inneres verarbeitet. Zusätzlich werden Auszüge aus dieser Datenbank wegen einer räumlichen Trennung des Netzwerkes und den Büros der Personalbörse auf Disketten in Einzelplatz-Personalcomputern gehalten, die sich in den Büroräumen der KVE-Personalbörse befinden. Diese PC stellen einen Mehrpersonenarbeitsplatz dar.

Eine Datenübermittlung erfolgt zum einen innerhalb der Senatsverwaltung für Inneres zwischen dem Netz und den Einzelplätzen mittels Disketten und zum anderen in Listenform durch Botengänge zwischen der Innenverwaltung und den jeweiligen Stellen im Ostteil der Stadt. Die Übergabe der Listen mit den Bewerberdaten wird quittiert.

Bei Feststellung der Nichtverwendbarkeit eines Bewerbers bzw. nach erfolgreicher Vermittlung des Bewerbers, werden die Daten auf den Disketten logisch gelöscht.

Die im Netzwerk gespeicherte Datenbank bot auf Grund der Netzsicherung im Rahmen einer technisch-organisatorischen Prüfung mit Ausnahme geringer Mängel keinen Anlaß zur Sorge. Anders verhielt sich das mit der Sicherung der Einzelplatz-Geräte in den Büros der Personalbörse. Hier wurden im Rahmen derselben datenschutzrechtlichen Überprüfung erhebliche Mängel gegenüber der technisch-organisatorischen Gerätesicherung nach § 5 Abs. 3 BlnDSG festgestellt.

Die beiden Einzelplatz-PC sind jeweils mit einer 30 MB Festplatte ausgerüstet, die durch Schlüsselschalter blockierbar ist. Allerdings existieren keine Schlüssel mehr für diese Rechner.

Zum Zeitpunkt der Prüfung wurde auf beiden Geräten eine Datenschutzsoftware eingesetzt, die den technisch-organisatorischen Anforderungen des § 5 Abs. 3 BlnDSG bei weitem nicht gerecht wird. Die Innenverwaltung sagte bei der Prüfung zu, bereits am nächsten Tag eine geeignete, die Vorgaben des § 5 Abs. 3 BlnDSG berücksichtigende Datenschutzsoftware zu installieren.

Im Rahmen der Stellungnahme der Innenverwaltung zu unserer Mängelfeststellung wurde uns zu unserem Befremden mitgeteilt, daß die zum Zeitpunkt der Prüfung bereits vorhandene geeignete Datenschutzsoftware bisher nicht installiert worden sei, da die Programmdisketten zur Erstellung einer neuen Programmversion (Upgrade) an den Hersteller zurückgesandt worden seien. Mit einer Installation dieser Software sei nun zu einem späteren Zeitpunkt zu rechnen.

Nach Ablauf dieser neuen Frist haben wir die KVE-Personalbörse erneut auf die Einhaltung der technisch-organisatorischen Maßnahmen zum Datenschutz nach § 5 Abs. 3 BlnDSG überprüft und festgestellt, daß die angekündigte Installation der geeigneten Datenschutzsoftware immer noch nicht erfolgt war.

Unklar ist, warum diese Software nicht – wie von der Innenverwaltung zugesagt – im September 1991 installiert wurde, da die beiden Programmpakete mit einer Hardware-Bootschutz-Karte vorhanden waren und umgehend installierbar gewesen wären. In diesem Fall hätte das Upgrading trotzdem wie beabsichtigt durchgeführt werden können.

2.5.3 Formulare und Postverkehr

Aufklärung bei der Datenerhebung

Das neue Berliner Datenschutzgesetz hat auch Auswirkungen auf die *formularmäßige Datenerhebung*, die nun ebenfalls als Phase der Datenverarbeitung definiert ist. Personenbezogene Daten sind grundsätzlich beim Betroffenen zu erheben und die erhebenden Stellen haben gegenüber dem Betroffenen verschiedene Aufklärungspflichten. So ist er in geeigneter Weise über den Zweck und bei beabsichtigten Übermittlungen über den Empfänger der Daten aufzuklären. Sofern die Daten beim Betroffenen aufgrund einer durch Rechtsvorschrift festgelegten Auskunftspflicht erhoben werden, ist er auf die Rechtsgrundlage hinzuweisen, im übrigen darauf, daß er die Auskunft verweigern kann. Sind die Angaben für die Gewährung einer Leistung erforderlich, so ist der Betroffene über die möglichen Folgen einer Nichtbeantwortung aufzuklären.

Ausnahmsweise dürfen bei Behörden und sonstigen öffentlichen Stellen die Daten ohne Kenntnis des Betroffenen nur erhoben werden, wenn dies eine Rechtsvorschrift erlaubt, der Betroffene in diese Form der Erhebung ausdrücklich eingewilligt hat oder eine rechtzeitige Kenntnisgabe an den Betroffenen nicht möglich ist und kein Anhaltspunkt dafür besteht, daß schutzwürdige Belange des Betroffenen beeinträchtigt werden. Dabei ist zu der letzten Alternative anzumerken, daß diese Variante äußerst restriktiv anzuwenden ist, weil die erhebende Stelle immer erklären muß, warum sie nicht beim Betroffenen selbst erhebt bzw. dessen Einwilligung einholt.

Bei privaten Dritten dürfen ausnahmsweise ohne Kenntnis des Betroffenen nur aufgrund einer besonderen Rechtsvorschrift Daten über ihn erhoben werden.

Das neue Berliner Datenschutzgesetz hat sich eine Stärkung der Bürgerrechte zum Ziel gesetzt. Das kommt auch in der

Benachrichtigungspflicht nach § 16 Abs. 2 BlnDSG zum Ausdruck. Danach ist der Betroffene von der Tatsache der Speicherung seiner personenbezogenen Daten in einer automatisierten Datei schriftlich zu benachrichtigen. Diese Benachrichtigung kann - und sollte zweckmäßigerweise immer - zusammen mit der Erhebung erfolgen.

Mit dieser neuen Rechtslage tut sich die Verwaltung noch schwer. Die Senatsverwaltung für Inneres, mit der wir seit mehreren Jahren wegen der Einheitsvordrucke für den Personalbereich und das Personenstandswesen verhandeln, hat sich trotz mehrerer Erinnerungen zu diesem Punkt bisher überhaupt noch nicht geäußert.

Die Senatsverwaltung für Schulwesen meint zu einem Formular, daß es für die Datenerhebung zwar keine bereichsspezifische Rechtsgrundlage gebe, aber derzeit unter Hinweis auf § 34 Abs. 1 BlnDSG sich die Befugnis zur Erhebung schlicht aus der Notwendigkeit des Funktionierens der Schule ergäbe. Der unterbliebene Hinweis auf eine Auskunftspflicht sei im übrigen datenschutzrechtlich irrelevant.

Diese Auffassung ist nicht nachvollziehbar. Nach § 34 Abs. 1 BlnDSG muß die Verarbeitung zur ordnungsgemäßen Aufgabenerfüllung erforderlich sein. Diese Erforderlichkeit muß dem Betroffenen bei der Datenerhebung aber gleichwohl erklärt werden.

Auch bei den geprüften Vordrucken anderer Verwaltungen fehlen fast durchgängig die aufklärenden Hinweise nach dem neuen Datenschutzgesetz.

Alle in der Berliner Verwaltung verwandten Vordrucke, mit denen personenbezogene Daten erhoben werden, sind bei der nächsten Neuauflage der neuen Rechtslage hinsichtlich der Aufklärungspflichten anzupassen.

Solange die Hinweise in den Formularen fehlen, wird die Verwaltung keinesfalls von der Aufklärungspflicht entbunden. Sie hat vielmehr den Betroffenen mündlich aufzuklären und wenn es im Einzelfall erforderlich sein sollte, diese Hinweise in einem gesonderten Aktenvermerk festzuhalten, weil nur die Schriftform bei Streitigkeiten (z. B. Anfechtung eines Verwaltungsaktes) den Nachweis in die erfolgte Aufklärung erbringen kann.

Vertraulichkeit bei der Post

Der Postaustausch in der Berliner Verwaltung hat uns in der Vergangenheit wiederholt beschäftigt[69]. Wir fordern seit Jahren - und das entspricht einem Bedürfnis vieler Bürger -, daß Schreiben an Behörden - zumal wenn sie höchstpersönliche Angaben enthalten - möglichst nahe an der zuständigen Stelle geöffnet werden. Das würde im Gegensatz zur gegenwärtigen Praxis, bei der die in einer Behörde eingehenden Schreiben zentral geöffnet und dann regelmäßig unverschlossen weitergeleitet werden, einen datenschutzgerechten Umgang in diesem Bereich sicherstellen. Der unüberschaubare Kreis von Mitarbeitern und unbefugten Dritten, denen der Inhalt der Schreiben zur Kenntnis gelangen könnte, würde stark begrenzt werden.

Dem hat sich die Senatsverwaltung für Inneres bisher nicht angeschlossen und verweist in diesem Zusammenhang auf bestehende Verwaltungsvorschriften, die den verschlossenen Versand bis zum zuständigen Sachbearbeiter auch bei der gegenwärtigen Praxis sicherstellen sollen. Dies ist für den Bürger nicht akzeptabel, weil bei ihm nicht fundierte Kenntnisse von Verwaltungsvorschriften vorausgesetzt werden dürfen. Um ein Informationsgleichgewicht herzustellen, haben wir ein *Merkblatt „Wie schreibe ich an Behörden?"* in Vorbereitung, das dem Bürger ein kleiner Anhaltspunkt sein kann, wie er den verschlossenen Versand seiner Briefe bis zu „seinem" Sachbearbeiter erreichen kann, ohne daß zuvor andere die Möglichkeit der Kenntnisnahme haben. Dazu ist beispielsweise notwendig, diese Schreiben persönlich zu adressieren. Als persönlich adressiert gilt jedes Schreiben, auf dem *zuerst* der Empfänger namentlich genannt wird, darunter folgt die Behördenbezeichnung und deren Anschrift. Briefe, die „zu Händen von Frau/Herrn ..." gerichtet sind oder bei denen zuerst die Behörde und dann der Name des Mitarbeiters genannt werden, gelten *nicht* als persönliche Schreiben und werden in der zentralen Poststelle geöffnet. Sofern so adressierte Briefe aber Zusätze wie „persönlich", „vertraulich" oder „eigenhändig" enthalten, sind diese der Behördenleitung oder dem von ihr Beauftragten ungeöffnet vorzulegen. An den Empfänger persönlich adressierte Sendungen erhält dieser ungeöffnet und hat diese - wenn der Inhalt dienstlicher Art ist - später unverzüglich in den Geschäftsgang zu geben. Dennoch ist auf diese Art sichergestellt, daß - im Gegensatz zum üblichen Schriftverkehr, der schon von den Mitarbeitern der Poststelle geöffnet wird - nur die Bearbeiter den Brief zur Kenntnis nehmen.

Schreiben, die an die Bezirksverordnetenversammlung gerichtet sind, werden generell ungeöffnet weitergeleitet. Dies gilt auch für Angebote auf Ausschreibungen und Schreiben an unabhängige Gremien wie beispielsweise Personal- und Jugendvertretungen.

3. Berichte aus den Geschäftsbereichen

Wie in jedem Jahr soll im folgenden eine beispielhafte Aufzählung von Einzelproblemen aus den Geschäftsbereichen die Spannbreite des Datenschutzes in Berlin beleuchten.

3.1 Bau- und Wohnungswesen

Benachrichtigung der Wohnungsaufsichtsämter über Gewerbeanzeigen

> Bürger, die ein Gewerbe angemeldet hatten, wurden vom Wohnungsaufsichtsamt angeschrieben, weil vermutet wurde, daß sie ihre Wohnung unter Verstoß gegen die Zweckentfremdungsverbotsverordnung als Gewerberaum nutzen.

Tatsächlich informieren die Gewerbeämter der Bezirke generell die Wohnungsaufsichtsämter über *Gewerbeanmeldungen.* Sie verweisen dazu auf die Ausführungsvorschriften zur Gewerbeordnung von 1980.

Diese Ausführungsvorschriften - die übrigens vorsehen, daß die Gewerbeämter *„sternförmig"* verschiedene öffentliche Stellen über Gewerbeanmeldungen zu unterrichten haben - entsprechen nicht den Anforderungen des Volkszählungsurteils des Bundesverfassungsgerichts, wonach Eingriffe in das informationelle Selbstbestimmungsrecht einer gesetzlichen Grundlage bedürfen[70]. Nach der Übergangsregelung im Berliner Datenschutzgesetz sind derartige Datenübermittlungen nur noch innerhalb der vorgegebenen Frist ohne gesetzliche Ermächtigung zulässig, soweit die Übermittlung zur Aufgabenerfüllung der Behörde erforderlich ist.

Die Ausführungsvorschriften legen fest, daß jeweils nur ein verkürzter Datensatz der Gewerbeanmeldung übermittelt werden darf.

Daß die Gewerbeämter sich offenbar hieran nicht immer halten, zeigte die Beschwerde eines Bürgers. In diesem Fall hatte das *Wohnungsaufsichtsamt* eine Kopie der gesamten Gewerbeanmeldung erhalten.

Vor Ablauf der Übergangsfrist muß eine hinreichend bestimmte gesetzliche Ermächtigung geschaffen werden, die Zweck, Umfang und Empfänger der Durchschriften von Gewerbeanzeigen festlegt.

Die Senatsverwaltung für Wirtschaft und Technologie ist zwar der Auffassung, daß § 12 Abs. 1 Satz 2 BlnDSG für derartige Datenübermittlungen bereits eine ausreichende gesetzliche Grundlage enthält. Danach ist die Übermittlung personenbezogener Daten an Behörden oder sonstige öffentliche Stellen zulässig, wenn sie vom Empfänger zur Erfüllung des gleichen Zwecks benötigt wird, zu dem die Daten erhoben worden sind. Dies ist jedoch in diesem Zusammenhang gerade nicht der Fall. Das Gewerbeamt erhebt die Daten zur Erfüllung seiner gesetzlichen Aufgaben, nämlich der Gewerbeüberwachung, während das

[69] vgl. JB 1987, 5.7; aber auch 1989, 4.9; und 1990, 3.11

[70] vgl. auch § 6 Abs. 1 BlnDSG

Wohnungsaufsichtsamt die Daten zu einem ganz anderen Zweck benötigt, nämlich Verstöße gegen die Zweckentfremdungsverbotsverordnung zu ahnden. Übermittlungen von Daten aus Gewerbeanzeigen durch die Gewerbeämter an die Wohnungsaufsichtsämter führen deshalb in jedem Fall zu einer Zweckentfremdung dieser Daten, die einer gesetzlichen Grundlage bedürfen.

Inzwischen hat die Senatsverwaltung für Bau- und Wohnungswesen im Rahmen des Artikelgesetzes eine Ergänzung des Zweckentfremdungsbeseitigungsgesetzes vorgesehen, in der die Datenverarbeitung bei den Wohnungsaufsichtsämtern geregelt ist, soweit sie zur Durchführung dieses Gesetzes erfolgt. In dieser Bestimmung ist auch die Befugnis der Wohnungsaufsichtsämter enthalten, Benachrichtigungen von anderen Behörden aus Gewerbeanzeigen in dem Umfang zu erhalten, wie es zur Erfüllung der Aufgaben nach diesem Gesetz erforderlich ist. Der Entwurf enthält ferner eine Aufstellung der Daten, die von den Bezirksämtern und den Fachaufsichtsbehörden zu dem genannten Zweck verarbeitet werden dürfen.

Die vorgesehene Regelung wird zwar den Anforderungen an eine hinreichende Rechtsgrundlage für die Datenübermittlung gerecht. Die Regelung von Übermittlungsbefugnissen in einem Gesetz, das die Aufgaben des Übermittlungs*empfängers* regelt, ist jedoch alles andere als normenklar. Den Gewerbeämtern, die datenschutzrechtlich für die Rechtmäßigkeit ihrer Datenübermittlungen verantwortlich sind, wird damit auferlegt, vor Benachrichtigungen anderer öffentlicher Stellen zunächst anhand bereichsfremder Spezialgesetze zu überprüfen, ob diese derartige Übermittlungen zulassen. Auch der Bürger, der ein Gewerbe anmeldet, kann anhand des Gesetzes, das diese Anwendung vorschreibt - der Gewerbeordnung -, nicht erkennen, daß seine Daten an eine Vielzahl anderer Behörden weitergereicht werden. Sachgerechter wäre die Schaffung einer ausdrücklichen gesetzlichen Ermächtigung in der Gewerbeordnung bzw. bis zur entsprechenden Änderung des Bundesrechts in einem Landesausführungsgesetz.

Auch das schon vorhandene Ausführungsgesetz zu einem anderen wichtigen Bundesgesetz muß um Befugnisse zur Datenverarbeitung ergänzt werden, nämlich das Ausführungsgesetz zum *Baugesetzbuch*. Den ursprünglichen Plan, dies im Rahmen des Artikelgesetzes zu erledigen, hat die Senatsverwaltung für Bau- und Wohnungswesen aus unbekannten Gründen fallengelassen, obwohl dieses Gesetz ohnehin gegenwärtig aus anderen Gründen geändert wird. Dennoch führt kein Weg daran vorbei, normenklar zu regeln, welche personenbezogenen Daten das Bauaufsichtsamt bei einem Bürger erheben darf, der eine Baugenehmigung beantragt. Lediglich für den Teilbereich des *Erschließungsbeitragsgesetzes* hat die Senatsverwaltung eine Datenverarbeitungsbefugnis vorgeschlagen.

Der Entwurf des Artikelgesetzes enthält auch erstmals Regelungen der Verarbeitung personenbezogener Daten im *Liegenschaftskataster* und in der *Bodenwirtschaftlichen Datei* (BOWIDA), die in das *Vermessungsgesetz* eingefügt werden soll. Diese Vorschläge müssen jedoch im Gesetzgebungsverfahren noch erheblich präziser gefaßt werden. Insbesondere müssen der Umfang der gespeicherten Daten im Liegenschaftskataster und in der BOWIDA klarer umrissen werden. Auch bedürfen Mehrfachspeicherungen derselben personenbezogenen Daten in beiden Datensammlungen bei der Senatsverwaltung für Bau- und Wohnungswesen wie auch - zusätzlich - bei der Senatsverwaltung für Stadtentwicklung und Umweltschutz einer besonderen Rechtfertigung.

Vermieter erfährt Einkommen seiner Mieter

Das Wohnungsamt teilte einem Vermieter in einem Freistellungsbescheid nach dem Wohnungsbindungsgesetz die genauen Einkünfte einer Mieterin mit.

Nach dem *Wohnungsbindungsgesetz* (WoBindG) darf der Vermieter eine öffentlich geförderte Mietwohnung (Sozialwohnung) nur an Inhaber eines Wohnberechtigungsscheines überlassen, der nach Prüfung der Einkommensverhältnisse des Mieters in Berlin von den Bezirksämtern aus gestellt wird. Nur in besonderen Fällen kann das bezirkliche Wohnungsamt auf Antrag des Vermieters eine Ausnahme nach § 7 WoBindG genehmigen, wobei es den Vermieter gleichzeitig verpflichtet, eine Ausgleichszahlung zu leisten. Diese Ausgleichszahlung kann der Vermieter durch einseitige Erklärung als Mietzuschlag an den Mieter „weiterreichen".

Das geltende Wohnungsbindungsrecht sieht zwar vor, daß die Auflage zur Entrichtung einer Ausgleichszahlung Bestandteil des Freistellungsbescheides ist, den das Wohnungsamt als Verwaltungsakt gegenüber dem Vermieter erläßt. Daß dabei dem Vermieter jedoch auch die genauen Einkommensverhältnisse seines Mieters offenbart werden, ist nicht erforderlich. Statt dessen sind mehrere datenschutzfreundliche Alternativen vorstellbar, von denen eine allerdings die Änderung des Wohnungsbindungsgesetzes voraussetzt. Während gegenwärtig der Vermieter die *Ausgleichsabgabe* praktisch für das Wohnungsamt beim Mieter einzieht, könnte der Bundesgesetzgeber das Wohnungsbindungsgesetz in der Weise ändern, daß die Ausgleichszahlungen in Zukunft (ähnlich wie die Fehlbelegungsabgabe) direkt beim Mieter erhoben wird. Damit würde eine Offenbarung der Einkommensverhältnisse gegenüber dem Vermieter unterbleiben. Dies hätte außerdem den Vorteil, daß der Mieter die Festsetzung der Ausgleichszahlung selbst gerichtlich überprüfen lassen könnte, was nach gegenwärtigem Recht nicht möglich ist[71]. Wir haben daher - mit Unterstützung anderer Landesbeauftragter für den Datenschutz - den Bundesbeauftragten für den Datenschutz gebeten, sich für eine Änderung des Wohnungsbindungsgesetzes einzusetzen.

Aber schon nach geltendem Bundesrecht kann ein datenschutzfreundlicheres Verfahren bei der Freistellung von der Sozialbindung praktiziert werden: So werden in Bremen lediglich Einkommensspannen als Grundlage für die Ausgleichszahlungen herangezogen, so daß dem Vermieter mit dem Bescheid zumindest keine detaillierten Einkommensverhältnisse seiner Mieter bekannt werden. In Hamburg wird sogar auf eine Differenzierung der Ausgleichszahlung in Abhängigkeit der Einkommenverhältnisse des Mieters verzichtet, und der Vermieter hat lediglich einen einheitlich festgelegten Betrag pro Quadratmeter Wohnfläche als Ausgleichszahlung zu leisten.

Sollte sich eine Gesetzesänderung in diesem Punkt nicht herbeiführen lassen, sollte das Land Berlin das Verfahren entsprechend der hamburgischen Lösung ändern.

3.2 Finanzen

Prüfung der ADV in der Berliner Steuerverwaltung

Im vergangenen Jahr schilderten wir das Problem der fehlenden Protokollierung des Zugriffs auf Daten der Steuerverwaltung. Hierzu wurde nunmehr eine Prüfung durchgeführt.

Wir haben uns bei der geplanten Überprüfung des Verfahrens *„Dezentrale Computerleistung in den Finanzämtern"* (DCL) in einem zufällig ausgewählten Finanzamt und der Oberfinanzdirektion auf die Berechtigungen zum Zugriff auf die Steuerdaten der Bürger, die technische Umsetzung der Benutzerprofile und die Protokollierung der Zugriffe auf die Daten anderer Finanzämter sowie die Zugriffe durch die Oberfinanzdirektion konzentriert.

Das DCL-Verfahren wird in einem dreistufigen, sternförmigen Rechnernetz betrieben. Die Sachbearbeiter in den Finanzämtern oder in der Oberfinanzdirektion arbeiten an Personalcomputern, die mit einem Finanzamtsrechner im jeweiligen Amt verbunden sind, der auch als Vermittlungsrechner zum zentralen Hauptrechner im Finanzamt Charlottenburg dient. In diesem Hauptrechner sind die Steuerdaten aller Berliner Steuerpflichtigen gespeichert und stehen zum Abruf durch die berechtigten Benutzer über das Netz bereit.

Zur Zeit ist das Netz noch nicht voll ausgebaut. In dem geprüften Finanzamt waren von den etwa 240 Mitarbeitern zur Zeit erst 60 Mitarbeiter mit dem unmittelbaren Zugriff auf das DCL-Verfahren befaßt. Es standen erst 20 Terminal-PCs zur Verfügung, wobei sich mehrere Nutzer ein Gerät teilen.

Die Zugriffsberechtigungen sind äquivalent zum Netzaufbau gegliedert, d. h. in der dreistufigen Netzhierarchie sind Berechtigungen für die PC-Ebene, die Finanzamtsrechner und den Haupt-

[71] vgl. BVerwG NJW 1987, S. 2829 f.

rechner im Finanzamt Charlottenburg vergeben. Im Gegensatz zu den Finanzämtern, in denen die Steuerbescheide errechnet werden, sind bei der Oberfinanzdirektion echte Fälle nur im Rahmen der Fachaufsicht über die Finanzämter zu bearbeiten. Die Anlage der Oberfinanzdirektion ist im wesentlichen für den Test- und Entwicklungsbetrieb sowie für die Behebung von Fehlern beim laufenden Betrieb des Gesamtnetzes vorgesehen. Für die Fehlersuche und -beseitigung muß auf aktuelle Daten der Finanzämter zugegriffen werden, weil sie sonst nicht wirksam vollzogen werden kann.

Auch für die Benutzerverwaltung im Gesamtverfahren ist die Oberfinanzdirektion zuständig. Sie stellt die Rahmenbedingungen auf, und die einzelnen Finanzämter füllen diesen Rahmen nach vorgegebenen Richtlinien aus. Entsprechend einer Anweisung zur „Differenzierung der Zugriffsberechtigungen" bleibt es dem einzelnen Finanzamt überlassen, welchem Mitarbeiter es die entsprechende Berechtigung zuteilt. In der Regel erhält jeder Sachbearbeiter mittels einer Verfügung Berechtigungen für Aufgaben, die seiner Funktionsbeschreibung im Geschäftsverteilungsplan entsprechen.

Auch in der Oberfinanzdirektion wird sowohl die Berechtigung für bestimmte Abfragen als auch die Nutzung bestimmter Geräte von den Vorgesetzten für den Sachbearbeiter vorgegeben. Ein sog. Starterprogramm prüft beim „Einloggen" die erteilten Berechtigungen und weist dem Sachbearbeiter sein jeweiliges Arbeitsmenü am Bildschirm zu.

Datenabrufe sind grundsätzlich nur aus den Datenbeständen des eigenen Finanzamtes zugelassen. Da im Hauptrechner jedoch die Daten der Speicherkonten aller Finanzämter einschließlich des Finanzamtes für Erbschafts- und Verkehrssteuern gespeichert werden, sind auch finanzamtsübergreifende Datenabrufe möglich. Sie sind zulässig bei Abfragen aus den Kfz-Steuer-Speicherkonten des Finanzamtes für Erbschafts- und Verkehrssteuern und bei Amtshilfeersuchen im Vollstreckungsbereich. Die Oberfinanzdirektion darf aufgrund eines streng geregelten Verfahrens im Einzelfall für Aufgaben der Fachaufsicht auf Speicherkonten der Finanzämter zugreifen.

Bei dem Kfz-Steuer-Datenbestand des Finanzamtes für Erbschafts- und Verkehrssteuern dürfen die berechtigten Sachbearbeiter auf alle Daten (wie Kfz-Halter, Kfz-Nr. und sonstige Zulassungsdaten) zugreifen. Der Zugriff dient in erster Linie der Aufrechnung von Guthaben beim Lohnsteuerjahresausgleich bzw. der Einkommensteuererklärungen mit eventuellen Schulden bei der Kfz-Steuer; inwieweit dies erforderlich ist, wird derzeit noch geprüft.

Die Paßwörter werden von der Oberfinanzdirektion generell vorgegeben. In Form einer Verfügung werden die Paßwörter von der Oberfinanzdirektion den Finanzämtern zugeleitet, wo sie dann durch die Vorsteher an die Sachbearbeiter vergeben werden. Die Berechtigungen sind zum Teil gerätebezogen, so daß man auch mit ordnungsgemäßer Berechtigung nicht von jedem Gerät aus arbeiten kann. Die Paßwörter können nach der Erstvergabe nicht vom Benutzer selbst verwaltet werden. Die Möglichkeit einer datenschutzfreundlicheren „Selbstverwaltung" der Paßwörter ist aber für die Zukunft vorgesehen.

Dies ist auch dringend erforderlich, denn die Geheimhaltung des Paßwortes ist während der schriftlichen Weiterleitung des Paßwortes entlang der Hierarchie von der Oberfinanzdirektion bis zum Sachbearbeiter im Finanzamt nicht sichergestellt. Das Risiko wäre bedeutend kleiner, könnte der Sachbearbeiter sofort nach Erhalt des Paßwortes dieses zur Bestimmung eines neuen, nur ihm bekannten Paßwortes verwenden.

Ein Änderungsrhythmus der Paßwörter ist nicht vorgeschrieben, er beträgt jedoch beim geprüften Finanzamt ein Jahr. Nach Ablauf dieser Frist erhält das Finanzamt von der Oberfinanzdirektion eine neue Liste mit Paßwörtern.

Sämtliche Abrufe innerhalb des DCL-Verfahrens werden programmgesteuert aufgezeichnet. Für die schnelle Recherche (hauptsächlich zur Fehlersuche) werden umfangreiche Protokolle erzeugt, die in der Regel nach einem Tag gelöscht werden. Davor werden sie jedoch verkürzt aufbereitet und in ein sog. System-Logbuch aufgenommen, welches dann Auskunft darüber gibt, welcher Benutzer sich zu welcher Zeit an- und abgemeldet und welches Programm und z. T. auch welche Befehle (Menüpunkte) er aufgerufen hat. Das System-Logbuch wird alle drei Monate ausgewertet.

Die finanzamtsübergreifenden Zugriffe werden ebenfalls protokolliert. Erfolgt der Zugriff von der Oberfinanzdirektion aus, findet eine vollständige *Protokollierung* statt, beim Zugriff eines Finanzamtes auf Daten anderer Finanzämter erfolgt im Vorgriff auf den Entwurf der *Steuerdaten-Abruf-Verordnung* (StDAV) eine Protokollierung nur bei 5 % der Abrufe, die nach einem zufallsbestimmten Stichprobenverfahren ausgewählt werden. Am Bildschirm erscheint dann die Nachricht, daß die Abfrage protokolliert wurde. In diesem Falle hat der Sachbearbeiter den Grund des Datenabrufs in einem Buch einzutragen, das neben jedem Terminal zu liegen hat. Die Innenrevision der Oberfinanzdirektion hat dann zu einem späteren Zeitpunkt die Protokollisten mit den Aufzeichnungen im Buch auf Übereinstimmung zu vergleichen. Beanstandungen waren bisher nicht zu verzeichnen.

Die Wirksamkeit eines solchen Protokollierungsverfahrens für die Abschreckung vor zweckfremdem und damit auch bei ansonsten berechtigten Personen rechtswidrigem Zugriff ist allerdings sehr beschränkt, weil der Abfragende über die Protokollierung unterrichtet wird. Da er bei allen protokollierten Abrufen damit rechnen muß, daß er sich vielleicht bezüglich der dienstlichen Notwendigkeit des Abrufs gegenüber der Innenrevision rechtfertigen muß, hat er bei zweckfremden Zugriffen genügend Zeit und Gelegenheit, einen dienstlichen Zusammenhang nachträglich zu konstruieren. Bei solchen Stichprobenprotokollen sollte daher auf die Meldung an den Abfrager verzichtet und die Aufzeichnung aller Abfragen verlangt werden.

IuK-Hinweise zu Datenschutz und Datensicherheit bei der Senatsverwaltung für Finanzen

Eine vorbildliche Initiative im Zusammenhang mit dem zunehmenden Einsatz der Informations- und Kommunikationstechnik (IuK-Technik) in der Berliner Verwaltung ist von der Senatsverwaltung für Finanzen ergriffen worden. Die Senatsverwaltung hat unter Berücksichtigung vieler Datenschutz- und Datensicherungsmaßnahmen, die wir in unseren Jahresberichten und sonstigen Publikationen empfohlen hatten, *IuK-Hinweise* erarbeitet, die für alle Mitarbeiter bindend sein sollen.

Positiv hervorzuheben ist insbesondere die Betonung der Verantwortlichkeit des Fachbereichs und die Aufgabenbeschreibung der Organisationsstelle mit der Trennung der Zuständigkeit für den behördlichen Datenschutzbeauftragten und die übrigen Mitarbeiter der Organisationsstelle in Fragen des Datenschutzes und der Datensicherheit, die ausführliche und für die Anwender besonders nützliche Auflistung der technischen Maßnahmen beim Zugriffsschutz und der Behandlung des Benutzerkennworts sowie das strikte Verbot der Nutzung privater IuK-Systeme.

Wir empfehlen auch den anderen Senatsverwaltungen, sich diesem Beispiel anzuschließen und für ihren Zuständigkeitsbereich ebenfalls Empfehlungen für die datenschutzgerechte Nutzung der IuK-Technik zu geben.

3.3 Gesundheit

Die Begutachtung des Ehemanns

> Eine Frau sucht die ehepsychologische Beratungsstelle eines bezirklichen Gesundheitsamtes auf, um sich dort beraten zu lassen. In der Folge erscheint zu einzelnen Sitzungen auch ihr Ehemann, über den die Psychologin – ohne sein Wissen – ein tiefenpsychologisches Gutachten erstellt. Dieses Gutachten wird der Ehefrau ausgehändigt, so daß sie es in das laufende Scheidungs- und Sorgerechtsverfahren vor dem Familiengericht einbringen kann.

Bereits die Erstellung des Gutachtens ohne Wissen des betroffenen Ehemannes steht im direkten Gegensatz zum Berliner Datenschutzgesetz, das im Regelfall die Datenerhebung beim Betroffenen mit seiner Kenntnis vorschreibt. Keiner der gesetzlichen Ausnahmetatbestände von diesem Grundsatz war in diesem Fall erfüllt. Ebenso unzulässig und unvereinbar mit der ärztlichen Schweigepflicht war die Weitergabe des Gutachtens an die Ehefrau ohne Einwilligung des Ehemannes, der nur zu dem

Zweck an einzelnen Sitzungen teilgenommen hatte, um den Beratungsdienst in Anspruch zu nehmen, nicht aber, um sich begutachten zu lassen. Die gemeinschaftliche Teilnahme an den Sitzungen mit der Ehefrau berechtigen auch die psychologischen Mitarbeiter des Gesundheitsamtes, die alle als Gehilfen des Amtsarztes der ärztlichen Schweigepflicht unterliegen, nicht dazu, der Ehefrau ein psychologisches Gutachten über den Ehemann auszuhändigen und zur weiteren Verwendung zu überlassen, wenn der Ehemann nicht eingewilligt hat. Es ist zwar zu begrüßen, daß der zuständige Amtsarzt diesen gravierenden datenschutzrechtlichen Verstoß anerkannt und sofortige Schritte zur Beseitigung der Folgen eingeleitet hat. Es bleibt allerdings abzuwarten, ob sich diese Folgen noch beseitigen lassen. Insbesondere wird das Familiengericht zu entscheiden haben, ob ein Gutachten, das unter solchen Umständen entstanden ist, verwertet werden darf.

Überschußinformationen für den Arbeitgeber

> Bei einer amtsärztlichen Überprüfung seiner Dienstfähigkeit im Auftrag des Arbeitsgebers wurde ein Bürger aufgefordert, sich nicht nur einer allgemeinärztlichen Untersuchung zu unterziehen, sondern auch einer nervenärztlichen Zusatzbegutachtung. Dabei wurde ihm ausdrücklich zugesichert, daß die Untersuchung vertraulich sei und die erhobenen Befunde aufgrund der ärztlichen Schweigepflicht nicht ohne sein Wissen offenbart werden dürften. Der Bürger verließ sich auf den zugesicherten Vertrauensschutz und zeigte eine besondere Offenheit bei der Darlegung seiner gesundheitlichen Situation. Um so empörter war er, als er in der Stellungnahme des Gesundheitsamtes gegenüber dem Arbeitgeber den Hinweis fand, daß nicht nur eine internistische Untersuchung, sondern auch eine neurologische Zusatzbegutachtung sowie eine weitere nervenärztliche Zusatzbegutachtung erfolgt seien und daß seine Arbeitsfähigkeit wegen einer „neurologischen/psychiatrischen Symptomatik" hochgradig eingeschränkt sei.

Dieses Vorgehen des Gesundheitsamtes war mit der ärztlichen Schweigepflicht nicht zu vereinbaren. Das Gesundheitsamt darf einem Arbeitgeber stets nur mitteilen, ob der untersuchte Arbeitnehmer ganz, teilweise oder überhaupt nicht dienstfähig ist. Weder dürfen einzelne Befunde noch Hinweise auf die Art der Untersuchungen oder festgestellte Symptome offenbart werden. Dies hat die Konferenz der Datenschutzbeauftragten in ihrem Beschluß zum Datenschutz im Recht des öffentlichen Dienstes[72] betont. Es gilt in gleicher Weise, wenn ein privater Arbeitgeber einen Arbeitnehmer vom Gesundheitsamt vertrauensärztlich untersuchen läßt.

Öffentlicher Gesundheitsdienst

Datenschutzrechtlich ungeklärt ist weiterhin das *Verhältnis des Jugendgesundheitsdienstes* (Kleinkinder und Säuglinge) *zum Schulgesundheitsdienst.* Hier gibt es Bestrebungen, die Dienste organisatorisch zusammenzufassen. Da der Kleinkinder- und Säuglingsdienst jedoch ausschließlich auf freiwilliger Betreuungsbasis tätig wird, entsteht hier ein Datenmaterial, das unter den strengen Schutzvorschriften der ärztlichen Schweigeordnung steht und somit auch einer besonderen Zweckbindung unterliegt. Diese Daten dürfen ohne Zustimmung der Betroffenen bei der Aufgabenerfüllung des Schulgesundheitsdienstes, der die gesetzlich vorgeschriebenen schulärztlichen Untersuchungen etwa bei der Einschulung durchführt, nicht verwendet werden. Dies ergibt sich aus dem Zweckbindungsgrundsatz des Berliner Datenschutzgesetzes.

An dieser Stelle wird deutlich, daß auch eine Novellierung des *Berliner Gesundheitsdienstgesetzes* vordringlich ist, damit zum einen die Aufgaben des öffentlichen Gesundheitsdienstes nach dem gegenwärtigen Entwicklungsstand gesetzlich klargestellt werden und zum anderen die erforderlichen Befugnisse zur Datenerhebung und -verarbeitung geschaffen werden. Orientierungspunkt muß dabei die Zielsetzung der ärztlichen Schweigepflicht und der Auftrag der öffentlichen Gesundheitsvorsorge bleiben, ohne daß dabei die jetzige Rechtsstellung der Betroffenen ausgehöhlt wird. Der Entwurf für eine datenschutzrechtliche Ergänzung des Gesundheitsdienstgesetzes, den die Senatsverwaltung für Gesundheit im Zusammenhang mit dem Artikelgesetz vorgelegt hat, enthält ebenso wie ein Entwurf zur Änderung des Gesetzes über Pflegeleistungen lediglich Blankettermächtigungen zur Datenverarbeitung, die nicht hinreichend normenklar sind. Dies ist umso erstaunlicher, als dieselbe Senatsverwaltung einen sehr viel präziseren Vorschlag zur Änderung des *Berliner Kammergesetzes* gemacht hat, der ebenfalls Teil des Artikelgesetzentwurfes ist. Darin wird im einzelnen aufgeführt, welche personenbezogenen Daten von welchen Kammern (Anwalts-, Ärzte-, Zahnärzte- und Apothekerkammer) verarbeitet werden dürfen.

Ruhiger ist es um die Frage des *Einsichtsrechts in die Unterlagen des sozialpsychiatrischen Dienstes* geworden. Hier hat die Entscheidung des Bundesverwaltungsgerichts vom 27. April 1989[73] deutlich den Weg gewiesen, so daß wir von einer großzügigen Einsichtsgewährung in der Verwaltungspraxis ausgehen. Gleichwohl ergab sich in einem Fall die Frage, ob sich das Einsichtsrecht auch auf die damit zusammenhängende Prozeßakte des Rechtsamtes bezieht.

Wir haben dies ablehnen müssen, weil die ärztliche Aufgabe von der prozessualen Interessenwahrnehmung zu trennen ist, so daß der Patient zwar Einsicht in die ärztlichen Unterlagen verlangen kann, nicht jedoch aus dem gleichen Rechtsgrund in die Prozeßakte. Für diese muß er sich vielmehr auf das Verwaltungsverfahrensgesetz stützen und die dort gegebenen Einschränkungen hinnehmen.

Eine weitere wichtige Rolle spielte die *Aufbewahrung von Untersuchungsunterlagen und Gutachten des vertrauensärztlichen Dienstes.* Anders als bei den Betreuungsaufgaben der ärztlichen Dienste, die in gewisser Weise dem Behandlungsbereich zugerechnet werden können und somit nach der Berufsordnung der Ärztekammer über zehn Jahre hinweg aufzubewahren sind, stellt die Begutachtung im Sinne einer Sachverhaltsfeststellung im Sinne des vertrauensärztlichen Dienstes keine Behandlung dar, so daß hier kürzere Fristen in Betracht kommen.

Vom Gesundheitsamt des Bezirks Tiergarten von Berlin ging schon vor Jahren eine erfreuliche Initiative aus mit dem Ziel, den Aktenbestand zu durchforsten und das nicht benötigte Material zu vernichten. Diese Initiative der zuständigen Amtsleitung ist durch einen Beschluß der Bezirksverordnetenversammlung nach unserer befürwortenden Stellungnahme unterstützt worden, wobei ausschlaggebend war, daß nach Eintritt der endgültigen Rechtskraft einer Verwaltungsentscheidung die zugrundeliegende amtsärztliche Untersuchung keiner weiteren Aufbewahrung mehr bedarf. Für spätere Untersuchungen werden diese Unterlagen nicht mehr benötigt, da vielmehr eine neue Sachverhaltsfeststellung - auf den neuen Zeitpunkt bezogen - erfolgen muß. Gemäß § 17 Abs. 3 BlnDSG sind personenbezogene Daten zu löschen, wenn ihre Kenntnis für die datenverarbeitende Stelle zur rechtmäßigen Erfüllung der in ihrer Zuständigkeit liegenden Aufgaben nicht mehr erforderlich ist und auch kein Grund zur Annahme besteht, daß durch die Löschung schutzwürdige Belange des Betroffenen beeinträchtigt werden. Der begutachtende Arzt kann sich auch ohne Kenntnis von Vorgutachten (z. B. zur Frage der gegenwärtigen Dienstfähigkeit) sachverständig äußern.

AIDS-Dokumentationssystem KLIMACS

Im Rahmen des Sofortprogramms der Bundesregierung zur AIDS-Bekämpfung ist beabsichtigt, in den Krankenhäusern ein Verfahren zur Unterstützung der AIDS-Bekämpfung auf dem medizinischen Sektor als rechnergestütztes Krankendokumentationssystem unter dem Namen „Klinisch-medizinische Analysen - Computer System (KLIMACS)" einzurichten. Die Entwicklung dieses Systems wird vom Kuratorium AIDS der Paul-Ehrlich-Gesellschaft betreut.

Um dem besonderen Bedürfnis des Datenschutzes bei derart sensiblen Datensammlungen in angemessenem Umfang Rechnung tragen zu können, wurde ein Konzept „Datenschutzanfor-

[72] Anlage 2.4

[73] BVerG 3 C 4.86

derungen an KLIMACS und seine Anwender" projektbegleitend entwickelt. Die Ausarbeitung dieses Konzeptes ist von einem speziellen Arbeitskreis der Konferenz der Datenschutzbeauftragten kritisch begleitet worden, so daß es den Landesdatenschutzbeauftragten nur noch obliegt, auf spezielle rechtliche Bedingungen der Länder sowie auf zusätzliche Detailhinweise zur technischen und organisatorischen Absicherung einzugehen.

Im Konzept wird als Rechtsgrundlage auf den Behandlungsvertrag zwischen dem Patienten und dem Krankenhaus in Verbindung mit dem Bundesdatenschutzgesetz abgestellt, jedoch eingeräumt, daß die Vorschrift in einzelnen Bundesländern durch länderrechtliche Vorschriften verdrängt bzw. modifiziert werden kann. Dies trifft für öffentlich-rechtliche Krankenhäuser in Berlin zu. Hier ist das Berliner Datenschutzgesetz als Rechtsgrundlage für die Datenverarbeitung anzuwenden.

Nach der Novellierung des Berliner Datenschutzgesetzes wirkt sich die Privilegierung von öffentlichen Institutionen, die mit privaten Institutionen im Wettbewerb stehen, nur noch auf landesunmittelbare Anstalten aus, zu denen die öffentlich-rechtlichen Krankenhäuser und Universitätskliniken nicht zählen.

Infolgedessen richtet sich die Bewertung der Zulässigkeit der Datenverarbeitung bei KLIMACS nach § 6 Abs. 1 BlnDSG. Dies bedeutet, daß sich die Verarbeitung personenbezogener Daten bei KLIMACS praktisch nur auf die Einwilligung stützen kann. Wir haben daher deutlich gemacht, daß die Einholung des Einverständnisses im Rahmen der Datenerhebung erfolgen müßte, wobei die Aufklärungspflicht, also die Information des Patienten, zu welchem Zweck die Datenerhebung durchgeführt wird, unbedingt einzuhalten ist. Weiter darf eine darüber hinausgehende Verarbeitung der Daten nur erfolgen, soweit dies im Rahmen der Zweckbestimmung erforderlich ist; eine Weitergabe der medizinischen Daten unterliegt darüber hinaus den Regeln der ärztlichen Schweigepflicht. So ist beispielsweise zu beachten, daß eine Nutzung zu Forschungszwecken eine Zweckänderung wäre, die ihrerseits der expliziten Einwilligung der Patienten bedürfte.

In Berlin existiert derzeit noch keine praktische Anwendung mit KLIMACS. Es ist jedoch vorgesehen, das Verfahren an den beiden Standorten Wedding und Charlottenburg des Universitätsklinikums Rudolf Virchow und im Universitätsklinikum Steglitz einzuführen.

Wir werden hier insbesondere auch auf die angemessenen technisch-organisatorischen Maßnahmen achten.

3.4 Inneres

3.4.1 Polizei

Allgemeines Sicherheits- und Ordnungsgesetz

Das Fehlen bereichsspezifischer Vorschriften zur Gewährleistung des Datenschutzes bei Sicherheits- und Ordnungsbehörden stellte den gravierendsten Mangel der Gesetzgebung dar. Dies ist von den Datenschutzbeauftragten seit ihrem Bestehen in den siebziger Jahren festgestellt worden. Auch Kritiker dieser Auffassung mußten spätestens seit dem Volkszählungsurteil einräumen, daß gerade diejenigen Stellen, deren Aufgabe die weitestgehenden Befugnisse zur Verarbeitung personenbezogener Daten erfordert, sich ohne hinreichende Rechtsgrundlagen in einem schwer hinnehmbaren Zustand befanden. Auch die Rechtsprechung, selbst wenn sie wie das Bundesverwaltungsgericht die Polizeipraxis rechtfertigte, hat zunehmend deutlicher auf die Defizite hingewiesen.

Es gereicht dem Land Berlin nicht zum Ruhme, wenn erst im vergangenen Jahr und das erst wegen des drohenden Ablaufs der Übergangsfrist im Datenschutzgesetz ein Entwurf zur Änderung des Allgemeinen Sicherheits- und Ordnungsgesetzes in den Gesetzgebungsprozeß eingebracht wurde. Wegen der nunmehr erforderlichen Eile wurde der Entwurf von den Koalitionsfraktionen aus der Mitte des Parlaments eingebracht - die gerade bei einem derart wichtigen Gesetz unerläßliche verwaltungsinterne Abstimmung einschließlich der Beratung mit dem Datenschutzbeauftragten wurde damit umgangen.

Dies wäre verschmerzbar gewesen, wenn sich der Entwurf durch ein besonderes Maß an kritischer Distanz zum Staat, und das heißt hier zu den Sicherheits- und Ordnungsbehörden ausgezeichnet hätte, wenn der Entwurf diesen Institutionen zwar die erforderlichen Mittel auch informationstechnischer Art in die Hand gegeben, aber klare, rechtsstaatlich einwandfreie Grenzen gezogen hätte.

Leider war das Gegenteil der Fall. Der Entwurf, der am 5. November in das Abgeordnetenhaus eingebracht wurde, hielt sich nicht nur auf der Linie traditioneller Vorstöße zur Legitimierung bisheriger und künftig erwünschter polizeilicher Maßnahmen (z. B. des Vorschlags des zuständigen Arbeitskreises der Innenministerkonferenz für einen Musterentwurf eines einheitlichen Polizeigesetzes), ja wollte der Berliner Polizei Befugnisse verschaffen, die ihr andernorts versagt wurden.

Zur Begründung diente die erforderliche Bekämpfung der *Organisierten Kriminalität*, eine Aufgabe, für deren rechtliche Bewältigung freilich der Bundesgesetzgeber zuständig ist, dem auch gerade ein entsprechender aus der Mitte des Bundesrates mit der Stimme Berlins eingebrachter Entwurf vorliegt. Ein Entwurf, der seinerseits heftige Kritik hervorrief[74] obwohl er im Vergleich zu dem Berliner ASOG-Entwurf geradezu als zurückhaltend bezeichnet werden muß.

Daß der Berliner Gesetzgeber insoweit überhaupt tätig werden konnte, liegt an einer Zielstellung, die mit der ASOG-Novellierung verfolgt werden soll, obwohl sie mit dem eigentlichen Anliegen der Legitimierung polizeilicher Datenverarbeitung zunächst nichts zu tun hat: Der Polizei soll nunmehr ausdrücklich die Aufgabe der vorbeugenden Bekämpfung von Straftaten (den Ordnungsbehörden zusätzlich eine entsprechende Aufgabe bei Ordnungswidrigkeiten) zugewiesen werden, die im Vorfeld der Strafverfolgung und damit außerhalb der Bundeszuständigkeit liegen soll.

Im Hinblick auf diese Aufgabe sollen der Polizei Befugnisse verschafft werden, die den Bereich der klassischen polizeilichen Tätigkeit verlassen. So war es bislang Allgemeingut, daß die Polizei nur dann gegenüber dem Bürger tätig werden kann, wenn sie auf Grund tatsächlicher Anhaltspunkte vergangene Straftaten verfolgt (als Hilfsbeamte der Staatsanwaltschaft) oder konkrete Gefahren abwehrt (in eigener Zuständigkeit). *Vorbeugende Straftatenbekämpfung* bedeutet dagegen Tätigwerden ohne derartige Voraussetzungen allein aufgrund der Vermutung, die Ermittlungen könnten einen Beitrag zur Aufklärung (und Verhinderung) irgendwelcher möglicherweise bevorstehender oder geschehener Straftaten leisten. Geradezu notwendigerweise werden damit auch Unbescholtene, ja völlig Unbeteiligte Objekte polizeilicher Maßnahmen.

Es wird geltend gemacht, daß die Sicherheitsbehörden schon immer in diesem Bereich Informationen verarbeitet hätten, beispielsweise zur Vorbereitung künftiger Strafverfolgung Kriminalakten auch nach Abschluß der Ermittlungen und Abgabe des Vorgangs an die Staatsanwaltschaft einbehalten und später genutzt hätten. Eine Rechtsgrundlage habe man früher nicht für nötig gehalten, erst das neue Bewußtsein um den Eingriffscharakter der Informationsverarbeitung habe eine gesetzliche Regelung und damit die Ausdehnung der Aufgabe nötig gemacht.

Dies mag sein. Es wäre allerdings angemessen gewesen, wenn im Zusammenhang mit der Regelung eine sorgfältige Abwägung der erforderlichen Mittel stattgefunden hätte, die dann auch zu einer Abschichtung der unerläßlichen Regelungen geführt hätte. Der in die Diskussion gebrachte ASOG-Entwurf verschafft demgegenüber den Sicherheitsbehörden jedmögliche Befugnisse, ohne - wie für ein Polizeigesetz eigentlich zu erwarten - klare Grenzen zu ziehen.

Darüber hinaus wurde die Gelegenheit wahrgenommen, ganz besonders *intensive Mittel der Informationserhebung* der Polizei auch ausdrücklich in die Hand zu geben, deren Einsatz bislang als problematisch oder rechtlich nicht zulässig galt: nachrichtendienstliche Mittel, polizeiliche Beobachtung, V-Leute, Rasterfahndung.

Für den Bereich der Strafverfolgung will der Entwurf des OrgKG[75] gerade den Einsatz dieser Mittel regeln, mit gewisser

[74] siehe unter 3.6

[75] Entwurf eines Gesetzes zur Bekämpfung des illegalen Rauschgifthandels und anderer Erscheinungsformen der organisierten Kriminalität (Bundesrat Drs 219/91)

Zurückhaltung. So sollen sie etwa nur dann zulässig sein, wenn bestimmte strafrechtliche Tatbestände erfüllt sind. Diesen rechtsstaatlich gebotenen Weg will der ASOG-Entwurf verlassen: Es soll ausreichen, daß der Einsatz der Mittel zur vorbeugenden Bekämpfung jeglicher erheblicher Straftaten eingesetzt werden, eine Beschränkung, die in ihrer Vagheit kaum eine Schranke setzt. Auch Befürworter des Entwurfs erkennen an, daß als eigentliche Schranke nur noch das Verhältnismäßigkeitsprinzip dienen soll - ein Weg zurück zum Preußischen Allgemeinen Landrecht (so ein wörtlicher Hinweis in einer der Anhörungen).

Es kann niemanden verwundern, daß der Berliner Datenschutzbeauftragte gegen diesen Entwurf heftigen Protest anmelden mußte.

Auch die Fraktion der F.D.P. hatte einen Entwurf für ein ASOG eingebracht. Sie hatte bereits vor Jahren auf die Dringlichkeit der ASOG-Novellierung hingewiesen.

Auch im Gesetzentwurf der Fraktion der F.D.P. werden die Informationseingriffe der Polizei weit in das Vorfeld konkreter Gefahr verlagert. Auch hier wird der Einsatz von verdeckten Ermittlern und technischen Mitteln, wie „Wanzen", Videoaufnahmen und Richtmikrofonen, nicht nur gegen potentielle Straftäter, sondern auch gegen „Kontakt- und Begleitpersonen" ermöglicht. Diese erheblichen Eingriffe in das Persönlichkeitsrecht werden allerdings an engere Voraussetzungen - Straftatenkatalog und Richtervorbehalt - geknüpft. Darüber hinaus werden besonders bedenkliche Informationseingriffe, wie die Rasterfahndung und die zu einem umfassenden Bewegungsbild der Betroffenen führende polizeiliche Beobachtung ausgeschlossen, und der verdeckte Einsatz technischer Mittel in Wohnungen auf den Schutz verdeckter Ermittler beschränkt.

Aus der Vielzahl der von uns vorgebrachten Kritikpunkte sollen nochmals folgende hervorgehoben werden:

Weitreichende Eingriffe, wie der Einsatz verdeckter Ermittler, das heimliche Abhören und langfristiges Observieren, werden davon abhängig gemacht, daß eine *Straftat von erheblicher Bedeutung* oder eine schwerwiegende *Ordnungswidrigkeit* bekämpft werden soll. Straftaten von erheblicher Bedeutung sind nach dem Gesetzentwurf Verbrechen sowie Vergehen, die aufgrund ihrer Begehungsweise, ihrer Dauer oder Schwere eine Gefahr für die Allgemeinheit darstellen und geeignet sind, die Sicherheit der Bevölkerung zu beeinträchtigen; dies gilt insbesondere für Straftaten, die banden-, gewerbs-, gewohnheits-, serienmäßig oder in anderer Weise organisiert begangen werden. Diese Tatbestandsvoraussetzungen sind nicht normenklar genug. Auch in der Stellungnahme der Bundesregierung zum OrgKG wurden verfassungsrechtliche Bedenken gegen eine Regelung erhoben, die schwerwiegende strafprozessuale (also einen Straftatverdacht voraussetzende) Eingriffsbefugnisse von einem derart unbestimmten Rechtsbegriff abhängig macht. Vielmehr kann nur ein enger Straftatenkatalog den Einsatz intensiver Erhebungsmittel rechtfertigen.

Keinesfalls kann die „Dauer oder Schwere" einer Ordnungswidrigkeit Anknüpfungspunkt für Eingriffe sein. Wenn Ordnungswidrigkeiten überhaupt den Katalogstraftaten gleichgestellt werden sollen, dann bedarf es hier zumindest einer Aufzählung gemeingefährlicher Tatbestände.

Die Polizei soll die Möglichkeit erhalten, personenbezogene Daten zu *erheben,* wenn das zur vorbeugenden Bekämpfung von Straftaten erforderlich ist. Nach dieser sehr allgemeinen Formulierung können nahezu voraussetzungslos Daten über jede Person erhoben werden, völlig unabhängig davon, ob es sich um Verdächtige oder Nichtverdächtige handelt. Ferner ist eine sehr weitgehende Auffangnorm für die *heimliche Datenerhebung* vorgesehen. Dies ist bedenklich, da zum informationellen Selbstbestimmungsrecht der Bürger gehört, daß sie überblicken, wer was wann und bei welcher Gelegenheit über sie weiß. Das bedeutet, daß grundsätzlich Daten offen beim Betroffenen zu erheben sind. Die in dem Entwurf aufgeführten Ausnahmetatbestände von diesem Grundsatz sind so weitgehend, daß es in der Praxis zu einer Umkehrung des Regel-Ausnahme-Verhältnisses kommen könnte.

Sowohl im Gesetzentwurf der Koalitionsfraktionen als auch in dem Entwurf der F.D.P.-Fraktion ist die Möglichkeit der Einrichtung von *Kontrollstellen* mit genereller Berechtigung zur Identitätsprüfung vorgesehen. Anders als bei Kontrollstellen für die Strafverfolgung, für deren Einrichtung ein konkreter Tatverdacht vorliegen muß, soll diese Maßnahme bereits im Vorfeld konkreter Gefahren zulässig sein, wenn bestimmte Straftaten zu befürchten sind. Darüber hinaus geht der Straftatenkatalog über den des § 111 StPO hinaus.

Verfassungsrechtlich bedenklich ist, daß routinemäßig an Kontrollstellen bei allen potentiellen Teilnehmern einer *Demonstration* die Identität festgestellt werden kann. Gerade Informationseingriffe gegen Teilnehmer von Versammlungen hat das Bundesverfassungsgericht im Volkszählungsurteil besonders hervorgehoben: „Wer damit rechnet, daß etwa die Teilnahme an einer Versammlung oder einer Bürgerinitiative behördlich registriert wird und daß ihm dadurch Risiken entstehen können, wird möglicherweise auf eine Ausübung seiner entsprechenden Grundrechte (Art. 8, 9 GG) verzichten. Dies würde nicht nur die individuellen Entfaltungschancen des Einzelnen beeinträchtigen, sondern auch das Gemeinwohl, weil Selbstbestimmung eine elementare Funktionsbedingung eines auf Handlungs- und Mitwirkungsfähigkeit seiner Bürger begründeten freiheitlichen demokratischen Gemeinwesens ist."

Auch *erkennungsdienstliche Maßnahmen* werden zugelassen, wenn dies „zur vorbeugenden Straftatenbekämpfung erforderlich" ist. Dies ist in dieser Allgemeinheit viel zu weitgehend. Damit ist nicht ausgeschlossen, daß auch wegen geringfügiger Delikte derartige Maßnahmen ergriffen werden. Erkennungsdienstliche Behandlungen sollten nur erfolgen, wenn der Betroffene eine schwerwiegende Straftat begangen hat und Tatsachen vorliegen, die die Annahme rechtfertigen, daß der Betroffene erneut eine schwerwiegende Straftat begehen wird und die erkennungsdienstlichen Unterlagen dann zur Aufklärung der Straftat erforderlich sind. Es ist jedenfalls auszuschließen, daß Bagatelldelikte[76] zu einer erkennnungsdienstlichen Behandlung führen.

Datenschutzrechtlich bedenklich ist ferner, daß die im Gesetzentwurf der Koalitionsfraktionen aufgeführten erkennungsdienstlichen Maßnahmen nur beispielhaft aufgezählt sind. Wie im F.D.P.-Entwurf sollte die Aufzählung der Maßnahmen abschließend sein. Nur so kann ausgeschlossen werden, daß z. B. tief in die Persönlichkeitsrechte eingreifende Maßnahmen wie *Blutuntersuchungen oder Genomanalysen* vorgenommen werden.

Die Polizei soll „bei oder im Zusammenhang mit" *Veranstaltungen oder Ansammlungen* Ermittlungen anstellen und von Teilnehmern *Bild- und Tonaufzeichnungen* anfertigen können. Diese Maßnahmen sind datenschutzrechtlich besonders bedenklich, da hiervon nicht nur Gewalttäter betroffen sind, sondern regelmäßig eine Vielzahl völlig unbeteiligter Personen, die in keinem Zusammenhang mit Ausschreitungen oder Gewalttätigkeiten stehen. Die Bild- und Tonaufzeichnung von Veranstaltungsteilnehmern kann nach dem Gesetzentwurf bereits erfolgen, wenn Tatsachen die Annahme rechtfertigen, daß diese Straftaten oder Ordnungswidrigkeiten begehen werden. Dies ist zu weitgehend. Derartige Maßnahmen sollten nur zur Verhinderung von Straftaten erfolgen. Darüber hinaus sollte, wie im F.D.P.-Entwurf, klargestellt werden, daß die Datenerhebungen offen, d. h. für die Betroffenen als polizeiliche Maßnahme erkennbar, durchzuführen sind.

Beide Gesetzentwürfe lassen polizeiliche Ermittlungsmethoden zu, die wegen ihrer *Heimlichkeit,* ihrer *Dauer* und der vorgesehenen *technischen Methoden* besonders schwerwiegend in das allgemeine Persönlichkeitsrecht der Betroffenen eingreifen. Dazu zählen die Observation (planmäßig angelegte heimliche Beobachtung einer Person länger als durchgehend 24 Stunden oder an mehr als 2 Tagen), der Einsatz z. B. von „Wanzen", Peilsendern, Richtmikrofonen und Infrarotkameras. Damit werden bis in die Wohnung hinein heimliche, tief in die Privatsphäre der Betroffenen eindringende Überwachungen in verfassungsrechtlich bedenklichem Umfang ermöglicht. Das Recht auf freie Entfaltung der Persönlichkeit und die Menschenwürde sichern jeder Person einen autonomen Bereich privater Lebensgestaltung, in der sie ihre Individualität entwickeln und wahren kann. Hierzu gehört auch der Anspruch, in dieser Sphäre für sich zu sein und sich selber zu gehören.

---

[76] vgl. hierzu unseren Jahresbericht 1990 zu Ziff. 3.5

Die Bundesregierung hat deshalb in ihrer Stellungnahme zum Bundesrats-Entwurf des OrgKG für den Bereich der Strafverfolgung den Einsatz technischer Mittel in Wohnungen abgelehnt. Sie hat Bedenken sowohl hinsichtlich der Zulässigkeit des Abhörens und Aufzeichnens des nicht öffentlich gesprochenen Wortes in Wohnungen als auch hinsichtlich der Zulässigkeit der Herstellung von Lichtbildern und Bildaufzeichnungen in Wohnungen geäußert. Dies muß grundsätzlich auch für den präventiven Bereich gelten, in dem noch nicht einmal als Eingriffsvoraussetzung das Vorliegen eines Straftatverdachts vorausgesetzt wird. Im F.D.P.-Entwurf ist der Einsatz technischer Mittel in Wohnungen ausgeschlossen.

Im Gesetzentwurf der Koalitionsfraktionen wird der Einsatz technischer Mittel bereits zugelassen, wenn die vorbeugende Bekämpfung einer Straftat von erheblicher Bedeutung auf andere Weise wesentlich erschwert oder verzögert würde. Dies ist angesichts des erheblichen Eingriffs in das Persönlichkeitsrecht zu weitgehend. Der Einsatz dieser Mittel muß vielmehr ultima ratio der Informationsverschaffung sein. Diese Maßnahmen können nur zulässig sein, wenn die Aufklärung des Sachverhalts auf andere Weise unmöglich ist. Dazu gehört, daß durch einen abschließenden Straftatenkatalog, der sich auf schwerwiegende Straftaten beschränkt, die gewerbs-, gewohnheitsmäßig oder bandenmäßig begangen werden, normenklare Voraussetzungen geschaffen werden.

Sowohl der Gesetzentwurf der Koalitionsfraktionen als auch der F.D.P.-Entwurf sieht den *Einsatz von verdeckten Ermittlern* und von *V-Leuten* vor, obwohl die Notwendigkeit dieser Maßnahmen im präventiven Bereich selbst unter Polizeipraktikern umstritten ist. Durch diese Maßnahmen wird in schwerwiegender Weise in den Grundsatz der Transparenz der Datenerhebung eingegriffen. Das Auftreten unter einer Legende und die verdeckte Weitergabe von den auf diese Weise erlangten Informationen führt zu einer Täuschung der Betroffenen, die tief in die Privatsphäre hineinreichen kann.

Derart erhebliche Eingriffe in das Persönlichkeitsrecht setzen zumindest voraus, daß bestimmte Tatsachen den Verdacht begründen, daß eine Straftat auf dem Gebiet der organisierten Kriminalität von dem Betroffenen begangen wurde. Der nicht einmal näher präzisierte Verdacht, eine Straftat von erheblicher Bedeutung könne begangen werden, rechtfertigt derartige Eingriffe nicht.

Ermöglicht werden soll das Erstellen (bis zu 2 Jahre dauernder) Bewegungsbilder durch die *polizeiliche Beobachtung*. Danach kann die Polizei zur vorbeugenden Bekämpfung von Straftaten von erheblicher Bedeutung und zur Abwehr von Gefahren für Leib, Leben oder Freiheit einer Person über Jahre festhalten, wann und wo sich eine Person, die als potentieller Straftäter eingestuft wird oder andere Personen, die als Kontaktpersonen angesehen werden, bei Grenz- oder Zollkontrollen festgestellt wurden. Im präventiven Bereich sollte von derart einschneidenden Maßnahmen abgesehen werden. Zumindest sollten für derartige Maßnahmen wesentlich kürzere Befristungen vorgesehen werden und Personen, die sich keiner Straftat verdächtig gemacht haben, von diesen Beobachtungen ausgenommen werden.

Die *Rasterfahndung* ist selbst im repressiven Bereich umstritten. Rasterfahndung ist ein Massengrundrechtseingriff, der ohne Rücksicht auf Verdachtsmomente oder Störereigenschaft eine große Zahl von Personen erfaßt, deren Daten zu ganz anderen Zwecken erhoben wurden. Eine Differenzierung zwischen Verdächtigen und Nichtverdächtigen, zwischen Störern und Nichtstörern findet nicht statt. Diese Maßnahme ist nicht nur wegen des erheblichen Eingriffs in das Persönlichkeitsrecht völlig unbeteiligter Personen bedenklich, sondern auch wegen des Zweckbindungsgebots, da sie tendenziell auf Zweckentfremdung angelegt ist. Der Datenabgleich kann zur Folge haben, daß ein großer Kreis von unbescholtenen Personen für polizeiliche Maßnahmen herangezogen wird, obwohl sie sich nicht verdächtig gemacht haben, sondern nur - zufällig - bestimmte Merkmale erfüllen. Dies ist besonders bedenklich im präventivpolizeilichen Bereich, wo noch nicht einmal ein auf eine bestimmte Person konkretisierter Tatverdacht vorliegen muß. Zudem ist eine Erforderlichkeit dieser Maßnahmen für präventive Zwecke kaum denkbar.

Im allgemeinen Datenschutzrecht Berlins wird besonderer Wert auf die *Transparenz der Datenverarbeitung* gegenüber Bürger und Öffentlichkeit gelegt. Es ist bedauerlich, daß gerade in dieser Hinsicht der Gesetzentwurf deutliche Rückschritte etwa bei der Offenlegung der eingesetzten Informationstechnik oder bei der Akteneinsicht des Bürgers vorsieht. Es ist zu hoffen, daß es gerade hier gelingt, das Niveau des Berliner Datenschutzgesetzes auch im Polizeirecht aufrecht zu erhalten.

Polizei und Schwangerschaftsabbrüche

Die Polizei wurde vor mehr als acht Jahren wegen des Selbstmordversuchs einer jungen Frau gerufen und vermerkte auf dem Einsatzbericht „Verdacht Schwangerschaftsabbruch". Weitere Anhaltspunkte oder Hinweise über die Hintergründe dieses Vermerks existieren nicht.

Die Polizei erhielt den Hinweis, daß eine junge Frau behaupte, ein Kind geboren zu haben. Daraufhin wurden polizeiliche Ermittlungen eingeleitet. Die betroffene Frau gab hierzu an, daß sie eine Fehlgeburt hatte. Die gynäkologische Untersuchung brachte keine Aufklärung. Die polizeilichen Ermittlungen endeten mit der ausdrücklichen Feststellung, daß der Verdacht sich nicht erhärtet habe und nicht geklärt werden konnte, ob die Betroffene überhaupt schwanger war.

Eine junge Frau wurde von ihrem ehemaligen Freund wegen illegalen Schwangerschaftsabbruchs angezeigt. Seine Aussage war widersprüchlich. So sagte er u. a. aus, die Betroffene sei im 7. Monat schwanger gewesen und habe nach einem Sturz das Kind verloren; auf der anderen Seite gab er an, nicht gewußt zu haben, ob sie überhaupt schwanger gewesen sei. Die junge Frau bestritt, schwanger gewesen zu sein. Sie teilte mit, daß ihr Gewicht sich damals wegen Hormonstörungen verändert habe.

Bei einer Hausdurchsuchung anläßlich eines Ermittlungsverfahrens in einem anderen Zusammenhang wurde in der Wohnung ein Embryo in einem Kaffeeglas gefunden. Die Betroffene gab hierzu an, sie habe den Embryo von ihrem Freund geschenkt bekommen und sei davon ausgegangen, daß er „nicht echt" sei. Die polizeilichen Ermittlungen endeten mit dem Vermerk, daß der Tatverdacht sich nicht konkretisieren ließ.

In allen Fällen wurden Daten über die Frauen über Jahre hinweg im Informationssystem Verbrechensbekämpfung gespeichert. Wir haben sie bei einer Überprüfung aller Datensätze im Zusammenhang mit § 218 StGB festgestellt.

Es ist bereits zweifelhaft, ob die jahrelange polizeiliche Erfassung von ehemals Schwangeren, die eines illegalen Schwangerschaftsabbruchs verdächtigt werden - nach Abschluß des Straf- oder Ermittlungsverfahrens - überhaupt für die Aufgabenerfüllung der Polizei erforderlich ist. Dies ist jedenfalls nicht der Fall bei den Frauen, die sich schon nach den Ermittlungen der Polizei nicht gemäß § 218 StGB strafbar gemacht haben.

Aber auch in den Fällen, in denen ein illegaler Schwangerschaftsabbruch vorliegt, ist eine Registrierung der betroffenen Frauen für die polizeiliche Arbeit nicht erforderlich.

Es liegt keine konkrete gegenwärtige Gefahr vor, für deren Bekämpfung diese Datenspeicherungen erforderlich sind. Für die vorbeugende Straftatenbekämpfung ist eine Speicherung der Tatverdächtigen nur verhältnismäßig, wenn diese eine schwerwiegende Straftat begangen haben und aufgrund konkreter Anhaltspunkte eine Wiederholungsgefahr besteht. Dies ist bei illegalen Schwangerschaftsabbrüchen durch schwangere Frauen nicht der Fall.

Zum einen ist angesichts der geringen Strafandrohung und der gesetzlichen Privilegierungen für Schwangere nach §§ 218, 219 StGB zweifelhaft, ob dieses Delikt von derart schwerwiegender Bedeutung ist, daß eine jahrelange Erfassung der Frauen zur vorbeugenden Straftatenbekämpfung verhältnismäßig ist. Zum anderen befinden sich die Frauen, die sich zu diesem Schritt entschließen, in einer besonderen Konfliktsituation. Eine konkret bestehende Wiederholungsgefahr ist hier nicht ersichtlich. Daß eine weitere Schwangerschaft und damit ein erneuter (auch ille-

galer) Schwangerschaftsabbruch grundsätzlich möglich ist, kann nicht als Begründung für eine vorsorgliche polizeiliche Speicherung herangezogen werden, da dann alle Frauen im gebärfähigen Alter vorsorglich registriert werden müßten. Darüber hinaus ist die polizeitaktische Notwendigkeit derartiger Speicherungen nicht erkennbar. Wie soll die Speicherung dieser Vorgänge zu einer Verhinderung oder Aufklärung künftiger illegaler Schwangerschaftsabbrüche dieser Frauen beitragen?

Im übrigen ist zu bemängeln, daß - nicht einmal bei völlig vagen Beschuldigungen und Verdächtigungen - der Verfahrensausgang in Erfahrung gebracht wurde. Es ist davon auszugehen, daß bei einem Großteil der Vorgänge Verfahrenseinstellungen oder Freisprüche erfolgt sind, die zu einer Löschung der Daten hätte führen müssen.

Der Polizeipräsident hat inzwischen mitgeteilt, daß bis auf einen Fall die Daten sämtlicher Frauen zu § 218 gelöscht wurden. In einem Fall sei die Prüfung noch nicht abgeschlossen. Zur künftigen Verfahrensweise hat der Polizeipräsident dargelegt, daß er bei Verdacht des Vorliegens eines Verstoßes nach § 218 StGB „ohne Speicherung weiterer Ermittlungsverfahren von der Erfassung der Frauen zur vorbeugenden Verbrechensbekämpfung absehen" werde.

Das bedeutet, daß jeder andere Straftatverdacht auch künftig zu einer polizeilichen Registrierung von Frauen wegen des illegalen Abbruchs ihrer Schwangerschaft führen wird.

Diese Verfahrensweise widerspricht dem verfassungsmäßigen Verhältnismäßigkeitsgrundsatz. Hier wird - überspitzt formuliert - nach dem Motto „Wer klaut, treibt auch noch mal ab" verfahren. Wie bereits dargelegt, ist die Registrierung von Frauen, die einen illegalen Schwangerschaftsabbruch begangen haben, für die Aufgabenerfüllung der Polizei schon wegen der Einmaligkeit dieser Zwangssituation nicht erforderlich. Ungeachtet der Problematik, daß durch eine polizeiliche Speicherung ohnehin künftig keine Schwangerschaftsabbrüche durch die betroffenen Frauen verhindert werden können, ist auch nicht ersichtlich, warum andere Straftaten, deren die Frauen völlig unabhängig von der illegalen Abtreibung verdächtigt werden, eine vorsorgliche Registrierung auch des Schwangerschaftsabbruchs zur vorbeugenden Straftatenbekämpfung erforderlich machen sollten.

Lichtbildsammlung und Lichtbildvorzeigekartei

In unserem letzten Jahresbericht hatten wir auf einen Fall hingewiesen, in dem ein junges Mädchen nach dem Diebstahl eines Schokoladenriegels durch Abnahme von Fingerabdrücken und Fotoaufnahmen erkennungsdienstlich behandelt wurde. Dies nahmen wir zum Anlaß einer eingehenden Prüfung.

Ende September 1991 waren in der Lichtbildsammlung der Polizei 116 444 Personen und in der Lichtbildvorzeigekartei 16 426 Personen registriert.

Ist die erkennungsdienstliche Behandlung ausschließlich für die Strafverfolgung erforderlich (§ 81 b 1. Alt. StPO), sind die gewonnenen Unterlagen zur Ermittlungsakte zu nehmen und an die Staatsanwaltschaft zu übersenden.

Bei der erkennungsdienstlichen Behandlung gem. § 81 b 2. Alt. StPO und § 16 Abs. 1 ASOG erfolgt dagegen eine karteimäßige Aufbewahrung der erkennungsdienstlichen Unterlagen. Die Lichtbilder werden in die Lichtbildsammlung und in bestimmten Fällen in die Lichtbildvorzeigekartei für die Vorlage an Zeugen in Strafverfahren aufgenommen.

§ 16 ASOG und § 81 b StPO regeln nur die Befugnis zur Durchführung erkennungsdienstlicher Maßnahmen. Es fehlen jedoch konkrete gesetzliche Regelungen, in denen die Speicherung in erkennungsdienstlichen Sammlungen erlaubt wird. Die Speicherung und Nutzung der erkennungsdienstlichen Unterlagen kann daher nur auf die Übergangsregelung des § 34 Abs. 1 BlnDSG gestützt werden.

Die Speicherung und weitere Nutzung erkennungsdienstlicher Unterlagen zur vorbeugenden Straftatenbekämpfung sollte sich deshalb auf erhebliche Straftaten beschränken, wenn eine konkrete Wiederholungsgefahr besteht.

Auch nach der Rechtsprechung des Bundesverwaltungsgerichts rechtfertigt nicht jede Anordnung einer erkennungsdienstlichen Maßnahme auch automatisch die Speicherung und weitere Nutzung zu präventiven Zwecken. Die Aufbewahrung von erkennungsdienstlichen Unterlagen ist danach nur zulässig, wenn unter Berücksichtigung aller Umstände des Einzelfalls - insbesondere angesichts der Art, Schwere und Begehungsweise der dem Betroffenen zur Last gelegten Straftaten, seiner Persönlichkeit sowie des Zeitraums, während dessen er strafrechtlich nicht (mehr) in Erscheinung getreten ist - Anhaltspunkte für die Annahme bietet, daß der Betroffene auch künftig oder anderwärts gegenwärtig strafrechtlich in Erscheinung treten wird und daß die erkennungsdienstlichen Unterlagen die dann zu führenden Ermittlungen fördern könnten.

Aufgrund der Ergebnisse unserer Überprüfung ergibt sich die Vermutung, daß die erforderliche differenzierte Einzelfallentscheidung und Prognosebeurteilung weder durch den Sachbearbeiter der ermittelnden Dienststelle, der die erkennungsdienstliche Maßnahme anordnet, noch durch die Stelle, die die Lichtbildsammlung und die Lichtbildvorzeigekartei führt, in ausreichendem Umfang erfolgt.

Der Sachbearbeiter der ermittelnden Dienststelle, der die erkennungsdienstliche Behandlung anordnet, gibt lediglich in einem Formular das Delikt an und kreuzt die Rechtsgrundlage an. Weder die konkreten Gründe für die Durchführung der erkennungsdienstlichen Behandlung, noch für die Einstellung in die Lichtbildsammlung - insbesondere die Prognoseentscheidung - werden dokumentiert. Dies macht der Stelle, die die Lichtbildsammlung führt, vor der Aufnahme der angelieferten erkennungsdienstlichen Lichtbilder in die Lichtbildsammlung eine Prüfung der Zulässigkeitsvoraussetzungen unmöglich. Diese übernimmt in der Regel ungeprüft die übersandten Fotos in die Lichtbildsammlung. Eigene Überprüfungen erfolgen nur in Ausnahmefällen, wenn die Unverhältnismäßigkeit der Speicherung schon aufgrund des angegebenen Delikts offensichtlich ist.

Die Stelle, die die Lichtbildsammlung führt, ist als speichernde Stelle verantwortlich für die Speicherung der erkennungsdienstlichen Fotoaufnahmen, auch wenn andere Stellen die erkennungsdienstlichen Maßnahmen durchführen. Sie muß deshalb in die Lage versetzt werden, eine eigenständige Entscheidung treffen zu können. Dies setzt voraus, daß eine Unterrichtung über den zugrundeliegenden Sachverhalt sowie die Gründe sichergestellt sind, die zu einer erkennungsdienstlichen Behandlung geführt haben und die eine weitere Speicherung rechtfertigen. Allein die Deliktsangabe und das Ankreuzen der Rechtsgrundlage über die erkennungsdienstliche Behandlung durch den Beamten der ermittelnden Dienststelle auf einem Formular reichen hierfür nicht aus.

Ferner ist es mit den dargelegten Grundsätzen zur Aufbewahrung erkennungsdienstlicher Unterlagen nicht zu vereinbaren, daß bei der Lichtbildvorzeigekartei bei bestimmten Delikten auf die Prüfung der Wiederholungsgefahr verzichtet wird. Auch und gerade bei dieser Kartei, in die Dritte Einsicht nehmen, sind alle Umstände des Einzelfalls (z. B. auch seit wann der Betroffene nicht [mehr] strafrechtlich in Erscheinung getreten ist) zu berücksichtigen und die Tatsachen, die der Prognoseentscheidung zugrundeliegen, konkret festzustellen. Zudem muß an der Erfassung der Beschuldigten in der Lichtbildvorzeigekartei, z. B. wegen der Art oder Schwere der von ihnen begangenen Straftat, ein besonderes Interesse dargelegt werden.

Wir empfehlen daher, daß die ermittelnde Dienststelle - wie dies bereits für das Personenfeststellungsverfahren vorgesehen ist - den erkennungsdienstlichen Unterlagen künftig eine kurze Begründung anfügt, aus der sich auch die Notwendigkeit der weiteren Speicherung für die vorbeugende Straftatenbekämpfung ergibt. Die Stelle, die die Lichtbildsammlung und die Lichtbildvorzeigekartei führt, wird damit in die Lage versetzt, durch entsprechende Prüfung seinen Pflichten als speichernde Stelle vor der Aufnahme in die Lichtbildsammlung nachzukommen.

Wir empfehlen ferner, daß auch die Stelle, die die Lichtbildvorzeigekartei führt, die Entscheidung für die Aufnahme und Speicherung in der Lichtbildvorzeigekartei künftig durch einen kur-

zen Vermerk dokumentiert und damit die Überprüfbarkeit dieser Entscheidung durch den Betroffenen, den Datenschutzbeauftragten und die Gerichte gewährleistet.

Zu kritisieren ist ferner, daß eine Überprüfung der Verfahrensausgänge selbst bei den in der Lichtbildvorzeigekartei gespeicherten Fotoaufnahmen unterbleibt. Es ist deshalb nicht auszuschließen, daß in den Karteien Lichtbilder von Personen enthalten sind, die keine Straftat begangen haben und daß diese sogar Zeugen im Rahmen von Strafverfahren vorgelegt werden. Dies ist ein Mißstand, auf den wir wiederholt bei der Datenspeicherung zur vorbeugenden Straftatenbekämpfung hingewiesen haben und der gerade bei der Lichtbildvorzeigekartei einen besonders schwerwiegenden Eingriff für den Betroffenen darstellt. Bis zur Einrichtung des von uns seit Jahren geforderten Rückmeldeverfahrens über den Verfahrensausgang sollte im Hinblick auf die notwendige Pflege der Lichtbildvorzeigekartei und der Lichtbildsammlung eine aktive Erkundigung nach dem Ausgang gerichtlicher Verfahren erfolgen.

3.4.2 Verfassungsschutz

Rechtliche Grundlagen fehlen

Wiederholt haben wir darauf hingewiesen[77], daß die erforderlichen gesetzlichen Grundlagen zum Umgang des Landesamtes für Verfassungsschutz mit den Daten der Bürger noch immer fehlen. Auch nach Inkrafttreten des novellierten *Bundesverfassungsschutzgesetzes* Ende 1990[78] waren keine Gesetzgebungsaktivitäten in Berlin erkennbar.

Wegen der schwerwiegenden Informationseingriffe, die mit der Arbeit des Landesamtes für Verfassungsschutz verbunden sind, ist eine intensive Beratung der zu schaffenden gesetzlichen Grundlagen erforderlich. Die Novellierung des Berliner Gesetzes über das Landesamt für Verfassungsschutz muß deshalb umgehend vorgelegt werden, damit die parlamentarische Beratung in einem der Bedeutung der Angelegenheit angemessenen Zeitrahmen erfolgen kann.

Keine Löschungen beim Verfassungsschutz

Weiterhin ungelöst ist das Problem des anwachsenen Datenberges wegen des in der letzten Legislaturperiode im Zusammenhang mit der Arbeit des Untersuchungsausschusses ergangenen Löschungs- und Vernichtungsverbots. Wir haben mehrfach darauf hingewiesen[79], daß dieses Verfahren nicht mehr tragbar ist. Wir haben eindringlich empfohlen, das Verbot aufzuheben, da es den betroffenen Bürgern nicht zuzumuten ist, daß ihre zu löschenden Daten, die in keinem Zusammenhang mit dem Auftrag des Untersuchungsausschusses stehen, dennoch weiterhin beim Landesamt für Verfassungsschutz gespeichert werden.

Sollte auch weiterhin die erforderliche Löschung der Daten unterbleiben, sind diese zumindest zu sperren. Die gesperrten Daten dürfen nicht mehr verarbeitet, insbesondere übermittelt oder sonst genutzt werden, es sei denn, daß die Nutzung zu wissenschaftlichen Zwecken oder zur Behebung einer Beweisnot unerläßlich ist und der Betroffene eingewilligt hat (§ 17 Abs. 2 BlnDSG). Durch technische und organisatorische Maßnahmen ist die Beachtung dieses Datenverarbeitungsverbots sicherzustellen. Die zu sperrenden Akten bzw. Aktenbestandteile und Daten aus manuellen Dateien sind gesondert zu lagern und durch organisatorische Maßnahmen ist sicherzustellen, daß ein Zugriff ausgeschlossen ist. Auch für Datenspeicherungen im bundesweiten Informationssystem NADIS sind besondere Schutzmaßnahmen erforderlich. Das Landesamt für Verfassungsschutz setzt sich im Rahmen der NADIS-Gremien dafür ein, daß hierfür die technischen Möglichkeiten zur Verfügung gestellt werden. Eine entsprechende Vereinbarung konnte bisher jedoch nicht erzielt werden.

Fotos beim Verfassungsschutz

Ein Bürger, der beim Landesamt für Verfassungsschutz in seine Akte Einsicht nahm, stellte zu seiner Überraschung fest, daß sich darin auch sein Paßfoto befand.

Unsere Überprüfung ergab, daß das Foto tatsächlich vom Landeseinwohneramt aus dem Paßantrag des Betroffenen stammt. Das Landesamt für Verfassungsschutz hatte das Foto beim Landeseinwohneramt abgeholt. Dem zugrunde lag die Zusendung einer Liste mit Namen von 520 Teilnehmern einer Demonstration, die von der Polizei eingeschlossen wurden und deren Identität festgestellt worden war.

Das Landesamt für Verfassungsschutz hatte Anhaltspunkte dafür, daß sich unter den festgenommenen Personen auch militante Autonome befanden und holte zur Auswertung die Paß- bzw. Ausweisfotos aller festgehaltenen Berliner und Berlinerinnen beim Landeseinwohneramt ab.

Nach dem Paßgesetz und der damals noch anwendbaren BK/O der Alliierten über Personalausweise dürfen die Paß- bzw. Ausweisbehörden anderen Behörden auf deren Ersuchen Daten aus dem Paß- bzw. Ausweisregister - wozu auch das Lichtbild gehört - nur übermitteln, wenn

- die ersuchende Behörde aufgrund von Gesetzen oder Rechtsverordnungen berechtigt ist, solche Daten zu erhalten,
- die ersuchende Behörde ohne Kenntnis der Daten nicht in der Lage wäre, eine ihr obliegende Aufgabe zu erfüllen und
- die Daten bei dem Betroffenen nicht oder nur mit unverhältnismäßigen Aufwand erhoben werden können oder nach Art der Aufgabe, zu deren Erfüllung die Daten erforderlich sind, von einer solchen Datenerhebung abgesehen werden muß.

Das Landesamt für Verfassungsschutz hat nach den genannten Bestimmungen als ersuchende Behörde die Verantwortung dafür zu tragen, daß diese Übermittlungsvoraussetzungen vorliegen.

Das Gesetz über das Landesamt für Verfassungsschutz enthält keine den Bestimmtheitsanforderungen des Bundesverfassungsgericht entsprechenden Normen zur Speicherung und Nutzung personenbezogener Daten. Auch die generalklauselartig formulierte Auskunftsberechtigung gegenüber anderen Behörden entspricht in keiner Weise den verfassungsrechtlichen Anforderungen, die an derart weitgehende Informationseingriffe zu stellen sind. Die erforderliche Berechtigung, die Paß- bzw. Ausweisfotos zu erhalten, konnte somit nur auf den Übergangsbonus gestützt werden.

Bis zur Herstellung eines verfassungsmäßigen Zustandes durch den Gesetzgeber reduziert sich die Befugnis zu Eingriffen in das verfassungsrechtlich geschützte Recht auf informationelle Selbstbestimmung auf das, was im konkreten Fall für die geordnete Weiterführung eines funktionsfähigen Betriebes unerläßlich ist. Mit diesem Grundsatz nicht zu vereinbaren ist die Anforderung und Nutzung von Lichtbildern sämtlicher von der Polizei festgestellten Teilnehmer einer Demonstration. Auch die Speicherung der Personalien aller Betroffenen im NADIS war von Anfang an unzulässig.

Von Maßnahmen des Verfassungsschutzes darf nur derjenige erfaßt werden, dessen Verhalten konkrete Anhaltspunkte für relevante verfassungsfeindliche Bestrebungen im Sinne von § 2 Abs. 1 Nr. 1 des Gesetzes über das Landesamt für Verfassungsschutz gezeigt hat. Das Bundesverfassungsgericht hat im Volkszählungsurteil den Schutz der Teilnehmer an Veranstaltungen vor Datenerhebungen und -speicherungen besonders hervorgehoben.

Deshalb ist gerade bei Demonstrationsteilnehmern eine besondere Zurückhaltung bei Informationseingriffen erforderlich.

Aufgabe des Verfassungsschutzes ist in erster Linie die Beobachtung von Personenzusammenschlüssen und nicht von Einzelpersonen. Eingriffe in das Recht auf informationelle Selbstbestimmung von Einzelpersonen, die nicht in einem oder für einen Personenzusammenschluß handeln, sind auf ein unerläßliches Maß zu beschränken. Deshalb hat auch der Bundesgesetzgeber im neuen Bundesverfassungsschutzgesetz darauf abgestellt, daß das Verhalten dieser Einzelpersonen nur relevant ist, wenn es als verfassungsfeindliche Bestrebung auf Anwendung von Gewalt gerichtet ist oder aufgrund seiner Wirkungsweise geeignet ist, ein Schutzgut dieses Gesetzes erheblich zu beschädigen. Einzelpersonen sollen nur vom Verfassungsschutz erfaßt werden, wenn sie

[77] letztmalig Jahresbericht 1990, Ziff. 3.5
[78] BGBl. 1990, S. 2953
[79] letztmals Jahresbericht 1990, Ziff. 3.5

Aktivitäten oder Verhaltensweisen an den Tag legen, die eine erhebliche Gefährdung darstellen, wie z. B. gewaltbezogene Einzeltäterschaft aus politischer Motivation.

3.4.3 Ausländer

Lernentwicklungsberichte gehören nicht in die Ausländerakte

Ein 17jähriger Schüler, der nicht die deutsche Staatsangehörigkeit besitzt, beschwerte sich bei uns darüber, daß die Ausländerbehörde ihn aufgefordert habe, eine Kopie des Lernentwicklungsberichts der von ihm besuchten Schule vorzulegen. Dieser drei Seiten lange Bericht enthält detaillierte Angaben über das schulische Verhalten des jungen Mannes und über seine Leistungen in den einzelnen Schulfächern.

Auf unsere Anfrage teilte die Ausländerbehörde mit, daß der junge Mann zwecks Erteilung einer *unbefristeten Aufenthaltserlaubnis* vorgesprochen habe. Voraussetzung hierfür sei bei einem ununterbrochenen Aufenthalt von weniger als fünf Jahren auch der Nachweis über ausreichende Deutschkenntnisse. Der Lernentwicklungsbericht wurde als Sprachnachweis in Fotokopie zur Akte genommen.

Dieses Verfahren war unzulässig. Gemäß § 9 BlnDSG ist die Speicherung personenbezogener Daten nur zulässig, wenn sie zur rechtmäßigen Aufgabenerfüllung und für den jeweils damit verbundenen Zweck erforderlich ist.

In dem Lernentwicklungsbericht sind überwiegend Angaben enthalten, die für die Beurteilung der Deutschkenntnisse in keiner Weise erforderlich sind. Das Wissen des Petenten über Oxidations- und Reduktionsreaktionen, über die Probleme der Sahelzone und die Situation in Südafrika, seine Leistungen in Englisch, Mathematik, Arbeitslehre, Bildende Kunst, Musik und Sport sowie sein Betragen im Unterricht sind für die Erteilung der beantragten unbefristeten Aufenthaltserlaubnis völlig überflüssige Angaben.

Die Ausländerbehörde hat die Kopien über den Lernentwicklungsbericht aus der Ausländerakte entfernt und dem betroffenen Schüler zurückgegeben.

Mit Inkrafttreten des neuen Ausländergesetzes am 1. Januar 1991 ist ein schriftlicher *Nachweis für die Sprachkenntnisse* bei der Erteilung der unbefristeten Aufenthaltserlaubnis nicht mehr vorgesehen. Es genügt danach, wenn sich der Ausländer auf einfache Art in deutscher Sprache mündlich verständigen kann. Die Ausländerbehörde hat ihre Mitarbeiter davon in Kenntnis gesetzt, daß keine Schulzeugnisse von Antragstellern gefordert werden dürfen und künftig nur die vom Gesetzgeber vorgesehenen Unterlagen vom Antragsteller verlangt und ggf. zur Akte genommen werden dürfen.

Ausländergesetz

Auf die datenschutzrechtliche Problematik des neuen Ausländergesetzes und den darin enthaltenen, sehr weitgehend formulierten Übermittlungspflichten sind wir im letzten Jahresbericht ausführlich eingegangen.

Eine stichprobenhafte *Überprüfung* bei der Ausländerbehörde hat nicht die Befürchtung bestätigt, daß massenweise Angaben über Ausländer von verschiedensten Behörden übermittelt werden.

Die angekündigten *bundeseinheitlichen Verwaltungsvorschriften,* die insbesondere auch die Datenübermittlungsbestimmungen konkretisieren und verfassungsgemäß begrenzen müssen, liegen auch nach über einem Jahr nach Inkrafttreten des Gesetzes noch immer nicht vor.

Im Februar 1991 legte der Bundesinnenminister einen ersten Entwurf von *vorläufigen Anwendungshinweisen* zu den Datenübermittlungsbestimmungen vor. Der Entwurf weist jedoch erhebliche Mängel auf:

- Die vorgesehene Einschränkung der erforderlichen *Einzelfallentscheidung* ist verfassungsrechtlich bedenklich. Auch Mitteilungen und Unterrichtungen dürfen nur unter strikter Beachtung des Verhältnismäßigkeitsgrundsatzes erfolgen. Vor jeder Übermittlung ist zu prüfen, ob die mit ihr verbundenen Nachteile für den Betroffenen so schwerwiegend sind, daß sie die öffentlichen Interessen an der Datenübermittlung überwiegen. In diesem Fall hat die Informationsweitergabe zu unterbleiben.
- Erkenntnisse, die laut Entwurf „im Rahmen" der Aufgabenerfüllung öffentlicher Stellen anfallen, dürfen nicht grundsätzlich *übermittelt* werden. Nur die Erkenntnisse dürfen übermittelt werden, die die zur Übermittlung verpflichtete Stelle zur Erfüllung *ihrer* Aufgaben erlangt hat. Es muß ausgeschlossen werden, daß öffentliche Stellen als verlängerter Arm der Ausländerbehörde Ausländer ausfragen oder sonst Daten erheben, die sie selbst für ihre Aufgaben nicht benötigen.
- Über Ausländer, die einem *besonderen Ausweisungsschutz* unterliegen, dürfen Daten grundsätzlich nicht rein vorsorglich an die Ausländerbehörde übermittelt werden. Aus Gründen der Rechtsklarheit ist eine differenzierte und klar begrenzte Datenübermittlungsregelung für die dem besonderen Ausweisungsschutz unterliegenden Ausländergruppen erforderlich. Die im Entwurf vorgesehene weitgehende Datenübermittlung auf Vorrat für diesen Personenkreis ist nicht hinnehmbar.
- Die übermittelnde Stelle ist nach dem Rechtsstaatsprinzip verpflichtet, vor jeder Übermittlung zu prüfen, ob die Informationen für den Erlaß einer konkreten ausländerrechtlichen Maßnahme erforderlich sind. Eine *Übermittlung auf Verdacht* ist unzulässig. Dies gilt ebenfalls für Bestimmungen, wonach Datenübermittlungen im Zweifel immer zu erfolgen haben, auch wenn die Eingriffsvoraussetzungen nicht eindeutig vorliegen und nur vermutet werden. Dies ist verfassungsrechtlich unzulässig. Datenübermittlungen haben bei Zweifeln an deren Rechtsmäßigkeit zu unterbleiben.

Auch das Bundesjustizministerium hat inzwischen eine Reihe der Datenübermittlungsregelungen in dem Entwurf der bundeseinheitlichen vorläufigen Anwendungshinweise kritisiert.

Der vom Bundesinnenministerium vorgelegte Entwurf von vorläufigen Anwendungshinweisen wurde in Berlin in einer Arbeitsgruppe unter Leitung der Ausländerbeauftragten mit unserer intensiven Mitwirkung und mit Beteiligung der betroffenen Verwaltungen eingehend beraten. Die Arbeitsgruppe hat mehrheitlich einen Alternativentwurf zu den Datenübermittlungsregelungen beschlossen, der weitgehend unsere Kritikpunkte berücksichtigt. Die Senatsinnenverwaltung hat den Alternativentwurf an den Bundesminister des Innern weitergeleitet.

Eine überarbeitete, die Datenschutzbelange in angemessener Form berücksichtigende Fassung der bundeseinheitlichen vorläufigen Anwendungshinweise oder Verwaltungsvorschriften wurde bisher nicht vorgelegt.

Allerdings hat die Senatsverwaltung für Inneres einen Entwurf von *vorläufigen Anwendungshinweisen zur Datenübermittlung* vorgelegt und den Berliner Senatsverwaltungen mitgeteilt, daß keine Einwände dagegen bestehen, daß der Entwurf auch den nachgeordneten Einrichtungen der Hauptverwaltungen oder den Bezirksverwaltungen zugeleitet wird. In keiner Weise berücksichtigt wurden unsere zu diesem Entwurf vorgebrachten Einwendungen und Änderungsvorschläge. Bemerkenswert ist weiterhin, daß zwar eine landesweite Verbreitung dieses Entwurfs erfolgt, jedoch die Senatsinnenverwaltung darauf hinweist, daß es sich „nicht um eine abschließende oder befristet geltende Interpretation handelt und das diesem Papier mit Blick auf die anders konzipierten Verwaltungsvorschriften des Bundes auch keine temporäre Verbindlichkeit zukommen kann". Damit dürfte die Verwirrung der Rechtsanwender komplett sein.

Ein weiteres Problem im Zusammenhang mit dem Ausländergesetz ist, daß darin keine Bestimmungen über die Speicherung personenbezogener Daten in Akten enthalten sind. Nach dem Berliner Datenschutzgesetz ist hierfür eine bereichsspezifische gesetzliche Grundlage zu schaffen.

Ausländerzentralregister

Die Verarbeitung von Informationen über ausländische Mitbürger richtet sich nicht nur nach den Bestimmungen im Ausländergesetz. Diese regeln insbesondere die Datenspeicherung bei

Ausländerbehörden, die Weitergabe dieser Daten und die Datenübermittlung durch andere Stellen an die Ausländerbehörden.

Daneben existiert als bundesweites Auskunftssystem über Ausländer das Ausländerzentralregister. Der Bundesminister des Innern hat nach jahrelangen Vorarbeiten und diversen Gesetzentwürfen[80] erneut einen Referentenentwurf für ein Ausländerzentralregistergesetz vorgelegt.

Dieser Gesetzentwurf ist wegen der darin vorgesehenen Funktionserweiterungen des Registers bedenklich. Nach dem Entwurf soll das Register sich nicht nur auf den Nachweis darüber beschränken, ob eine Ausländerbehörde Unterlagen über einen bestimmten Ausländer führt. Es ist darüber hinaus eine Nutzung für polizeiliche Aufgaben vorgesehen, z. B. durch die Einstellung des polizeilichen Fahndungsbestandes und die Registrierung aller Ausländer, die nach Auffassung der Polizei bestimmte Straftaten planen, begehen, begangen haben oder als potentielle Opfer in Betracht kommen. Ferner besteht die Gefahr, daß wesentliche Angaben dem Ausländerzentralregister selbst entnommen werden und der Rückgriff auf die bei den örtlichen Ausländerbehörden vorhandenen Akten unterbleibt. Dies kann dazu führen, daß verkürzte, aus dem Zusammenhang gerissene Daten zur Grundlage von Entscheidungen gegen den Betroffenen gemacht werden.

Überdies umgeht der Gesetzentwurf die Datenübermittlungsbestimmungen des Ausländergesetzes. So ist z. B. abweichend vom Ausländergesetz vorgesehen, daß das Bundeskriminalamt, der Verfassungsschutz oder die mit grenzpolizeilichen Aufgaben betrauten Behörden Daten über möglicherweise gefährdete Ausländer an das Ausländerzentralregister übermitteln und damit den Ausländerbehörden zur Verfügung stellen.

Die weitreichenden Übermittlungspflichten verschiedenster Behörden an das Ausländerzentralregister, umfangreiche Zugriffsmöglichkeiten z. B. durch Polizei, Staatsanwaltschaft, Gerichte und Verfassungsschutz, bis hin zum Online-Zugriff, der Umfang der gespeicherten Daten und nicht zuletzt die Verknüpfungen mit polizeilichen Zwecken machen das Ausländerzentralregister zu einem zentralen Informationssystem über Ausländer, das in der konzipierten Form nicht mit dem Grundsatz der Verhältnismäßigkeit zu vereinbaren ist.

Erkennungsdienstliche Behandlung von Asylbewerbern

Am 3. Mai 1991 hat die Ständige Konferenz der Innenminister und -senatoren der Länder im Zusammenhang mit der *Einführung eines automatisierten Fingerabdruckverfahrens* (AFIS) beschlossen, „das erkennungsdienstliche Material *aller* Asylantragsteller zu erfassen". Dies wird dahingehend verstanden, daß alle Ausländer, die einen Asylantrag stellen, erkennungsdienstlich zu behandeln sind. Dabei soll jeweils ein 10-Finger-Abdruck genommen werden.

Gemäß § 13 Abs. 1 *Asylverfahrensgesetz* (AsylVfG) sind erkennungsdienstliche Maßnahmen nur zulässig, wenn die Identität des Betroffenen nicht eindeutig bekannt ist. Bei jedem einzelnen Betroffenen, der nach dieser Vorschrift einer erkennungsdienstlichen Behandlung unterzogen werden soll, ist somit konkret festzustellen, aufgrund welcher Tatsachen Zweifel daran bestehen, daß die angegebenen Personalien zutreffen. Eine pauschale erkennungsdienstliche Behandlung *aller* Asylbewerber - ohne Berücksichtigung des Einzelfalles - widerspricht § 13 AsylVfG.

In Berlin werden generell Asylbewerber aus Ghana, Senegal, Zaire und Libanon sowie Palästinenser erkennungsdienstlich behandelt. Die Senatsverwaltung für Inneres vertritt hierzu die Auffassung, daß diese bundesweit geübte Praxis einer erkennungsdienstlichen Behandlung von Asylbewerbern aus Staaten, in denen aufgrund polizeilicher Erfahrung häufig gefälschte Identitätspapiere in Gebrauch sind oder auch legale Möglichkeiten eines vereinfachten Wechsels der Identität bestehen, sich im Rahmen des geltenden Rechts halte. Die Identität dieser Personen sei „nicht eindeutig bekannt" im Sinne des § 13 Abs. 1 AsylVfG.

Wir haben gegen die Praxis, Asylbewerber aus bestimmten Herkunftsländern generell erkennungsdienstlich zu behandeln, erhebliche Bedenken. Selbst wenn bei Asylbewerbern aus bestimmten Staaten erfahrungsgemäß häufig Fälle von Identitätstäuschung vorkommen, kann dies nicht von der Prüfung der Erforderlichkeit im Einzelfall nach § 13 AsylVfG entbinden. Es ist mit dem Gesetz nicht zu vereinbaren, pauschal bei jedem Asylbewerber aus den genannten Ländern und jedem Palästinenser von einer Identitätstäuschung auszugehen.

Es liegt inzwischen jedoch ein Arbeitspapier des Bundesinnenministers mit dem Titel „Entwurf eines Gesetzes zur Neuregelung des Asylverfahrens" vor, das im Gegensatz zum geltenden § 13 AsylVfG die erkennungsdienstliche Behandlung *aller* Asylsuchender vorsieht. Da erkennungsdienstliche Maßnahmen in das allgemeine Persönlichkeitsrecht und u. U. in die körperliche Bewegungsfreiheit eingreifen (Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1; Art. 2 Abs. 2 GG), bedarf es einer gesetzlichen Ermächtigung, die den rechtsstaatlichen Anforderungen an Bestimmtheit und Verhältnismäßigkeit gerecht wird. Dies ist bei einer Regelung, die pauschal für alle Asylbewerber ohne besondere Voraussetzungen erkennungsdienstliche Maßnahmen vorsieht, zu bezweifeln.

3.4.4 Statistik

Der *Entwurf eines Landesstatistikgesetzes* ist am 14. November 1991 zum dritten Mal in das Abgeordnetenhaus eingebracht worden[81]. Es ist zu hoffen, daß dieser Entwurf, der in seinen Grundzügen einer jahrelangen Forderung des Berliner Datenschutzbeauftragten entspricht, nun endlich zügig verabschiedet wird. Damit würde die amtliche Statistik im Land Berlin zum ersten Mal auf eine gesetzliche Grundlage gestellt, die längst überfällig ist.

In zwei Punkten berücksichtigt der Entwurf unsere Empfehlungen allerdings noch nicht. So läßt der Entwurf die Deanonymisierung von statistischen Einzeldatensätzen zu, die aus dem Verwaltungsvollzug für statistische Zwecke genutzt werden. Dies würde das Statistikgeheimnis gegenüber dem Bundesrecht in nicht hinnehmbarer Weise einschränken.

Zudem soll die gesetzliche Vorgabe, daß Daten aus dem Verwaltungsvollzug nur aufgrund einer Rechtsverordnung dem Statistischen Landesamt zur Verfügung gestellt und von diesem nur aufgrund einer Rechtsvorschrift miteinander verknüpft und ausgewertet werden dürfen, lediglich für Daten gelten, die dem Statistischen Landesamt nach Inkrafttreten des Gesetzes übermittelt worden sind. Nach der Begründung des Entwurfs können Daten, die dem Statistischen Landesamt vor Inkrafttreten des Landesstatistikgesetzes aus dem Verwaltungsvollzug ohne gesetzliche Grundlage übermittelt wurden, auf Dauer weitergespeichert bleiben, ohne daß die erforderliche besondere Verarbeitungsbefugnis zumindest nachträglich geschaffen werden muß. Dies widerspricht dem Berliner Datenschutzgesetz, das jede Verarbeitung - also auch Nutzung - personenbezogener Daten entweder von einer besonderen Rechtsvorschrift oder von der Einwilligung der Betroffenen abhängig macht. Der Gesetzgeber hat deshalb nur zwei Möglichkeiten: entweder kann er dem Statistischen Landesamt eine Übergangsfrist bis zur Löschung dieser bisher aus dem Verwaltungsvollzug übermittelten Daten einräumen, oder er muß (ggf. innerhalb einer bestimmten Frist) eine Verarbeitungsbefugnis für diese bereits vorhandenen Daten durch besondere Rechtsvorschrift schaffen. Hinsichtlich der Übermittlung von Daten aus dem Verwaltungsvollzug kann dies auch durch Rechtsverordnung geschehen.

Das Statistische Landesamt führte im Frühjahr 1991 im Auftrag des Statistischen Amtes der EG und des Statistischen Bundesamtes eine Testbefragung auf freiwilliger Basis durch, bei der die Interviewer *Laptops* zur Erfassung der Antworten einsetzten. Grundlage dieses Versuchs war das Fragenprogramm der Mikrozensus-Befragung, das der Interviewer menügesteuert auf dem tragbaren Computer abrufen und elektronisch „ausfüllen" konnte. Die Befragung erstreckte sich auf ca. 500 Haushalte und wurde durch ein Anschreiben angekündigt, in dem allerdings der Einsatz von Laptops nicht erwähnt wurde, um einen Test unter realen Bedingungen „mit Überraschungseffekt" durchführen zu können. Allerdings erhielt der Befragte in jedem Fall die Möglichkeit, einen Fragebogen in seiner Wohnung per Hand auszu-

[80] vgl. Beschluß der Konferenz der Datenschutzbeauftragten vom 4./5. Mai 1987; Jahresbericht 1987, Anlage 4

[81] Drs 12/820

füllen und ihn per Post zurückzuschicken, falls er die Befragung mittels des Bauchladen-Computers ablehnte.

Wir haben eine Reihe von Empfehlungen zur Sicherung der Daten auf dem Laptop gegeben, die unseren bereits im vergangenen Jahr gegebenen allgemeinen Empfehlungen für den Einsatz von Laptops entsprachen[82]. Entscheidend ist jedoch beim Einsatz tragbarer Computer zur Durchführung statistischer Befragungen, daß dem Befragten tatsächlich die Wahlmöglichkeit eingeräumt wird, ob er dem Interviewer gegenüber die Fragen mündlich beantworten will und ihm evtl. bei der Eingabe der Antworten in den Computer über die Schulter schauen will oder ob er es vorzieht, den Fragebogen in Papierform auszufüllen und direkt per Post dem Statistischen Landesamt zuzusenden, ohne daß der Interviewer von den Antworten Kenntnis nehmen kann. Dieses Wahlrecht hat Verfassungsrang, wie das Bundesverfassungsgericht im Volkszählungsurteil von 1983 betont hat. Es darf auch bei einer technikunterstützten Befragungsmethode (deren Akzeptanz bei den Befragten durchaus zweifelhaft ist) nicht ausgehöhlt werden.

3.5 Jugend und Familie

Der Unterhaltspflichtige wird bei seinem Arbeitgeber angeschwärzt

Ein bezirkliches Jugendamt sandte ein Absageschreiben, das ein Unterhaltspflichtiger zum Beleg dafür eingereicht hatte, daß seine Stellenbewerbung erfolglos geblieben war, an den Betrieb, der die Absage verfaßt hatte, mit der Bitte, die Echtheit des Schreibens zu überprüfen. Dabei war zwar die Anschrift des Betroffenen abgedeckt, jedoch konnte der Betrieb aufgrund der eigenen Unterlagen den abgelehnten Stellenbewerber schnell herausfinden. Außerdem hatte das Jugendamt den Betrieb darauf hingewiesen, daß der Betroffene als Vater seit Jahren seiner Unterhaltspflicht nicht nachgekommen und aufgefordert worden sei, seine Bemühungen um einen Arbeitsplatz nachzuweisen.

In einem weiteren Fall versuchte ein Mitarbeiter eines Jugendamtes als Unterhaltsbeistand beim Arbeitgeber Auskunft über die Einkommensverhältnisse des Unterhaltspflichtigen zu erlangen.

In beiden Fällen lehnten die befragten Arbeitgeber die Erteilung von Auskünften ab und wandten sich an uns.

Die Betreuung Unterhaltsberechtigter ist eine wesentliche Aufgabe der Jugendämter, die sie durch Unterhaltsbeistandschaft, Pflegschaft, Vormundschaft oder durch einfache Beratung erfüllen. Die *Verletzung der Unterhaltspflicht* ist alles andere als ein Kavaliersdelikt. Dennoch ist festzustellen, daß die Jugendämter gelegentlich Methoden anwenden, die den rechtlich vorgesehenen Rahmen überschreiten und z. T. den Unterhaltsberechtigten selbst schaden können. Obwohl das Bürgerliche Gesetzbuch und die Zivilprozeßordnung ein rechtlich geordnetes Verfahren dafür vorsehen, um Informationen über die Einkommensverhältnisse eines Unterhaltspflichtigen zu erlangen (Auskunftsanspruch, Stufenklage), nehmen die Jugendämter z. T. eine quasi fahndungsähnliche Ermittlungstätigkeit auf und wenden sich dabei - wie in den beiden geschilderten Fällen - häufig an Arbeitgeber, um die Einkommenssituation des Schuldners zu klären. Diese kriminalistische Vorgehensweise ist nicht nur ungeeignet zur Aufgabenerfüllung, sondern kann auch zu einem Verstoß gegen das Sozialgeheimnis führen. Der Amtsvormund und Amtspfleger darf nach § 68 Sozialgesetzbuch (SGB) VIII nur solche personenbezogenen Daten erheben, deren Kenntnis zur Erfüllung der jeweiligen Aufgabe erforderlich ist. Dies bedeutet auch, daß die Daten in einer Art und Weise erhoben werden müssen, die zu dem geringst möglichen Eingriff in das informationelle Selbstbestimmungsrecht des Schuldners führt. Da das Bürgerliche Gesetzbuch einen Auskunftsanspruch des Berechtigten und eine entsprechende Auskunftspflicht des Unterhaltsverpflichteten vorsieht, ist die Anfrage bei Arbeitgebern nicht erforderlich und damit unzulässig. Die Anfrage beim Arbeitgeber kann sogar zu einem Arbeitsplatzrisiko für den Unterhaltsverpflichteten und damit auch zu einem Unterhaltsrisiko für den Unterhaltsberechtigten führen könnte.

Kinder- und Jugendhilfegesetz

Grundsätzlich hat das zu Beginn des Jahres 1991 in Kraft getretene Kinder- und Jugendhilfegesetz[83] eine größere datenschutzrechtliche Klarheit in Teilbereichen der Jugendarbeit geschaffen. Die Schutzvorschrift in § 65 SGB VIII zum besonderen Vertrauensverhältnis verbessert die Arbeitsbedingungen der *Familienbetreuung* erheblich. Einerseits wird das Vertrauensverhältnis besonders geschützt, andererseits ist eine Durchbrechung dieses Grundsatzes im höherwertigen Interesse des Kindeswohls bei einer konkreten Gefährdung gesetzlich erlaubt, ohne daß in jedem Fall - wie bisher - der übergesetzliche Notstand des Strafgesetzbuchs herangezogen werden müßte.

Aus § 63 Abs. 2 SGB VIII ergibt sich außerdem eine gesetzliche Verpflichtung zur differenzierenden Aktenführung, d. h. eine aufgabenbezogene und personenbezogene Dokumentation. Dies entspricht einer langjährigen Forderung des Berliner Datenschutzbeauftragten. Ferner ist zu begrüßen, daß in § 63 Abs. 3 SGB VIII die Datenerhebung ohne Mitwirkung des Betroffenen interessen- und datenschutzgerecht geregelt wurde. Dadurch kann vor allem besonders schutzwürdigen Kindern und Jugendlichen der nötige Schutz selbst dann gewährt werden, wenn das familiäre Umfeld der Betreuung ablehnend gegenübersteht.

Wie sind Einkommensnachweise zu erbringen?

Ein Bezirksamt hatte von Eltern, deren Kinder in einer Tagespflegestelle untergebracht sind, zwecks Festsetzung der Kostenbeteiligung als Einkommensnachweis den Bescheid über den Lohnsteuerjahresausgleich gefordert. Eine Kopie, auf der die nicht erforderlichen Einzelheiten geschwärzt sind, wurde nicht akzeptiert.

Das Bezirksamt hat dazu erklärt, nach § 2 des *Kita-Kostenbeteiligungsgesetzes* gelte die Summe der im letzten Kalenderjahr vor Festsetzung der Kostenbeteiligung erzielten Einkünfte als Einkommen, was nur anhand des Steuerbescheides feststellbar sei. Im übrigen hätten die Eltern nach § 96 SGB VIII über Einkommen und Vermögen Auskunft zu erteilen, soweit dies zur Entscheidung über den Einsatz des Einkommens und Vermögens oder die Bemessung des Aufwendungsersatzes erforderlich sei. Auf Verlangen seien über die Höhe des Einkommens Belege vorzulegen.

Weder im Kita-Kostenbeteiligungsgesetz noch im SGB ist jedoch die Form des Nachweises näher festgelegt. § 96 SGB VIII schreibt lediglich vor, daß auf Verlangen Belege vorzulegen sind, soweit dies im Einzelfall erforderlich ist. Demzufolge bleibt die Wahl eines geeigneten Beleges dem Nachweispflichtigen überlassen, wobei die Vorlage des Steuerbescheides lediglich eine von verschiedenen Möglichkeiten darstellt. Denkbar wäre beispielsweise auch eine neutrale Bescheinigung des Finanzamtes.

Unabhängig davon kann der Nachweispflichtige selbstverständlich die für die Entscheidung unerheblichen und somit nicht erforderlichen Teile des Steuerbescheides unkenntlich machen. Die Nachweispflicht besteht nur in dem Umfang, der zur Entscheidungsfindung erforderlich ist.

Bewährungsaufsicht per Computer?

Die Senatsverwaltung für Jugend und Familie, die die Aufsicht über die Berliner Bewährungshelfer führt und in diesem Zusammenhang auch eine Zählkartenstatistik zur Bewährungshilfe erstellt, will diese Statistik in Zukunft PC-gestützt führen. Bereits jetzt bereitet das Statistische Landesamt im Auftrag der Senatsverwaltung für Jugend und Familie die *Bewährungshilfe-Statistik* auf, wie dies auch bei den meisten Justizstatistiken der Fall ist. In Zukunft sollen die Statistik-Daten ein- bis zweimal im Jahr auf Diskette durch Boten dem Statistischen Landesamt zur Aufbereitung überbracht werden.

Weniger problematisch als diese Bewährungshilfe-Statistik ist die Führung der zugrundeliegenden Probanden-Datei bei der Senatsverwaltung für Jugend und Familie. Sie bedarf nach dem

[82] Jahresbericht 1990, 2.4

[83] Jahresbericht 1990, 3.3

Berliner Datenschutzgesetz einer gesetzlichen Grundlage, die bisher fehlt. Nach dem 31. März 1992 wird die Führung dieser Datei (sei es auf Karteikarten, sei es PC-gestützt) rechtswidrig sein, wenn bis dahin das *Berliner Bewährungshelfergesetz* nicht entsprechend ergänzt worden ist.

Wenn eine gesetzliche Grundlage für die Verarbeitung dieser Daten im Verwaltungsvollzug geschaffen worden ist, bedarf die statistische Auswertung dieser Daten keiner zusätzlichen einzelstatistischen Rechtsgrundlage, da es sich um eine Geschäftsstatistik i. S. d. Entwurfs für ein Landesstatistikgesetz handelt. Sobald dieser Gesetzentwurf verabschiedet worden ist, kann die Bewährungshilfe-Statistik vom Statistischen Landesamt im Auftrag und nach den Weisungen der Senatsverwaltung für Jugend und Familie aufbereitet werden. Auch im Rahmen dieser Auftragsdatenverarbeitung dürfen personenbezogene Daten nur im erforderlichen Umfang an den Auftragnehmer weitergegeben werden. Die Senatsverwaltung für Jugend und Familie ist deshalb um Prüfung gebeten worden, ob auf die Angabe des vollständigen Geburtsdatums und der laufenden Nummer des Dienstregisters vor der Herausgabe der Daten an das Statistische Landesamt verzichtet werden kann. Das Ergebnis dieser Prüfung steht noch aus.

Überprüfung von bezirklichen Vormerkdateien für den Kindertagesstätten- und Tagespflegebereich (KITA-Verfahren)

Einen Schwerpunkt der diesjährigen Prüfungen des Personal-Computer-Einsatzes in der Berliner Verwaltung bildete das bezirkliche Verfahren zur Vormerkung von Kindertagesstättenplätzen. Dieses Verfahren ist durch die Senatsverwaltung für Jugend und Familie entwickelt worden und soll berlinweit in den zuständigen Ämtern der Bezirksverwaltungen zur Unterstützung der KITA-Platzvergabe und zur Erstellung der KITA-Statistik eingesetzt werden. Mit einer Ausnahme ist das KITA-Verfahen in den westlichen Bezirken auch realisiert worden, lediglich das Bezirksamt Kreuzberg bevorzugt für diese Zwecke ein schon zuvor entwickeltes eigenes Verfahren.

Das KITA-Verfahren dient der Vormerkung von Kindern für Kindertagesstättenplätze und beinhaltet daher personenbezogene Daten des Kindes sowie die für die Bearbeitung relevanten Daten der Eltern. Zusätzlich werden im Interesse des Kindeswohles Angaben zu einer etwaigen Behinderung des Kindes zur besonderen Betreuung erfaßt. Dies bedeutet, daß die Datensammlung sehr sensible Daten enthält und daher besonders hohe Anforderungen an Datenschutz und Ordnungsmäßigkeit gestellt werden müssen.

Die Rechner sind jeweils isolierte Einzelplatz-Geräte unter dem Betriebssystem MS-DOS. Neben dem Einsatz für das KITA-Verfahren werden sie außerdem für Textverarbeitung in Zusammenhang mit der KITA-Anwendung genutzt.

In Papierform werden regelmäßig Namen, Adressen und Wartezeiten der erfaßten Bürger an die Kindertagesstätten des Bezirkes übermittelt, um die Vergabeplanung für die Kindertagesstättenplätze durchzuführen.

Darüber hinaus werden regelmäßig aggregierte, nicht mehr personenbeziehbare Daten (z. B. Anzahl der Bürger, die einen KITA-Platz suchen, Pflegesatzdurchschnitt) auf Disketten an die Senatsverwaltung für Jugend und Familie für statistische Zwecke übermittelt.

Bei der Überprüfung dieses Verfahrens in sechs Bezirksämtern wurde festgestellt, daß grundlegende Maßnahmen zur Datensicherheit zwar getroffen worden waren, deren Güte und Umfang im Hinblick auf die Anforderungen an technisch-organisatorische Maßnahmen nach § 5 Abs. 3 BlnDSG zur Gewährleistung des Datenschutzes aber nicht ausreichen.

So sind alle überprüften Geräte zwar mit Datensicherheitssoft- und -hardware ausgestattet, jedoch bedurften diese Werkzeuge der individuellen Anpassung an die Systemumgebung und die Datensensibilität. Hierbei wurden mitunter erheblich voneinander abweichende Installationen angetroffen, beispielsweise bezüglich einer sinnvollen Abstufung der Zugriffsrechte, der Bildschirmabschaltung, der Länge der Paßwörter oder der programminternen Protokollierungsfunktion über Dateizugriffe.

Eine Protokollierungsfunktion in Systemen mit derart sensiblen Daten ist unverzichtbar. Daneben ist eine Bildschirmabschaltung zu installieren, die entweder automatisch nach festen Zeitabständen den Bildschirm abschaltet oder aber manuell vom Sachbearbeiter zu aktivieren ist, falls dieser sich kurzfristig vom Gerät entfernt. Es ist allerdings darauf zu achten, daß eine Reaktivierung der Darstellung des Bildschirminhaltes nur durch erneute Eingabe des Paßwortes möglich sein darf. Sinn der Bildschirmabschaltung ist die Verhinderung einer unbefugten Kenntnisnahme vertraulicher Informationen durch Dritte.

Bezüglich der Abstufung der Zugriffsrechte ist zu beachten, daß nicht jeder Mitarbeiter, der im Rahmen seiner Tätigkeit Daten abrufen darf, diese auch verändern oder löschen können muß. Ebenso benötigt der Sachbearbeiter im Normalfall keinen Betriebssystemzugriff, wenn ihm alle erforderlichen Programmaufrufe und -funktionen durch ein softwareseitig geschütztes Menüsystem angeboten werden.

Bei allen Prüfungen des berlinweiten Verfahrens in den Bezirken ergab sich, daß die Senatsverwaltung für Jugend und Familie die höchsten Systemverwalterrechte hatte. Dies war in der Einführungsphase des Verfahrens sicher darauf zurückzuführen, daß die Senatsverwaltung als überbezirklicher Koordinator die Systeme eingerichtet hat. Allerdings hätten nach Beendigung des Probebetriebes die Systemverwaltung und die höchsten Berechtigungsstufen auf das jeweilige Bezirksamt übergehen müssen, damit dieses auch tatsächlich Herr seiner Daten ist. Ohne die Systemverwalterrechte sind die Bezirksämter nicht in der Lage, eine effektive System- und Dateipflege zu betreiben und können so nicht die Verantwortung für die in ihrem Zuständigkeitsbereich anfallende Datenverarbeitung übernehmen.

Die Systemwartung und -pflege durch die Senatsverwaltung ist für dieses Verfahren aus datenschutzrechtlichen Gründen nicht hinnehmbar, da es im Rahmen einer ordnungsgemäßen Systemverwaltung immer zu Zugriffen auf Dateien mit personenbezogenen Daten kommt, die in dieser Konstellation rechtswidrig wären.

Wir haben diese Problematik mit der Senatsverwaltung erörtert und Konsens dahingehend erzielt, daß die Systemverwaltung des KITA-Verfahrens unverzüglich auf die Bezirksämter übertragen wird.

Verschiedentlich wurden Mängel hinsichtlich der Raumsicherung festgestellt. Diese Mängel sind mit den Bezirksämtern erörtert worden und sind bereits teilweise behoben worden, bzw. werden derzeit durch geeignete Maßnahmen nachgebessert.

In einem Fall wurde auf einem KITA-PC unbefugt eingespielte Software entdeckt. Hierbei handelt es sich um einen schwerwiegenden Verstoß gegen die Ordnungsmäßigkeit der Datenverarbeitung, der insbesondere als problematisch anzusehen war, da es sich bei der Software um ein mächtiges Dienstprogramm zur Bearbeitung von Datenmengen handelte, das völlig unsachgemäß installiert war.

Insgesamt war bei den Überprüfungen festzustellen, daß nur ein sehr geringer Teil der Sachbearbeiter bzw. Systemverwalter eine ausreichende Schulung für die zu bewältigenden Aufgaben erhalten hatten. Wir haben in unseren Stellungnahmen gegenüber den Bezirksämtern darauf hingewiesen, daß eine adäquate Schulung für eine ordnungsgemäße Systemverwaltung unerläßlich ist.

Versendung der Elternbriefe durch den Arbeitskreis Neue Erziehung

Der Arbeitskreis Neue Erziehung (ANE) wird als eingetragener Verein von der Senatsverwaltung für Jugend und Familie gefördert. Er gibt u. a. die sog. Elternbriefe für Eltern von Kindern im nichtschulfähigen Alter heraus und versendet sie.

Bis zum Jahre 1978 wurde der ANE durch die Säuglingsfürsorgestellen von der Geburt Erstgeborener unterrichtet, damit er bei diesen Familien mit dem Versand der Elternbriefe beginnen konnte.

Mit dem Inkrafttreten des ersten Berliner Datenschutzgesetzes am 1. 1. 1979 mußte diese Praxis eingestellt werden, da § 11 BlnDSG in damaliger Fassung für die Übermittlung an private Stellen wie der ANE die Einwilligung der betroffenen Eltern verlangte, die praktisch nicht eingeholt werden konnte.

Statt dessen wurde ein *Adreßmittlungsverfahren* eingerichtet, welches die Übermittlung von personenbezogenen Daten an eine private Organisation überflüssig machte: Die Senatsverwaltung für Jugend und Familie erhielt vom ANE Umschläge, Elternbriefe und sonstiges zu versendendes Material, ließ sich vom Landeseinwohneramt aus dem Melderegister die erforderlichen Adreßdaten selektieren, auf Aufklebern gedruckt übermitteln, klebte die Aufkleber auf die gefüllten Umschläge und versandte sie dann. Es erfolgte eine Übermittlung der Adreßdaten vom Landeseinwohneramt an die Senatsverwaltung für Jugend und Familie gemäß § 10 BlnDSG alter Fassung.

Dieses Verfahren galt nur für den Versand der ersten vier Elternbriefe. Da der ANE dadurch mit den Eltern in Kontakt kam, wurden alle weiteren Elternbriefe aufgrund der Bestellung der Eltern direkt vom ANE versandt.

Das Verfahren sollte jetzt verändert werden, weil die Senatsverwaltung für Jugend und Familie das Aufkleben nicht mehr weiter durchführen will. Ferner wurde angedacht, den Doppelbezug von Elternbriefen in den ersten Lebensmonaten des Kindes zu verhindern. Dazu kam es, wenn die Eltern Elternbriefe schon sehr früh beim ANE bestellten, so daß vom ANE direkt als auch über die Senatsverwaltung für Jugend und Familie der Versand erfolgte.

Ein weiterer Grund, die Sache neu aufzugreifen, war die neue Bewertung der Übermittlung vom Landeseinwohneramt an die Senatsverwaltung für Jugend und Familie angesichts der Rechtslage nach dem neuen Berliner Datenschutzgesetz. Für diese Übermittlung muß ab 1. 4. 1992 eine explizite Rechtsgrundlage vorliegen. Das Meldegesetz sowie die dazugehörige Rechtsverordnung gibt dies nicht her.

Voraussetzung für die Fortsetzung des Datenstroms vom Landeseinwohneramt an die Senatsverwaltung für Jugend und Familie ist die Aufnahme der regelmäßigen Übermittlung in der Anlage 4 der Durchführungsverordnung zum Meldegesetz.

Unter dieser Voraussetzung haben wir keine Bedenken, wenn die Senatsverwaltung für Jugend und Familie vom Landeseinwohneramt einen Datenträger (Diskette) mit den Adreßdaten erhält. Diese Diskette wird an den ANE weitergegeben, damit dieser im Rahmen einer Auftragsdatenverarbeitung gemäß § 3 BlnDSG im Auftrag der Senatsverwaltung für Jugend und Familie mit seinem EDV-System die Adressen auf eine Postkarte druckt. Die Postkarte wird so in dem Umschlag mit den Elternbriefen, die vom ANE bereitgestellt werden, eingefügt, daß die Adresse im Sichtfenster erscheint. Die Postkarte dient als Antwort- bzw. Bestellkarte für den weiteren Bezug der Elternbriefe ab Brief 4. Rücklaufende Bestellungen können dann mit OCR-Scannern gelesen werden. Die daraus resultierenden Adreßdaten speichert und verarbeitet der ANE dann in eigener Verantwortung auf der Basis von § 28 BDSG.

Der geplante Datenabgleich zwischen ANE-Bestelldaten und den Meldedaten zur Vermeidung von Doppelversendungen der Elternbriefe wurde verworfen. Statt dessen koordinieren sich ANE und Senatsverwaltung so, daß letztere stets die ersten drei Elternbriefe und der ANE erst ab dem 4. Brief den Versand übernimmt, unabhängig vom Zeitpunkt der Bestellung beim ANE.

3.6 Justiz

Datenschutz in der Strafprozeßordnung läßt weiter auf sich warten

Der Entwurf für ein *Strafverfahrensänderungsgesetz* (StVÄG) vom Juni 1989, der die Aufnahme der erforderlichen Datenschutzbestimmungen in die Strafprozeßordnung vorsieht, ist noch immer nicht im Bundestag eingebracht worden.

Stattdessen liegt dem Bundestag ein überarbeiteter Entwurf des Bundesrates zu einem „Gesetz zur Bekämpfung des illegalen Rauschgifthandels und anderer Erscheinungsformen der Organisierten Kriminalität" *(OrgKG)* vor, der sich - in bedenklicher Weise - auf einzelne Probleme des Strafverfahrensrechts beschränkt.

Nachdem ein erster Entwurf des Bundesrates zum OrgKG der Diskontinuität zum Opfer gefallen ist[84], hat der Bundesrat im April 1991 erneut einen Gesetzentwurf beschlossen[85].

Der neue Gesetzentwurf zum OrgKG weist zwar datenschutzrechtliche Verbesserungen auf, indem er den Einsatz bestimmter schwerwiegender Ermittlungsmethoden (Rasterfahndung, verdeckte Ermittler) an einen Straftatenkatalog knüpft. Andere erhebliche Eingriffe in die Privatsphäre sollen allerdings noch immer an den schwammigen Begriff der „Straftaten von erheblicher Bedeutung" gebunden werden.

Auch der neue Gesetzentwurf beschränkt sich - anders als sein Name vermuten läßt - keineswegs auf die sog. Organisierte Kriminalität, sondern geht weit darüber hinaus. Es sind auch weiterhin geheime und seit Jahren umstrittene Ermittlungsmethoden vorgesehen. Heimliche Foto- und Videoaufnahmen sollen ohne besondere Beschränkungen zulässig sein. Unverdächtige Personen können nach wie vor von derartigen Maßnahmen bereits betroffen sein, wenn es der „Erforschung des Sachverhalts" oder der „Ermittlung des Aufenthaltsorts des Täters" dient. Nicht einmal vor Wanzen, Peilsendern und Richtmikrophonen sollen unverdächtige Personen verschont bleiben. Wird „eine Verbindung" mit dem Täter vermutet, können gegen jede Person Wanzen oder andere Abhörgeräte eingesetzt werden. Während die Informationseingriffe der Strafverfolgungsbehörden in zum Teil bedenklichem Umfang erweitert werden, fehlen im Gesetzentwurf maßgebliche Datenschutzrechte der Bürger. So sind nach wie vor Akteneinsichtsrechte für Betroffene und differenzierte Regelungen über die Verarbeitung der erlangten personenbezogenen Daten nicht vorgesehen. Auch die schon im vorigen Entwurf enthaltenen verfassungsrechtlich bedenklichen Einschränkungen richterlicher Kontrollen zugunsten polizeilicher Eilanordnungen beim Einsatz geheimer Abhörmethoden wurden beibehalten.

Der Datenschutz stellt sich Bemühungen nicht entgegen, bei besonders gefährlichen Formen der Kriminalität auch besondere Ermittlungsmethoden einzusetzen. Über dieses Ziel schießt der Bundesratsentwurf jedoch hinaus.

Die Datenschutzbeauftragten des Bundes und der Länder haben - gegen die Stimme Bayerns - am 25. Juni 1991[86] in einer Entschließung erneut auf die datenschutzrechtlich bedenklichen Regelungen in dem Gesetzentwurf zum OrgKG hingewiesen und halten es für geboten, daß Bundestag und Bundesrat im weiteren Gesetzgebungsverfahren diese Probleme aufgreifen und die - wiederholt geäußerten - datenschutzrechtlichen Vorschläge berücksichtigen.

Justizmitteilungsgesetz

Der Bundesminister für Justiz hat den Landesjustizverwaltungen im November 1991 einen neuen Referentenentwurf eines Gesetzes über Mitteilungen der Justiz in Zivil- und Strafsachen (Justizmitteilungsgesetz) zugeleitet, der die bisherigen Verwaltungsvorschriften über Mitteilungen in Zivilsachen und in Strafsachen (MiZi und MiStra) weitgehend ablösen soll.

Das Gesetz soll die erforderlichen Rechtsgrundlagen für die Datenübermittlungen, die im Justizbereich anfallen, schaffen.

Gegenüber dem Vorentwurf weist der neue Entwurf zwar einige Verbesserungen auf, hat aber wesentliche datenschutzrechtliche Kritikpunkte nicht ausgeräumt, auf die wir schon seit dem ersten Entwurf 1986 hingewiesen haben.

Der Entwurf genügt nicht dem verfassungsrechtlichen Bestimmtheitsgebot, da er sich im wesentlichen mit weitgefaßten Rahmenvorschriften und Generalklauseln begnügt, die nach der Konzeption des Bundesministers für Justiz erst durch Verwaltungsvorschriften ausgefüllt oder konkretisiert werden sollen. So kann der Bürger aus dem Gesetz nicht erkennen, an wen bei welcher Gelegenheit personenbezogene Daten von ihm übermittelt werden. Zumindest sollten Inhalt und Voraussetzungen der Übermittlungstatbestände in einer Rechtsverordnung aufgrund einer gesetzlichen Ermächtigung festgelegt werden.

Die Vielzahl der im Entwurf enthaltenen Generalklauseln sind auch deshalb sehr bedenklich, weil die Gefahr besteht, daß diese als Auffangtatbestand für Datenübermittlungen herangezogen werden können, die sonst Beschränkungen unterliegen.

[84] Jahresbericht 1990, 3.6
[85] Bundesrat Drs. 219/91

[86] Anlage 2.3

Die Regelung über die Mitteilungen in Strafsachen, insbesondere soweit die Übermittlungen berufsbezogene oder dienstrechtliche Maßnahmen auslösen können, ist zu unpräzise. Es müßte klargestellt werden, daß Mitteilungen nur erfolgen dürfen, wenn das für den Betroffenen geltende Dienst- oder Berufsrecht eine Speicherung dieser Angaben in den Personalakten zuläßt und an die festgestellten Verfehlungen Rechtsfolgen knüpft. Soweit die Straftat des Betroffenen nicht unmittelbar mit dienstlichen Aufgaben im Zusammenhang steht, sollte eine Datenübermittlung auf erhebliche Rechtsverletzungen beschränkt werden.

Nicht akzeptabel ist, daß der Entwurf auch weiterhin keine konkreten Angaben der Übermittlungsempfänger enthält.

Ebenso fehlt eine Klarstellung, daß die Polizei über den Ausgang der von ihr an die Staatsanwaltschaft abgegebenen Strafverfahren unterrichtet wird. Nur dann ist es der Polizei möglich, ihren Datenbestand zu berichtigen und notwendige Datenlöschungen vorzunehmen[87].

Begrüßenswert ist, daß der Zeitpunkt, zu dem Mitteilungen erfolgen dürfen, nun klarer geregelt wurde. Dennoch sollte verdeutlicht werden, daß in Strafsachen vor Erhebung der öffentlichen Anklage keine Datenübermittlungen erfolgen. Zu begrüßen ist auch die Regelung, daß der Betroffene bei Mitteilungen grundsätzlich zu benachrichtigen ist. Allerdings soll die Unterrichtung gleichzeitig mit der Datenübermittlung erfolgen. Wir haben hiergegen Bedenken, da nur eine *vor* Übermittlung der Daten erfolgende Benachrichtigung sicherstellt, daß der Betroffene seine schutzwürdigen Belange rechtzeitig geltend machen kann.

Datenschutz im Strafvollzug

Endlich liegt zumindest ein Referentenentwurf zur Änderung des *Strafvollzugsgesetzes* vor, der die Datenverarbeitung auf die erforderliche gesetzliche Grundlage stellen soll.

Der Gesetzentwurf trägt jedoch den datenschutzrechtlichen Regelungsbedürfnissen im Strafvollzug nicht hinreichend Rechnung:

Im Rahmen der *Besucherüberwachung* ist vorgesehen, daß die Besuche aus Gründen der Sicherheit auch von der Zustimmung des Besuchers zur Einholung von Auskünften über ihn bei anderen Behörden abhängig gemacht werden können. Dies ist ein massiver Eingriff in das nach dem Strafvollzugsgesetz garantierte Besuchsrecht des Gefangenen. Angesichts der Tatsache, daß die Besucher ohnehin optisch und akustisch überwacht werden, ist die Erforderlichkeit dieser Regelung zudem fraglich. Zumindest aber sollte klargestellt werden, daß die Zustimmung zur Einholung von Auskünften nur dann verlangt werden darf, wenn konkrete Anhaltspunkte für ein mögliches Sicherheitsrisiko gegeben sind.

Die Erhebung von Daten über Personen, die nicht Gefangene sind, sollte nicht durch eine Generalklausel zugelassen werden. Hier muß konkret festgelegt werden, welche Auskünfte die Justizvollzugsanstalt bei welchen Stellen einholen darf. Aber auch die Erhebung von Daten über die Gefangenen selbst sollte konkreter, orientiert an spezifischen Einzelsachverhalten, normiert werden.

Weiterhin soll gesetzlich geregelt werden, daß die Vollzugsbehörde die Annahme von Paketen an Gefangene von der Kenntlichmachung durch *Paketmarken* abhängig machen darf. Diese Maßnahme ist eine Diskriminierung der Gefangenen, da dadurch im allgemeinen postalischen Verkehr der Gefangenenstatus gegenüber Dritten offenbart wird. Die in der Begründung angeführten Argumente, daß der Verzicht auf Paketmarken für die Justizvollzugsanstalten einen erheblichen Mehraufwand bedeute, überzeugt nicht. Die Anstalt muß auch ohne Verwendung von Paketmarken vor Ausgabe des Paketes an einen Gefangenen prüfen, ob dieser zum Erhalt des Paketes berechtigt ist.

Erfreulicherweise wurde eine bisher bestehende Regelung gestrichen, daß *erkennungsdienstliche Unterlagen* über Gefangene in kriminalpolizeilichen Sammlungen verwahrt werden dürfen.

Hingegen ist nicht akzeptabel, daß auch die bisher vorgesehene Löschungsregelung für diese Unterlagen entfallen soll. Für die Aufbewahrung erkennungsdienstlicher Unterlagen nach Entlassung des Gefangenen besteht keine Notwendigkeit. Bei sogenannten Kurzstrafern oder Gefangenen, die Ersatzfreiheitsstrafen ableisten, ist die Notwendigkeit für so einen massiven Eingriff wie den einer erkennungsdienstlichen Behandlung ohnehin zu bezweifeln.

Es fehlt darüber hinaus eine Regelung über die Führung der *Gefangenenpersonalakte.* Die Gefangenenpersonalakte ist die wichtigste und umfangreichste Datensammlung in den Justizvollzugsanstalten; sie kann als Kernstück der personenbezogenen Aktenführung in jeder Justizvollzugsanstalt bezeichnet werden. Daher sollte die Regelung über die Datenspeicherung eine spezielle Norm enthalten, die festlegt, welchen Inhalt die Gefangenenpersonalakten haben und wie sie geführt werden sollen. Ebenfalls ist datenschutzrechtlich unerläßlich, daß neben der getrennten Führung der Gesundheitsakten auch Sonderhefte für die in der Anstalt tätigen Psychologen und Sozialarbeiter mit besonderen Zugangsberechtigungen vorgesehen werden.

Die vorgesehenen Aufbewahrungsfristen für Gefangenenpersonalakten, Gesundheitsakten und Krankenblätter (30 Jahre) sind entschieden zu lang. Für eine Aufbewahrung dieser Daten nach Entlassung des Gefangenen ist eine Notwendigkeit nicht ersichtlich.

Bei den Datenübermittlungsregelungen für den öffentlichen Bereich fehlt eine konkrete Benennung der Übermittlungsempfänger und der zu übermittelnden Daten. Zu bezweifeln ist ferner, ob in allen aufgezählten Fällen eine Datenübermittlung über den Kopf des Gefangenen hinweg zulässig ist. Eine Datenübermittlung an Stellen, deren Hilfe der Gefangene freiwillig in Anspruch nimmt (z. B. Entlassenenfürsorge, Träger der Sozial- und Arbeitslosenhilfe sowie Verbände der Wohlfahrt) sollte nur mit dessen Einwilligung erfolgen. Die Datenübermittlung an private Stellen sollte nur nach einer vorherigen Anhörung des Gefangenen zugelassen werden.

Der Entwurf sieht die Möglichkeit der Mitüberwachung von Bezugspersonen eines Gefangenen vor. Daten von Personen, die nicht Gefangene sind, sollen zur Abwehr jeder unmittelbar drohenden Gefahr für die öffentliche Sicherheit genutzt werden dürfen. Angesichts der Eingriffsintensität in die Rechte von Personen, die nicht Gefangene sind, erscheint die vorgesehene Regelung unverhältnismäßig.

Das im Gesetzentwurf vorgesehene Recht anderer Behörden, in Gefangenenakten Einsicht zu nehmen, ist zu weitgehend. Die Übermittlung dieser Daten ist strikt auf das Erforderliche zu beschränken. Es kann nicht hingenommen werden, daß allein aus Gründen des Aufwands, die eine Auskunftserteilung mit sich bringen würde, stattdessen die ganze Akte übersandt wird.

Die als Generalklausel formulierte Durchbrechung der *ärztlichen Schweigepflicht* „zur Erfüllung der nach dem Strafvollzugsgesetz geregelten Aufgaben und zur Abwendung gegenwärtiger Gefahren für Leib oder Leben" ist angesichts der Massivität des Eingriffs zu unpräzise. Die zu erfüllenden Aufgaben sollten katalogmäßig aufgezählt werden. Ferner ist eine Meldung schon leicht ansteckender Krankheiten, die nach der Formulierung „zur Abwendung von gegenwärtigen Gefahren für Leib und Leben" bereits erfaßt wären, nicht verhältnismäßig.

Bedenklich ist die Verkürzung des durch § 19 Bundesdatenschutzgesetz gewährleisteten *Akteneinsichtsrechts* für Gefangene. Gefangene sind ebenso Grundrechtsträger wie andere Bürger, so daß es uneingeschränkt bei der Regelung des Bundesdatenschutzgesetzes bleiben sollte.

Der Referentenentwurf vernachlässigt den besonders problematischen Bereich der sogenannten *„Häftlingsüberwachung"*. Gerade in diesem Bereich werden die Rechte der Gefangenen und deren Bezugs- bzw. Kontaktpersonen durch die permanente Überwachung der Besuche, des Briefverkehrs und der Telefongespräche in gravierendem Maß beeinträchtigt, so daß ein gesteigertes Bedürfnis nach Schaffung von spezialgesetzlichen Rechtsgrundlagen besteht.

[87] vgl. 3.4.1

Gesetz zur Ausführung des Gerichtsverfassungsgesetzes

Auf Landesebene werden für den Justizbereich die notwendigen Konsequenzen aus den schleppenden Gesetzgebungsaktivitäten im Bund gezogen.

Dem Abgeordnetenhaus von Berlin liegt ein Entwurf des Senats über ein Ausführungsgesetz zum Gerichtsverfassungsgesetz *(AGGVG)*[88] vor, das die Datenverarbeitung bei den Gerichten und Staatsanwaltschaften bereichsspezifisch regeln soll.

Wir haben bereits zum Referentenentwurf kritisch Stellung genommen und uns für die Verankerung wesentlicher datenschutzrechtlicher Grundgarantien - wie das Auskunfts- und Akteneinsichtsrecht des Betroffenen, den Grundsatz, daß personenbezogene Daten in erster Linie beim Betroffenen selbst zu erheben sind - eingesetzt.

Der jetzt vorliegende Gesetzentwurf trägt unseren Einwänden größtenteils Rechnung.

Er beschränkt die *Auskunfts- und Akteneinsichtsrechte* der Gerichte, Staatsanwaltschaften und deren Hilfsbeamte insoweit, als Auskünfte nur erteilt werden dürfen, soweit dies für einzelne Verfahren erforderlich ist. Hierzu ist anzumerken, daß Auskunft grundsätzlich Vorrang vor Akteneinsicht und Übersendung der Akte hat, und Akteneinsicht nur erfolgen darf, wenn dies zur Aufgabenerfüllung der anfragenden Stelle unerläßlich ist.

Innerhalb des laufenden Verfahrens haben die Betroffenen ein Akteneinsichtsrecht nach Maßgabe des Verfahrensrechts. Außerhalb laufender Verfahren ist dem Betroffenen Auskunft zu erteilen, ob und ggf. welche Daten zu seiner Person in Dateien der Justizbehörden gespeichert sind und zu welchen Zwecken sie innerhalb der letzten zwei Jahre verwandt wurden. Zum Anspruch auf Akteneinsicht und zu Benachrichtigungspflichten gegenüber dem Betroffenen sieht der Gesetzentwurf vor, daß diese Rechte nach Maßgabe des jeweiligen Verfahrensrechts bestehen. Die Auskunft darf nur verweigert werden, soweit ein Gesetz dies zuläßt oder eine Abwägung ergibt, daß die Rechte des Betroffenen hinter dem öffentlichen Interesse an der Geheimhaltung, insbesondere weil die Auskunft den Untersuchungszweck gefährden würde, oder aufgrund eines überwiegenden Geheimhaltungsinteresses Dritter zurücktreten müssen.

Hervorzuheben ist, daß Einigkeit mit der Justizverwaltung darüber besteht, daß die Vorschriften des Berliner Datenschutzgesetzes über Auskunfts- und Akteneinsichtsrechte des Betroffenen und über Benachrichtigungspflichten auch im Justizbereich Anwendung finden, es sei denn, Verfahrensvorschriften stehen dem entgegen.

Ein wesentlicher Kritikpunkt ist der im Gesetzentwurf vorgesehene Ausschluß der *Dateibeschreibungspflicht* für nicht automatisiert geführte Dateien. Danach soll die in § 19 Abs. 2 BlnDSG vorgesehene, sehr differenzierte Verpflichtung zur Beschreibung des Inhalts und der Nutzung von Dateien für die Justiz entfallen bei Karteien, die auf der Grundlage einer Rechts- oder Verwaltungsvorschrift geführt werden. Diese Einschränkung ist sehr bedenklich, da die Dateibeschreibung sowohl für automatisierte Dateien als auch für manuelle Dateien die notwendige Voraussetzung für das beim Berliner Datenschutzbeauftragten zu führende Dateienregister ist. Nur ein lückenloses Dateienregister gewährleistet eine wirksame Datenschutzkontrolle durch den Berliner Datenschutzbeauftragten und stellt die Informationsrechte der Bürger sicher.

Die Senatsverwaltung für Justiz vertritt hingegen die Auffassung, daß die Zielrichtung von § 19 Abs. 2 BlnDSG an Justizregistern vorbeilaufe. Die Dateibeschreibungen würden angesichts der großen Zahl der Register und Verzeichnisse einen immensen Verwaltungsaufwand verursachen, dem aus Sicht der Justizverwaltung kein vernünftiger Nutzen für das informationelle Selbstbestimmungsrecht der Bürger gegenüberstehe.

Dem ist nicht zuzustimmen. Nur wenn für *alle* Dateien, aus denen personenbezogene Daten übermittelt werden, eine Dateibeschreibung und Anmeldung zum Dateienregister erfolgt, kann der Bürger klären, wo seine Daten gespeichert sein können. Es ist unzumutbar, daß die Betroffenen über Karteien der Justizverwaltung keinen vollständigen Überblick erhalten sollen und sich statt dessen Informationen über diese Datensammlungen aus den Amtsblättern oder Gesetz- und Verordnungsblättern zusammensuchen sollen. Zudem dürften die Rechts- und Verwaltungsvorschriften über Justiz-Karteien und -Register in der Regel nicht den umfangreichen inhaltlichen Anforderungen der Dateibeschreibung nach dem Berliner Datenschutzgesetz entsprechen. Reine Praktikabilitätserwägungen („Verwaltungsaufwand") dürfen nicht zu einer Einschränkung der Datenschutzrechte des Bürgers und der Kontrollrechte des Datenschutzbeauftragten führen.

Der gläserne Rechtsanwalt

In Berlin ist am 1. Januar 1992 eine Allgemeine Verfügung der Senatsverwaltung für Justiz über Mitteilungen von Klagen, Vollstreckungsmaßnahmen u. a. gegen Angehörige rechtsberatender Berufe in Kraft getreten[89], die die geltende Verwaltungsvorschrift vom 8. Oktober 1970 ablösen soll.

Darin wird geregelt, welche Sachverhalte, die den Gerichten und Gerichtsvollziehern über Angehörige rechtsberatender Berufe bekannt geworden sind, an die zuständigen aufsichtsführenden Stellen (Rechtsanwaltskammer, Notarkammer, Patentanwaltskammer, Präsident des Deutschen Patentamts u. a.) zu übermitteln sind. Rechtsgrundlage sind § 36 a Abs. 3 der Bundesrechtsanwaltsordnung (BRAO), § 64 a Abs. 3 der Bundesnotarordnung (BNotO), § 32 a Abs. 3 der Patentanwaltsordnung (PatAnwO) und § 36 a Abs. 3 i.V.m. § 207 Abs. 2 bzw. § 209 Abs. 1 BRAO. Danach ist die Übermittlung personenbezogener Daten zulässig, wenn dies für bestimmte Maßnahmen, wie z. B. Rücknahme bzw. Widerruf von Erlaubnissen, Zulassungen, die Amtsenthebung, Einleitung eines rüge- oder ehrengerichtlichen Verfahrens, von Bedeutung sein kann, soweit hierdurch schutzwürdige Belange des Betroffenen nicht beeinträchtigt werden oder das öffentliche Interesse das Geheimhaltungsinteresse des Betroffenen überwiegt. Nach der Allgemeinen Verfügung sollen z. B. gegen Rechtsanwälte erhobene Forderungsklagen, Räumungsklagen, der Erlaß von Vollstreckungsbescheiden und Anträge im Rahmen der Zwangsvollstreckung an die Rechtsanwaltskammer übermittelt werden.

Zwar enthält die Mitteilungsanordnung gegenüber der bisherigen Verwaltungsvorschrift einige begrüßenswerte Änderungen, z. B. soll die Entscheidung über die Mitteilungspflicht nunmehr nur noch der Richter bzw. der zuständige Rechtspfleger treffen und künftig eine Übermittlung von Mahnanträgen unterbleiben. Es bestehen jedoch aus datenschutzrechtlicher Sicht noch erhebliche Bedenken.

Dem in § 9 BlnDSG normierten verfassungsrechtlichen Grundsatz, daß personenbezogene Daten nur nach einer positiven Entscheidung über die Erforderlichkeit übermittelt werden dürfen, wird in der Anordnung nicht ausreichend Rechnung getragen. Die Mitteilungen dürfen nach der Anordnung nur unterbleiben, wenn der mitzuteilende Sachverhalt „offensichtlich" für Maßnahmen nach der BRAO, der BNotO oder der PatAnwO ohne Bedeutung ist oder wenn gesetzliche Verwendungsregelungen entgegenstehen. Damit wird der verfassungsmäßige Verhältnismäßigkeitsgrundsatz nicht hinreichend berücksichtigt. Danach haben die Richter bzw. Rechtspfleger, die über die Datenübermittlungen entscheiden, *vor* jeder Übermittlung eine einzelfallbezogene Abwägung der schutzwürdigen Belange der Betroffenen mit dem öffentlichen Interesse vorzunehmen und insbesondere die Erforderlichkeit zu prüfen. Die Auffassung der Justizverwaltung, durch das Aussortieren von Fällen „offensichtlicher Bedeutungslosigkeit" von den sonst grundsätzlich zu übermittelnden Sachverhalten sei eine Erforderlichkeitsprüfung gewährleistet, ist unzutreffend. Die Anordnung kehrt den datenschutzrechtlichen Grundsatz, daß Datenübermittlungen nur zulässig sind, wenn die Voraussetzungen zweifelsfrei festgestellt werden, in sein Gegenteil um. Entgegen diesem datenschutzrechtlichen Prinzip ist vorgesehen, daß Datenübermittlungen im Zweifel immer zu erfolgen haben, es sei denn, die Mitteilung ist für standesrechtliche Maßnahmen *offensichtlich* ohne Bedeutung. Der über die Übermitt-

[88] Drs 12/1813

[89] ABl. S. 113

lung entscheidende Richter bzw. Rechtspfleger muß die positive Überzeugung gewinnen, daß die Übermittlung rechtmäßig ist. Eine Begrenzung dieser Prüfpflicht auf offensichtlich rechtswidrige Übermittlungen ist unzulässig.

Bedenklich ist ferner, daß die Anordnung eine Mitteilung aller Klagen und Vollstreckungsbescheide - unabhängig von der Höhe der Forderung - zuläßt. Zum Schutz der Rechtspflege oder der Mandantschaft vor Anwälten oder Notaren mit „zerrütteten Vermögensverhältnissen" ist die Übermittlung jeder Forderungsklage oder jedes Vollstreckungsbescheides - auch bei Kleinstbeträgen - weder erforderlich noch verhältnismäßig.

Der Argumentation der Justizverwaltung, daß mehrere geringe Forderungstitel möglicherweise mehr über den Vermögensverfall eines Rechtsanwaltes oder Notars aussagen als ein einziger Titel in größerer Höhe und deshalb übermittelt werden müssen, können wir uns nicht anschließen. Den der Datenübermittlung zugrundeliegenden Vorschriften in der BRAO, BNotO und PatAnwO ist als klarer Regelungszweck lediglich zu entnehmen, daß Informationen, die so gewichtig sind, daß sie für bestimmte standesrechtliche Maßnahmen von Bedeutung sein können, spontan unter Durchbrechung der Zweckbindung übermittelt werden dürfen. Durch die übermittelten Daten soll unmittelbar eine standesrechtliche Maßnahme veranlaßt werden. Die Regelungen bezwecken jedenfalls nicht normenklar, der Rechtsanwalts-, Notar- und Patentanwaltskammer, dem Landgerichtspräsidenten und Präsidenten des Deutschen Patentamtes zu ermöglichen, ein derartiges „finanzielles Persönlichkeitsprofil" aller Kammerangehörigen auf Vorrat anzulegen.

Möglicherweise einmal in Betracht kommende standesrechtliche Maßnahmen berechtigen nicht zu einer regelmäßigen Übermittlung auch von geringfügigen Forderungen. Derartige vorsorgliche Datenübermittlungen verstoßen gegen das Verbot der Vorratsspeicherung.

Eine Unterrichtung des Betroffenen ist im Gegensatz zu dem Referentenentwurf zum Justizmitteilungsgesetz in der Anordnung nicht vorgesehen. Es ist erforderlich, daß die Betroffenen vor der Datenübermittlung informiert werden, damit sie ihre schutzwürdigen Belange rechtzeitig geltend machen können. Dem Einwand der Senatsverwaltung für Justiz, eine Benachrichtigung vor Übermittlung sei unnötig, weil man bei allen Betroffenen die Kenntnis der einschlägigen Verwaltungsvorschriften voraussetzen darf, überzeugt nicht. Keinesfalls kann angenommen werden, daß jeder Angehörige eines rechtsberatenden Berufes diese Anordnung im einzelnen kennt. Ferner weiß ein Rechtsanwalt, selbst wenn er den Inhalt der Vorschrift kennt, bei einem gegen ihn anhängigen Gerichtsverfahren noch nicht, wie die Entscheidung über die Datenübermittlung ausfallen wird.

Grundbuch als Hilfsmittel von Maklern

Zahlreiche Bürger, die Eigentumsrückübertragungsansprüche für ein Grundstück im Ostteil der Stadt geltend gemacht hatten, haben sich bei uns darüber beschwert, daß sie von Maklern und Kaufinteressenten wegen der Grundstücke angeschrieben wurden. In einem Fall hat der Makler dem Bürger mitgeteilt, er habe seine Adresse von einem Notar erhalten, der in die Grundakten eingesehen habe.

Hat ein Bürger die Rückübertragung von Eigentum an einem Grundstück beantragt, teilt das Amt zur Regelung offener Vermögensfragen Name und Anschrift der Antragsteller den Grundbuchämtern mit, die zwecks Absicherung vermögensrechtlicher Ansprüche diese Mitteilung in der entsprechenden Grundakte ablegen, so daß bei Einsichtnahmen die Personalien des Antragstellers feststellbar sind. Für die Datenübermittlung an die Grundbuchämter fehlt bisher eine gesetzliche Grundlage. Nach § 12 Grundbuchordnung (GBO) ist jedem die Einsicht in das Grundbuch gestattet, der ein berechtigtes Interesse darlegt. Der Begriff „berechtigtes Interesse" ist weit gefaßt. Es muß kein rechtliches Interesse vorliegen, sondern auch tatsächliche, insbesondere wirtschaftliche Interessen können ein Einsichtsrecht in das Grundbuch einräumen. Notare sind besonders privilegiert. Sie können nach §§ 43, 46 Grundbuchverfügung Einsicht nehmen, ohne dem Grundbuchamt ein berechtigtes Interesse darlegen zu müssen.

Bei den von uns vorgenommenen Überprüfungen bei Liegenschaftsämtern im Ostteil der Stadt konnten die Beschwerdefälle nicht nachvollzogen werden, da die Liegenschaftsämter uns wegen fehlender Aufzeichnungen über die Einsichtnahmen keine Auskünfte geben konnten, welche personenbezogenen Daten aus Grundakten an welche Stellen übermittelt wurden.

Wir haben die Senatsverwaltung für Justiz auf diesen Mißstand hingewiesen und die Notwendigkeit einer Protokollierungspflicht von Datenübermittlungen hervorgehoben, da nur eine schriftliche Fixierung der Übermittlungen die Grundbuchämter in die Lage versetzt, hierüber Auskünfte an die Betroffenen zu erteilen und eine nachträgliche datenschutzrechtliche Überprüfung ermöglicht.

Die Protokollierungspflicht von Datenübermittlungen ist auch vom Bundesverfassungsgericht im sog. Volkszählungsurteil als wesentliche Sicherung des informationellen Selbstbestimmungsrechts betont worden. Eine Überprüfung der Zulässigkeit der Einsichtnahme vor dem Hintergrund des informationellen Selbstbestimmungsrechts der betroffenen Antragsteller ist nur möglich, wenn der Zeitpunkt, der Zweck, der Empfänger, die Art und der Umfang der bei Grundbucheinsichtnahmen übermittelten Daten festgestellt werden können.

Im Hinblick auf das dem Abgeordnetenhaus vorliegende Ausführungsgesetz zum Gerichtsverfassungsgesetz, das die Protokollierung von Akteneinsichtsnahmen für den Bereich der Justiz vorsieht, hat uns die Senatsverwaltung für Justiz mitgeteilt, daß nunmehr durch eine Anordnung sichergestellt werde, daß künftig in den Grundakten Datum, Bezeichnung des Grundstücks und Name des Einsichtnehmenden festgehalten werden. Hinsichtlich der Privilegierung der Notare sollte noch eine Änderung der Grundbuchverfügung erfolgen, die auch für Notare die Darlegung eines berechtigten Interesses zur Einsichtnahme in Grundbücher vorsieht.

3.7 Kulturelle Angelegenheiten

Beiräte für dezentrale Kulturarbeit

Die Förderung der dezentralen Kulturarbeit soll durch Beiräte unterstützt werden, die von den Bezirksämtern eingesetzt werden, jedoch in ihrer Mehrheit aus Vertretern privater Institutionen oder Privatpersonen bestehen. Diese Beiräte sollen mit ihrem fachlichen Rat das Bezirksamt bei der Entscheidung über Anträge zur Gewährung von Fördermitteln unterstützen. Dazu sollen ihnen die Anträge, die personenbezogene Daten enthalten, ohne Einwilligung der Antragsteller übergeben werden.

Diesem Vorhaben haben wir - zunächst noch unter den Voraussetzungen des alten Berliner Datenschutzgesetzes - widersprochen, da der durch Bezirksamtsbeschluß einzusetzende *Beirat für dezentrale Kulturarbeit* nicht als öffentliche Stelle anzusehen war, so daß nach § 11 BlnDSG alter Fassung eine Weitergabe der Anträge an den Beirat die Einwilligung der Antragsteller zur Voraussetzung hatte. In der Frage, ob nun der Beirat „sonstige öffentliche Stelle" im Sinne des Berliner Datenschutzgesetzes sei und in diesem Falle die Übermittlung nach § 10 BlnDSG alter Fassung die Einwilligung nicht zur Voraussetzung brauchte, entspann sich ein kontrovers geführter Schriftwechsel mit der Senatsverwaltung für kulturelle Angelegenheiten, die mit Schützenhilfe der Senatsverwaltung für Inneres die Auffassung vertrat, daß Beiräte auch ohne förmliche Beleihung öffentliche Stellen seien. Dieser Auffassung sind wir entgegengetreten, da eine derartige, ohne gesetzliche Ermächtigung erfolgende Ausweitung des öffentlichen Bereiches die strengen Übermittlungsvorschriften vom öffentlichen in den privaten Bereich umgehen würden.

Letztlich mußte zu dieser Frage keine endgültige Klärung herbeigeführt werden, denn mit dem Inkrafttreten der neuen Berliner Datenschutzgesetzes wurde das Problem im Sinne des informationellen Selbstbestimmungsrechts auf andere Weise geklärt: Selbst unter der Annahme, daß die Beiräte als öffentliche Stellen anzusehen seien, wäre die Übermittlung der Anträge nur möglich, wenn entweder die Einwilligung der Betroffenen vorliegt oder sie unter Beachtung des Zweckbindungsgebotes zur Erfüllung gesetzlich zugewiesener Aufgaben erforderlich ist. Da keine gesetzliche Aufgabenzuweisung für derartige Kulturarbeit vorliegt, entfällt die zweite Alternative.

Es bleibt also vorerst bei der Notwendigkeit der Einwilligung. Wir haben deshalb empfohlen, daß die Antragsteller gebeten werden, ihre Einwilligung zur Übermittlung an die Beiräte zu geben, damit diese ihre Förderungsvorschläge gegenüber den Bezirksämtern abgeben können. Im Falle der Verweigerung der Einwilligung muß das Bezirksamt ohne den fachlichen Beistand seines Beirates entscheiden.

Neue IuK-Projekte für die Berliner Kultur

Als Erweiterung des bereits existierenden Ausleihverbuchungssystems will die *Amerika-Gedenkbibliothek* (AGB) ein *„Integriertes Bibliothekssystem"* aufbauen, in das nach der Wiedervereinigung der beiden Stadthälften auch die Staats- und Stadtbibliotheken aus dem Ostteil Berlins aufgenommen werden sollen.

Die datenschutzrechtliche Bewertung des „Integrierten Bibliothekssystems für die AGB" zeigt erneut, daß sich weder über eine gesetzliche Aufgabenzuweisung für die Bibliotheken die Erforderlichkeit der Verarbeitung personenbezogener Daten nach den Vorgaben des § 9 BlnDSG begründen läßt, geschweige denn die nach § 6 Abs 1 BlnDSG erforderliche Rechtsgrundlage für eine solche Datenverarbeitung vorhanden ist. Mag die bestehende Datenverarbeitung noch durch den gem. § 34 Abs. 1 BlnDSG bestehenden Übergangsbonus notdürftig rechtlich abgedeckt sein, so ist jede Erweiterung der Datenverarbeitung jedoch unzulässig, solange das von uns seit nunmehr 6 Jahren geforderte Bibliotheksgesetz noch immer aussteht. Zwischenzeitlich liegt hierzu ein Entwurf vor.

Bei der Einführung des Systems in verschiedenen Ausbaustufen ist geplant, einen Datenverbund zwischen Städtischen Bibliotheken und dem Deutschen Bibliotheksinstitut (DBI) herzustellen. Dabei sollen auch unmittelbare Zugriffsbefugnisse eröffnet werden. Auch diese Ausbaustufen müssen gesetzlich geregelt werden, da ein automatisiertes Verfahren zum Abruf personenbezogener Daten durch Dritte nur eingerichtet werden darf, wenn ein Gesetz dies ausdrücklich zuläßt.

In der künftigen gesetzlichen Regelung müssen darüber hinaus die Daten benannt werden, die bei der Bibliotheksbenutzung erhoben und verarbeitet werden dürfen; die Verarbeitungszwecke, die Nutzungsdauer der Daten sowie die geplanten statistischen Erhebungen sind in Art und Umfang präzise festzulegen. Insbesondere ist durch das Gesetz sicherzustellen, daß die Anonymität der erhobenen Daten für statistische Untersuchungen von Anfang an gewährleistet ist. Daten über den Beruf und Ausbildungsstand der Benutzer mögen zwar für die künftige Beschaffungsstrategie interessant und bedeutungsvoll sein. Sie sind jedoch nicht zur Abwicklung des Benutzungsverhältnisses erforderlich. Diese Daten dürfen also nur auf freiwilliger Basis und anonym erhoben werden.

Sollte die AGB als Auftragnehmer für die Stadtbibliotheken oder für das Deutsche Bibliotheksinstitut (DBI) werden, so ist zu gewährleisten, daß die Verantwortung im datenschutzrechtlichen Sinne bei den datenverarbeitenden Stellen, also den Städtischen Bibliotheken bzw. dem DBI verbleibt.

Hinsichtlich der technischen und organisatorischen Maßnahmen des Datenschutzes und der Datensicherheit haben wir der AGB vor allem folgende Empfehlungen gegeben:

- Bei der Erweiterung des Anwendersystems sind weitere Schnittstellen geplant, um zusätzliche Arbeitsabläufe der AGB zu integrieren, u. a. Haushaltswesen und -abrechnung, Materialwirtschaft. Ein besonderes Augenmerk muß dabei auf die Speicher-, Benutzer- und Zugriffskontrolle, auf die bestehenden und auch fortzuführenden Datenverknüpfungen, vor allem bei den Ausleih-, Gebühren- und Mahnvorgängen gelegt werden.
- Auch beim Datenaustausch, insbesondere beim Direktzugriff auf Fremddatenbanken, ist auf die strikte Einhaltung der Maßnahmen zur Zugriffs-, Übermittlungs- und Eingabekontrolle zu achten.
- Strenge Datenschutzmaßstäbe sind auch bei den Abfragen der Benutzer- und Kontendaten anzulegen. Dies gilt insbesondere dann, wenn in der Endausbaustufe alle Leser-Terminals installiert worden sind, da diese prinzipiell mit allen Funktionen arbeiten können sollen.

Auch die Einführung des ADV-Verfahrens im *Landesarchiv Berlin* ist rechtlich bedenklich, da dem Verfahren keine Rechtsvorschrift zugrunde liegt. Wie von uns seit langem gefordert, muß auch hier eine gesetzliche Grundlage, z. B. ein Landesarchivgesetz, die entsprechenden Verarbeitungsbefugnisse im Zusammenhang mit dem Verfahren regeln.

3.8 Schulwesen, Berufsbildung und Sport

IuK-Einsatz in der Schule

> Der Schuldatenschutzbeauftragte einer Neuköllner Schule sah keinen Ausweg mehr: Er legte eine Dienstaufsichtsbeschwerde gegen einen Lehrerkollegen ein, der für Aufgaben der Schulverwaltung schulische und betriebliche Daten in einer Datenbank gespeichert hatte, Listen, Programme und Disketten zur häuslichen Weiterbearbeitung mit nach Hause genommen hatte, dann längerfristig erkrankte, die Schule verließ und die Unterlagen nicht mehr herausgeben wollte. Die Organisation des Betriebspraktikums der Schüler wurde damit erheblich beeinträchtigt.

Ob dieser Fall repräsentativ für die Praxis des Einsatzes von IuK-Technik in Schulen ist, kann von uns nicht beurteilt werden. Aber alles, was wir bisher beobachteten, spricht dafür, daß derart sorgloser Umgang mit der Technik in Schulen wohl eher die Regel als die Ausnahme ist.

In diesem Zusammenhang war es eher noch harmlos, daß sich die Schule in Abhängigkeit von einem Lehrerkollegen begab, indem sie es hinnahm, daß er wichtige ADV-Unterlagen mit nach Hause nahm, obwohl dieses auch unter Berücksichtigung der Ausführungsvorschriften über Schülerunterlagen nicht hätte geschehen dürfen. Diese geben keinen Freiraum, Angelegenheiten der Schulorganisation auf häuslichen Privat-PCs unter Ausschaltung interner und externer Kontrollmöglichkeiten zu bearbeiten. Trotz der bösen Erfahrungen rechtfertigte der Schuldatenschutzbeauftragte das Verhalten der Schule damit, daß die Entwicklung von Anwendungsverfahren für die Schule, die nur bei großer Motivation der Lehrer mit hohem persönlichem Einsatz und großem Zeitaufwand möglich sei, im Rahmen der Dienstzeit nicht realisiert werden könne. Er wies darauf hin, daß eine solche Praxis allgemein üblich sei.

Unsere bisherigen Erfahrungen stehen nicht im Widerspruch zu dieser Aussage. Alle Schulen stehen vor dem Problem, daß einheitliche IuK-Hilfsmittel für schulorganisatorische Aufgaben nicht zur Verfügung stehen, und jede Schule für sich entweder auf dem Markt nach geeigneten Produkten umsehen muß oder Informatiklehrer bzw. autodidaktisch geschulte Lehrer dazu veranlassen muß, die notwendigen Programme selbst zu fertigen. Dabei stehen Gestaltungsziele wie Sicherheit, Ordnungsmäßigkeit, Transparenz erfahrungsgemäß nicht im Vordergrund. Hinzu kommt, daß der Datenschutz in der Schule auch als Führungsaufgabe nicht immer ernst genommen wird. Es hängt wie auch bei allen anderen Behörden wesentlich davon ab, wie die Verantwortlichen der datenverarbeitenden Stellen - hier die Schulleiter - die Notwendigkeit des Datenschutzes einschätzen, ob sie Datenschutz als wesentliche Voraussetzung für die Nutzung von IuK-Technik für schulische Zwecke oder als lästige Gesetzespflicht ansehen, die formal zwar zähneknirschend zu beachten ist, sonst aber als hinderlich abgetan wird. Wir wurden zu einer Lehrerkonferenz der Schule, deren Fall oben beschrieben wurde, eingeladen, um dem Datenschutzbeauftragten bei seiner Überzeugungsarbeit im Lehrerkollegium zur Seite zu stehen. Es zeigte sich aber leider, daß auch die Schulleitung die Beachtung der Regeln des Datenschutzes als eher exotische Randerscheinung ansah, gegen die man zwar nichts machen könne, die man aber auch nicht als eigene Sache ansehe. Daß in einem solchen Umfeld der Schuldatenschutzbeauftragte wenig Chancen für seine Arbeit hat, ist völlig klar, und daß dann Pannen wie oben beschrieben geschehen, ist zwangsläufig.

> Der Konrektor einer Berufsschule speichert personenbezogene Daten der Lehrer für die Ermittlung der Fehlzeitenverursacher auf seiner Schule unter Duldung der Schulleitung auf seinem privaten Heimcomputer.

Über diese Art der Verarbeitung personenbezogener Daten beschwerte sich ein Petent zu Recht, denn unabhängig davon, ob

die Verarbeitung inhaltlich rechtens war, war auch dies keine Aufgabe, zu deren Erfüllung Personaldaten auf einem privaten Rechner in der Privatwohnung des Konrektors verarbeitet werden durften. Grundsätzlich muß bei einem tatsächlich bestehenden Bedarf an IuK-Technik dieser durch eine Beschaffung der Schule zur Verfügung gestellt werden.

Viele Anfragen erreichten uns zur Bestellung und Funktion von *Schuldatenschutzbeauftragten*. Nach den Ausführungsvorschriften für Schülerunterlagen haben Schulen Datenschutzbeauftragte zu bestellen, wenn bei ihnen personenbezogene Daten automatisiert verarbeitet werden. Mit Inkrafttreten des neuen Berliner Datenschutzgesetzes ist diese Regelung überholt: Schulen haben jetzt behördliche Datenschutzbeauftragte gem. § 19 Abs. 5 BlnDSG auch dann zu bestellen, wenn die Verarbeitung personenbezogener noch nicht automatisiert durchgeführt wird.

Rechtsgrundlagen für die Verarbeitung von Schülerdaten fehlen

Die obenstehenden Überlegungen gelten unter der Voraussetzung, daß die Verarbeitung von Schülerdaten überhaupt rechtlich zulässig ist. Daran muß aber jetzt gezweifelt werden, denn die Senatsschulverwaltung hat ihre Bemühungen um die datenschutzrechtlich erforderlichen gesetzlichen Grundlagen für die Verarbeitung von Schülerdaten in der Schule im Berichtszeitraum offensichtlich eingestellt. Jedenfalls hat sie auf unsere diesbezüglichen Empfehlungen zu einem ersten Arbeitsentwurf im vergangenen Jahr nicht reagiert. Erst kürzlich sind wir über einen Entwurf zur Änderung des Schulgesetzes informiert worden, der im Rahmen des Artikelgesetzes verabschiedet werden soll. Ob die Datenverarbeitung in der Schule noch vor Ablauf des Übergangsbonus auf eine datenschutzgerechte gesetzliche Grundlage gestellt werden kann, bleibt abzuwarten.

In einer - nicht unbedeutenden - Einzelfrage hat die Senatsverwaltung allerdings im vergangenen Jahr eine alte Forderung des Berliner Datenschutzbeauftragten aufgegriffen, indem sie durch eine Änderung der Ausführungsvorschriften über Schülerunterlagen mit Wirkung vom 1. Mai 1991 auch minderjährigen Schülern ohne Zustimmung der Eltern die *Einsichtnahme in ihre Schülerunterlagen* gestattet hat, soweit der Schulleiter die Zustimmung der Eltern nicht im Einzelfall für erforderlich hält[90]. Damit wird der Grundrechtsmündigkeit heranwachsender Schüler endlich Rechnung getragen.

Lehrerindividualdatei (LID)

Die Aktualisierung der Lehrerindividualdatei hat nicht nur die alten Fragen nach ihrer Existenzberechtigung aufgeworfen, sondern erneut zu kritischen Anfragen über die Rechtmäßigkeit des Erhebungsverfahrens geführt.

Durch einen Schulleiter sind wir auf ein Rundschreiben der Senatsverwaltung für Schule, Berufsbildung und Sport an die Schulleitungen zur Aktualisierung der Lehrerindividualdatei aufmerksam gemacht worden, das den heutigen Datenschutzgesetzen nicht entspricht.

Das Rundschreiben läßt an keiner Stelle erkennen, daß es sich bei der Fortschreibung der LID um eine Datenerhebung im Auftrag der Bezirksämter handelt. Durch die Bezugnahme auf die dienstliche Verpflichtung der Schulleiter zur Mitarbeit an der Erledigung der Aufgaben auch der Schulaufsichtsbehörde wird vielmehr nahegelegt, die Senatsverwaltung erhebe die Daten nicht als Auftragnehmerin der Bezirke, sondern aus eigener Befugnis.

Die Erhebung ist datenschutzrechtlich jedoch nur als Auftragsdatenerhebung nach § 3 BlnDSG zulässig, was bereits in der Vergangenheit anerkannt worden war.

Nach § 6 Abs. 1 BlnDSG ist eine Datenerhebung ohne ausdrückliche Einwilligung des Betroffenen nur zulässig, soweit eine spezielle normenklare Rechtsvorschrift dies erlaubt. Auch gesetzliche Aufgabenzuweisungen an die Senatsverwaltung für Schule, wie etwa Planungs- oder Aufsichtsaufgaben, ersetzen nicht die von § 6 Abs. 1 Nr. 1 BlnDSG geforderten besonderen Verarbeitungsbefugnisse.

Das Rundschreiben war außerdem insofern mißverständlich formuliert, als der Eindruck erweckt wurde, der Schulleiter solle alle Eintragungen im Aktualisierungsbogen selbst vornehmen. Datenschutzrechtlich war es bereits nach altem Recht unzulässig, wenn die befragten Schulleiter Informationen, über die sie selbst nicht verfügen, bei der Lehrerpersonalstelle abfragten oder abfragen ließen. Als vorübergehende Lösung haben wir seinerzeit einer Verfahrensweise zugestimmt, bei der der Schulleiter die Erhebungsbögen insoweit ausfüllt, als er Fragen aus eigenem Wissen beantworten kann. Anschließend sollte er die Erhebungsbögen über die Lehrerpersonalstelle des zuständigen Bezirksamts mit der Bitte um Vervollständigung durch Angaben aus den Personalakten an die Senatsverwaltung zurückschicken.

Dieses Verfahren ist nach neuem Recht nicht mehr zulässig. Für die Verarbeitung von Personaldaten sind die einschlägigen Regelungen des neuen Bundesdatenschutzgesetzes heranzuziehen. § 13 Abs. 2 BDSG sieht vor, daß Erhebungen grundsätzlich bei den Betroffenen stattzufinden haben. Die Voraussetzungen für eine ausnahmsweise Erhebung bei anderen Stellen liegen bei der Aktualisierung der Lehrerindividualdatei nicht vor. Weder gibt es eine Rechtsvorschrift, die die Erhebung bei anderen Stellen als den Betroffenen vorsieht oder zwingend voraussetzt (vgl. § 13 Abs. 2 Nr. 1 BDSG) noch machen die zu erfüllenden Verwaltungsaufgaben ihrer Art nach eine Erhebung bei anderen Stellen erforderlich (vgl. § 13 Abs. 2 Nr. 2 a) BDSG). Auch die eventuellen Schwierigkeiten, die Daten bei den betroffenen Lehrern selbst zu erheben, wird man nicht als unverhältnismäßig ansehen können (vgl. § 13 Abs. 2 Nr. 2 b) BDSG).

Da die Daten zur Fortschreibung der Lehrerindividualdatei bei den Betroffenen selbst zu erheben sind, müssen diese auch auf den Zweck der Erhebung sowie auf ihre nach dem Beamtenrecht bestehene Auskunftspflicht gegenüber ihrer Dienstbehörde (dem Bezirksamt) hingewiesen werden.

3.9 Soziales

Automation in der Sozial- und Jugendhilfe - Projekt BASIS

Mit dem Projekt *„Berliner Automatisiertes Sozial- und Jugendhilfe Interaktions-System (BASIS)"* sollen die Arbeitsplätze der Sozial- und Jugendhilfe-Sachbearbeiter in den Bezirken und in der Zentralen Sozialhilfestelle für Asylbewerber des Landesamtes für Zentrale Soziale Aufgaben die anerkanntermaßen notwendige Automationsunterstützung erhalten. Dabei ist keineswegs vorgesehen, ein neues Verfahren für Berlin zu entwickeln. Es ist vielmehr geplant, in anderen Kommunen entwickelte, zum Teil auch praktisch erprobte Verfahren auf die Eignung für Berlin zu prüfen und nach einer Entscheidung an die Berliner Verhältnisse anzupassen. Erprobt werden insbesondere die Verfahren PROSOZ-Bremen und PROSOZ-Herten. Bei PROSOZ-Bremen handelt es sich um ein für Bremen entwickeltes Verfahren mit zentral geführtem Datenbestand, auf den mit Hilfe von PCs oder PC-Netzen von den dezentralen Anwendern zugegriffen werden kann. Bei PROSOZ-Herten handelt es sich um ein ähnliches Verfahren für kleinere Kommunen ohne zentralen Datenbestand, bei dem die Daten bei den Anwendern dezentral vorgehalten werden, die dafür über PC-Netze oder Mehrplatzanlagen verfügen. PROSOZ-Bremen ist in einigen Bezirksämtern erprobt worden PROSOZ-Herten wird derzeit erprobt.

Die nötigen Untersuchungen und Erprobungen werden von einer Projektgruppe durchgeführt, der an der Erprobung beteiligte Bezirksämter, das Landesamt für Informationstechnik und beteiligte Senatsverwaltungen angehören. Auf politischer Ebene verfolgt ein Lenkungsausschuß die Projektarbeit, dem Staatssekretäre der beteiligten Hauptverwaltungen und Sozialstadträte der beteiligten Bezirke angehören. Der Berliner Datenschutzbeauftragte gehört dem Lenkungsausschuß mit beratendem Status an.

Derzeit ist eine Entscheidung über das letztlich zu realisierende Verfahren noch nicht getroffen worden. Wir favorisieren weder PROSOZ-Bremen noch PROSOZ-Herten noch andere in die Diskussion gebrachte Verfahren. Alle bekannten Alternativen bedürfen sowohl aus rechtlicher als auch aus technischer Sicht einer speziellen Bewertung. Dies betrifft vor allem die Zulässigkeit der Datenbasis, die Benutzerprofile und ihre Umsetzung auf

[90] ABl. 1991, S. 705

die technischen Systeme, die Sicherheit der eingesetzten IT-Systeme und die Rahmenbedingungen für den ordnungsmäßigen Einsatz sowie ggf. die Sicherheit der verwendeten Datenübertragungstechniken. Nicht zuletzt wird auch die Umsetzung formeller Pflichten (Melde- und Benachrichtigungspflichten, Aufklärungspflichten etc.) Gegenstand weiterer Beratung sein.

Zum Verfahren PROSOZ-Bremen existiert ein Datenschutzkonzept für den Einsatz in Bremen, das mit dem Bremischen Datenschutzbeauftragten mit befriedigendem Ergebnis abgestimmt worden ist. Wieweit die Ergebnisse übertragbar sind, wird noch zu prüfen sein, wenn die Entscheidung für das Verfahren abzusehen ist. Dabei wird zu prüfen sein, inwieweit das in Berlin verfolgte Konzept von dem abweicht, das der Bremische Datenschutzbeauftragte begleitet hat und ob in Berlin andere rechtliche Rahmenbedingungen als in Bremen vorliegen.

Zu den rechtlichen Rahmenbedingungen ist festzustellen, daß sowohl in Bremen als auch in Berlin die Datenschutzbestimmungen des Sozialgesetzbuches (SGB) mit der in § 79 SGB X geregelten Verweisung auf das Bundesdatenschutzgesetz gelten.

Allerdings ergeben sich Abweichungen aus der unterschiedlichen Organisation der beiden Stadtstaaten. In Berlin obliegt die Gewährung der Sozial- bzw. Jugendhilfe den 23 Bezirken als eigenständige Aufgabe. Sozial- und Jugendhilfe sind ihrerseits unterschiedlichen Abteilungen der Bezirksverwaltungen zugeordnet. Dies bedeutet, daß allein auf Bezirksebene die Funktionen des BASIS-Verfahrens auf insgesamt 46 verschiedene speichernde Stellen i. S. d. § 3 Abs. 8 BDSG aufgeteilt werden. Jede dieser speichernden Stellen arbeitet mit dem Datenbestand der jeweils von ihnen zu betreuenden Klienten. Datenschutzrechtlich hat eine Abgrenzung der Datenbestände zwischen den speichernden Stellen in einer technischen Weise zu erfolgen, die den unbefugten und unkontrollierten Zugriff auf die Daten jeweils anderer Stellen ausschließt.

Bei einer dezentralen Datenhaltung (Modell PROSOZ-Herten) hätte dies die Abschottung der Bestände der Abt. Sozialwesen von der des Amtes für Jugendhilfe, bei der zentralen Datenhaltung im LIT (Modell PROSOZ-Bremen) die Segmentierung des Gesamtbestandes in 46 voneinander abgeschottete Einzelbestände zur Folge.

Jede Übermittlung dezentral gehaltener Bestände an andere Bezirke bzw. jeder Datenzugriff, der die genannten Abschottungen überwindet, ist eine Übermittlung gem. § 3 Abs. 5 Nr. 3 BDSG, im letzten Falle gar ein Abruf gem. Alternative b) der genannten BDSG-Vorschrift. Jede derartige Übermittlung ist insbesondere auch eine Offenbarung von Sozialdaten im Sinne des SGB X.

Die Zulässigkeit solcher Offenbarungen richtet sich nach den Bestimmungen der §§ 67 - 78 SGB X. Die Zulässigkeit der Übermittlung im Zuge des Direktabrufs richtet sich darüber hinaus nach § 10 BDSG. Demnach ist die Einrichtung von Abrufverfahren unter Beachtung bestimmter Verfahrens- und Gestaltungsvorschriften zulässig, wenn es unter Berücksichtigung der schutzwürdigen Interessen der Betroffenen und der Aufgaben oder Geschäftszwecke der beteiligten Stellen angemessen ist.

Wegen unserer bei verschiedenen Gelegenheiten geäußerten Bedenken zum bezirksübergreifenden Zugriff auf Sozialdaten für die Abwehr von Leistungserschleichung durch Mehrfachbeantragung konzentriert sich die datenschutzbezogene Diskussion zwischen den Beteiligten auf dieses Leistungsmerkmal. Dabei betonen Verfechter dieser Möglichkeit die Praktikabilität des gegenseitigen Datenabgleichs zur Vermeidung des Unterstützungsbetrugs und verweisen auf eine entsprechende Forderung des Rechnungshofs von Berlin. Dabei wird verkannt, daß weder Gesichtspunkte der Praktikabilität noch Forderungen des Landesrechnungshofes gesetzliche Vorgaben des Datenschutzes außer Kraft setzen können.

Die Bedenken gelten sowohl für den Datenabgleich mittels Datenträgeraustausch (Herten-Version) als auch im Gesamtbestand (Bremen-Version). Dabei spielt keine Rolle, daß der Abgleich durch eine beauftragte Stelle (LIT) erfolgt. Für die Übermittlung ist ausschlaggebend, daß Daten - wenn auch nur vorübergehend - für Zwecke anderer speichernder Stellen zur Verfügung gestellt werden.

Zur Beurteilung, ob eine explizite Ermächtigung für einen bezirksübergreifenden Abgleich bestimmter BASIS-Daten nach den Anforderungen des § 15 BlnDSG geschaffen werden könnte, ist darauf hinzuweisen, daß wir diesen Abgleich für unangemessen und ungeeignet halten, Unterstützungsbetrug aufzudecken.

Ob es überhaupt angemessen ist, großen technischen Aufwand und gravierende Eingriffe in das informationelle Selbstbestimmungsrecht der Betroffenen in Kauf zu nehmen, um Unterstützungsbetrügereien zu verhindern, kann nicht beurteilt werden, da es keine Angaben darüber gibt, wie häufig solche Ereignisse auftreten.

Die Eignung des Verfahrens ist ebenfalls zu bezweifeln; da die Unterstützung nur von den Behörden des Wohnbezirks geleistet wird, kann eine Doppelbeantragung nur erfolgen, wenn ein Antragsteller seinen Wohnsitz in einen anderen Bezirk oder Gemeinde verlagert. Im Falle einer Ummeldung innerhalb Berlins mag der geplante Abgleich erfolgreich sein, nicht jedoch bei einer Ummeldung von einer Gemeinde außerhalb Berlins, da diese ihre Daten nicht zum Abgleich beiträgt.

Geeignet wäre vielmehr die Prüfung der Meldeverhältnisse des Antragstellers. Wären diese unklar oder läge bei einer kürzlich erfolgten Ummeldung der Verdacht vor, daß die Sozialbehörden der früheren Wohngemeinde nicht vom Umzug unterrichtet wurden und daher weiterzahlen, dann stünden für die Übermittlung im begründeten Einzelfall mit §§ 68, 69 SGB X Rechtsgrundlagen zur Verfügung. In diesem Falle könnte gar zur besseren Wahrnehmung der informationellen Selbstbestimmung die Einwilligung der Betroffenen zur Nachfrage bei anderen Stellen gem. § 67 Satz 1 Nr. 1 SGB X in Betracht kommen.

Für die Prüfung der Meldeverhältnisse unter Einbeziehung früherer Wohnsitze bei Antragstellern könnte das Melderegister herangezogen werden, sofern die Angaben der Antragsteller dazu geprüft werden müßten. Ob über eine Ergänzung der Anlage 5 der Durchführungsverordnung für das Berliner Meldegesetz ein Online-Zugriff auf das ADV-Verfahren EWW legitimiert werden kann, bleibt späterer Prüfung vorbehalten.

Ein weiterer - bereits erwähnter Gesichtspunkt - wird die Abschottung zwischen Sozial- und Jugendhilfe sein. Auch hier ist ein Austausch von Daten aus Dateien oder Akten bzw. ein gemeinsamer Zugriff auf solche Datenbestände nur in Einzelfällen begründbar, wie wir z. B. im Zusammenhang mit den gemeinsam geführten Sozialleistungskarteien immer wieder betont haben. Wie dies gestaltet werden soll, ist uns bisher nicht bekannt, da Unterlagen zu diesem Leistungsmerkmal noch nicht vorliegen und die entsprechende Diskussion dieses Problems bisher nicht stattgefunden hat.

3.10 Stadtentwicklung und Umweltschutz

Der Einwender darf nicht „verpfiffen" werden

Wer eine Anlage errichten und betreiben will, die schädliche Einwirkungen auf die Umwelt verursachen kann, bedarf einer Genehmigung nach dem Bundes-Immissionsschutzgesetz. Nach der 9. Verordnung zur Durchführung dieses Gesetzes (9. BImSchV) ist demjenigen, der eine entsprechende Genehmigung beantragt hat, *„der Inhalt der Einwendungen"* bekanntzugeben, die andere Bürger gegen die geplante Anlage erhoben haben[91]. Eine Befugnis der Genehmigungsbehörde, dem Antragsteller alle Namen und Anschriften der Einwender zu offenbaren, ergibt sich daraus nicht, denn sie gehören nicht zum „Inhalt der Einwendungen". Diese gegenwärtige Rechtslage ist auch datenschutzgerecht, denn es wäre unverhältnismäßig, demjenigen, der eine behördliche Genehmigung gegen den Widerstand anderer Bürger erhalten will, bereits zu Beginn des Verfahrens die Personalien aller Einwender mitzuteilen.

Allerdings plant der Bundesminister für Umwelt, Naturschutz und Reaktorsicherheit eine Änderung dieser Rechtslage zu Lasten der Einwender. Er will die Durchführungsverordnung dahingehend ändern, daß in Zukunft *„die Einwendungen"* (nicht nur ihr Inhalt) dem Antragsteller bekanntzugeben sind. Dadurch soll die Weitergabe auch der Einwendernamen ermöglicht wer-

[91] (§ 12 Abs. 2 Satz 1 9. BImSchV)

den. Ob in der neuen Formulierung eine normenklare Befugnis im Sinne des Berliner Datenschutzgesetzes zur Offenbarung von personenbezogenen Einwenderdaten gesehen werden kann, ist fraglich. Selbst auf einer normenklaren Rechtsgrundlage wäre jedoch die pauschale und undifferenzierte Weitergabe der Namen und Anschriften aller Einwender ein unzulässiger Eingriff in ihr informationelles Selbstbestimmungsrecht. Die Tatsache, daß diese personenbezogenen Daten dem Antragsteller in einem Erörterungstermin oder einem möglichen späteren Rechtsstreit bekannt werden können, rechtfertigt jedenfalls nicht die Weitergabe sämtlicher Daten der Einwender bereits zu Beginn des Verfahrens.

Erfreulicherweise teilt die Senatsverwaltung für Stadtentwicklung und Umweltschutz unsere Bewertung und hat diese Position auch gegenüber dem Bundesminister für Umwelt, Naturschutz und Reaktorsicherheit vertreten. Dem Vernehmen nach ist die Angelegenheit von den Ländervertretern sehr kontrovers diskutiert worden; derzeit ist nicht erkennbar, ob das Bundesumweltministerium an der Änderung festhalten will.

Jedenfalls hat die Senatsverwaltung für Stadtentwicklung und Umweltschutz zugesagt, daß sie - auf der Grundlage der derzeitigen Rechtslage - alle Einwendungen unabhängig von der Art des Verwaltungsverfahrens lediglich *anonymisiert* an den Antragsteller weiterleiten wird. Nur soweit die Mitteilung von Angaben über die Einwender im Einzelfall ausnahmsweise für eine sachgerechte Rechtswahrung seitens des Antragstellers erforderlich ist[92], werden persönliche Daten auf Anforderung des Antragstellers nach Kontaktaufnahme mit dem Einwender weitergegeben.

Darüber hinaus ist hervorzuheben, daß die Senatsverwaltung auch für den Fall einer Änderung der Rechtsverordnung eine Lösung vorsieht, die schutzwürdige Belange der Einwender soweit wie möglich berücksichtigt: So soll bereits in der öffentlichen Bekanntmachung des beantragten Vorhabens darauf hingewiesen werden, daß Einwendungen an den Antragsteller weitergereicht werden und daß dies auf Wunsch der jeweiligen Einwender auch in anonymisierter Form geschehen kann. Entsprechend soll zukünftig bei Vorhaben nach dem Abfallgesetz, die der Planfeststellung unterliegen, verfahren werden.

Bodenbelastungskataster

Das Berliner Grundwasser ist in seiner Qualität bekanntermaßen überdurchschnittlich gut. Wenngleich Berlin von katastrophalen Fällen von Verunreinigungen bislang verschont geblieben ist, stellt doch die Senatsverwaltung für Stadtentwicklung und Umweltschutz eine zunehmende Bedrohung dieses „Lebensmittels Nummer Eins" durch Altlasten in den Böden fest.

Mit Hilfe eines Bodenschutzgesetzes sollen jetzt Verschmutzungen gezielt erfaßt und auch gegen den Willen des Verursachers untersucht werden dürfen, um geeignete Vorsorge- bzw. Schadensbegrenzungs- und -beseitigungsmaßnahmen einleiten zu können.

Da dabei nicht nur Daten von Grundstücken des Landes Berlin oder juristischer Personen des Privatrechts, sondern auch personenbezogene Daten anderer Grundstückseigentümer verarbeitet werden, hatten wir schon in den Vorjahren gefordert[93], das zu diesem Zweck aufgebaute flächendeckende und rechnergestützte *Altlastenverdachtsflächenkataster* entsprechend dem Berliner Datenschutzgesetz auf die erforderliche bereichsspezifische Rechtsgrundlage zu stellen.

Mit dem vorliegenden Entwurf eines Gesetzes zur Vermeidung und Sanierung von Bodenverunreinigungen *(Bodenschutzgesetz)* hat die Senatsverwaltung für Stadtentwicklung und Umweltschutz einen begrüßenswerten Schritt in die richtige Richtung getan und Regelungen für die Speicherung und Nutzung der benötigten Daten in einem *Bodenbelastungskataster* vorgesehen. Diese bedürfen allerdings in mehreren Punkten noch der Präzisierung:

- Es muß normenklar geregelt werden, welche Daten in das Kataster aufgenommen werden sollen. Da der Zweck des Gesetzes nur die Information über den Zustand eines bestimmten Grundstücks sein soll, nicht aber die Erleichterung juristischer Schritte gegen den Verunreiniger, ist eine Speicherung der Namen von Grundstückseigentümern oder sonstigen für ein belastetes Grundstück Verantwortlichen in diesem Kataster nicht erforderlich und damit unzulässig.
- Vorgesehen ist, daß die zuständige Behörde alle ihr zugänglichen Informationen über tatsächliche oder vermutete Bodenverunreinigungen nicht nur im Rahmen der Erforderlichkeit sammeln darf, sondern bereits soweit sie zur Erfüllung ihrer Aufgaben „von Nutzen" sind. Dies ist zu weit gefaßt. Um den Anforderungen des Datenschutzes gerecht zu werden, sollte der Gesetzgeber hier zunächst zwischen personenbezogenen Daten und sonstigen Informationen unterscheiden. Für erstere ist konkret Art, Zweck und Umfang der Datenverarbeitung zu regeln. Informationen ohne Personenbezug können dagegen schon dann verarbeitet werden, wenn sie zwar (noch) nicht erforderlich, aber für die Behörde nützlich sind.
- Konkreter als im bisherigen Entwurf der Senatsumweltverwaltung muß geregelt werden, unter welchen besonderen Voraussetzungen personenbezogene Daten bei Dritten oder beim Betroffenen, aber ohne sein Wissen erhoben werden dürfen. Nach dem Volkszählungsurteil und dem Berliner Datenschutzgesetz ist die offene Datenerhebung beim Betroffenen die zentrale Voraussetzung der Transparenz jeder staatlichen Datenverarbeitung für den Bürger. Soll von ihr ausnahmsweise abgewichen werden, wofür es gerade im Bereich des Umweltrechts, das häufig umgangen wird, gute Gründe gibt, so muß der Gesetzgeber genauer festlegen, unter welchen Voraussetzungen dies zulässig ist.
- Schließlich ist zwar zu begrüßen, daß jede Person ein Einsichtsrecht in das Bodenbelastungskataster erhalten soll. Dieses Einsichtsrecht soll aber nach dem Vorschlag der Senatsumweltverwaltung eingeschränkt werden, soweit die Einsichtsnahme Rückschlüsse auf Betriebs- und Geschäftsgeheimnisse zuläßt. Hier muß zunächst klarer definiert werden, was Betriebs- und Geschäftsgeheimnisse sind, weil darüber häufig in der Praxis gestritten wird. So ist die Überschreitung bestimmter Grenzwerte für Einleitungen in Gewässern schon nach den geltenden Regelungen zur Einsicht in das Wasserbuch kein Betriebs- und Geschäftsgeheimnis. Selbst wenn solche Geheimnisse berührt sind, kann eine datenschutzgerechte Abwägung ergeben, daß der Grundstückseigentümer aufgrund des überwiegenden öffentlichen Informationsinteresses die Einsichtnahme in das Bodenbelastungskataster hinnehmen muß. Das Bodenschutzgesetz sollte Kriterien für eine derartige Abwägung enthalten.

Gesetzliche Grundlagen für Stadtplanung und Friedhofsverwaltungen

Die Senatsverwaltung für Stadtentwicklung und Umweltschutz hat erfreulicherweise einen ersten Entwurf für ein *Gesetz über die Datenverarbeitung für Zwecke der räumlichen Stadtentwicklung, Stadt- und Regionalplanung und Bodenwirtschaft* erarbeitet, das an die Stelle des Gesetzes über eine Erhebung für Zwecke der Stadtplanung vom 16. Oktober 1969 treten und den Anforderungen des neuen Berliner Datenschutzgesetzes genügen soll. Wir haben hierzu ergänzende Empfehlungen gegeben.

Schließlich muß auch der Umgang mit personenbezogenen Daten auf den Berliner Friedhöfen (z. B. in Grabstellenkarteien) auf eine bereichsspezifische Rechtsgrundlage gestellt werden. Die Senatsumweltverwaltung hat im Rahmen der Beratungen des Artikelgesetzes eine entsprechende *Ergänzung des Friedhofsgesetzes* vorgeschlagen, die allerdings noch verbesserungsbedürftig ist.

3.11 Wissenschaft und Forschung

Offenbarungszwang für Prüfungskandidaten

Ein Student meldet sich zur Prüfung an, wird aber kurz vor dem entscheidenden Termin krank und legt der Prüfungskommission eine entsprechende Bescheinigung seines Hausarztes vor, wonach er prüfungsunfähig ist. Daraufhin fordert

[92] vgl. 7. Jahresbericht des Landesbeauftragten für den Datenschutz Nordrhein-Westfalens, S. 141
[93] vgl. zuletzt Jahresbericht 1990, 3.8

ihn die Prüfungskommission auf, seinen Hausarzt von der ärztlichen Schweigepflicht zu befreien und ihm zu gestatten, der Prüfungskommission auch Einzelheiten der Diagnose mitzuteilen. Diese Aufforderung ergeht an jeden Prüfungskandidaten, der sich kurz vor der Prüfung krank meldet, mittels eines Formblatts.

Über dieses an der Technischen Universität Berlin übliche Verfahren beschwerten sich sowohl Prüfungskandidaten als auch Ärzte bei uns. Der Präsident der Technischen Universität vertrat zunächst den Standpunkt, über die Prüfungsfähigkeit eines Kandidaten habe allein die Prüfungskommission des jeweiligen Fachbereichs zu entscheiden. Die Prüfungskommission könne diese Entscheidung nicht auf einen Arzt delegieren, sondern müsse selbst prüfen, ob der unbestimmte Rechtsbegriff der „Prüfungsunfähigkeit" im Einzelfall erfüllt sei. Diese Entscheidung sei gerichtlich überprüfbar.

Es ist zwar richtig, daß die Entscheidung über die fehlende *Prüfungsfähigkeit eines Kandidaten* letztlich bei der Prüfungskommission liegt. Diese darf aber nicht pauschal und ausnahmslos in jedem Fall den Kandidaten auffordern, seinen behandelnden Arzt von der Schweigepflicht zu entbinden, sondern allenfalls dann, wenn im Einzelfall Zweifel daran bestehen, daß die Feststellung des Arztes zutrifft. Bei einem erstmaligen Rücktritt von der Prüfung aus Krankheitsgründen sind solche Zweifel in der Regel nicht gerechtfertigt.

Der Akademische Senat der Technischen Universität hat daraufhin beschlossen, den Fachbereichen nahezulegen, ihre Prüfungsordnungen in der Weise zu ändern, daß von einer schematischen Anforderung der ärztlichen Diagnosen oder beim Kandidaten festgestellten Symptome abgesehen werden soll. Darüber hinaus empfahl der Akademische Senat, den Prüfungskandidaten einen einmaligen Rücktritt ohne Begründung innerhalb einer bestimmten Frist zu gestatten, so daß der Prüfling nicht gezwungen sei, sich „krankschreiben" zu lassen, wenn er sich der Prüfung nicht gewachsen fühle.

Diese Empfehlung des Akademischen Senats ist zu begrüßen. Neuerliche Beschwerden im vergangenen Jahr deuten allerdings darauf hin, daß die Fachbereiche zum Teil noch immer das alte, datenschutzrechtlich mangelhafte Verfahren praktizieren.

Die Senatsverwaltung für Wissenschaft und Forschung hat im Rahmen des Artikelgesetzes einen Vorschlag zur *Ergänzung des Hochschulgesetzes* gemacht, der die längst erforderliche Rechtsgrundlage für die Verarbeitung aller *Studentendaten* schaffen soll. Welche Studentendaten die Hochschulen im einzelnen verarbeiten dürfen, wird der Senat durch Rechtsverordnung zu regeln haben. Dies ist nur hinnehmbar, wenn die Rechtsverordnung möglichst gleichzeitig mit dem Artikelgesetz in Kraft tritt.

Studenten beurteilen Professoren

An den Berliner Hochschulen wird - wie auch in anderen Bundesländern - verstärkt darüber nachgedacht, wie das Lehrangebot verbessert werden kann. Zu diesem Zweck wird an der Technischen Universität aufgrund einer Initiative der Kommission für Lehre und Studium ein Forschungsprojekt *„Evaluation der Lehre"* durchgeführt, bei dem Studenten auf Fragebögen Lehrveranstaltungen und Dozenten beurteilen sollen. Dies geschieht auf Fragebögen, die zwar weder den Namen des ausfüllenden Studenten noch des jeweiligen Dozenten, wohl aber eine Veranstaltungsnummer enthalten, so daß der Bezug zum beurteilten Dozenten jederzeit herstellbar ist. Auf den Fragebögen werden nicht nur Meinungen der Studenten („Es bestand ein angenehmes Klima zwischen dem Professor und den Studierenden."), sondern auch personenbezogene Informationen über die Dozenten erhoben („Professor ist für die Studierenden auch außerhalb der Lehrveranstaltungen ansprechbar."). Die Studenten haben die Möglichkeit, den ausgefüllten Fragebogen in einem verschlossenen Umschlag direkt an den Leiter des Forschungsprojekts zu schicken. Dieser plante ursprünglich, nach Auswertung der Fragebögen die Ergebnisse - bezogen auf die jeweils beurteilte Lehrveranstaltung -, den Dekanen bzw. geschäftsführenden Direktoren mit der Bitte zuzusenden, sie in geeigneter Weise hochschulintern zu veröffentlichen.

Wir haben die Forscher darauf hingewiesen, daß die Befragung nach dem Berliner Datenschutzgesetz nur mit Einwilligung der beurteilten Professoren und Dozenten wie auch der Studenten zulässig ist, solange der Gesetzgeber keine Pflicht zur Mitwirkung bzw. Auskunftserteilung regelt. Auf dieses *Freiwilligkeitserfordernis* müssen die Professoren und Dozenten bereits hingewiesen werden, wenn ihnen die Fragebögen mit der Bitte zugeleitet werden, sie den Studenten in den Lehrveranstaltungen auszuhändigen. Sie müssen außerdem darauf hingewiesen werden, daß sie keinerlei Nachteile zu befürchten haben, wenn sie die Fragebögen nicht verteilen.

Dasselbe gilt für eine spätere personenbezogene Veröffentlichung der Bewertung einzelner Lehrveranstaltungen, selbst wenn diese nur innerhalb der Hochschule erfolgt. Der jeweilige Professor oder Dozent muß die Möglichkeit haben, der Veröffentlichung dieser Ergebnisse zu widersprechen, ohne Nachteile befürchten zu müssen. Auch hierauf ist er vor der Ausgabe der Fragebögen hinzuweisen. Entscheidet er sich dafür, die Fragebögen zwar zu verteilen, macht aber seine Einwilligung in die spätere personenbezogene Veröffentlichung vom Ergebnis und der Auswertung der Befragung abhängig, so muß ihm auch dies ermöglicht werden. In jedem Fall muß dem jeweiligen Professor oder Dozenten zuerst das Auswertungsergebnis der Befragung zugeleitet werden, bevor es an die Dekane oder geschäftsführenden Direktoren zu einer möglichen Veröffentlichung weitergegeben wird.

Schließlich sollte klargestellt werden, daß die Ergebnisse der Untersuchungen nicht zu den Personalakten der bewerteten Professoren oder Dozenten genommen werden und daß die von den Studenten ausgefüllten Fragebögen unmittelbar nach Abschluß der Auswertung vernichtet werden.

Probleme des Forschungsprivilegs

Die *Wissenschaftsklausel* im Berliner Datenschutzgesetz (§ 30) läßt unter bestimmten Umständen die Übermittlung von personenbezogenen Daten durch öffentliche Stellen für Zwecke der wissenschaftlichen *Forschung ohne Einwilligung* der Betroffenen zu[94]. Die Anwendung dieser Vorschrift in der Praxis ist noch von einer erheblichen Unsicherheit gekennzeichnet.

Wesentlich ist zunächst, daß die oberste Landesbehörde, die der privilegierten Übermittlung für Zwecke wissenschaftlicher Forschung zustimmen muß, zu prüfen hat, ob der Forschungszweck überhaupt die Verwendung *personenbezogener* Daten erfordert. Ist dies der Fall, so muß weiter untersucht werden, warum die Einwilligung der Betroffenen nicht eingeholt werden kann. Die bloße Erklärung des Forschers ist hierfür nicht ausreichend.

In jedem Fall darf die Übermittlung personenbezogener Daten nur für *bestimmte* wissenschaftliche Forschungsvorhaben erfolgen. Eine Übermittlung allgemein für unbestimmte Forschungszwecke und für eine unbestimmte Zeit läßt das Berliner Datenschutzgesetz nicht zu. Dies haben wir auch dem Statistischen Landesamt mitgeteilt, das die Kandidatendatei der Bundestags- und Abgeordnetenhauswahlen für einen nicht näher konkretisierten Forschungszweck auf Dauer speichern will. Das Forschungsvorhaben muß organisatorisch und zeitlich abgrenzbar sein.

Die Zustimmung der obersten Landesbehörde muß die Art der zu übermittelnden personenbezogenen Daten näher beschreiben. Auch dies wurde im Berichtszeitraum von einer Senatsverwaltung versäumt.

Stimmt eine oberste Landesbehörde der Übermittlung personenbezogener Daten für Forschungszwecke zu, obwohl die gesetzlichen Voraussetzungen nicht vorliegen, so hat der Berliner Datenschutzbeauftragte dies zu beanstanden. Die Zustimmung der obersten Landesbehörde ist kein datenschutzrechtlicher Freibrief für die übermittelnde Stelle.

Schließlich haben wir im Bereich des Polizeirechts und für die Justiz[95] eine spezielle Forschungsklausel vorgeschlagen, die bereichsspezifisch die Verwendung der besonders sensiblen personenbezogenen Dateien und Akten der Polizei für Forschungszwecke regeln soll. Dabei haben wir uns an Gesetzentwürfen des Bundesjustizministeriums zum Strafvollzugs- und Strafverfahrensrecht orientiert.

[94] Jahresbericht 1990, 3.10
[95] s. 3.6

4. Aus der Arbeit der Dienststelle

Die Dienststelle

Die personelle Situation der Dienststelle hat sich etwas gebessert: Wir konnten die drei Stellen, die uns im Rahmen des Beschlusses der Landesregierung vom 27. November 1990 zugewiesen wurden, mit Mitarbeitern bzw. Mitarbeiterinnen aus dem Ost-Teil Berlins besetzen. Der erhebliche Aufgabenzuwachs, der seit der Vereinigung der beiden Stadthälften auf uns zugekommen ist, kann jedoch auch mit diesen zusätzlichen Stellen nicht bewältigt werden.

Dies ist auch dadurch anerkannt worden, daß trotz der Finanznot für den Haushalt 1992 eine weitere Stelle bewilligt wurde - jedoch nicht ohne eine andere Stelle mit einem „kw-Vermerk" zu versehen (was bedeutet, daß wir bei einem Wechsel der derzeitigen Stelleninhaberin die Stelle wieder verlieren).

Aufgabengebiete

Die Öffentlichkeitsarbeit nahm erneut einen hohen Stellenwert ein. Wir haben in unserem unregelmäßig erscheinenden Informationsdienst weiterhin über aktuelle Datenschutzfragen berichtet. Auch haben wir uns im Rahmen unserer personellen Möglichkeiten an Fortbildungsveranstaltungen beteiligt und auch wieder in Rundfunksendungen über Datenschutzfragen informiert.

Nach der Novellierung des Berliner Datenschutzgesetzes und des Bundesdatenschutzgesetzes haben wir eine Broschüre herausgegeben, damit die Bürger, aber auch die Mitarbeiter in der Verwaltung, möglichst schnell über die neuen gesetzlichen Regelungen informiert sind. Eine Gesetzessammlung mit den wichtigsten Gesetzen und Bestimmungen zum Datenschutz hat diese Aktion ergänzt. Nicht nur aus der gesamten Berliner Verwaltung und von den Berliner Bürgerinnen und Bürgern, sondern auch bundesweit erreichten uns Anforderungen für diese Broschüre, denen wir gerne nachkommen. Die zahlreichen Anfragen aus der Verwaltung zeigen, daß diese Gesetzessammlung offenbar zu einem wichtigen Hilfsmittel in den verschiedensten Bereichen geworden ist.

Daneben haben wir weiterhin Informationsmaterialien zu besonderen Themen des Datenschutzes herausgegeben, wie z. B. zu Telekommunikation und Medien sowie zu dem datenschutzgerechten Einsatz von Laptops.

Aufgrund des großen Erfolges unseres Aufklebers „Schnüffeln verboten" haben wir uns zu einer Fortführung dieser Aktion entschlossen. Unser neuer Aufkleber „Unsere Daten sind Privatsache" soll Interesse am Datenschutz wecken und für Datenschutzbelange auch in Alltagssituationen auf unkomplizierte und ansprechende Weise werben.

Das Interesse und Informationsbedürfnis der Bürgerinnen und Bürger aus dem Ost-Teil der Stadt ist nach wie vor groß. Wir haben auch 1991 in erheblichem Umfang Beratungsgespräche mit Ost-Berliner Bürgern geführt und Auskünfte zu Datenschutzfragen erteilt.

Die Zahl der Beschwerden und Beratungsersuchen ist insgesamt im vergangenen Jahr insbesondere bei den Bürgereingaben deutlich angestiegen. Unabhängig davon wurden eine Vielzahl von Beratungs- und Informationsgesprächen in der Dienststelle sowie telefonisch geführt.

Weil das Land Brandenburg 1991 noch kein eigenes Datenschutzgesetz und keinen Datenschutzbeauftragten hatte, besuchten uns auch viele Bewohner aus dem Umland bzw. wandten sich schriftlich an uns.

Die meisten Beschwerden richteten sich - wie bereits in den Vorjahren - gegen den Geschäftsbereich der Innenverwaltung (in erster Linie waren der Sicherheitsbereich und das Meldewesen betroffen), gefolgt von den Gesundheits- und Sozialverwaltungen. Auch zum Querschnittsbereich Personaldatenverarbeitung erreichte uns eine Vielzahl von Eingaben. Der Trend, die Eingaben mittels der neuen Telekommunikationsdienste Telefax und Bildschirmtext zu versenden, ist stärker geworden. Erneut erreichten uns viele Beschwerden gegen die Datenverarbeitung Privater, die aufgrund der bekannten Aufgabenzuweisungen an die Senatsverwaltung für Inneres abgegeben wurden.

Auch die Beratungsersuchen aus der Verwaltung haben nach wie vor einen erheblichen Umfang. Das Problembewußtsein für Datenschutzfragen hat sich in der Verwaltung deutlich gewandelt. Es ist eine steigende Bereitschaft zu beobachten, uns in datenschutzrechtlich problematischen Angelegenheiten einzuschalten, was jedoch nicht in jedem Fall bedeutet, daß die Verwaltung unseren Empfehlungen auch nachkommt. Bei den Beratungsersuchen stehen die Bereiche Bildung und Forschung sowie Gesundheit nach wie vor ganz vorn. Auch der Bereich Technik und Organisation hat eine große Anzahl von Beratungen in der Verwaltung durchgeführt. Die Schwerpunkte lagen auch diesmal bei der Sozialverwaltung und der Innenverwaltung, insbesondere beim Landesamt für Informationstechnik. Intensive Beratungen erfolgten aber auch bei der Kulturverwaltung, der Senatsverwaltung für Justiz, Bau- und Wohnungswesen und bei verschiedenen Bezirksämtern.

Nach § 19 Abs. 5 Berliner Datenschutzgesetz sind die Behörden und sonstigen öffentlichen Stellen verpflichtet, einen behördlichen Datenschutzbeauftragten zu bestellen. Zu seinen Aufgaben gehört es u. a., die bei der Verarbeitung personenbezogener Daten tätigen Personen durch geeignete Maßnahmen mit den einschlägigen Datenschutzvorschriften vertraut zu machen (§ 37 Abs. 1 Nr. 2 Bundesdatenschutzgesetz). So ist in diesem Zusammenhang wiederholt der Wunsch an uns herangetragen worden, ob nicht wir diese Aufgabe übernehmen könnten. Diesen Bitten konnten wir nicht entsprechen, da wir mit unserem kleinen Personalkörper dazu nicht in der Lage sind und anderenfalls unsere originären Aufgaben nach § 24 BlnDSG nicht mehr erfüllen könnten.

Abgeordnetenhaus

Nach dem neuen Berliner Datenschutzgesetz hat der Datenschutzbeauftragte das Recht, vor dem Parlament zu reden. Der Berliner Datenschutzbeauftragte hat am 13. Juni 1991 erstmals von seinem Rederecht anläßlich der parlamentarischen Beratung[96] seines Jahresberichtes 1990, Gebrauch gemacht.

Schwerpunkt der Beratungen im Unterausschuß Datenschutz war unser Jahresbericht 1990 und verschiedene andere Fragen. So wurde von Berliner Behörden eine Liste der aus dem Ost-Teil der Stadt übernommenen Datenbestände aufgestellt, die demnächst beraten werden soll.

Auch in anderen Ausschüssen hatten wir Gelegenheit, zu Datenschutzfragen im Zusammenhang mit Gesetzgebungsvorhaben Stellung zu nehmen.

Kooperation

Entsprechend seiner gesetzlichen Verpflichtung hat der Datenschutzbeauftragte eng mit allen anderen Stellen zusammengearbeitet, die wie er die Aufgabe der Kontrolle und Weiterentwicklung des Datenschutzes haben. Dies gilt in der Berliner Verwaltung vor allem für die nach dem neuen Datenschutzgesetz vorgeschriebenen behördlichen Datenschutzbeauftragten, die allerdings noch nicht in allen Behörden bestellt worden sind. Ein effektiver Datenschutz kann nur über ein Netzwerk der Kontrolle und Beratung sichergestellt werden.

Auf nationaler Ebene ist die *Konferenz der Datenschutzbeauftragten des Bundes und der Länder,* die im Berichtszeitraum unter dem Vorsitz des Bundesbeauftragten für den Datenschutz zwei ordentliche und eine außerordentliche Sitzung abgehalten hat, das wichtigste Forum der Zusammenarbeit. Die dort gefaßten Beschlüsse sind im Anhang abgedruckt. Vor allem die häufigen Treffen der Arbeitskreise der Konferenz sind für die praktische Arbeit der Dienststelle von erheblicher Bedeutung.

Der Arbeitskreis Medien tagte zweimal unter Berliner Vorsitz. Er bereitete eine Konferenzentschließung zum Datenschutz in der Telekommunikation[97] vor.

Im Jahr 1992 führt die Landesbeauftragte für den Datenschutz Baden-Württemberg den Vorsitz in der Konferenz.

[96] vgl. Anlage 1
[97] vgl. Anlage 2.2

Sehr intensiv war auch 1991 die Zusammenarbeit in der *Arbeitsgruppe Telekommunikation und Medien* der Internationalen Konferenz der Datenschutzbeauftragten, die zweimal unter dem Vorsitz Berlins zusammentrat. Auf einer zusätzlichen Sitzung der Vertreter der EG-Datenschutzbeauftragten wurde ein Memorandum zum Vorschlag der EG-Kommission für eine ISDN-Richtlinie erarbeitet. Der Bericht der Arbeitsgruppe Telekommunikation und Medien zu weiteren international bedeutsamen Fragen der Telekommunikation wurde von der 13. Internationalen Konferenz in Straßburg zustimmend zur Kenntnis genommen[98].

Auch beteiligten wir uns an den Beratungen, die in einer Arbeitsgruppe des Europarats für eine Empfehlung zum Datenschutz bei Telekommunikationsdienstleistungen stattfanden. Diese Empfehlung wird voraussichtlich Einfluß auf die Ausgestaltung der EG-ISDN-Richtlinie haben.

Außerdem veranstalteten wir wie bei jeder Internationalen Funkausstellung seit Bestehen der Dienststelle auch im vergangenen Jahr ein *Symposium*, das diesmal unter dem Thema „Datenschutz: Komfort und Freiheit des Kunden in der Telekommunikation" stand. Die bei dieser Veranstaltung gehaltenen Vorträge werden demnächst in einer Dokumentation veröffentlicht.

Die Zusammenarbeit mit der *Aufsichtsbehörde* für den Datenschutz bei der Senatsverwaltung für Inneres gestaltete sich auch im vergangenen Jahr gut.

Schließlich rief der Berliner Datenschutzbeauftragte eine *Arbeitsgruppe Datenschutz in den neuen Bundesländern* ins Leben, in der sich Vertreter der Aufbaustäbe für den Datenschutz in Mecklenburg-Vorpommern, Brandenburg, Sachsen-Anhalt, Sachsen und Thüringen sowie des Bundesbeauftragten für den Datenschutz und der Datenschutzbeauftragte der Treuhandanstalt mehrfach über den Stand der datenschutzrechtlichen Entwicklung in den neuen Ländern unterrichteten. Auch diese Arbeitsgruppe soll ihre Tätigkeit fortsetzen, nach dem die Kontrollzuständigkeit des Bundesbeauftragten für den Datenschutz in den fünf neuen Ländern nach dem Einigungsvertrag am 31. Dezember 1991 geendet hat und in den neuen Bundesländern hoffentlich bald ausnahmslos Landesbeauftragte für den Datenschutz gewählt sein werden.

Berlin, den 25. März 1992

Dr. Hansjürgen Garstka
Berliner Datenschutzbeauftragter

[98] vgl. Anlage 3

Anlagen

1. Rede des Berliner Datenschutzbeauftragten vor dem Berliner Abgeordnetenhaus am 13. Juni 1991

Es ist zwar keine Neuigkeit in der deutschen Parlamentsgeschichte, wenn ein Datenschutzbeauftragter vor einer Volksvertretung das Wort ergreift - in dem Land, das als erstes in der Welt vor über 20 Jahren ein Datenschutzgesetz schuf, nämlich in Hessen, ist dies gute Tradition. Gleichwohl scheint es mir von Bedeutung zu sein, wenn gerade das Land Berlin dem vom Bundesverfassungsgericht erst vor wenigen Jahren anerkannten Grundrecht der Bürgerinnen und Bürger auf informationelle Selbstbestimmung dadurch besondere Achtung gezollt hat, daß der Gesetzgeber an der Schwelle zur deutschen Einigung dem Landesbeauftragten für den Datenschutz ein Rederecht in diesem Hause eingeräumt hat. Die Übergabe meines Jahresberichtes für das Jahr 1990 sowie die inzwischen erfolgte Stellungnahme des Senats nehme ich zum Anlaß, zum ersten Mal von diesem gesetzlichen Recht Gebrauch zu machen.

Im Mittelpunkt des Berichtes stehen, wie könnte es anders sein, die Probleme, die die *Einigung Deutschlands* und für uns in erster Linie Berlins, auch für den Datenschutz aufwarf. Von jeher habe ich die These vertreten, daß gerade die Mißachtung der informationellen Selbstbestimmung der DDR-Bürger einer der wesentlichen Gründe für das revolutionäre Aufbegehren und schließlich die Wende im Jahre 1989 war. Der Senat hat sich dieser Auffassung angeschlossen.

Aus dieser Erkenntnis heraus ergeben sich neben vielen Aufgaben im Detail zwei wichtige Konsequenzen:

Dem *informationellen Erbe* der DDR kommt erhebliche Bedeutung sowohl für die individuelle als auch für die gesellschaftliche Aufarbeitung dieses Teiles der deutschen Geschichte zu. Zwar fällt die Hinterlassenschaft des Ministeriums für Staatssicherheit in die Zuständigkeit des Bundes, obwohl einige Argumente für die starke Einbindung der Länder sprachen und heute noch sprechen. Soweit möglich hat daher der Sonderbeauftragte der Bundesregierung unsere Unterstützung erfahren und wird sie weiterhin erhalten. In der DDR sind aber in allen Verwaltungsbereichen Datensammlungen entstanden, deren Erhebung, Verwaltung und Verwertung mit unserem gemeinsamen Grundrechtsverständnis nicht übereinstimmen und deren Aufarbeitung ansteht. Ich sage bewußt „Aufarbeitung", nicht aber „Löschung": Zwar gehört es zu den datenschutzrechtlichen Grundforderungen, rechtswidrig erhobene Daten zu löschen; dieser Grundsatz kann aber nur dann gelten, wenn nicht gerade durch die Löschung Interessen der Betroffenen beeinträchtigt werden: Das neue Berliner Datenschutzrecht räumt zu recht hier ein Anhörungsrecht ein - es wird angemessen zu berücksichtigen sein: Die Vernichtung von Datenbeständen darf nicht zum Instrument der Reinwaschung von Verfehlungen werden.

Auch gibt es Sammlungen, deren Entstehen zwar in der Zielsetzung, nicht aber in den Methoden ihrer Verwaltung den Menschenrechten entsprechen: Zweifellos von wissenschaftlichem Wert, steht das nationale Krebsregister der DDR in einem nur schwer zu überwindenden Widerspruch zu Art und Weise seiner Entstehung. Es verstößt gegen das Persönlichkeitsrecht der betroffenen krebskranken Patienten, wenn ihre Ärzte Namen und Krankheiten hinter dem Rücken der Betroffenen an ein Zentralregister weitergeben.

Dieses Beispiel, wie andere, etwa das frühere zentrale Einwohnerregister, das Statistische Amt, die Rundfunkanstalten, die Akademie der Wissenschaften zeigen ein weiteres: Viele der Einrichtungen der DDR, die Daten im Interesse des Staates gegen die Interessen der Bürger sammelten, fallen nunmehr in die Zuständigkeit der Länder und haben ihren Sitz in Berlin. Es ist allerdings nur ein mäßiges Interesse des Landes festzustellen, Verantwortung für die datenschutzgerechte Verwaltung dieser Daten auch in den Fällen zu übernehmen, in denen andere Länder auf dem Boden Berlins Daten verarbeiten lassen - ein gewisser Widerspruch zum Anspruch Berlins auf Regierungsfunktionen, der meines Erachtens auch in einer besonderen Verantwortlichkeit im Rahmen der Länderkompetenzen zum Ausdruck kommen sollte.

Zum anderen:

Betroffenheit und Verstrickung in das System sind offensichtlich erheblich komplizierter, als dies den rechtsstaatsgewohnten Westbürgern oft klar ist. Zwar schützt der Datenschutz keine Personen, die gegen die Menschlichkeit verstoßen haben; er bewahrt diejenigen, die sich in den Dienst eines unmenschlichen Systems gestellt haben eben nicht vor der Aufklärung ihres Anteils, und wenn jemand in den *öffentlichen Dienst der neuen Bundesrepublik* eintreten will, muß er sich von den zuständigen Stellen mit seiner Vergangenheit konfrontieren lassen - mit allen Konsequenzen, die dies für die Einschätzung seiner Verfassungstreue hat.

Dies entbindet die Verwaltung aber keineswegs davon, ihrerseits rechtsstaatlich zu handeln. Diese Selbstverständlichkeit droht bei der Übernahme einer Vielzahl von Bürgern der ehemaligen DDR in den öffentlichen Dienst der neuen Bundesrepublik mitunter in den Hintergrund zu geraten. Zwar haben sich Berlins öffentliche Stellen im Gegensatz zu anderen nicht dazu verstiegen, bei der Überprüfung der zu übernehmenden Personen in Bausch und Bogen personenbezogene Daten der Verwandten oder gar Daten über den mehr oder minder großen Anteil an der Wende abzufragen. Aber auch hier hat es einer Intervention des Datenschutzbeauftragten bedurft, Polizeibeamte vor der selbstbezichtigenden Fragestellung zu bewahren, ob sie an Folterungen oder anderen menschenunwürdigen Maßnahmen teilgenommen hätten. Die rechtsstaatlichen Grundsätze gelten ohne Ansehen der Person und niemand ist verpflichtet, sich selbst einer Straftat zu bezichtigen.

Dennoch ist es auch nach der Stellungnahme des Senats zu unserem Bericht unklar, auf welche Weise und wie lange die Antworten auf die Fragen des Berliner Fragebogens aufbewahrt werden dürfen: Mir scheint eine Anlehnung an die Regeln des Disziplinarverfahrens am angemessensten einschließlich der dort verankerten Löschungsfristen.

Dies muß auch Folgen für die Auswertung der Fragebogen haben. Sie dürfen nicht schablonenhaft nach Art einer schriftlichen Führerscheinprüfung in der Weise ausgewertet werden, daß beim Ankreuzen bestimmter Antwortmöglichkeiten automatisch und ohne Anhörung des Betroffenen die Kündigung ausgesprochen wird.

Welchen Aufwand es für eine Dienststelle wie der unseren bedeutet, sich mit diesen und den vielen anderen mit der Einigung verbundenen Fragestellungen zu befassen, muß nicht betont werden. Wenn der Senat in seiner Stellungnahme mit Blick auf die bevorstehenden Aufgaben erklärt, „es sei eine der wichtigsten Aufgaben, der sich unsere Behörde zusammen mit der Verwaltung gemeinsam zu stellen habe, den mit der Materie bisher nicht vertrauten Mitarbeitern aus den ehemaligen DDR-Behörden den Stellenwert des Rechts auf informationelle Selbstbestimmung im Sinne des Grundrechts auf Menschenwürde bewußt zu machen und ihnen die rechtlichen Komponenten und die Technik des Datenschutzes schnell und effektiv zu vermitteln", so hoffe ich doch auch, daß er unserer Behörde die nötigen Mittel verschafft. Sie zu bewilligen, meine Damen und Herren Abgeordneten ist Ihre Aufgabe, um deren Wahrnehmung ich Sie dringlich bitte.

Ich habe bewußt bei den datenschutzrechtlichen Problemen der deutschen Einigung verweilt, weil diese eine Dimension unserer Aufgabe eröffnet haben, mit der wir bisher nicht konfrontiert waren.

Gleichwohl gebietet es der heutige Anlaß, auch, oder vielleicht gerade deswegen auf die Probleme einzugehen, die in der Kontinuität der Aufgabe des Berliner Datenschutzbeauftragten stehen. Hier möchte ich betonen, daß in Berlin *Gesetzgeber und Verwaltung* stets in besonderem Maße für Probleme des Datenschutzes aufgeschlossen waren. Nicht erst das seit 1. November vergangenen Jahres gültige neue Berliner Datenschutzgesetz, sondern auch bereits das erste Datenschutzgesetz aus dem Jahre 1978 sowie die darauffolgenden speziellen Datenschutzgesetze, waren - ungeachtet der jeweiligen Mehrheitsverhältnisse in diesem Hause - ein Ausdruck hohen Datenschutzbewußtseins, das dieser von der Grundeinstellung her den Menschenrechten stets aufgeschlossenen Stadt auch angemessen ist.

In dieser Legislaturperiode stehen trotzdem enorme *gesetzgeberische Aktivitäten* bevor, um das Berliner Recht auf den vom Bundesverfassungsgericht geforderten, aber auch durch das neue Berliner Datenschutzgesetz vorgezeichneten Stand zu heben. Angemessene Gesetze in den verschiedensten Geschäftsbereichen - ich nenne beispielhaft nur die Polizei, den Verfassungsschutz, das Personalwesen, das Bauwesen, das Schulwesen, nicht zu vergessen die Finanzverwaltung - sind erforderlich, wobei hervorzuheben ist, daß die Spezialgesetze keine Ablaßbriefe für die schlichte Festschreibung des status quo, sondern ernsthafter Prüfstein sein sollten, ob überall dem Prinzip der informationellen Sparsamkeit entsprochen wurde.

Ein Vorschlag, den ich schon vor einiger Zeit öffentlich gemacht habe, würde Berlin weltweit zu einem Vorreiter der rechtlichen Bewältigung der Informationsgesellschaft machen - die Einbindung der bestehenden und der erforderlichen informationsrechtlichen Regelungen in ein einheitliches *Informationsgesetzbuch*, das dann von einer allgemeinen Umschreibung informationsrechtlicher Ansprüche ausgehend das Recht des Datenschutzes, der Organisation des Informations- und Kommunikationswesens, der Statistik, des Archivwesens regeln und auch das notwendige Pendant zum Datenschutz umfassen würde - das Recht des Bürgers auf Zugang zu den staatlichen Informationen.

Vor schwierigen Aufgaben anderer Art wird die *Verwaltung* durch die Entwicklung der Informations- und Kommunikationstechnik gestellt. Sie ist gekennzeichnet durch zwei gegenläufige Tendenzen: Die Dezentralisierung einerseits, die Vernetzung der Systeme andererseits.

Auf den ersten Blick scheint die *Dezentralisierung* der Datenverarbeitung der datenschutzrechtlichen Forderung entgegenzukommen, einzelne Anwendungen voneinander abzuschotten. Dies ist auch richtig. Es muß aber darauf geachtet werden, daß mit der Vereinzelung der Datenverarbeitung nicht gleichzeitig die Kontrollmöglichkeiten eingeschränkt werden; die erforderliche Transparenz gegenüber der eigenen Dienststelle, aber natürlich auch gegenüber den Kontrollinstanzen muß erhalten bleiben. Am gravierendsten stellt sich dieses Problem bei dem verständlichen Wunsch, auch zu Hause einen Computer nutzen zu können, wenn es üblich und erlaubt ist, dienstliche Aufgaben dort zu erledigen: Er wird nicht nur von Lehrern vorgebracht, die ihren Arbeitsplatz zu Hause haben, sondern auch von Mitarbeitern in so sensitiven Bereichen wie etwa der Staatsanwaltschaft oder der Steuerverwaltung. Hier muß dringend eine Regelung geschaffen werden, die verhindert, daß kontrollfreie Räume der öffentlichen Datenverarbeitung entstehen.

Ganz gegensätzliche Probleme wird die umfassende *Vernetzung* aufwerfen, die die bisher isoliert nebeneinander stehenden Verfahren in eine neue Form der Verwaltungseinheit einbinden wird. Sind alle Geräte an ein einziges Netz angeschlossen, ist prinzipiell ein Zugriff auf alle Daten möglich - dies muß natürlich ausgeschlossen werden. Hier ein ausgewogenes Verhältnis zu finden, dürfte die bedeutsamste Aufgabe sein, vor der die Verwaltungsautomation in den nächsten Jahren steht. Wie beim Informationsgesetzbuch wäre es eine hervorragende Aufgabe für dieses Land, auch bei der Bewältigung der technischen Probleme eine Vorreiterrolle für andere Länder zu übernehmen.

Sehr geehrte Damen und Herren,

meine bisherigen Ausführungen erwecken den Eindruck, als gebe es keine Kritik an der *Umsetzung des Datenschutzgesetzes* in den Organistionseinheiten der Berliner Verwaltung, die seit nunmehr fast dreizehn Jahren dem Berliner Datenschutzrecht verpflichtet sind. Dieser Eindruck stimmt leider nicht ganz. Zwar räume ich gerne ein, daß die Berliner Verwaltung im Vergleich mit anderen Ländern viel Verständnis für den Datenschutz aufbringt: Dies mag auf den angesprochenen weltstädtischen Anspruch zurückgehen oder auch darauf, daß der Berliner Datenschutzbeauftragte von Anfang an die Belange der Verwaltung gesehen und in seine Entscheidung einbezogen hat - dies war bereits ein Grundsatz meines Vorgängers in diesem Amte und entspricht auch meiner Einstellung.

Auf der anderen Seite ist aber noch immer Unverständnis für das Menschenrecht jedes Einwohners dieser Stadt auf Datenschutz spürbar, für das einzutreten der Gesetzgeber jede öffentliche Stelle verpflichtet hat, die personenbezogene Daten verarbeitet. Dies zeigt sich mitunter nicht nur auf der Ebene von Verwaltungsmitarbeitern, die den zusätzlichen Aufwand, den der Datenschutz zwangsweise mit sich bringt, nicht gerade schätzen. Vielmehr gibt es auch noch immer grundsätzliche Vorbehalte gegen unser Anliegen. Die Stellungnahme des Senats ist trotz allen Wohlwollens, das dem Datenschutz entgegengebracht wird, nicht frei von derartigen Zügen.

So bedaure ich es, daß gerade die *Senatsverwaltung für Stadtentwicklung und Umweltschutz*, der wir uns wegen der kritischen Einstellung gegenüber den Gefahren technologischer Entwicklungen verbunden fühlen, sich zu erheblicher Kritik an unserem Bericht veranlaßt sieht, obwohl inhaltliche Meinungsverschiedenheiten nicht vorhanden sind.

Ein weiteres Beispiel ist die Einstellung der *Polizei*, die in der Senatsstellungnahme ihren Ausdruck findet. Seit Bestehen der Datenschutzgesetze hat es sich die Polizei besonders schwer mit der Einsicht gemacht, daß ihre - sicherlich erforderliche - Ermittlungstätigkeit ebenso unter einem Gesetzesvorbehalt steht wie der körperliche Eingriff. Der sogenannte „Übergangsbonus" wird hier so extensiv wie nirgends ausgelegt. Der Senat räumt in seiner Stellungnahme zwar ein, daß ein modernes Polizeigesetz, das auch die Datenverarbeitung der Polizei regelt, dringend erforderlich sei. Er lehnt es aber ab, in den konkreten, in unserem Bericht angesprochenen Fällen Konsequenzen zu ziehen: Eine nach unserer Feststellung zu pauschal durchgeführte erkennungsdienstliche Behandlung wird gerechtfertigt, die Speicherung von Daten von Prostituierten, die sich keiner Straftat schuldig gemacht haben, soll auch gegen den Willen der Betroffenen erfolgen.

Auch gegen die Prüfpraxis des Datenschutzbeauftragten ist Widerstand spürbar. Erhebliche Meinungsverschiedenheiten bestehen vor allem bei der Frage, in welchem Umfang der Datenschutzbeauftragte Transparenz gegenüber dem Bürger herstellen kann, wenn er Mängel bei der Verarbeitung personenbezogener Daten feststellt. Der selbstverständlichen Befugnis des Datenschutzbeauftragten, den Bürger in die Lage zu versetzen, seine Rechte gegenüber der datenverarbeitenden Stelle durchzusetzen, stellt die Polizei einen umfassenden Geheimhaltungsanspruch gegenüber, der aus unserer Sicht in der behaupteten allgemeinen Form nicht gerechtfertigt ist.

Ich betonte bereits, daß diese Einstellungen nicht typisch für die Berliner Verwaltung sind. Ich bin auch überzeugt davon, daß die Notwendigkeit des Datenschutzes für eine moderne Verwaltung von allen Stellen gesehen wird. Die Risiken der Informationsgesellschaft können nur ausgeglichen werden durch ein höchstmögliches Maß an Transparenz einerseits, an strenger Kontrolle der Datenverarbeitung andererseits. Nur so kann sich das informationelle Selbstbestimmungsrecht des Bürgers, und damit seine Persönlichkeit in der Informationsgesellschaft entfalten.

Ich bitte Sie, meine Damen und Herren Abgeordneten, den Berliner Datenschutzbeauftragten, der durch den Gesetzgeber bewußt an die Seite des Parlaments gerückt wurde, in dieser Aufgabe zu unterstützen. Wir werden uns unsererseits bemühen, Ihnen jede mögliche Hilfestellung zu geben.

Ich bin vor eineinhalb Jahren von diesem Hause gewählt worden - darf ich hier sagen: *Obwohl* ich Politikwissenschaftler bin? - In meinem Studium habe ich mich intensiv mit dem Politikwissenschaftler *Platon* beschäftigt - eine Sentenz aus seinem Werk hat mich dabei sehr beeindruckt - sie scheint mir ein Leitmotiv, unter das ich gerade die Arbeit des Datenschutzbeauftragten stellen möchte:

„Gerechtigkeit wird nur dort herrschen, wo sich die vom Unrecht nicht Betroffenen genauso entrüsten wie die Beleidigten."

2. Entschließungen der Konferenz der Datenschutzbeauftragten des Bundes und der Länder

2.1 Beschluß der Sonderkonferenz am 29. Januar 1991 zum Vorschlag der EG-Kommission für eine Richtlinie zum Schutz von Personen bei der Verarbeitung personenbezogener Daten

I.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat in der Vergangenheit zu wiederholten Malen die Untätigkeit der Europäischen Gemeinschaft im Bereich des Datenschutzes kritisiert. Kernpunkt dieser Kritik war die Befürchtung, daß die Dynamik der wirtschaftlichen Entwicklung in Richtung auf den vollendeten Binnenmarkt zu einem „informationellen Großraum" mit einem engen Netzwerk grenzüberschreitender Datenflüsse führt, ohne daß gleichzeitig der Grundrechtsschutz in der Gemeinschaft bei der Verarbeitung und dem Austausch persönlicher Daten gewährleistet wird.

II.

Daher begrüßt die Konferenz, daß die EG-Kommission im Juli 1990 den „Vorschlag für eine Richtlinie des Rates zum Schutz von Personen bei der Verarbeitung personenbezogener Daten" vorgelegt hat. Der Kommissionsvorschlag geht in einer Reihe von Punkten über die Konvention des Europarats zum Datenschutz von 1980 hinaus und berücksichtigt insoweit die technische und rechtliche Entwicklung des vergangenen Jahrzehnts. Positiv bewertet die Konferenz vor allem die Intention des Entwurfs, den Datenschutz in der EG nicht auf dem kleinsten gemeinsamen Nenner, sondern auf einem möglichst hohen Niveau zu harmonisieren. Sie legt allerdings entscheidenden Wert darauf, daß die Mitgliedstaaten die Möglichkeit behalten, den Datenschutz in der nationalen Gesetzgebung weiterzuentwickeln.

III.

Zahlreiche bewährte Vorschriften und Instrumente aus dem deutschen Datenschutzrecht sind in den Richtlinientext aufgenommen worden. Die Bewertung der einzelnen Bestimmungen des Richtlinienentwurfs kann jedoch nicht isoliert aus dem Blickwinkel des deutschen Datenschutzrechts erfolgen. Jeder nationale Gesetzgeber muß bei Rechtsharmonisierung auf europäischer Ebene bereit sein, einzelne seiner Regelungen auf dem Hintergrund der Erfahrungen und Vorstellungen anderer Mitgliedstaaten in Frage zu stellen. Zur Abstimmung der Auffassungen auf EG-Ebene besteht ein intensiver Meinungsaustausch zwischen der Konferenz und den Datenschutzinstitutionen der Partnerländer.

IV.

Die Konferenz hält, abgesehen von der Bereinigung von redaktionellen Unstimmigkeiten, einige Änderungen im Richtlinienvorschlag für notwendig, um die Gleichwertigkeit des Schutzes auf dem Niveau, das die Mitgliedsländer mit bestehender Datenschutzgesetzgebung bereits erreicht haben, sicherzustellen. Folgende Korrekturen sind dabei vorrangig:

1. Datenschutz muß, jedenfalls im Bereich der öffentlichen Verwaltung, für alle Unterlagen mit personenbezogenen Daten gelten. Die in der Richtlinie vorgesehene Beschränkung des Anwendungsbereichs auf die Verarbeitung personenbezogener Daten in „Dateien" ist ebenso technisch überholt wie Anlaß zu einer Fülle von Interpretationsproblemen.
2. Für die Verwendung und Weitergabe persönlicher Daten muß das Prinzip strikter Zweckbindung gelten und ausdrücklich statuiert werden. Wenn der Entwurf die bloße Vereinbarkeit der Zwecke von Erhebung, Speicherung und Übermittlung genügen läßt, werden inakzeptable Verarbeitungsfreiräume eröffnet; die Transparenz des Datenumgangs geht für den einzelnen verloren.
3. Der Anspruch auf Auskunft über die gespeicherten Daten ist das elementarste Individualrecht der Betroffenen. Nur gravierende Interessen der Allgemeinheit oder Dritter dürfen im Ausnahmefall diesen Auskunftsanspruch einschränken. Der im Entwurf vorgesehene Katalog von Fällen der Auskunftsverweigerung muß daher deutlich vermindert werden.
4. Der Forderung des Entwurfs, daß die Erhebung von Daten nur „nach Treu und Glauben" erfolgen darf, kann uneingeschränkt zugestimmt werden. Doch muß dieses Prinzip im Interesse des einzelnen konkretisiert werden. Es gilt klarzustellen, daß persönliche Angaben vorrangig beim Betroffenen selbst zu erheben sind. Die Ausnahmefälle, in denen Informationen ohne Kenntnis des Betroffenen beschafft werden dürfen, sollten soweit wie möglich in der Richtlinie konkret benannt werden.
5. Der Datenschutz der EG-Bürger darf nicht an den Gemeinschaftsgrenzen haltmachen. Ziel der Richtlinie muß neben der EG-internen Harmonisierung auch sein, den Schutz des Betroffenen beim Datenexport in Drittländer zu gewährleisten. Dies setzt voraus, daß im Empfängerland ein dem EG-Standard gleichwertiges Datenschutzniveau besteht. Daß der Richtlinienentwurf sich mit einem „angemessenen" Schutz im Zielland zufriedengibt, genügt nicht. Notwendig ist schließlich, das Verfahren zur Feststellung des Datenschutzstandards in Drittländern übersichtlich und praktikabel auszugestalten.
6. Auf der EG-Ebene bedarf es einer unabhängigen Datenschutzinstanz, die alle EG-Organe in Datenschutzfragen berät und für die Überwachung der Einhaltung sowie die einheitliche Anwendung der Richtlinie sorgt. Die im Richtlinienvorschlag vorgesehene „Gruppe für den Schutz personenbezogener Daten" erfüllt - betrachtet man ihre Struktur, Aufgaben und Kompetenzen - diese Anforderungen nicht. Die Unabhängigkeit der Datenschutzkontrolle auf EG-Ebene wird in Zweifel gezogen, wenn den Vorsitz nicht ein gewähltes Mitglied dieser - aus den nationalen Datenschutzorganen zusammengesetzten - „Gruppe", sondern ein Vertreter der EG-Kommission führt. Klargestellt werden muß weiter, daß das Votum der „Gruppe" im vorhinein bei allen den Datenschutz betreffenden Initiativen und Entwürfen der Kommission einzuholen ist. Ansprechpartner der „Gruppe" darf nicht ausschließlich die EG-Kommission, sondern muß auch das Europäische Parlament sein.
7. Da die Kommission die entsprechende Anwendung der Richtlinie auf die personenbezogene Datenverarbeitung ihrer eigenen Dienststellen beschlossen hat, muß sie auch umgehend für eine unabhängige Kontrolle dieses Bereichs Sorge tragen.

V.

Die Konferenz weist darauf hin, daß die vorliegende Richtlinie durch Regelungen für besondere Anwendungsbereiche ergänzt werden muß. Sie sind insbesondere für den Arbeitnehmer- und Sozialdatenschutz vordringlich. Die Kommission sollte schon jetzt ihre Bereitschaft erklären, entsprechende Regelungen zu treffen, und möglichst bald erste Vorschläge vorlegen.

VI.

Die Konferenz begrüßt die Gesprächsbereitschaft der Kommission und geht davon aus, daß der bereits begonnene Dialog zu einer substantiellen Verbesserung des Richtlinienvorschlags führen wird. Die Konferenz wird diese Entschließung der EG-Kommission, dem Europäischen Parlament sowie der Bundesregierung zuleiten. Informiert werden ebenfalls die Datenschutzkontrollinstitutionen der Partnerländer in der Gemeinschaft.

2.2 Beschluß der 41. Konferenz am 8. März 1991 zu Telekommunikation und Datenschutz

I.

Die Telekommunikation hat außerordentlich stark an Bedeutung gewonnen und ersetzt häufig den Brief oder auch das persönliche Gespräch: Über die dreißig Millionen deutschen Telefone werden monatlich rund drei Milliarden Gespräche geführt. Für die Privatsphäre des Bürgers in einer freiheitlichen Gesellschaft ist es unverzichtbar, daß Telefongespräche unkontrolliert und unbeobachtet geführt werden können. Von existentieller Bedeutung wird dies, wenn der Bürger in Notlagen gerät, aus denen er sich nur mit vertraulicher Beratung und Hilfe befreien

kann. Daher unterstützen sowohl die Kirchen als auch Hilfs- und Beratungsorganisationen die Forderungen des Datenschutzes, das „Grundrecht auf unbeobachtete Kommunikation" zu sichern.

Dieser Forderung muß die technische Ausgestaltung der Telekommunikationsnetze und -dienste folgen, und die rechtlichen Regelungen müssen diesen sich aus der Verfassung ergebenden Auftrag erfüllen. Der Gesetzgeber hat in dem am 1. Juli 1989 in Kraft getretenen Poststrukturgesetz die Bundesregierung aufgefordert, „Rechtsverordnungen zum Schutz personenbezogener Daten der am Fernmeldeverkehr Beteiligten" zu erlassen. Der Ausschuß für Post und Telekommunikation und der Innenausschuß des Deutschen Bundestages haben mehrfach den Schutz des Fernmeldegeheimnisses angemahnt.

Die vom Bundesminister für Post und Telekommunikation vorgelegten Entwürfe von Verordnungen über den Datenschutz bei Dienstleistungen der Deutschen Bundespost TELEKOM (TDSV) und über den Datenschutz für Unternehmen, die Telekommunikationsdienstleistungen erbringen (UDSV), widersprechen in wesentlichen Punkten dem Grundrecht auf unbeobachtete Kommunikation. Dabei ist besonders unverständlich, daß der Bundesminister von bereits früher gemachten Zusagen an den Deutschen Bundestag wieder abgerückt ist.

Die Entwürfe bleiben in wichtigen Punkten unter dem Datenschutzniveau, das von der EG-Kommission in ihrem Richtlinienentwurf zum Schutz personenbezogener Daten und der Privatsphäre in öffentlichen digitalen Telekommunikationsnetzen für den europäischen Binnenmarkt angestrebt wird.

II.

Ein wesentlicher Mangel besteht in der beabsichtigten Vollerfassung aller Verbindungsdaten von Telefongesprächen: Für jedes Telefonat soll bis zur Versendung der Entgeltrechnung bei der Deutschen Bundespost TELEKOM festgehalten werden, wer wann wie lange und mit wem telefoniert hat, nach Wahl des Kunden achtzig Tage darüber hinaus. Eine monatliche Auflistung dieser dem Fernmeldegeheimnis unterliegenden Informationen (Einzelentgeltnachweis) sollen Kunden - auch Arbeitgeber - auf Wunsch erhalten können. Außerdem können nach § 12 Fernmeldeanlagengesetz (FAG) auch Gerichte und Staatsanwaltschaften bei strafrechtlichen Ermittlungen jeder Art, also auch bei Bagatelldelikten, ohne besondere Voraussetzungen auf diese Daten zugreifen.

Abzulehnen ist auch die vorgesehene Beschränkung des Kunden auf die Alternative, daß von einem Anschluß die Telefonnummer des Anrufers immer oder nie beim Angerufenen angezeigt wird. Dem Recht auf informationelle Selbstbestimmung entspricht es, daß der Anrufer in jedem Einzelfall entscheiden kann, ob seine Rufnummer beim Angerufenen angezeigt wird. Umgekehrt hat jeder Angerufene selbstverständlich das Recht, nur Gespräche entgegenzunehmen, bei denen die Nummer des Anrufers angezeigt wird.

III.

Die Datenschutzbeauftragten fordern:

1. Alle - durch die computergesteuerte Vermittlungstechnik entstehenden - Verbindungsdaten sind nach dem Ende der Verbindung mit folgender Maßgabe unverzüglich zu löschen:

   In die Entgeltdatenverarbeitung dürfen nur diejenigen Daten eingehen, die zur Berechnung der Entgelte in Summenform unerläßlich sind. Auf Antrag des Kunden darf zur Prüfung der Richtigkeit des in Rechnung gestellten Entgelts oder zur Erstellung eines Einzelentgeltnachweises die Rufnummer des Angerufenen nur in einer zumindest um die letzten vier Ziffern verkürzten Form gespeichert werden. Die Daten sind spätestens achtzig Tage nach dem Absenden der Entgeltrechnung zu löschen.

   Die Entscheidung des Kunden über die Form der Abrechnung muß auch bei der Abrechnung zwischen verschiedenen Netzbetreibern respektiert werden.

2. Die Erstellung von „Kommunikationsprofilen", die Aussagen über das persönliche Telefonierverhalten des Bürgers und die Nutzung anderer Telekommunikationsdienste enthalten, muß ausgeschlossen sein.

3. Bei der Anzeige der Rufnummer des Anrufers beim Angerufenen müssen beide die Wahlmöglichkeit haben, diese Anzeige entweder auf Dauer oder im Einzelfall „auf Knopfdruck" zu unterdrücken.

4. Ausnahmen von diesen Grundsätzen - zum Beispiel zur Aufklärung telefonischer Bedrohungen oder in Notfällen - müssen begründet, ausdrücklich geregelt und für den Betroffenen transparent sein.

5. Die Konferenz bekräftigt ihre Forderung (Beschluß vom 4./5. Oktober 1990), Eingriffe in das grundgesetzlich geschützte Fernmeldegeheimnis (Art. 10 GG) auf das unerläßliche Maß zu beschränken und insbesondere nicht schon im Bereich der Bagatellkriminalität zuzulassen. Die Regelung des § 12 FAG hat im Zuge der technischen Entwicklung eine verfassungsrechtlich bedenkliche neue Qualität erhalten, da sie nunmehr auch die bei Einsatz neuer Kommunikationstechniken anfallenden Abrechnungs-, Verbindungs-, Nutzungs- und Inhaltsdaten umfaßt. Statt im FAG sollten die Eingriffsmöglichkeiten in das Fernmeldegeheimnis im Rahmen der Strafverfolgung - schon aus Gründen der Normenklarheit - in der Strafprozeßordnung unter engen Voraussetzungen und Beschränkungen abschließend geregelt werden.

2.3 Entschließung der Konferenz vom 25. Juni 1991 - gegen die Stimme Bayerns - zum Bundesratsentwurf eines Gesetzes zur Bekämpfung des illegalen Rauschgifthandels und anderer Erscheinungsformen der Organisierten Kriminalität

Schon seit Jahren haben Datenschutzbeauftragte von Bund und Ländern eine angemessene gesetzliche Regelung zu den in die Freiheitsrechte der Bürger eingreifenden Strafverfolgungsmaßnahmen, wie der Rasterfahndung, des Einsatzes Verdeckter Ermittler und des Einsatzes besonderer technischer Observationsmittel gefordert. Sie bedauern, daß hierzu die Bundesregierung nicht schon längst einen Entwurf vorgelegt hat. Der Bundesrat mit seinem Ende April 1991 beschlossenen Gesetzentwurf wird diesem Anliegen ebenfalls nicht gerecht.

Zum Schutz der Persönlichkeitsrechte der Bürger wie im Interesse wirksamer Aufgabenerfüllung durch die Strafverfolgungsorgane bedarf es klarer Rechtsgrundlagen. Der Datenschutz stellt sich Bemühungen nicht entgegen, den zunehmenden Herausforderungen, denen die Bürger unseres Staates durch die organisierte Kriminalität, insbesondere durch die Drogenkriminalität ausgesetzt sind, in erforderlicher Weise zu begegnen. Über dieses Ziel schießt der Bundesratsentwurf aber hinaus. Zwar enthält der Entwurf gegenüber früheren Vorschlägen des Bundesrates insofern eine Verbesserung, als nunmehr die Rasterfahndung und der Einsatz Verdeckter Ermittler an einen Straftatenkatalog gebunden werden sollen. Es bestehen aber weiterhin Bedenken, daß schwerwiegende Eingriffe in die Privatsphäre, wie der Einsatz von Peilsendern, schon bei „Straftaten von erheblicher Bedeutung" möglich sind.

Mit diesem schwammigen Begriff statt eines präzisen Kataloges von Straftaten wird der Einsatz der geheimen Ermittlungsmethoden weit über den Bereich der organisierten Kriminalität hinaus ausgedehnt. Diese Mittel werden damit für sämtliche Straftaten außerhalb der Bagatell- und Kleinkriminalität verfügbar.

Nach dem Gesetzentwurf wären auch über völlig unbeteiligte Personen heimliche Bild- und Filmaufnahmen zulässig, wenn es „der Erforschung des Sachverhalts" oder der „Aufenthaltsermittlung des Täters" dient. Gegen unverdächtige Personen sollen Wanzen und Peilsender eingesetzt werden können, wenn eine „Verbindung" - was immer darunter verstanden werden soll - mit dem Täter vermutet wird.

Selbst in privaten Wohnungen sollen Gespräche, die im Beisein eines Verdeckten Ermittlers geführt werden, heimlich abgehört und aufgezeichnet werden.

Es ist außerdem problematisch, daß derart schwerwiegende Eingriffe wie der Einsatz Verdeckter Ermittler nach dem Gesetzentwurf nicht in allen Fällen vom Richter angeordnet werden

müssen, sondern weitgehende Eilkompetenzen für Polizei und Staatsanwaltschaft vorgesehen sind.

Ein weiteres Problem liegt darin, daß durch den Einsatz geheimer Ermittlungsmethoden gewonnene Informationen in zu weitem Umfang für andere Zwecke verwendet werden können. Offen bleibt insbesondere, ob die gewonnenen Erkenntnisse der Polizei für eine jahrelange Speicherung zur vorbeugenden Straftatenbekämpfung überlassen werden dürfen. Dies sieht der Gesetzentwurf undifferenziert nicht nur für Tatverdächtige, sondern sogar für andere Personen wie Begleiter oder zufällig betroffene Dritte vor.

Die Datenschutzbeauftragten halten es deshalb für dringend geboten, daß Bundestag und Bundesrat im weiteren Gesetzgebungsverfahren diese Probleme aufgreifen und die - wiederholt geäußerten - datenschutzrechtlichen Vorschläge berücksichtigt werden. Die Stellungnahme der Bundesregierung zu dem Entwurf des Bundesrates sollte diese Bemühungen unterstützen.

2.4 Entschließung der 42. Konferenz am 26./27. September 1991 zum Datenschutz im Recht des öffentlichen Dienstes

I.

Die Daten von Arbeitnehmern werden im Laufe ihres beruflichen Lebens in vielfältiger Weise vom Arbeitgeber verarbeitet. Allein schon im Hinblick auf die große Zahl der über Arbeitnehmer erhobenen Daten und mit Rücksicht auf die Abhängigkeit des Arbeitnehmers vom Arbeitgeber ist eine gesetzliche Regelung der Verarbeitung von Personaldaten zwingend erforderlich. Auch gegenüber Beamten und anderen im öffentlichen Dienst Tätigen kann die Verarbeitung ihrer Daten nicht allein auf die hergebrachten Grundsätze des Berufsbeamtentums gestützt oder in Verwaltungsvorschriften geregelt werden. Vielmehr ist eine gesetzliche Grundlage vonnöten. Sie muß um so konkreter sein, je tiefer in das Persönlichkeitsrecht der Betroffenen eingegriffen wird.

II.

In der Auseinandersetzung um das Recht des öffentlichen Dienstes beeinträchtigen zwei grundlegende Fehleinschätzungen eine angemessene Regelung des Datenschutzes. Es trifft nicht zu, daß die Kenntnis des Dienstherrn über seine Bediensteten alle persönlichen Lebensumstände vollständig und lückenlos umfassen muß. Es ist ferner unrichtig, daß gesetzliche Regelungen überflüssig sind, weil stets die Einwilligung der Betroffenen eingeholt werden kann.

Zum einen wäre es mit der Würde des Menschen unvereinbar, wollte man ihn in seiner ganzen Persönlichkeit registrieren. Zwar ist der Angehörige des öffentlichen Dienstes dem Staat gegenüber besonders eng verpflichtet; er bleibt aber auch gegenüber seinem Dienstherrn Grundrechtsträger: Auch seine personenbezogenen Daten dürfen nur erhoben und verarbeitet werden, soweit das für die Begründung und Abwicklung des Dienstverhältnisses erforderlich ist.

Zum anderen macht der Rückgriff auf die Einwilligung gesetzliche Regelungen keineswegs überflüssig. Zwar ist die Erhebung und Verarbeitung personenbezogener Daten mit Einwilligung des Betroffenen grundsätzlich auch dann zulässig, wenn eine gesetzliche Grundlage fehlt. Die Einwilligung wird jedoch zur Farce, wenn sie faktisch erzwungen wird, weil z. B. eine Bewerbung ohne Einwilligung nicht berücksichtigt wird. Soweit bestimmte Angaben verfügbar sein müssen, sind sie gesetzlich präzise vorzuschreiben, aber zugleich auf den erforderlichen Umfang zu begrenzen.

III.

Neben der Neuordnung des Personalaktenrechts bedürfen auch andere Teilbereiche des öffentlichen Dienstrechts der datenschutzgerechten gesetzlichen Regelung. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hält insbesondere die Lösung folgender Probleme für vorrangig:

1. *Bewerbung um Einstellung in den öffentlichen Dienst*

   Es ist - für den Bewerber transparent - festzulegen,
   - welche personenbezogenen Informationen von ihm verlangt bzw. über ihn eingeholt, wie sie genutzt werden dürfen und wann sie zu löschen sind,
   - ob und unter welchen Voraussetzungen und in welchem Stadium des Verfahrens der Bewerber sich Tests, Untersuchungen und Überprüfungen zu unterziehen hat,
   - ob und inwieweit private Institutionen daran mitwirken und welche vertraglichen Sicherungen zum Schutz personenbezogener Daten zu vereinbaren sind,
   - daß die Daten jeweils erst zu dem Zeitpunkt, in dem sie für das Verfahren erforderlich werden, und mit dem geringstmöglichen Eingriff erhoben werden.

2. *Sicherheitsüberprüfung*

   Es ist bereichsspezifisch gesetzlich festzulegen,
   - wer im öffentlichen Dienst einer Sicherheitsüberprüfung unterzogen wird,
   - welche personenbezogenen Daten dafür erhoben und verarbeitet werden,
   - wie das Verfahren gestaltet wird, insbesondere welche Stellen mit welchen Befugnissen am Verfahren beteiligt sind, und unter welchen Voraussetzungen Sicherheitsbedenken anzunehmen sind,
   - daß die im Rahmen der Sicherheitsüberprüfung erhobenen Daten grundsätzlich nur für diesen Zweck verwendet werden dürfen,
   - daß der Betroffene über das Ergebnis der Sicherheitsüberprüfung zu unterrichten ist.[99]

3. *Ärztliche Untersuchung*

   Es ist durch Gesetz oder ergänzende Rechtsverordnung festzulegen,
   - unter welchen Voraussetzungen die ärztliche Untersuchung eines Bewerbers oder Bediensteten angeordnet werden kann,
   - daß jede ärztliche Untersuchung einen präzisen Untersuchungsauftrag voraussetzt, der Anlaß und Gegenstand der Untersuchung möglichst exakt definiert und den Umfang der Untersuchung eingrenzt,
   - wie das Arztgeheimnis und der Datenschutz sicherzustellen sind,
   - wann und in welchem Umfang Versicherungen und früher behandelnde Ärzte über frühere Untersuchungen und Maßnahmen befragt werden und diese offenbaren dürfen,
   - daß Ärzte und Versicherungen Daten nicht ohne Kenntnis des Betroffenen und nur mit Einwilligung des Bewerbers offenbaren dürfen,
   - daß die Unterlagen der ärztlichen Untersuchungen nicht für andere Zwecke verwendet werden und nicht mit solchen vermengt werden dürfen, die anderen Zwecke dienen, und daß sie zu vernichten sind, sobald sie nicht mehr benötigt werden,
   - daß der Arzt der personalverwaltenden Stelle nur das Endergebnis seiner Untersuchung und - soweit erforderlich - nur tätigkeitsbezogene Risiken mitzuteilen hat,
   - daß dem Betroffenen ein Recht auf Einsicht in die beim Arzt verbliebenen Untersuchungsunterlagen zusteht.

4. *Beihilfen*

   Gesetzlich festzulegen sind die Grundlagen eines datenschutzgerechten Beihilfeverfahrens, insbesondere die Abschottung der Beihilfestelle, das Verbot automatisierter Speicherung von Diagnosedaten und anderen medizinischen Einzelangaben, die Zweckbindung der Daten sowie ein eigener Beihilfeanspruch der Angehörigen.

5. *Personalinformationssysteme*

   Es muß dienstrechtlich gewährleistet sein, daß
   - automatisierte Systeme zur Verarbeitung von Personaldaten zu unterschiedlichen Zwecken (z. B. Urlaubsdatei,

[99] Auf ihre Forderungen zur Sicherheitsüberprüfung (Geheimschutzgesetz) in den Entschließungen vom 13. 9. 1985, 18. 4. 1986 und 22. 3. 1990 nimmt die Konferenz Bezug.

Telefondatenerfassung, PC-Betriebsdaten) nicht zu umfassenden Persönlichkeitsprofilen verknüpft werden,
- alle vorgesehenen Auswertungen von Personaldaten in einer Übersicht, die dem Betroffenen zugänglich sein muß, zusammengefaßt werden,
- Kontrollen der Bediensteten mit Hilfe automatisierter Systeme unzulässig sind; Ausnahmen bedürfen einer gesetzlichen, insbesondere personalvertretungsrechtlichen Regelung.

IV.

Die Datenschutzbeauftragten des Bundes und der Länder fordern die für das Personalrecht zuständigen Minister und den Gesetzgeber auf, die auf der Grundlage der Rechtsprechung des Bundesverfassungsgerichts verfassungsrechtlich notwendigen Vorschriften zu erlassen.

3. Bericht der Arbeitsgruppe Telekommunikation und Medien der Internationalen Datenschutzkonferenz über Probleme des Telemarketing, der Kartentelefone und der elektronischen Directories und Beschluß der 13. Internationalen Konferenz der Datenschutzbeauftragten am 4. 10. 1991

BERICHT

Telemarketing

Der schnell zunehmende Gebrauch des Telefons für Zwecke der Direktwerbung (Telemarketing) bedroht die Privatsphäre der Verbraucher ernsthaft.

Es gibt zwei Hauptprobleme, die durch das Telemarketing für die Privatsphäre entstehen.

Das erste hängt mit der störenden Wirkung nicht erbetener telefonischer Verkaufsangebote auf die Verbraucher zusammen: Je öfter Anrufe für Werbezwecke entgegengenommen werden, desto störender wird der Verbraucher sie empfinden. Die Störung wird sogar noch verschärft, wenn die Anrufe von Anrufautomaten ausgelöst und durchgeführt werden.

Das zweite Problem betrifft die Nutzung von personenbezogenen Dateien, die für das Telemarketing eingesetzt oder als sein Ergebnis aufgebaut werden. Derartige Dateien können die informationelle Selbstbestimmung beeinträchtigen.

Telefonische Direktwerbung kann stattfinden:

a) im Zusammenhang mit einer bestehenden Beziehung zwischen dem Werbetreibenden und dem Verbraucher
und
b) wo keine derartige Beziehung besteht (cold calls).

Im Fall a), selbst solche Verbraucher, die im Rahmen einer bestehenden Beziehung angerufen werden, sollten das Recht haben, weiteren Anrufen zu widersprechen. Die Erfahrung in einigen europäischen Ländern hat gezeigt, daß Telefonpräferenzsysteme (Listen von Anschlußinhabern, die nicht für Werbezwecke angerufen werden wollen) nicht immer hinreichend wirksam die Privatsphäre schützen.

Im Fall b) sollten Verbraucher außerhalb einer bestehenden Geschäftsbeziehung nur angerufen werden, wenn diese Anrufe auf die Initiative des Verbrauchers zurückgehen.

Der Einsatz von Anrufautomaten sollte ohne die vorherige ausdrückliche Zustimmung des Verbrauchers nicht erlaubt sein, unabhängig davon, ob eine Geschäftsbeziehung besteht oder nicht.

Es sollten effektive Maßnahmen ergriffen werden, um unerwünschtes grenzüberschreitendes Telemarketing zu unterbinden.

Neue Techniken sollten nicht ohne Sicherungen zum Schutz der Privatsphäre eingeführt werden. Soweit diese Techniken Teilnehmerverzeichnisse benutzen, sollte den Teilnehmern an den neuen Diensten bereits bei Abschluß des Vertrages die kostenlose Möglichkeit eingeräumt werden, nicht in das Teilnehmerverzeichnis aufgenommen zu werden.

Diese Grundsätze sollten in gleicher Weise auf andere Telekommunikationstechniken wie Telefax oder Electronic Mail (elektronische Post) angewandt werden.

Die schnelle Entwicklung neuer Techniken zeigt, daß die Konferenz neue Entwicklungen sorgfältig beobachten sollte, um notwendige zusätzliche Maßnahmen zu empfehlen.

Kartentelefone

In den letzten Jahren sind elektronische Zahlungsmittel für das Telefonieren in öffentlichen Einrichtungen entwickelt worden.

Im Zusammenhang mit der Digitalisierung der Telefonnetze (bei der Einzelheiten des Anrufs im Netz gespeichert werden) ist die Möglichkeit des anonymen Zugangs zum Telefonnetz eine wichtige Sicherung der Privatsphäre.

Insofern ist die schnelle Entwicklung anonymer Telefonkarten auf Guthabenbasis, die in öffentlichen Telefonzellen benutzt werden können, sehr ermutigend.

Dennoch hat die internationale Mobilität des einzelnen - ergänzt durch Entwicklungen beim Mobiltelefon - dazu beigetragen, daß bestimmte Möglichkeiten angeboten werden, die die Anonymität herkömmlicher Telefonkarten entfallen lassen und dadurch Datenschutzprobleme erzeugen.

Diese Möglichkeiten führen dazu, daß identifizierbare Zahlungsmittel (Bankkarten, Kreditkarten, Telekarten) den Kunden vorzugsweise angeboten werden, obwohl es keine unausweichlichen technischen oder organisatorischen Gründe gibt, um diese Alternative zu wählen.

Dementsprechend sollte auf internationaler Ebene besondere Aufmerksamkeit darauf verwendet werden, die Gestaltung, das Angebot und die Anbringung von Geräten zu fördern, die eine echte Auswahl zwischen den verschiedenen - anonymen oder identifizierbaren - Zahlungsmethoden ermöglichen.

Wenn der Einsatz eines identifizierbaren elektronischen Zahlungsmittels angeboten wird, muß besondere Aufmerksamkeit darauf verwendet werden, daß durch angemessene technische Maßnahmen Mißbrauch unterbunden wird. Insbesondere sollte es die Möglichkeit der Authentifizierung des Karteninhabers geben.

Schließlich sollten nur solche personenbezogenen Daten an die Kartengesellschaft übermittelt werden, die zur Rechnungsstellung erforderlich sind. Es sollte nicht möglich sein, von diesen Daten Rückschlüsse entweder auf die Nummer des Angerufenen oder den Ort des Telefons zu ziehen, von dem aus angerufen wurde.

Karteninhaber sollten vor Zweckentfremdung ihrer personenbezogenen Daten geschützt sein und auf angemessene Weise darüber informiert werden, welche Art von Daten das Kartentelefon erhebt und welche Art von Daten dem jeweiligen Diensteanbieter übermittelt wird.

Elektronische Post und damit zusammenhängende Teilnehmerverzeichnisse

Die Entstehung und schnelle Verbreitung der elektronischen Post unterstreicht, wie wichtig es ist, den Schutz personenbezogener Daten zu gewährleisten, die in elektronischen Teilnehmerverzeichnissen in Zusammenhang mit diesen Systemen gespeichert werden.

Die 12. Internationale Datenschutzkonferenz hat in ihrem Beschluß vom 19. September 1990 auf die Probleme hingewiesen, die bei öffentlichen Telekommunikationsnetzen und beim Kabelfernsehen insbesondere in bezug auf elektronische weltweite Teilnehmerverzeichnisse bestehen.

Nach eingehenderer Prüfung der Probleme elektronischer Teilnehmerverzeichnisse weist die Arbeitsgruppe auf folgende weitere Punkte hin:

Personenbezogene Daten sollten in derartigen Verzeichnissen nur mit der informierten Einwilligung des Teilnehmers gespeichert werden.

Betroffene sollten über spezielle Datenschutzrisiken informiert werden, die sich aus einem Eintrag in das Verzeichnis ergeben.

Die Identität der für das Verzeichnis verantwortlichen Stelle und der Umfang der personenbezogenen Daten, die für das Funktionieren des Verzeichnisses notwendig sind, sollten eindeutig festgelegt werden.

Technische Maßnahmen sollten getroffen werden können, um eine Verarbeitung (z. B. Umdrehen oder Kopieren des Verzeichnisses) zu unterbinden, die dem Datenschutz widerspricht.

Zusätzliche Probleme entstehen allerdings jetzt bei den Verzeichnissen, die im Zusammenhang mit Systemen der elektronischen Post geführt werden. Diese Probleme beziehen sich auf die Entstehung eines Verzeichnistyps, der völlig andere Eigenschaften besitzt als das herkömmliche elektronische Telefonbuch. Derartige Verzeichnisse sind gewöhnlich in Systemen der elektronischen Post eingebettet. Während sie viele Jahre lang vorhanden waren, haben die technischen Schwierigkeiten des Zugangs und der Manipulation solcher Verzeichnisse auf der normalen Nutzerebene ihre Wirkung aus datenschutzrechtlicher Sicht reduziert. Jetzt jedoch ist mit der Festlegung des X.500-Standards, dessen Hauptziel die Ermöglichung von Schnittstellen für Verzeichnisse aller Systeme der elektronischen Post ist, die Schaffung großer verteilter elektronischer Verzeichnisse technisch erleichtert worden, und die damit zusammenhängenden Datenschutzprobleme müssen gelöst werden.

Diese Probleme betreffen offensichtlich:

die Entstehung eines einheitlichen Personenkennzeichens für Eintragungen in das Verzeichnis (in der Literatur als „distinguished name" bezeichnet). Die weltweite Erstrekkung der geplanten Verzeichnisse unter dem X.500-Standard unterstreicht zusätzlich die Datenschutzprobleme, die mit einheitlichen Personenkennzeichen verbunden sind;

die verstärkten benutzerfreundlichen Möglichkeiten, die zur Verfügung gestellt werden für die Durchsuchung und Verarbeitung dieser Verzeichnisse;

Probleme im Zusammenhang mit der Möglichkeit, nicht in das Verzeichnis aufgenommen zu werden, da das Verzeichnis gerade die Aufgabe hat, den aktiven Betrieb der elektronischen Post zu gewährleisten.

BESCHLUSS

Die 13. Internationale Konferenz der Datenschutzbeauftragten begrüßt den Bericht der Arbeitsgruppe Telekommunikation und Medien und unterstreicht die Bedeutung der beschriebenen Probleme in den Bereichen des Telemarketing, der Kartentelefone und der elektronischen Verzeichnisse.

4. Merkblatt des Berliner Datenschutzbeauftragten zu den Aufgaben eines behördlichen Datenschutzbeauftragten (behDSB)

In der folgenden Zusammenfassung sind die Aufgaben eines behDSB dargestellt, die sich aufgrund des neuen Berliner Datenschutzgesetzes (§ 19 Abs. 5 BlnDSG i. V. m. den §§ 36, 37 Bundesdatenschutzgesetz [BDSG]), aber auch anhand von Erkenntnissen und Empfehlungen des Berliner Datenschutzbeauftragten (BlnDSB) aus Prüfungen und Kontakten mit Behörden und sonstigen öffentlichen Stellen, die in der Regel auch datenverarbeitende Stellen (dv-Stellen) sind, ergeben.

Generell wird aus Gründen einer unabhängigen und neutralen Stellung des behDSB empfohlen, daß dieser zur Wahrnehmung seiner Aufgaben weisungsfrei und in dieser Funktion nur dem Chef der dv-Stelle bzw. seinem Stellvertreter unterstellt ist. Eine direkte organisatorische Unterstellung ist nicht zwingend und in den Fällen, in denen der behDSB diese Funktion lediglich nebenamtlich ausübt, auch nicht möglich. Wesentlich ist hierbei das direkte Vortragsrecht in Angelegenheiten des Datenschutzes. Der behDSB kann sich bei der Wahrnehmung seiner Aufgaben auch von Leitern und Mitarbeitern sachkundiger Bereiche (z. B. Organisationsstelle, Iuk-Benutzerservice u. a.) beraten lassen. Wird die Funktion des behDSB einer Dienstkraft zusätzlich übertragen, sind Inkompatibilitätsprobleme zu beachten. Daher sollte diese Funktion insbesondere nicht dem Leiter Personal, Leiter Organisation, Leiter DV oder Leiter von Organisationseinheiten mit intensiver Anwendung personenenbezogener Daten übertragen werden.

Für seine Tätigkeit gelten die Vorschriften der §§ 36, 37 Bundesdatenschutzgesetz entsprechend. Dabei wird insbesondere auf die folgenden Voraussetzungen aus § 36 BDSG hingewiesen: Erforderliche Fachkenntnis und Zuverlässigkeit; Benachteiligungsverbot; Verschwiegenheitspflicht; Unterstützung durch die dv-Stelle (insb. Sachmittel).

Die schriftlich vorzunehmende Bestellung des behDSB sollte in Anlehnung an § 36 Abs. 1 BDSG zum frühestmöglichen Zeitpunkt erfolgen (einen Stellvertreter schreibt das Gesetz nicht vor, jedoch ist dringend anzuraten, einen solchen aus Gründen einer kontinuierlichen Aufgabenwahrnehmung einzusetzen).

Zur Erfüllung seiner Aufgaben sind dem behDSB in entsprechender Anwendung der für den BlnDSB geltenden Vorschrift des § 28 BlnDSG bestimmte Befugnisse einzuräumen. Danach ist es ihm zu ermöglichen,

- alle Räume zu betreten (für Prüfungen und Besichtigungen) und
- in alle dienstlichen Unterlagen einzusehen (personenbezogene Daten zur Kenntnis zu nehmen).

Aus dem BlnDSG bzw. aus § 37 BDSG abgeleitete Aufgaben:

- Sicherstellung der Ausführung des BlnDSG sowie anderer Rechtsvorschriften über den Datenschutz für ihren Geschäftsbereich (§ 19 Abs. 1 Satz 1 BlnDSG, § 37 Abs. 1 BDSG). Dem behDSB wird eine übergeordnete koordinierende und überwachende Funktion zugewiesen. Die dv-Stellen bleiben in der Verantwortung für die Beachtung datenschutzrechtlicher Bestimmungen. Der behDSB kontrolliert deren Einhaltung. Hierzu kann er auch Stellungnahmen einholen. Bei Meinungsverschiedenheiten zwischen der dv-Stelle und dem behDSB entscheidet die Hausleitung. Beiden Parteien bleibt es jedoch unbenommen, in solchen Fällen den BlnDSB einzuschalten.
- Gewährleistung der ordnungsgemäßen Anwendung der DV-Programme, mit deren Hilfe personenbezogene Daten verarbeitet werden sollen (§ 19 Abs. 1 Satz 2 BlnDSG, § 37 Abs. 1 Nr. 1 BDSG); zu diesem Zweck ist der behDSB über Vorhaben der automatisierten Verarbeitung personenbezogener Daten rechtzeitig zu unterrichten, um bereits bei der Entwicklung dieser Automationsvorhaben Belange des Datenschutzes berücksichtigen zu können.
- Schulung der bei der Verarbeitung personenbezogener Daten tätigen Personen in den Erfordernissen des Datenschutzes, seiner Notwendigkeit und Bedeutung (§ 37 Abs. 1 Nr. 2 BDSG). Die diesbezüglichen Informationen für die Mitarbeiter können auch in schriftlicher Form erfolgen; bei kleineren Stellen können auch im Rahmen von Dienstbesprechungen Anregungen und Informationen zu Datenschutzfragen weitervermittelt werden.
- Beratende Mitwirkung bei der Auswahl der bei der Verarbeitung personenbezogener Daten tätigen Personen (§ 37 Abs. 1 Nr. 3 BDSG). Es ist hinreichend, die Beteiligung am Personalauswahlverfahren auf allgemeine Vorgaben zu beschränken und die Teilnahme an Vorstellungsgesprächen auf besondere Fälle einzugrenzen. Die beratende Mitwirkung bei der Personalauswahl beinhaltet kein Vetorecht.
- Führung des Dateien- (§ 19 Abs. 2) und des Geräteverzeichnisses (§ 19 Abs. 4), die ihm von den dv-Stellen zur Verfügung zu stellen sind (§ 37 Abs. 2 BDSG); Weiterleitung an den BlnDSB zum Dateienregister.
- Verpflichtung auf das Datengeheimnis (§ 8 Abs. 2), sofern nicht durch die Personalverwaltung/Büroleitung vorgenommen.

Spezielle Aufgaben:

1. *Aufbau* der Datenschutz-Organisation:
   - Information über die einschlägigen Datenschutzvorschriften im Hause
   - Entwicklung und Bekanntmachung von hausinternen Datenschutz-Richtlinien
   - Auswahl von Datenschutz-Kontaktpersonen in den Fachbereichen (bei Bedarf) und Kontaktpflege mit Fachleuten aus dem eigenen Haus (z. B. DV-Spezialisten) in bezug auf Datensicherheit und Datenschutz
   - Eigene Aus- und Fortbildung des behDSB und seines Stellvertreters im Hinblick auf die erforderlichen Rechts- und DV- Kenntnisse.
2. *Beratung* bei Fragen zum Datenschutz:
   - Behördenintern aufgrund seiner Stellung und Fachkompetenz
   - Erteilung von Auskünften bzw. Benachrichtigungen bei Eingaben bzw. Fragen von Betroffenen (Bürger, Mitarbeiter) zu datenschutzrelevanten Themen
   - Stellungnahmen zu Datenschutzproblemen
3. *Prüfungen:*
   - Schwachstellen- bzw. Risikoanalyse
   - Prüfungen auf Zulässigkeit der Verarbeitung von Mitarbeiter- bzw. anderer personenbezogener Daten
   - Kontrolle der Einhaltung der eigenen Datenschutzrichtlinien bzw. der Vorschriften des BlnDSG (in erster Linie der technischen und organisatorischen Maßnahmen nach § 5 BlnDSG; die eigenständigen Kontrollen können im Rahmen von Rundgängen oder gezielten Überprüfungen erfolgen)
   - Beauftragung bzw. Einbeziehung Dritter im Prüffall (z. B. BlnDSB, andere externe Kontrollinstitutionen [in besonderen Fällen nach Abstimmung mit der Hausleitung])
4. *Mitwirkung* bei
   - der Auswahl technischer Neuheiten bzw. neuer Arbeitstechniken, die für die Verarbeitung personenbezogener Daten in Frage kommen;
   - neuen Projekten sowie baulichen und organisatorischen Änderungen mit Datenschutz-/Datensicherungsbezug;
   - den Weisungen für die Auftragsdatenverarbeitung, sofern der Datenschutz berührt ist.
5. *Kontaktpflege* mit dem BlnDSB:
   - Erfahrungsaustausch
   - Inanspruchnahme des BlnDSB in Zweifelsfragen (§ 37 Abs. 1 Satz 2 BDSG); u. a. bei Fragen im Zusammenhang mit § 25 Abs. 1 Satz 6 BlnDSG „Anhörung des BlnDSB bei der Aufnahme von Dateien in das besondere Dateienregister"
6. *Entsorgung* von Unterlagen mit personenbezogenen Daten:
   - Beratung bei der Vernichtung von hausinternem Datenträgermaterial
   - Überprüfung des Vernichtungsvorgangs