Abgeordnetenhaus von Berlin

Drucksache 12/ 76

12. Wahlperiode

Bericht

des Berliner Datenschutzbeauftragten
zum 31. Dezember 1990

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 1990

Der Berliner Datenschutzbeauftragte hat dem Abgeordnetenhaus und dem Regierenden Bürgermeister jährlich einen Bericht über das Ergebnis seiner Tätigkeit vorzulegen (§ 29 Berliner Datenschutzgesetz in der Fassung vom 17. Dezember 1990)[1]. Der letzte Bericht ist zum Ablauf der vorherigen Amtszeit am 31. Oktober 1989 vorgelegt worden. Einerseits um den beschriebenen Zeitraum entsprechend der offenkundigen Intention des Gesetzgebers auf das Kalenderjahr zu erstrecken, andererseits um bereits dem neuen Abgeordnetenhaus die Möglichkeit der Erörterung zu geben, wird in diesem Bericht über den Zeitraum bis zum 31. Dezember 1990 berichtet. Dies soll in den Folgejahren ebenso gehandhabt werden.

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

Inhaltsverzeichnis

Einleitung

1. Datenschutz in Berlin 1990

1.1 Datenschutz ist Menschenrecht
1.2 Stand des Informationsrechts
1.3 Die Entwicklung der Informationsverarbeitung in Berlin bis heute

2. Schwerpunkte 1990

2.1 Das Erbe der DDR
2.2 Kein Datenschutz 2. Klasse für Ausländer
2.3 Datengigantomanie bei Telekommunikation und Medien
2.4 Computer als Schoßhündchen - Risiken und datenschutzrechtliche Anforderungen beim Einsatz von Laptops

3. Berichte aus den Geschäftsbereichen

3.1 Bau- und Wohnungswesen
3.2 Finanzen
3.3 Frauen, Familie und Jugend
3.4 Gesundheit und Soziales
3.5 Inneres
3.6 Justiz
3.7 Schule, Berufsbildung und Sport
3.8 Stadtentwicklung und Umweltschutz
3.9 Wirtschaft und Verkehr
3.10 Wissenschaft und Forschung
3.11 Technik, Organisation und Geschäftsordnung

4. Aus der Arbeit der Dienststelle

Anlagen

1. Entschließungen der Konferenz der Datenschutzbeauftragten des Bundes und der Länder sowie der Datenschutzkommission Rheinland-Pfalz
1.1. Entschließung der 38. Konferenz am 26./27. Oktober 1989 zum Entwurf eines Schengener Zusatzübereinkommens über den schrittweisen Abbau der Grenzkontrollen
1.2 Entschließung der 38. Konferenz am 26./27. Oktober 1989 über den Datenschutz in der Europäischen Gemeinschaft
1.3 Entschließung der 38. Konferenz am 26./27. Oktober 1989 zum Entwurf einer EG-Statistikverordnung
1.4 Entschließung der 38. Konferenz am 26./27. Oktober 1989 über Genomanalyse und informationelle Selbstbestimmung
1.5 Beschluß der 39. Konferenz am 22./23. März 1990 zum Datenschutz im deutsch-deutschen Verhältnis
1.6 Beschluß der 39. Konferenz am 22./23. März 1990 zum Bundesdatenschutzgesetz und zum Bundesverfassungsschutzgesetz
1.7 Beschluß der 39. Konferenz am 22./23. März 1990 zur Einrichtung eines Arbeitskreises Europäische Gemeinschaft
1.8 Entschließung der Sonderkonferenz am 27. Juni 1990 zum Entwurf eines Gesetzes zur Bekämpfung des illegalen Rauschgifthandels und anderer Erscheinungsformen der organisierten Kriminalität
1.9 Beschluß der 40. Konferenz am 4./5. Oktober 1990 zur Stärkung des Schutzes des Brief-, Post- und Fernmeldegeheimnisses sowie des nichtöffentlich gesprochenen Wortes
1.10 Beschluß der 40. Konferenz am 4./5. Oktober 1990 zur Neuregelung des Melderechtsrahmengesetzes
1.11 Beschluß der 40. Konferenz am 4./5. Oktober 1990 zur Erarbeitung von Krebsregistergesetzen in Bund und Ländern
2. Entschließungen der Internationalen Konferenz der Datenschutzbeauftragten
2.1 Entschließung der 12. Internationalen Konferenz am 19. September 1990 über Datenschutz und die Europäische Gemeinschaft
2.2 Beschluß der 12. Internationalen Konferenz am 19. September 1990 zu Problemen öffentlicher Telekommunikationsnetze und des Kabelfernsehens

Einleitung

Der Zeitraum, über den hier zu berichten ist, beginnt am 1. November 1989. Eine gute Woche später begann mit der Öffnung der Berliner Mauer für dieses Land eine neue Epoche. Der Prozeß der Wiedervereinigung, der für Berlin am Ende des Berichtszeitraums mit dem Zusammentritt des neuen Abgeordnetenhauses einen ersten Abschluß gefunden hat, prägte in ganz erheblichem Maße auch die Arbeit unserer Dienststelle.

Beginnend mit noch zögerlichen Kontaktversuchen von Mitarbeitern und Mitarbeiterinnen der verschiedensten Institutionen der DDR, die erste Informationen über den Datenschutz erbaten, wurde zunehmend unsere Beratung in praktischen und theoretischen Fragen gesucht, bis sich schließlich ab 3. Oktober auch die formelle Zuständigkeit des Berliner Datenschutzbeauftragten auf die Ost-Berliner Stellen erstreckte.

Gleichwohl spiegelt dieser Bericht nur einen kleinen Teil der hier geleisteten Arbeit wider. Wir haben uns bemüht, in den einzelnen Teilen Probleme anzusprechen, die sich bei den ersten Kontakten mit den Dienststellen des Ostteils der Stadt ergaben. Das meiste bleibt unerwähnt, weil viele Fragestellungen zwar für diese neu waren, für denjenigen, der seit Jahren die Arbeit des Datenschutzbeauftragten verfolgt, aber nicht mehr berichtenswert sind.

[1] GVBl. 1991, S. 16 ff

Auf der anderen Seite wirft das völlig andere Staatsverständnis der früheren DDR ganz schwerwiegende neue Fragen auf, deren Erörterung auch im Hinblick auf Zwänge, die das Regelungswerk zur deutschen Einigung schuf, sehr schnell aufgenommen werden mußte, deren Beantwortung aber noch lange nicht gelungen ist. Sie können in diesem Bericht erst grob skizziert werden und bleiben sicherlich ein wesentliches Thema für die kommenden Jahre.

Der Bericht konzentriert sich im übrigen auf die Themen, die die Datenschutzdiskussion in Bund und Land beherrscht haben.

Datenschutz ist ein gesellschaftliches Problem, das in einem Spannungsfeld zwischen drei Elementen steht: der einzelnen Person als Trägerin des informationellen Selbstbestimmungsrechts, dem Datenschutzrecht als dem normativen Rahmen für die Gewährleistung dieses Rechts sowie der Datenverarbeitung als der Technik, deren Risiken der Datenschutz begegnen soll. So war es konsequent, daß wir die Organisation der Datenschutzkontrolle in Berlin auf diese drei Aspekte hin orientiert haben: Bürger, Recht und Technik sind auch die Themen der drei Grundsatzkapitel dieses Berichts.

Es folgen vier Schwerpunkte der Arbeit im Jahre 1990: die neuen Probleme, vor die uns die Wiedervereinigung der Stadt stellt, die datenschutzrechtlichen Fragestellungen des neuen Ausländergesetzes, der neuen Entwicklungen von Telekommunikation und Medien sowie der tragbaren Computer (Laptops).

Wie in jedem Jahr ist der Hauptteil des Berichts einzelnen Problemen der verschiedenen Geschäftsbereiche des Senats gewidmet. Ihre Behandlung füllt den Alltag des Datenschutzbeauftragten. Entsprechend der Bedeutung, die dem Bürger und seinen Problemen beim Datenschutz zukommt, haben wir dieses Mal versucht, eine Reihe von uns vorgetragenen, aber auch denkbaren Fällen einzuarbeiten und im Text hervorzuheben. Sie sollten die verschiedenen Formen der Betroffenheit verdeutlichen, von denen die Bürgerinnen und Bürger berührt sein können.

Den Texten vorangestellt wird jeweils ein kurzer Überblick über die Datenverarbeitung in den Geschäftsbereichen, der den Leserinnen und Lesern die Bedeutung der Informationstechnik vor Augen führen soll.

Einige Angaben zur praktischen Arbeit in unserer Dienststelle schließen den Bericht ab.

1. Datenschutz in Berlin 1990

1.1 Datenschutz ist Menschenrecht

Die neue *Berliner Verfassung,* die seit Januar 1991 für das ganze Berlin gilt, gewährt jedem einzelnen das Recht, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen. Sie greift damit die Formulierung auf, mit der das Bundesverfassungsgericht den Gehalt des informationellen Selbstbestimmungsrechts umschrieben hat. Datenschutz ist die juristisch-technische Umsetzung dieses Rechtes.

Das informationelle Selbstbestimmungsrecht ist ein Menschenrecht. Es steht jedermann zu. Dies ist konsequent: Das Gericht führt das informationelle Selbstbestimmungsrecht auf die Menschenwürde und das Recht auf freie Entfaltung der Persönlichkeit zurück, Rechte, die das Menschsein ausmachen und damit jedem Menschen zukommen.

Daraus folgt für den Datenschutz zweierlei:

Bei der Beurteilung, ob der Datenschutz gewährleistet ist, darf die Zugehörigkeit zu einer bestimmten Personengruppe keine Rolle spielen. Weder Herkunft noch Stellung oder gar Krankheiten dürfen zum Anlaß einer unsachgerechten Ungleichbehandlung genommen werden. Immer wieder werden Versuche unternommen, gegen diesen elementaren Grundsatz zu verstoßen:

Das neue *Ausländergesetz* kehrt das Prinzip, daß der Staat nur im Einzelfall in das informationelle Selbstbestimmungsrecht eingreifen darf und dies zu rechtfertigen hat, in sein Gegenteil um: Alle öffentlichen Stellen werden verpflichtet, Meldungen über ausländische Mitbürger zu erstatten, wenn staatliche Maßnahmen erforderlich scheinen. Die individuelle Abwägung erscheint unerwünscht.

Die *Presse* nimmt immer wieder das Recht in Anspruch, zumindest über prominente Mitbürger nach Belieben sensible Daten veröffentlichen zu können. Gerade am Ende des vergangenen Jahres hat ja in Berlin die Erkrankung eines bekannten Schauspielers zu entsprechenden Schlagzeilen geführt. Das Informationsinteresse der Öffentlichkeit kann nur insoweit Vorrang vor der Privatsphäre der „Personen der Zeitgeschichte" haben, als diese in einem Zusammenhang mit deren öffentlicher Tätigkeit steht.

Nicht einmal dem *Querulanten* ist das Recht auf Datenschutz abzusprechen, auch wenn seine ausholenden Ausführungen dem Beamten auf die Nerven gehen: Gerade bei diesem Personenkreis stellt häufig die Mißachtung seiner informationellen Selbstbestimmung das Anfangsunrecht dar, das ihn in sein Verhalten treibt.

Und nicht zuletzt: Manch einer Einstellungsbehörde schien bereits die Tatsache, daß jemand im *Staatsdienst der DDR* stand, Rechtfertigung genug, Daten zu erheben, deren Ermittlung bei uns längst als verfassungswidrig erkannt ist.

Allen diesen Personen kommt das informationelle Selbstbestimmungsrecht in gleichem Maße zu, jede Differenzierung ist im Einzelfall begründungs- und erklärungsbedürftig.

So gesehen erfährt das informationelle Selbstbestimmungsrecht eine weitere Stütze: auch als Recht der Außenstehenden, Gestrauchelten, Mißverstandenen auf informationelle Gleichbehandlung.

Die andere Konsequenz der Menschenrechtsqualität ist die, daß Instanzen, die sich um die Wahrung des Datenschutzes zu bemühen haben – und hier steht der Datenschutzbeauftragte an erster Stelle –, in besonderem Maße den Menschen in den Mittelpunkt ihrer Bemühungen stellen müssen. Dies unterscheidet sie gerade von denjenigen, die um der Funktionsfähigkeit der Verwaltung willen lästige Schutzmaßnahmen gerne als Hemmnisse ihrer angeblich wohltuenden Tätigkeit ansehen.

Dies heißt nicht nur, daß den Beschwerden von Bürgern mit besonderem Eifer nachgegangen werden muß. Dies ist in unserer Dienststelle selbstverständlich von Anfang an geschehen.

Darüber hinaus muß versucht werden, den *Voreingenommenheiten des Bürgers* selbst zu begegnen. Derartige Einstellungen finden sich auch noch zehn Jahre nach Inkrafttreten und Umsetzen der Datenschutzgesetze:

Etwa die pharisäische Haltung, jeder könne alles über einen wissen, man habe nichts zu verbergen – eine Haltung, die sich in der Regel schlagartig ändert, wenn der Sohn wegen eines Ladendiebstahls von der Polizei verhört oder durch die Post ein Bankauszug in Klarsichtfolie zugestellt wird.

Oder – umgekehrt – die Resignation, die der Empörung über einen Datenmißbrauch folgt; auch sie ist verfehlt, denn die Datenschutzgesetze enthalten ein mannigfaltiges Instrumentarium zur Folgenbeseitigung, aber auch zum präventiven Schutz vor Mängeln. Schon gar nicht angezeigt ist Furcht vor negativen Konsequenzen. Selbst ein Auskunftsersuchen beim Verfassungsschutz darf nicht dazu führen, daß dieses zur Ursache einer Erfassung als Verdächtiger wird.

Derartige Einstellungen stellen den Datenschutzbeauftragten vor besondere Aufgaben. Er muß aufklären, motivieren, Furcht abbauen. Wir haben unser Augenmerk im vergangenen Jahr in besonderem Maß auf diese Aufgabe gelenkt, wenn auch wiederum mit den zur Verfügung stehenden personellen und materiellen Mitteln, vor allem aber in der zur Verfügung stehenden Zeit, nur ein Bruchteil des Erforderlichen geleistet werden konnte.

Das *eigene Engagement des Bürgers* ist dabei unerläßlich. Die Datenschutzgesetze geben ihm zumal nach der Verabschiedung der Novellen in Bund und Land wichtige Mittel in die Hand: Die datenverarbeitenden Stellen sind verpflichtet, den Umfang ihrer Datenverarbeitung gegenüber dem Datenschutzbeauftragten transparent zu machen. Die Meldungen können eingesehen werden; Mittel, Auszüge daraus auszudrucken oder zu kopieren, stehen zur Verfügung. Die Stellen müssen den Bürger mehr als zuvor individuell über den Umfang der Datenverarbeitung aufklären, und zwar bereits bei der Datenerhebung – dies kann den Anstoß für eine Nachfrage geben.

Der entscheidende Schritt ist allerdings, daß der Bürger entschlossen ist, sich tatsächlich über die über ihn gespeicherten Daten zu informieren. Jede Stelle, inzwischen auch die Sicherheits- und Finanzbehörden, sind verpflichtet, ihm die gewünschten Auskünfte zu geben. Ausnahmen müssen begründet werden. Der Auskunft folgen effektive Rechte: Ansprüche auf Berichtigung, auf Löschung, auf Unterlassung, im schlimmsten Fall auf Schadensersatz und Schmerzensgeld oder gar die Möglichkeit, einen Strafantrag zu stellen. Niemand sollte Scheu haben, diese Rechte wahrzunehmen.

Der Bürger selbst hat allerdings ebenfalls Pflichten.

Auch hier muß dafür geworben werden, daß jeder sich für das informationelle Selbstbestimmungsrecht des anderen einsetzt. Daß dies noch keine Selbstverständlichkeit ist, zeigt die geringe Beachtung, die manche der Diskretion in Warteschlangen beimessen. Zwar haben viele Einrichtungen, etwa die Berliner Sparkasse, auf Drängen der Datenschutzbeauftragten Hinweise auf die gebotene Vertraulichkeit angebracht. Die Beobachtung zeigt aber, daß sich das Verhalten kaum geändert hat. Anders nur bei Geldautomaten: Motiv sollte hier allerdings ebenfalls der Respekt vor dem anderen sein und nicht die Furcht, daß die eigene Geheimzahl ausgespäht werden könnte.

Noch wichtiger wird die Achtung vor den Rechten anderer dann, wenn private Informationstechnik eingesetzt wird. Auch hier ist noch viel zu tun: Es überrascht uns nicht mehr, wenn wir feststellen, daß derselbe Lehrer, der im Unterricht vehement die Ziele des Datenschutzes vertritt, auf seinem häuslichen PC intensive Auswertungen der Leistungen, aber auch der Fehlleistungen und -zeiten seiner Schüler vornimmt, ohne die vorgeschriebenen Meldungen vorgenommen zu haben. Angesichts eines Standes der Technik, bei dem taschenkalendergroße Computer gestatten, gewaltige Datenmengen zu verarbeiten, treffen die datenschutzrechtlichen Pflichten jedermann.

Daraus folgt, daß die Intensität der Nutzung der Datenverarbeitung auch eine entsprechende Kenntnis der Folgen und Risiken der Datenverarbeitung begleiten muß. Im Berichtsjahr haben wir uns bemüht, in verstärktem Maße aufzuklären und zu beraten.

Daß es dabei häufig zu kontroversen Diskussionen kommt, ist klar: Ist doch die Euphorie verständlich, die die zunehmenden Nutzungsmöglichkeiten der Informationstechnik begleitet. Das Bewußtsein für die Risiken sollte allerdings mit der entstehenden Informationsgesellschaft Schritt halten und nicht erst einsetzen, wenn uns diese unserer Privatsphäre beraubt hat.

1.2 Stand des Informationsrechts

Die rechtliche Verankerung des informationellen Selbstbestimmungsrechts ist von grundlegender Bedeutung für den Stellenwert des Datenschutzes in Staat und Gesellschaft. Gerade hier haben sich im vergangenen Jahr in Bund und Land einschneidende Veränderungen ergeben, die einerseits dem Datenschutz neue Impulse geben, andererseits aber auch rückschrittliche Tendenzen aufweisen.

Berliner Verfassung

Nach der Wende in der ehemaligen DDR entstand auch in Ost-Berlin ein Runder Tisch, der nach intensiven Diskussionen einen Entwurf für eine *Verfassung von Berlin* entwickelte. Aufgrund unserer Empfehlungen fanden auch Artikel zum Datenschutz Eingang in die von der Stadtverordnetenversammlung am 11. Juli 1990 beschlossene Verfassung. Damit erhielt erstmals der Datenschutz in einem Teil Berlins auch formal Verfassungsrang[2]. Diese in ihrer Geltung auf die östlichen Stadtbezirke beschränkte Verfassung gewährleistete in Artikel 8 für jeden Bürger den Anspruch auf Schutz seiner persönlichen Daten, auf Einsicht in Akten und Dateien, soweit sie ihn betreffen und Rechte Dritter nicht berührt werden, und auf Auskunft über zu seiner Person gespeicherte Daten. Darüber hinaus war zum Schutz der Rechte der Berliner und Berlinerinnen und zur Unterstützung der Stadtverordnetenversammlung die Bestellung eines Datenschutzbeauftragten vorgesehen (Artikel 23 Abs. 2), dessen Funktion die Stadtverordnetenversammlung für die Übergangszeit bis zur Vereinigung der Stadt dem Berliner Datenschutzbeauftragten übertragen konnte (Artikel 87 Abs. 1). Eine derartige Übertragung ist zwar vor dem 3. Oktober 1990 nicht mehr erfolgt, durch die Erstreckung des Berliner Datenschutzgesetzes auf die östlichen Bezirke trat diese Wirkung aber von Gesetzes wegen ein.

Das Berliner Abgeordnetenhaus hat mit der Verabschiedung des 22. Gesetzes zur Änderung der Verfassung von Berlin vom 3. September 1990[3] auch in die bisher in den westlichen Bezirken geltende Verfassung eine Garantie des Datenschutzes aufgenommen. Artikel 21 b gewährleistet das Recht des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen. Einschränkungen dieses Rechts bedürfen eines Gesetzes. Sie sind nur im überwiegenden Allgemeininteresse zulässig.

Diese verfassungsrechtliche Gewährleistung ist durch den Beschluß des neugewählten Abgeordnetenhauses vom 11. Januar 1991 auf das gesamte Land Berlin erstreckt worden und an die Stelle der von der Stadtverordnetenversammlung verabschiedeten Verfassung getreten. Damit wurde zumindest in allgemeiner Form ein wesentlicher Grundsatz der Rechtsprechung des Bundesverfassungsgerichts in der Verfassung des Landes Berlin verankert.

Artikel 88 Abs. 2 dieser Verfassung sieht vor, daß sie während der ersten Wahlperiode des Gesamtberliner Abgeordnetenhauses einer Überarbeitung zu unterziehen ist. Grundlage der Überarbeitung sollen die von der Stadtverordnetenversammlung am 22. April 1948 und am 11. Juli 1990 beschlossenen Verfassungen sowie die gegenwärtig geltende Verfassung von Berlin sein. Bei dieser Überarbeitung wird es darauf ankommen, das Grundrecht auf Datenschutz präziser zu formulieren und auszuweiten. Dafür enthält die von der Stadtverordnetenversammlung verabschiedete Verfassung vom 23. Juli 1990 Formulierungen, auf die zurückgegriffen werden sollte.

Berliner Informationsgesetzbuch

Dem von vielen Autoren in der ganzen Welt beschworenen Herannahen der „Informationsgesellschaft", in der die Informationsverarbeitung der wesentliche Faktor des gesellschaftlichen Beziehungsgeflechts ist, muß mit klaren rechtlichen Vorgaben insbesondere für die staatliche Datenverarbeitung begegnet werden. Diese können sich nicht auf die Datenschutzgesetze im engeren Sinne beschränken, sondern müssen die Informationsverarbeitung in allen ihren Phasen abdecken. Wir haben dafür die Formel geprägt, daß - in Anlehnung an andere umfassende Kodifizierungen - ein *Informationsgesetzbuch* entwickelt werden sollte. Die wesentlichen Elemente eines solchen Gesetzeswerkes wären neben einem am Ende zu schaffenden allgemeinen Teil, der die Grundstrukturen eines Informationsrechtes vor die Klammer ziehen müßte, ein den Vorgaben des Bundesverfassungsgerichts entsprechendes Datenschutzgesetz, ein Gesetz, das die verschiedenen allgemeinen Anwendungsformen der Informationstechnik in der Berliner Verwaltung regeln muß (IuK-Gesetz), ein Gesetz, das gegenüber der informationstechnischen Infrastruktur die Transparenz für den Bürger sichern muß (Informationsfreiheitsgesetz) und schließlich Gesetze, die die Sekundärverwertung der erhobenen Daten für allgemeine staatliche oder gesellschaftliche Zwecke regeln (Statistikgesetz, Archivgesetz).

Bis zum Ende der vergangenen Legislaturperiode ist es lediglich gelungen, ein neues *Datenschutzgesetz* zu verabschieden - ein Gesetz allerdings, das trotz einer hohen Komplexität des Regelungsgehaltes die Vorgaben des Bundesverfassungsgerichts in bisher einmaliger Weise umsetzt.

Das Gesetz beruht auf einem Entwurf der Fraktionen der SPD und der AL, der am 6. April 1990 in erster Lesung im Plenum des Abgeordnetenhauses und in der Folgezeit ausführlich im Innenausschuß sowie im Unterausschuß „Datenschutz" des Innenausschusses beraten wurde. Während dieser Beratungen haben wir mehrfach Stellung zum Gesetzentwurf genommen. Bis zu seiner Verabschiedung durch das Plenum des Abgeordnetenhau-

[2] GVAbl. 1990, S. 1 ff

[3] GVBl. 1990, S. 1877

ses am 27. September 1990 wurde der Entwurf stark verändert, wobei allerdings unsere Vorschläge nur zum Teil berücksichtigt wurden.

So verstehen Bürger häufig nicht, aus welchen Gründen die Kontrolle des Datenschutzes bei öffentlichen und privaten Stellen verschiedenen Institutionen übertragen ist. Der ursprüngliche Entwurf der Gesetzesnovelle hatte dementsprechend vorgesehen, daß der Berliner Datenschutzbeauftragte auch die Aufgaben der Aufsichtsbehörde für nichtöffentliche Stellen erhält. Im beschlossenen Gesetz wurde diese Regelung nicht übernommen, es bleibt dabei, daß diese Aufgaben von einem Referat der Innenverwaltung wahrgenommen werden (das gleichzeitig für das Statistische Landesamt, die Berliner Geschäftsordnung, die Herausgabe von Amtsblatt und Lohnsteuerkarten sowie die Entnazifizierung zuständig ist). Nach wie vor wird dem Bürger nur schwer zu vermitteln sein, daß er sich zwar an den Datenschutzbeauftragten wenden kann, wenn er glaubt, seine Daten würden von der AOK oder der Sparkasse rechtswidrig verarbeitet, daß der Datenschutzbeauftragte seinen Beschwerden jedoch nicht nachgehen kann, wenn sie sich gegen eine private Krankenversicherung oder eine Bank richten.

Die materiell-rechtlichen Regelungen des neuen Berliner Datenschutzgesetzes sind jedoch außerordentlich bürgerfreundlich. Hervorzuheben ist, daß jeder Bürger jetzt Anspruch auf gebührenfreie Auskunft über die zu seiner Person gespeicherten Daten hat und daß sich das Datenschutzgesetz jetzt ausdrücklich auch auf Akten bezieht. Personenbezogene Daten sind grundsätzlich beim Betroffenen mit seinem Wissen zu klar definierten Zwecken und nicht hinter seinem Rücken zu erheben. Damit in engem Zusammenhang steht der ebenfalls erstmals gesetzlich verankerte Grundsatz der Zweckbindung, der es den datenverarbeitenden Stellen verbietet, personenbezogene Daten ohne Einwilligung des Betroffenen oder besondere gesetzliche Grundlage zu anderen als den Zwecken zu verwenden, die für die Erhebung maßgeblich waren. Dem Bürger wäre nicht viel damit geholfen, wenn die Verwaltung zwar verpflichtet wäre, personenbezogene Daten stets offen bei ihm für bestimmte Zwecke zu erheben, die ihm auch mitgeteilt werden müssen, die Verwaltung jedoch anschließend vom Bürger unbemerkt die Daten zu allen möglichen anderen Zwecken verwenden dürfte.

Von weitreichender Bedeutung dürfte die Regelung sein, daß eine Verarbeitung personenbezogener Daten nur zulässig ist, wenn eine besondere Rechtsvorschrift außerhalb des Datenschutzgesetzes sie erlaubt oder der Betroffene eingewilligt hat. Auch die besondere, bereichsspezifische Vorschrift rechtfertigt die Datenverarbeitung nur dann, wenn sie einen dem Berliner Datenschutzgesetz vergleichbaren Datenschutz gewährleistet. Damit ist klargestellt, daß das Datenschutzgesetz selbst in aller Regel keine Befugnisse zur Verarbeitung personenbezogener Daten für die öffentlichen Stellen bereithält. Derartige Befugnisse hat der Gesetzgeber außerhalb des Datenschutzgesetzes bereichsspezifisch zu treffen. Damit setzt das Berliner Datenschutzgesetz als erstes den entsprechenden Grundsatz konsequent um, den das Bundesverfassungsgericht im Volkszählungsurteil von 1983 formuliert hat. Zugleich wird deutlich, daß der Landesgesetzgeber sich bei der Verabschiedung des Datenschutzgesetzes bewußt war, daß mit diesem Gesetz nicht etwa alle Regelungen getroffen oder ersetzt werden sollten, die das Bundesverfassungsgericht für die Verarbeitung personenbezogener Daten in der öffentlichen Verwaltung angemahnt hat.

Zwar enthält das neue Datenschutzgesetz Übergangsvorschriften, die die Fortsetzung der Verarbeitung und unter bestimmten Umständen auch die Zweckentfremdung personenbezogener Daten bis zum 31. Dezember 1991 rechtfertigen, wenn dies zur Erfüllung der in der Zuständigkeit der speichernden Stellen liegenden Aufgaben erforderlich ist. Diese Übergangsvorschriften versuchen eine kurzfristige Verlängerung des der Verwaltung vom Bundesverfassungsgericht zugebilligten sogenannten Übergangsbonus, der an sich schon mit dem Ablauf der letzten Legislaturperiode des Deutschen Bundestages verbraucht war. Gerade vor diesem Hintergrund müssen die Übergangsvorschriften des Berliner Datenschutzgesetzes restriktiv ausgelegt werden. Das neue Abgeordnetenhaus ist aufgefordert, so schnell wie möglich über die eigentlichen informationsrechtlichen Regelungen hinaus bereichsspezifische Regelungen zu schaffen, die die bestehenden Defizite beseitigen. Lücken bestehen insbesondere noch im Bereich des Sicherheitsrechts (Allgemeines Sicherheits- und Ordnungsgesetz, Landesverfassungsschutzgesetz) sowie im Bildungsbereich (Hochschulgesetz, Schulgesetz), obwohl gerade hier gewaltige Datensammlungen bestehen.

Parallel zur Beratung des Datenschutzgesetzes wurde bei der Senatsverwaltung für Inneres der Entwurf eines *Gesetzes über den Einsatz der Informations- und Kommunikationstechnik im Land Berlin* (IuK-Gesetz) erarbeitet. Wir haben dieses Vorhaben von Anfang an begrüßt und mit inhaltlichen Empfehlungen unterstützt, weil die Senatsinnenverwaltung damit eine alte Forderung des Berliner Datenschutzbeauftragten aufgegriffen hat[4]. Der uns zuletzt vorgelegte Entwurf enthielt eine ganze Reihe sehr positiver Regelungsansätze. Unter anderem sah er vor, daß die Einführung neuer und die Erweiterung bestehender Verfahren der Informations- und Kommunikationstechnik dann der Zustimmung des Berliner Datenschutzbeauftragten bedarf, wenn dieser im Einzelfall besonders schwerwiegende Gefahren für das informationelle Selbstbestimmungsrecht sieht. Stimmt der Berliner Datenschutzbeauftragte nicht zu, sollte der Senat die beabsichtigte Maßnahme nur mit Zustimmung des Abgeordnetenhauses durchführen dürfen.

Leider erlahmte das Interesse der Innenverwaltung an diesem zentralen Gesetzesvorhaben in der zweiten Hälfte des Berichtszeitraums sichtlich, so daß es nicht mehr zu einem Senatsbeschluß oder gar zu einer Einbringung ins Parlament kam.

Die Verabschiedung eines IuK-Gesetzes durch das neue Parlament ist vor dem Hintergrund des neuen Berliner Datenschutzgesetzes aus zwei Gründen vordringlich:

Zum einen nennt das Datenschutzgesetz bereits eingangs als eine seiner Aufgaben, „die auf dem Grundsatz der Gewaltenteilung beruhende verfassungsmäßige Ordnung vor einer Gefährdung infolge der automatisierten Datenverarbeitung zu bewahren" (§ 1 Abs. 1 Nr. 2 BlnDSG).

Zum anderen zwingt das Datenschutzgesetz den Gesetzgeber aus guten Gründen dazu, alle Formen der Verarbeitung personenbezogener Daten in Akten, Karteien, Listen und automatisierten Dateien, auch soweit sie nur internen Zwecken dienen, gesetzlich zu regeln, wenn sie nicht eingestellt werden sollen. Für eine Reihe von Verarbeitungsformen, wie sie in der öffentlichen Verwaltung typisch und im wesentlichen auch ähnlich sind (z. B. Textverarbeitung und Bürokommunikation), könnten derartige Verarbeitungsbefugnisse in einem IuK-Gesetz enthalten sein.

Gewissermaßen in letzter Minute wurde im vergangenen Jahr die Chance vertan, dem Land Berlin zu den fortschrittlichsten informationsrechtlichen Bestimmungen zu verhelfen, die es gegenwärtig in der Bundesrepublik gibt. Die damaligen Koalitionsfraktionen hatten im Juni gemeinsam den Entwurf eines *Gesetzes zur Förderung der Informationsfreiheit* (Informationsfreiheitsgesetz - IFG –)[5] eingebracht. Dieser Entwurf sollte jedem Berliner und jeder Berlinerin einen grundsätzlichen Anspruch auf Akteneinsicht in der öffentlichen Verwaltung geben.

Die Datenschutzbeauftragten haben stets die Auffassung vertreten, daß informationelle Selbstbestimmung auch den Zugang zu solchen Informationen beinhaltet oder zumindest voraussetzt, die den jeweiligen Bürger nicht im datenschutzrechtlichen Sinne „betreffen". Das Bundesverfassungsgericht hat hervorgehoben, daß nur der informierte Bürger auch politische Entscheidungen insbesondere bei Wahlen treffen kann[6]. Auch die Datenschutzgesetze sehen nicht nur den Schutz personenbezogener Daten vor, sondern sie verpflichten auch zur Sicherung des „Informationsgleichgewichts" und regeln bestimmte Informationsflüsse. In diesem Sinne ergänzen sich Datenschutz und Informationsfreiheit notwendigerweise und schließen sich keineswegs - wie man zunächst annehmen könnte - kategorisch aus. Zwar sind Vorkehrungen zum Schutz personenbezogener Daten auch dann notwendig, wenn ein Bürger Einsicht in eine Akte (z. B. im Zusam-

[4] vgl. JB 1988, S. 14, Ziff. 4.1

[5] Drs. 11/958

[6] BVerfGE 20, 169, 174 - SPIEGEL -

menhang mit einer Straßenplanung oder der Genehmigung eines Industriebetriebes) nehmen will. Dabei hat der Gesetzgeber jedoch abzuwägen zwischen dem Informationsinteresse eines Bürgers, der zwar nicht am Genehmigungsverfahren selbst beteiligt ist, aber dennoch von den Auswirkungen des Vorhabens betroffen sein kann, und dem informationellen Selbstbestimmungsrecht der an dem Verfahren direkt beteiligten Personen. Dem Informationsinteresse der Bürger wird man jedenfalls den Vorrang gegenüber den Interessen der Verwaltungsmitarbeiter daran einräumen müssen, ihre Beteiligung an einem bestimmten Verfahren nicht offenzulegen. Wer in der öffentlichen Verwaltung arbeitet, muß regelmäßig hinnehmen, daß seine Tätigkeit dem Bürger bekannt wird. Transparenz des Verwaltungshandelns läßt sich nicht länger auf die an einem formalen Verwaltungsverfahren beteiligten Bürger beschränken. Andererseits darf ein genereller Anspruch auf Akteneinsicht nicht dazu führen, daß jeder Sozialhilfeempfänger oder Steuerschuldner mit der Offenbarung seiner Daten gegenüber Dritten rechnen muß, die Akteneinsicht in die entsprechenden Akten verlangen. Dem stehen schon die bundesrechtlich geregelten Sozial- und Steuergeheimnisse entgegen.

Der von den Koalitionsfraktionen eingebrachte Entwurf eines Informationsfreiheitsgesetzes enthielt eine praktikable Regelung des beschriebenen Abwägungsproblems zwischen Informationszugang und Datenschutz. Sowohl der Innen- als auch der Rechtsausschuß des Abgeordnetenhauses stimmten ihm im Oktober mehrheitlich zu. Auch in die Stadtverordnetenversammlung wurde der Entwurf noch rechtzeitig eingebracht. Gerade für die Menschen im Ostteil der Stadt hätte ein ausdrückliches Recht auf Zugang zu Informationen angesichts ihrer vierzigjährigen Erfahrung besondere Bedeutung gehabt. Dennoch wurde der Entwurf vom Plenum des Abgeordnetenhauses wider Erwarten und ohne erkennbaren Grund nicht mehr abschließend beraten. Ein sinnvoller Schritt auf dem Weg zu einem Informationsgesetzbuch wurde nicht getan.

Auch dieses gescheiterte Gesetzgebungsvorhaben kann jedoch nicht ohne weiteres zu den Akten gelegt werden. Seit der Ministerrat der Europäischen Gemeinschaft am 7. Juni 1990 eine Richtlinie über den freien Zugang zu Informationen über die Umwelt[7] erlassen hat, sind auch die Bundesrepublik und das Land Berlin verpflichtet, spätestens bis zur Einführung des Europäischen Binnenmarktes Ende 1992 entsprechende Vorschriften zu erlassen. Der Landesgesetzgeber sollte das Vorhaben aus der abgelaufenen Legislaturperiode deshalb bald wiederaufgreifen und sich auch nicht auf Regelungen zum Informationszugang im Umweltbereich beschränken. Informationsfreiheit ist auch in anderen Bereichen staatlichen Handelns eine notwendige Ergänzung der informationellen Selbstbestimmung.

Nicht besser erging es dem eher noch dringlicher erforderlichen Entwurf eines *Landesstatistikgesetzes:* Der Entwurf für dieses von uns bereits seit Jahren angemahnte Gesetz[8] wurde zwar entsprechend unseren Vorschlägen datenschutzrechtlich nochmals verbessert, allerdings erst im Frühjahr 1990 erneut ins Parlament eingebracht. Obwohl genügend Zeit vorhanden gewesen wäre, um diesen in der Sache gut vorbereiteten Gesetzentwurf trotz der besonderen Situation der Vereinigung Berlins noch im Abgeordnetenhaus und in der Stadtverordnetenversammlung zu verabschieden, nachdem alle parlamentarischen Ausschüsse ihm zugestimmt hatten, kam es nicht mehr zu einer Abstimmung im Plenum des Abgeordnetenhauses. Der Gesetzentwurf muß deshalb in der jetzt begonnenen Legislaturperiode so schnell wie möglich erneut eingebracht werden, um endlich eine gesetzliche Grundlage für die amtliche Statistik im Land Berlin zu schaffen.

Noch nicht einmal bis zu einem Senatsentwurf gelangt ist der Entwurf für ein *Landesarchivgesetz,* der schon seit Jahren in den Schubladen der Kulturverwaltung ruht. Dieses Gesetz ist Voraussetzung für einen rechtmäßigen Zugriff von Historikern auf die archivierten Aktenbestände des Landes: Insbesondere der Erforschung der Zeit des Nationalsozialismus sind damit Hemmnisse in den Weg gelegt, die zurecht von den Forschern beklagt werden.

Bundesrecht

Während in Berlin das novellierte Berliner Datenschutzgesetz als einziges Gesetz mit informationsrechtlichem Gehalt verabschiedet wurde, hat der Bundesgesetzgeber im Berichtszeitraum eine ganze Reihe von Gesetzen beschlossen, die das Recht des Bürgers auf informationelle Selbstbestimmung berühren.

An erster Stelle ist hier das neue *Bundesdatenschutzgesetz* zu nennen, das der Bundestag nach mehr als zehnjährigen Bemühungen um eine Novellierung des ersten Bundesdatenschutzgesetzes mit Zustimmung des Bundesrates beschlossen hat (Artikel 1 des Gesetzes zur Fortentwicklung der Datenverarbeitung und des Datenschutzes vom 20. Dezember 1990)[9]. Das neue Gesetz, das für die Datenverarbeitung im Bereich der Personal- und Sozialverwaltung sowie für die öffentlichen Wirtschaftsunternehmen auch für das Land Berlin Bedeutung hat, enthält zwar vereinzelte Verbesserungen gegenüber dem alten Rechtszustand. Insgesamt ist allerdings festzustellen, daß der Bundesgesetzgeber die notwendigen Konsequenzen aus dem Volkszählungsurteil des Bundesverfassungsgerichts bei weitem nicht mit derselben Konsequenz gezogen hat wie der Berliner Gesetzgeber. Immerhin konnte der ursprüngliche Gesetzentwurf im Vermittlungsausschuß noch verbessert werden. Dabei wurden einige Vorschläge der Konferenz der Datenschutzbeauftragten des Bundes und und der Länder[10] aufgegriffen.

Gravierend eingeschränkt wird die verfassungsrechtlich gebotene unabhängige Datenschutzkontrolle im öffentlichen Bereich sowohl im Bund als auch in den Ländern durch die sogenannte Widerspruchsklausel. Auch hier hat der Bundesgesetzgeber gewissermaßen einen Schritt vor und zwei Schritte zurück getan. Zwar stellt das neue Gesetz zunächst klar, daß die Kontrolle der Datenschutzbeauftragten sich auch auf solche personenbezogenen Daten erstreckt, die einem Berufs- oder besonderen Amtsgeheimnis, insbesondere dem Steuergeheimnis, aber auch dem Arztgeheimnis, dem Post- und Fernmeldegeheimnis, dem Personaldatengeheimnis und dem Statistikgeheimnis unterliegen. Insbesondere die Finanzverwaltung hatte in der Vergangenheit den Datenschutzbeauftragten - auch in Berlin - das Steuergeheimnis sogar dann entgegengehalten, wenn der Datenschutzbeauftragte auf die Beschwerde eines Petenten hin dessen Steuerakte einsehen wollte. Hier ist jetzt erfreuliche Klarheit geschaffen.

Die Regelung hat jedoch einen Pferdefuß: Personenbezogene Daten, die dem Post- und Fernmeldegeheimnis oder dem Arztgeheimnis unterliegen oder in Personalakten bzw. in den Akten über die Sicherheitsüberprüfung enthalten sind, dürfen die Datenschutzbeauftragten nicht kontrollieren, wenn der Betroffene der Kontrolle der auf ihn bezogenen Daten im Einzelfall gegenüber dem Datenschutzbeauftragten widerspricht. Man muß sich vergegenwärtigen, was dies in der Praxis bedeuten kann: Will der Datenschutzbeauftragte z. B. die Patientendatenverarbeitung eines Krankenhauses systematisch überprüfen, was in der Vergangenheit ohne weiteres möglich war, so muß er damit rechnen, daß die speichernde Stelle den Beginn der Prüfung zunächst davon abhängig macht, daß sie vorher Gelegenheit erhält, alle gegenwärtigen und früheren Patienten auf ihr Widerspruchsrecht hinzuweisen. Damit wird eine spontane und systematische Überprüfung der Verarbeitung von derart sensiblen Daten praktisch unmöglich gemacht. Die speichernde Stelle erhält genügend Zeit, um etwaige datenschutzrechtliche Mängel selbst auszuräumen, bevor der Datenschutzbeauftragte Gelegenheit zur Überprüfung erhält. Das Bundesdatenschutzgesetz versucht zwar, diese Schwierigkeit mit der Regelung zu mildern, daß die öffentliche Stelle die Betroffenen in allgemeiner Form über das ihnen zustehende Widerspruchsrecht unterrichtet (also z. B. durch eine entsprechende Klausel im „Kleingedruckten" des Krankenhausaufnahmevertrages oder durch einen Aushang). Auch diese Regelung erscheint jedoch wenig praktikabel und ist nicht geeignet, eine effektive Datenschutzkontrolle im öffentlichen Bereich zu ermöglichen.

Diese Widerspruchsklausel des neuen Bundesdatenschutzgesetzes will den betroffenen Bürger glauben machen, die Daten-

[7] 90/313/EWG - ABl. Nr. L 158/56 v. 23. Juni 1990

[8] vgl. zuletzt JB 1989, Ziff. 4.4, S. 28

[9] BGBl. I, S. 2954 ff

[10] vgl. deren Beschluß vom 22./23. März 1990, Anlage 1.6

schutzbeauftragten neigten dazu, Daten von Betroffenen gegen deren erklärten Willen zu überprüfen. Das Gegenteil ist der Fall. Es hat stets zu den wichtigsten Grundsätzen in unserer Arbeit gehört, daß ein Bürger, dem wir die vertrauliche Überprüfung seiner Beschwerde zugesagt haben, sich auf diese Zusage verlassen konnte. Auch hat sich bisher kein Bürger darüber beschwert, daß seine Daten - in seinem Interesse - vom Datenschutzbeauftragten überprüft worden sind.

Die Erstreckung dieser Einschränkung auf die Kontrollkompetenzen der Landesbeauftragten ist zudem verfassungswidrig, denn es steht dem Bundesgesetzgeber nicht zu, die Kontrollkompetenz der Landesbeauftragten für den Datenschutz zu beschneiden. Die Datenschutzkontrolle ist ein gleichberechtigter Teil der internen Kontrolle der Landesverwaltung auf einer Stufe mit dem Rechnungshof. Niemand ist bisher auch auf die Idee gekommen, den Rechnungshöfen die Prüfung von personenbezogenen Unterlagen dann zu untersagen, wenn die Betroffenen dem widersprechen.

Enttäuschend sind auch die Regelungen im neuen Bundesdatenschutzgesetz für den privaten Bereich. So wird der Adressenhandel, der im Zuge der deutschen Vereinigung auch in den fünf neuen Bundesländern sein Unwesen treibt, in unverständlicher Weise bevorzugt. Bürger der ehemaligen DDR, die naturgemäß in diesem Bereich besonders sensibel sind, haben sich uns gegenüber mehrfach fassungslos über die gezielt versandte Flut von Werbematerial geäußert. Insgesamt hat das Bundesdatenschutzgesetz das Gefälle zwischen dem Datenschutzstandard im öffentlichen Bereich und dem im privaten Bereich nicht gemildert, sondern eher noch verschärft.

Das neue Bundesdatenschutzgesetz wird mit einer Ausnahme am 1. Juni 1991 in Kraft treten: Die Verpflichtungen der speichernden Stellen, die ein automatisiertes Abrufverfahren eingerichtet haben, die Überprüfung der Übermittlung personenbezogener Daten zumindest durch geeignete Stichprobenverfahren zu ermöglichen, tritt erst am 1. Januar 1993 in Kraft. Damit wird die erforderliche Datenschutzkontrolle für zwei Jahre suspendiert.

Wohl mit dem Ziel, datenschutzrechtliche Errungenschaften des Bundesdatenschutzgesetzes im Bereich der Nachrichtendienste nicht allzu wirksam werden zu lassen, wurden gleichzeitig mit dem BDSG ein Bundesverfassungsschutzgesetz sowie Gesetze über den Bundesnachrichtendienst und den Militärischen Abschirmdienst erlassen, die im Gegensatz zum BDSG auch sofort in Kraft traten.

Einen erheblichen Fortschritt im Bereich der Sozialverwaltung stellt die Verabschiedung eines Kinder- und Jugendhilfegesetzes als 8. Buch des Sozialgesetzbuches dar, das längst überfällig war.

Über diese Gesetze sowie über die erheblichen legislatorischen Defizite, die noch auf Bundesebene bestehen, wird unter 3. bei den einzelnen Geschäftsbereichen berichtet.

Europäisches Informationsrecht

Das Zusatzabkommen zum Schengener Übereinkommen von 1985[11], das die Einrichtung eines Informationssystems zur grenzüberschreitenden Fahndung („Schengener Informationssystem") vorsieht, ist - nach einer Verzögerung im Zuge der deutschen Vereinigung - in Kraft getreten. Eine Ausdehnung auf andere europäische Staaten (z. B. Italien) steht bevor.

Zu dem Entwurf des Zusatzabkommens haben sich die Datenschutzbeauftragten des Bundes und der Länder noch im Herbst 1989 geäußert[12] und vor allem betont, daß die Polizei in der Bundesrepublik solange keine personenbezogenen Daten in das Schengener Informationssystem eingeben darf, wie es keine entsprechenden Regelungen in den Polizeigesetzen der Länder und in der Strafprozeßordnung gibt. Eine entsprechende Vorschrift ist in das Zusatzabkommen aufgenommen worden. Auch das in Deutschland geltende Trennungsgebot zwischen Polizei und Verfassungsschutz darf bei der Nutzung des Schengener Informationssystems nicht ausgehöhlt werden.

[11] vgl. dazu Jahresbericht 1989, 4.4 S. 25

[12] vgl. Anlage 1.1

Die Diskussionen über dieses erste europäische Informationssystem im Sicherheitsbereich haben gezeigt, wie schwierig es ist, das informationelle Selbstbestimmungsrecht der Bürger auch dann effektiv zu sichern, wenn Daten zwischen Ländern mit unterschiedlich hohem Datenschutzstandard ausgetauscht werden sollen.

Mittlerweile hat auch die Kommission der europäischen Gemeinschaft die Bedeutung des gemeinschaftsweiten Datenschutzes gerade im Hinblick auf den Europäischen Binnenmarkt, der in weniger als zwei Jahren verwirklicht werden soll, erkannt und am 18. Juli 1990 ein Paket von sechs Maßnahmen beschlossen, die zu einer Verankerung des informationellen Selbstbestimmungsrechts auf der Ebene des Gemeinschaftsrechts führen sollen[13]. Es enthält

- den Vorschlag für eine Richtlinie des Rates zum Schutz von Personen bei der Verarbeitung personenbezogener Daten,
- den Entwurf einer Entschließung der im Rat vereinigten Vertreter der Regierungen der Mitgliedsstaaten der Europäischen Gemeinschaften,
- eine Erklärung der Kommission betreffend die Anwendung der Grundsätze der Richtlinie zum Schutz von Personen bei der Verarbeitung personenbezogener Daten auf die Organe und Einrichtungen der Europäischen Gemeinschaften (SYN 287),
- den Vorschlag für eine Ratsrichtlinie zum Schutz personenbezogener Daten und der Privatsphäre in öffentlichen digitalen Telekommunikationsnetzen insbesondere im Diensteintegrierenden digitalen Telekommunikationsnetz (ISDN) und den öffentlichen digitalen Mobilfunknetzen,
- die Empfehlung für einen Ratsbeschluß zur Aufnahme von Verhandlungen über den Beitritt der Europäischen Gemeinschaften zum Übereinkommen des Europarats zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten und
- den Vorschlag für einen Ratsbeschluß auf dem Gebiet der Informationssicherheit (SYN 288).

Dieses Paket von Gesetzgebungsinitiativen und Maßnahmen kann als ein Erfolg der dringenden Appelle angesehen werden, die die 11. Internationale Konferenz der Datenschutzbeauftragten in Berlin an die EG-Kommission gerichtet hatte. Vor allem die beiden Richtlinienentwürfe enthalten auch inhaltlich sehr positive Ansätze, die es im jetzt beginnenden Gesetzgebungsverfahren auf europäischer Ebene auszubauen und gegen widerstreitende nationale und wirtschaftliche Interessen zu verteidigen gilt. Wenn die beiden Richtlinien vom Ministerrat gebilligt werden, so verpflichten Sie die Mitgliedsstaaten, bis spätestens zum 1. Januar 1993 die erforderlichen Rechts- und Verwaltungsvorschriften zu erlassen. Sollte dies jedoch nicht oder nicht im erforderlichen Umfang geschehen, so kann sich nach der Rechtsprechung des Europäischen Gerichtshofes nach diesem Zeitpunkt jeder Gemeinschaftsbürger direkt auf die Vorschriften der Richtlinien berufen, wenn er seine Rechte durchsetzen will. Auch aus diesem Grund kommt der beginnenden europäischen Informationsgesetzgebung große Bedeutung zu.

1.3 Die Entwicklung der Informationsverarbeitung in Berlin bis heute

Kleine Historie der Datenverarbeitung in der Berliner Verwaltung

Als der Datenschutzbeauftragte im Jahre 1979 in Berlin (West) erstmalig sein Amt antrat, wurde selbstverständlich automatisierte Datenverarbeitung seit mehr als zwei Jahrzehnten von öffentlichen Stellen betrieben. Die wesentlichen technologischen Strukturen waren zu diesem Zeitpunkt geprägt durch zentrale große Datenverarbeitungssysteme, die in arbeitsteilig organisierten Rechenzentren - vor allem im *Landesamt für Elektronische Datenverarbeitung (LED)* - betrieben wurden. Programmsysteme wurden in eigener Regie oder im Programmierverbund mit anderen Bundesländern entwickelt. Gegenüber den frühen Jahren der

[13] KOM (90) 314 endg-SYN 287-288

automatisierten Datenverarbeitung hatten sich in den 70er Jahren die Dialogsysteme durchgesetzt, zwar zentral betriebene und programmierte Systeme, jedoch mit dezentralen Zugriffsmöglichkeiten über Datensichtgeräte. Typische Beispiele: das automatisierte Melderegister (ADV-Verfahren Einwohnerwesen - EWW - und das polizeiliche Informationssystem (Informationssystem Verbrechensbekämpfung - ISVB - in Verbindung mit dem bundesweiten Informationssystem der Polizei - INPOL -). Vorherrschend waren jedoch noch Batch-Systeme: Die Daten wurden dezentral mittels Erfassungsbelegen und Datenerfassungssystemen erfaßt, an die zentralen Rechnersysteme weitertransportiert und dort verarbeitet.

Bis heute hat sich in dieser Hinsicht einiges verändert. Weitere Aufgaben der Verwaltung sind mittels Großrechnertechnologie automatisiert worden (z. B. die Unterstützung der Amts- und Staatsanwaltschaften - ASTA - oder der Liegenschaftsverwaltung mit dem Automatisierten Liegenschaftsbuch - ALB -). Bisher nicht automatisierte Verfahren der Verwaltung stehen ebenfalls vor der Automatisierung mit Dialogverfahren, und klassische Batch-Verfahren werden auf Dialogsysteme umgestellt. Insoweit hat sich bruchlos ein Trend fortgesetzt, der bereits vor zwanzig Jahren in Gang gesetzt worden war. Auch ist nach wie vor das LED wichtigster Betreiber von großen EDV-Anlagen für die Verwaltungsverfahren.

Zwar hat es auch schon Ende der 70er Jahre Kleinrechner, die „Mittlere Datentechnik", gegeben. Die ersten *Personalcomputer* waren mit geringer Leistungsfähigkeit auf dem Markt, ohne daß man erkennen konnte, daß mit ihnen der Grundstein für eine EDV-Nebenwelt zur klassischen Datenverarbeitung gelegt wurde. Parallel zum Ausbau der Großdatenverarbeitung mit Dialogsystemen begann dann der Siegeszug der Personalcomputer auch in der Berliner Verwaltung, häufig als „Automation von unten" auf Anregung autodidaktisch geschulter, vom Computer begeisterter Verwaltungsmitarbeiter, die für ihren Arbeitsbereich damit Rationalisierungschancen sahen.[14)]

Zu den isolierten Personalcomputern - besser wäre der Begriff „persönliche Computer" - gesellten sich bald komplexere Systeme für den Einsatz am Arbeitsplatz: PC-Netze und Mehrplatzsysteme mit dem Betriebssystem UNIX und seinen Varianten. Sie haben mit den PCs eine wesentliche Eigenschaft im Gegensatz zu den oben erwähnten Großsystemen gemein: Sie werden in der Anwendungsumgebung betrieben und verwaltet, nicht in professionell geführten arbeitsteiligen Rechenzentren fernab der Anwendersphäre. Ihr Betrieb und ihre Anwendung bedürfen nur vergleichsweise geringerer EDV-Fachkenntnisse, vor allem, weil sie auf standardisierten Betriebssystemen beruhen und daher vom Softwaremarkt mit Programmen „von der Stange" versorgt werden können, die zunehmend in Richtung größerer Anwendungs- und Benutzerfreundlichkeit auch für relative Laien entwickelt werden.

Neben diesen Trends, die durch die *Miniaturisierung* und stetige *Verbesserung des Preis-/Leistungsverhältnisses* die automatisierte Datenverarbeitung für viele Bereiche der Verwaltung erschlossen haben, hat eine weitere Entwicklungslinie der letzten Jahre die Einsatzformen der Informationstechnik wesentlich geprägt. Gemeint ist die *Integration von Telekommunikation und Datenverarbeitung,* schon im verwaltungsinternen Sprachgebrauch repräsentiert durch die Ablösung des Begriffs „Automatisierte Datenverarbeitung" durch den Begriff *„Informations- und Kommunikationstechnik"* (IuK).

Behördeninterne Bürokommunikationssysteme werden überall eingeführt, behördenübergreifende Bürokommunikationssysteme wie z. B. das Senatsinformationssystem sind in konkreter Planung. Hinzu kommt die Ablösung alter analoger Telefonnebenstellenanlagen durch digitale, ISDN-fähige Nebenstellenanlagen für vielfältige Kommunikationsmöglichkeiten.

Der Stand der Informationstechnologien der Berliner Verwaltung heute

Als Ergebnis all dieser Entwicklungen ergibt sich derzeit folgendes Bild der IuK-Technik in der Verwaltung des Berliner Westens:

- Trotz aller gegenläufigen Tendenzen zur Dezentralisierung und Vernetzung hat der Betrieb *zentraler Großdatenverarbeitungssysteme* für die großen Verfahren an Bedeutung nicht verloren. Dabei verdrängen Dialogverfahren zunehmend Batch-Verfahren mit dezentraler Datenerfassung. Bei den Dialogverfahren kommt man zunehmend ab von solchen mit (fast) ausschließlich zentraler Rechnerleistung und kommt zu mehrstufig aufgebauten sternförmigen Netzen, in denen wesentliche Verarbeitungsleistungen mit den dezentralen Workstations oder mit zwischengeschalteten Netzrechnern abgewickelt werden und der zentrale Großrechner nur die zentral vorzuhaltenen Leistungen, z. B. die Datenhaltung, erbringen muß (z. B. Steuerverwaltung und in Zukunft das automatisierte Haushaltswesen).
- *Isolierte Personalcomputer* werden ebenfalls noch in großer Breite eingesetzt. Die Pionieranwendungen einzelner Mitarbeiter werden allerdings zurückgedrängt zugunsten von abgestimmt entwickelten PC-Anwendungen. In der Tendenz geht die Bedeutung isolierter PCs aber zurück.
- Stattdessen kommen *PC-Netze* in Mode. Da mit der dezentralen PC-Technologie ganze Arbeitsgebiete automationsgestützt abgewickelt werden sollen und damit jeder Mitarbeiter gleichermaßen dialoggestützt arbeiten kann, ist der Einsatz von dezentralen Mehrplatzsystemen vonnöten. Bisher haben sich im Bereich der dezentralen Verwaltung vorwiegend PC-Netze im Gegensatz zu UNIX-Systemen durchgesetzt, während letztere offensichtlich für die Realisierung von Bürokommunikationsanwendungen auf dem Vormarsch sind.
- Isolierte PCs, PC-Netze und Mehrplatzsysteme mit UNIX werden fast ausschließlich für Anwendungen benutzt, die bisher nicht automatisiert unterstützt wurden: *Bürokommunikation* mit dezentraler Datenhaltung, die früher in Karteien erfolgte, Textverarbeitung (hier werden die Schreibmaschinen zunehmend verdrängt) und sonstige Unterstützung der Bürotätigkeit (Kommunikation, Vorgangsverwaltung, Wiedervorlagen, Terminorganisation usw.). Die Vermutung, solche Systeme würden in die Domäne der Großrechneranwendungen eindringen, hat sich jedoch bisher nicht bewahrheitet.
- Die dezentralen Anlagen ermöglichen auch die *individuelle Datenverarbeitung.* Wer über sie verfügt, kann nach eigenem Ermessen und in eigener Verantwortung und - hoffentlich - abgeschottet von anderen Anwendungen der Dienststelle seine Arbeit mit Computerunterstützung erledigen: Zur Erarbeitung von Texten, für individuelle Karteien (z. B. Adressen, Telefonnummern, Stichwörter), für die eigene Arbeitsorganisation (Wiedervorlagen, Terminkalender, Tischrechner usw.). Ob damit die Effizienz und Zielstrebigkeit der eigenen Arbeit gefördert oder nur Motivationseffekte erreicht werden, läßt sich nur individuell ermitteln.
- Neu ist für die Verwaltung jetzt auch der Einsatz tragbarer Computer, sogenannter *Laptops.* Dabei spielt weniger die individuelle Datenverarbeitung eine Rolle, als vielmehr die Automationsunterstützung von Außendiensttätigkeiten. Zu erwähnen ist hier die abzusehende Ausstattung der Betriebsprüfer der Finanzämter mit solchen Rechnern.
- Die Beschaffung *digitaler, ISDN-fähiger Telefonnebenstellenanlagen* ist bei Neu- oder Ersatzbeschaffungen heute weitgehend obligatorisch. Der Nebenstellenbereich ist somit der Entwicklung des öffentlichen Telefonnetzes vorausgeeilt, in dem die Einführung des ISDN erst begonnen hat (bisher sind erst einige ISDN-Vermittlungsstellen in Betrieb). Bemerkenswert ist, daß mit dieser Entwicklung bisher getrennt betrachtete und getrennt verwaltete Technologien zusammengefaßt werden. Die Neuorganisation der Telekommunikation, die Aufgabenverteilung zwischen Bauverwaltung (Fernsprechen) und Innenverwaltung (Datenverarbeitung) ist nach wie vor nicht konfliktfrei umgesetzt.
- Die *verwaltungsübergreifende Vernetzung* wird seit Jahren als dringend überholungsbedürftig angesehen. Die Neukonzeption des Verwaltungsnetzes ist jedoch daran gescheitert, daß die Herstellerfirma der zugesagten Anforderungen nicht Herr werden konnte. Ein Neuanfang ist geplant.

[14)] Vgl. JB 1985, S. 4 f., JB 1988, S. 3 f., JB 1989, S. 15 ff.

Diese informations- und kommunikationstechnische Infrastruktur stellt den Rahmen für die umfassende automatisierte Verarbeitung von personenbezogenen Daten in der Westberliner Verwaltung dar.

EDV-Politik

Als Werkzeug zur Rationalisierung der Verwaltung hatte die EDV unabhängig von politischen Strömungen und Zielsetzungen zunächst dienende, nicht aber gestaltende Funktion. Das Umdenken erfolgte, als mit der Verbreitung dezentraler Datenverarbeitungskapazitäten der gestaltende Charakter der Informationstechnologie auf Arbeits- und Verwaltungsabläufe und -organisation erkennbar war, als aus „ADV-Technik" „IuK-Technik" geworden war. War von ADV-Politik kaum die Rede, so ist seit etwa 1987 die *IuK-Politik* ein Vorrangiges Thema der Verwaltungsreform.

Geprägt war die neue Politik zunächst durch das Ziel, Leitungsstrukturen der Verwaltung durch den Einsatz von Bürokommunikationssystemen effizienter zu gestalten, durch Vernetzung im Rahmen des Senatsinformationssystems den Informations- und Datenaustausch zu intensivieren und aktueller zu machen. Es sollte darum gehen, den Informationsstand der Leitung zu verbessern und somit bessere Grundlagen zur Entscheidungsfindung zu erhalten.

Bevor dieses umgesetzt werden konnte, wurde die politische Zielsetzung seit 1989 umgepolt. Statt Automation von oben nach unten sollte jetzt die Automation von unten nach oben gerichtet sein. Nicht die Unterstützung von Entscheidungsprozessen der Leitungsstrukturen, sondern die Verbesserung der Bürgerfreundlichkeit dort, wo der Bürger mit der Verwaltung in Kontakt tritt, wurde erstes Ziel. Repräsentativ hierfür sei die Forcierung der Automation in den Wirtschaftsämtern der Bezirke (Gewerbedatei) und der Sozialämter (FÜDA, SODA, PROSOZ) genannt. Das Konzept des Senatsinformationssystems wurde nicht verworfen, aber unter anderen Vorzeichen weiterverfolgt.

Mit der Vereinigung der beiden Stadthälften wurden die Prioritäten der IuK-Politik zunächst auf andere Probleme gelenkt, so daß eine weitere Akzentuierung nicht erfolgen konnte.

Datenschutz und sichere Informationstechnik

Die Tendenz permanenten Fortschritts, der allenthalben die Entwicklung der Informationstechnologie prägt, läßt sich ohne weiteres nicht auf die technischen Aspekte des Datenschutzes übertragen.

Dies hängt mit verschiedenen Tendenzen zusammen:

- Zentrale Datenverarbeitung durch einen für viele Verwaltungen arbeitenden Auftragnehmer wie z. B. das LED ist dadurch geprägt, daß dort, wo gestaltend auf den Einsatz der Informationstechnologie Einfluß genommen werden kann, Wert auf bauliche und personelle Funktionentrennungen, nachvollziehbare Abläufe und Verfahren gelegt wird. Die Organisation eines solchen Dienstleisters ist darauf ausgerichtet, für alle Auftraggeber in gleichmäßiger und sicherer Weise die Dienstleistung Datenverarbeitung zu erbringen. Mit anderen Worten: In solchen DV-Umgebungen wird auf Professionalität der Datenverarbeitung geachtet.

  Bei zentraler Datenverarbeitung ist wegen des Auftretens von Auftraggebern und Auftragnehmern darüber hinaus ein „behördliches Vier-Augen-Prinzip" installiert. Damit entsteht eine Hemmschwelle für den Auftraggeber, unbekümmert rechtliche Schranken der Datenverarbeitung zu ignorieren.

- Bei der dezentralen Datenverarbeitung sind diese für die Sicherheit und Ordnungsmäßigkeit der Datenverarbeitung bedeutsamen Merkmale nicht mehr gegeben. Beim PC ist die Funktionentrennung völlig aufgehoben. Daß zumindest eine Funktionentrennung zwischen Gestaltern und Anwendern technisch erzwungen werden muß, wenn ein Minimum an Integritäts- bzw. Ordnungsmäßigkeitsanforderungen von der Datenverarbeitung erfüllt werden soll, hat sich erst vor kurzem als konsensfähig erwiesen.

- Die Entwicklung der Betriebssysteme, die heute Industriestandard sind und zunehmend auch formal standardisiert werden, hat Sicherheitsgesichtspunkte nicht oder kaum berührt, obwohl die Integration von Sicherheitsfunktionalitäten in den Funktionsrahmen der Betriebssysteme seit längerem als anzustreben angesehen wird.

  Beispiele: Das am weitesten verbreitete PC-Betriebssystem MS-DOS ist für die individuelle Datenverarbeitung konzipiert worden und enthält daher keine Möglichkeiten, Benutzerrechte differenziert zu verwalten. Spezielle Sicherheitssysteme, die dies ermöglichen und auch einen minimalen Mindestrahmen für die ordnungsgemäße, damit professionelle Datenverarbeitung stecken sollen, wurden nachträglich entwickelt und mit großem Variantenreichtum, aber geringer Markttransparenz auf den Markt geworfen.

  UNIX ist zwar ein System für den Mehrbenutzerbetrieb, enthält also Möglichkeiten, Zugriffsrechte differenziert zu vergeben. Da seine Väter aber mehr die Förderung der Kommunikation zwischen den Benutzern als deren Abschottung gegeneinander im Auge hatten, auf jeden Fall keine Sicherheitsbedürfnisse befriedigen wollten, enthält die Rechteverwaltung unter UNIX viele Fallstricke. Im Ergebnis wird UNIX zu Recht nach den amerikanischen Sicherheitskriterien in der geringsten Kategorie (marginaler Schutz) eingestuft. Fairerweise ist hier zu erwähnen, daß große Anstrengungen unternommen werden, um durch Erweiterungen des Betriebssystems, durch Umstrukturierungen oder durch Neugestaltung des Betriebssystemkerns, UNIX-Derivate höherer, ja sogar höchster Sicherheitsklassen zu erreichen. Für die Masse der „normalen" UNIX-Derivate bleiben Zusatzinstrumente, die die Benutzerverwaltung besser organisieren helfen und den Zugriff auf die Betriebssystem-Ebene sinnvoll einschränken, eine Hoffnung für den Einsatz unter normalen Sicherheitsanforderungen[15].

  Bemerkenswert bleibt letztlich, daß das Ziel der *Sicherheit, Integrität* und *Zuverlässigkeit* der Datenverarbeitung mit dem ansonsten schnellen technischen Fortschritt nicht in gleicher Intensität verfolgt wurde wie andere Qualitätskriterien. Begründet wurde es mit dem mangelnden Interesse des Informationstechnik-Marktes, für Sicherheit Mittel aufzuwenden. Nachdem spektakuläre Durchbrechungen unzureichender Sicherheitsschranken die Öffentlichkeit aufgeschreckt hatten, wurde das Manko zunehmend erkannt. Es werden jetzt große Anstrengungen unternommen, Betriebssysteme und Datenbanken sicherer zu gestalten und nicht manipulierbare Sicherheitssysteme zu entwickeln. Unterstützt wird dies durch neue staatliche Einrichtungen, in der Bundesrepublik etwa das Bundesamt für Sicherheit in der Informationstechnik (BSI), die die Erfüllung von Sicherheitsanforderungen bei Betriebssystemen und Sicherheitssystemen auf gesetzlicher Grundlage (BSI-Errichtungsgesetz vom 17. Dezember 1990)[16] amtlich evaluieren und zertifizieren.

Allerdings ist der Einsatz sicherer Systeme nur eine Seite des ordnungsgemäßen und sicheren Verwendens der Datenverarbeitung. Sie müssen auch in sorgfältiger Weise installiert und benutzt werden. Wenn dies nicht mit dem notwendigen Bewußtsein für die ordnungsgemäße Abwicklung computerunterstützten Verwaltungshandelns erfolgt, bleibt das Ergebnis unzureichend. Viele Überprüfungen haben uns in den letzten Jahren gezeigt, daß behördliche und persönliche Leichtfertigkeit bei der Datenverarbeitung noch längst nicht ausgestorben ist.

Datenverarbeitung in den neuen Bezirken

Wie andere Lebensbereiche wies die Datenverarbeitung in der ehemaligen DDR viele Aspekte auf, die einen Vergleich mit der westdeutschen Situation sehr erschweren.

Von grundsätzlicher Bedeutung war hier zunächst der unterschiedliche Staatsaufbau. Den zentralen Staatsorganen waren erheblich mehr Aufgaben zugewiesen als in der Bundesrepublik.

---

15) Siehe unsere Empfehlungen zum datenschutzgerechten Einsatz von UNIX-Systemen, Jahresbericht 1989, S. 48 f. – Anlage 3 –.

16) BGBl. I, S. 2834 ff.

Dies führte dazu, daß auf der Ebene des Ministerrates der DDR gewaltige Datensammlungen entstanden waren, die zum Teil automatisch verarbeitet wurden. So führte die Volkspolizei eine *zentrale Personendatenbank,* die Daten über die DDR-Bürger aus den verschiedensten Lebensbereichen enthielt und einerseits verschiedenen öffentlichen Stellen zur Verfügung stand, andererseits aber vor den Bürgern geheimgehalten wurde.

Nutznießer war vor allem das *Ministerium für Staatssicherheit,* dessen erschreckende Datensammlungen ja Gegenstand intensiver Berichterstattung in den Medien waren. Viele automatisiert geführte Datenbestände wurden nach der Wende vernichtet; ein Umstand, der einerseits beruhigt, andererseits aber heute den Zugang zu den schier unendlichen Datensammlungen zu Rehabilitationszwecken erschwert.

Aber auch andere Ministerien verfügten über große Datensammlungen, etwa zur Durchführung der *„Kaderpolitik"*, zur Zahlbarmachung von Bezügen, zur Verwaltung von Steuern und Zöllen, zur Kontrolle des Hochschul- und Fachschulwesens. Hinzu kamen andere verselbständigte, gleichwohl zentralstaatliche Einrichtungen mit eigenen Daten. Hervorzuheben sind der FDGB, der bedeutende Aufgaben im Rahmen der Sozialverwaltung wahrnahm (z. B. Rentenzahlung), die Staatliche Versicherung (mit einem Monopol für Lebens- und Sachversicherungen) sowie die Akademie der Wissenschaften auf dem Gebiet der Forschung (einschließlich der zwangsweisen Erhebung und Verarbeitung personenbezogener Daten wie etwa beim Krebsregister).

Seit der Vereinigung fallen viele dieser Aufgaben in die Zuständigkeit der Länder, mithin auch des Landes Berlin. Dies bedeutet, daß die Datenbestände, soweit deren Existenz mit der Rechtsordnung noch vereinbar ist, in die Verantwortung von Landesbehörden überführt werden muß - eine Aufgabe, die im vergangenen Jahr allenfalls begonnen wurde.

Hinzu kamen auch auf Bezirks- und Kreisebene (in Berlin: auf Magistratsebene) weitere Datensammlungen, von denen aus oder in die hinein Daten aus den zentralen Sammlungen flossen.

Eine erste, noch wenig strukturierte, aber zwangsläufig auch unvollständige Übersicht über personenbezogene Datensammlungen im Ostteil der Stadt, die von der Magistratsverwaltung für Inneres im Jahre 1990 erstellt worden war, ergab, daß sich die Datensammlungen von Ostberliner Magistrats- und Bezirksverwaltungen auf zwei Bereiche konzentrieren:

Zunächst ist die Verarbeitung von Personal- bzw. Kaderdaten hervorzuheben, die zum Teil nach zentralen Vorgaben zur Personalaktenführung geführt wurden, zum anderen Teil aber völlig nach Belieben der jeweiligen Stelle organisiert waren.

Als zweites fallen die vielen Datensammlungen im Gesundheitsbereich auf. Das frühere DDR-Gesundheitswesen war in eine große Zahl von Einrichtungen untergliedert, die eine eigene Datenhaltung betrieben. In Ost-Berlin hat es fast 1 250 kreis- oder bezirksgeleitete Einrichtungen des Gesundheitswesens gegeben, die ihrerseits nach eigenem Bedarf Personal- und Patientendateien aufgebaut haben. Diese Dateien werden in geringer Zahl in automatisierter Form geführt.

Selbstverständlich gibt es in vergleichsweise geringerer Menge auch personenbezogene Daten aus anderen Bereichen der kommunalen Ost-Berliner Verwaltung, sie stellen aber nur einen Bruchteil dessen dar, was in den beschriebenen beiden Bereichen gemeldet wurde. Dabei bleibt zu bedenken, daß wesentliche staatliche Bereiche früher zentral organisiert waren und deren Dateien somit nicht in der Übersicht enthalten waren, so z. B. die Polizei und das Meldewesen.

Auch die technische Seite der Datenverarbeitung wies grundsätzliche Unterschiede zur Verwaltung im Westen Berlins auf. Bedingt durch den großen technologischen Rückstand bei der Datenverarbeitungstechnik, die mangelnde Verfügbarkeit und die technische Rückständigkeit der Telekommunikationsinfrastruktur ist der Automationsstand wesentlich geringer und eine Vernetzung kaum gegeben. Zwar sind erste Ansätze erkennbar, daß eine Anpassung der Verhältnisse im Technologieeinsatz der öffentlichen Stellen der östlichen Stadthälfte erfolgen wird, dennoch überwiegen nicht automatisierte Verfahren, Verfahren mit einfachsten PCs und Großrechnersystemen, die dem westlichen Standard von vor 15 bis 20 Jahren entsprechen. Derzeit scheint die Tendenz zu überwiegen, die existierenden großen öffentlichen Anwendungen auf vorhandende Westberliner Systeme zu übernehmen oder gar ersatzlos zu streichen, sofern es vergleichbare Datensammlungen im Westteil der Stadt bisher noch nicht gab.

Es wird zu unseren wesentlichen Aufgaben in diesem Jahr gehören, die Zusammenführung der Datensammlungen kritisch zu beobachten und mit dafür Sorge zu tragen, daß die Ordnungsmäßigkeit der Datenverarbeitung Gesamtberlins durch die Vereinigung keine Einbußen erleidet, sondern im Gegenteil auch den Ost-Berliner Bürgern hinreichende Sicherungen ihres informationellen Selbstbestimmungsrechts verschafft werden.

2. Schwerpunkte 1990

2.1 Das Erbe der DDR

Für die Bürger in der DDR war *Datenschutz ein Fremdwort.* Nicht etwa, weil die Diskussion um dieses Menschenrecht von der Staatsführung nicht verfolgt worden wäre. Daß man dies tat, zeigt der Umstand, daß vor einigen Jahren, als Praktiker der Datenverarbeitung, aber auch einige vereinzelte Wissenschaftler auf dieses Thema aufmerksam machten, ein Verbot erging, dieses Wort zu benutzen. Es ist nicht nur eine Ironie des Schicksals, sondern eher eine hoffnungsvoll stimmende Konsequenz, 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.

Ministerium für Staatssicherheit

Zuallererst wird jeder dabei an das unheilvolle Wirken des *Ministeriums für Staatssicherheit* denken. Diese Einrichtung sammelte nicht nur im Laufe ihres Bestehens Akten, die zusammengenommen die Länge von 150 Kilometern deutlich übersteigen. Sie dokumentieren Eingriffe in die Persönlichkeitsrechte, die weder vor dem (auch in der DDR strafbaren) Bruch des Brief- und Telefongeheimnisses noch vor dem Beobachten und Belauschen der Schlafzimmer von „Beobachtungsobjekten" Halt machten. Man verschaffte sich auch (in bürokratisch-detailliert dokumentierten Verfahren) Zugang zu allen wichtig erscheinenden Datensammlungen des Staates in allen Geschäftsbereichen und auf allen Ebenen: Eine der Aufgaben der Historiker, die sich diesem Thema widmen müssen, wird sicherlich der Nachweis sein, zu welchen Folgen die Möglichkeit der Bildung von Persönlichkeitsprofilen führen kann. Er wird bestätigen, daß die Verhinderung derartiger Verfahren eine Hauptaufgabe des Datenschutzes sein muß.

Es wirkt geradezu zynisch, wenn es trotz der brutalen Eingriffe in die informationelle Selbstbestimmung in der DDR seit Anfang 1989 eine „Anordnung zur Gewährleistung der Datensicherheit" gab, auf Grund derer eine ganze Bürokratie von Datensicherheitsbeauftragten geschaffen wurde. Datensicherheit wurde als „Ordnung und Geheimschutz in der sozialistischen Gesellschaft" definiert. Die Regelung stellte auf die technischen Voraussetzungen der Datenverarbeitung bei öffentlichen Stellen und in staatlich gelenkten Betrieben ab, ohne den einzelnen Bürger zu schützen. Konsequenterweise fehlte es an Vorschriften zur Zulässigkeit der Verarbeitung von personenbezogenen Daten und zum Recht auf Auskunft, Sperrung oder Löschung. Ganz im Gegenteil: Diese Regelung diente dazu, selbst die Existenz von Datensammlungen vor dem Bürger geheimzuhalten.

Noch in der Volkskammer der DDR war die Frage ein beherrschendes Thema, auf welche Weise die Datensammlungen des MfS künftig verwaltet werden sollten. Dabei war bereits unklar, welche staatliche Ebene dafür künftig zuständig sein sollte. Da es sich hier materiell gesehen um eine polizeirechtliche Materie handelte, sprach einiges dafür, die Verwaltung in die Hände der Länder zu geben. Das Ziel, eine einheitliche Regelung der Sicherung der und des Zugangs zu den Unterlagen sicherzustellen, war ausschlaggebend dafür, daß schließlich bereits in dem noch von der Volkskammer erlassenen Gesetz einem *Sonderbeauftragten* diese schwere Aufgabe überantwortet wurde. Bei der Diskussion

über die Regelungen und später beim Aufbau der Dienststelle konnten wir - unbeschadet der Zuständigkeit des Bundes für diese Aufgabe - ein wenig Hilfe leisten.

Deutsche Einigung

Von der Senatskanzlei wurden wir bei den äußerst komplizierten und aufwendigen Arbeiten zur Gestaltung der beiden Verträge zur deutschen Einigung beteiligt, dem Vertrag über die Schaffung einer Währungs-, Wirtschafts- und Sozialunion zwischen der Bundesrepublik Deutschland und der Deutschen Demokratischen Republik *(Staatsvertrag)* als auch dem Vertrag zwischen der Bundesrepublik Deutschland und der Deutschen Demokratischen Republik über die Herstellung der Einheit Deutschlands *(Einigungsvertrag)*. Die Grundsätze für die Übermittlung personenbezogener Informationen zur Durchführung des Staatsvertrags (Anlage VII) enthalten zum Teil unsere Empfehlungen. Auch die detaillierten Vorschriften über das Zentrale Einwohnerregister der DDR, die unverzügliche Löschung der Personenkennzahl und die übergangsweise Datenschutzkontrolle in den fünf neuen Bundesländern beruhen teilweise auf unseren Vorschlägen. Daß auch aus datenschutzrechtlicher Sicht die eine oder andere Vorschrift besser von der DDR in die Bundesrepublik übernommen worden wäre, zeigt das Problem des öffentlichen Aufgebots, das mit der Vereinigung in den fünf neuen Bundesländern wieder eingeführt wurde, ohne daß über den Sinn dieses Anachronismus und die damit verbundenen Risiken für das informationelle Selbstbestimmungsrecht ernsthaft nachgedacht worden wäre.

Personenkennzahl

Die *Personenkennzahl* spielt eine bedeutsame Rolle bei der datenschutzgerechten Neugestaltung der Verwaltungen in der ehemaligen DDR. Für jeden Bürger wurde eine Nummer - PKZ - vergeben, unter der er in behördlichen und auch anderen Dateien gespeichert wurde. Diese PKZ begleitete den Bürger in sämtlichen Situationen des Lebens. Auch nach der Vereinigung verlangten Krankenhäuser bei der Aufnahme von Patienten diese Kennzahl, die Wohnungsvermittlungen nahmen Anträge nur bei Nennung des persönlichen Kennzeichens an und im Zulassungsschein wurde die PKZ des Fahrzeughalters eingetragen.

Auch die staatliche Versicherung verwendete die PKZ als Versicherungsnummer, so daß die PKZ mit der Übernahme durch westliche Versicherungen auch in den privatwirtschaftlichen Bereich gelangte.

Dies ist nach unserem Verständnis verfassungswidrig: Am 5. Mai 1976 lehnte der Rechtsausschuß des Deutschen Bundestages die Einführung einer PKZ für die Bundesrepublik aus diesem Grunde ab. Das Bundesverfassungsgericht legte dann am 13. Dezember 1983 in seiner Entscheidung zum Volkszählungsgesetz dar, daß die Einführung einer einheitlichen, für alle Register und Dateien geltenden PKZ ein entscheidender Schritt dazu wäre, den einzelnen Bürger in seiner ganzen Persönlichkeit zu registrieren und zu katalogisieren, und damit gegen das Persönlichkeitsrecht verstoßen würde.

Im Einigungsvertrag ist geregelt, daß sämtliche nach Personenkennzahlen geordnete Dateien unverzüglich zu bereinigen und die Kennzahlen zum frühestmöglichen Zeitpunkt zu löschen sind.

Die Berliner Behörden wurden aufgefordert, die Angabe der PKZ von dem Bürger nicht mehr zu verlangen, die PKZ nicht weiter zu übermitteln und auch bei der Neuausfertigung von Dokumenten nicht mehr zu verwenden. Der Rücklauf von den angeschriebenen Stellen läßt erkennen, daß bei Neuvorgängen auf die Verwendung der PKZ verzichtet wird und im Altbestand für eine zügige Löschung, die bis Mitte 1991 abgeschlossen sein dürfte, gesorgt wird. Auch im Versicherungsbereich erfolgt die Umstellung von der PKZ auf eine normale Versicherungsnummer.

Zentrale Datensammlungen

Die Rolle *Berlins als Hauptstadt der DDR* erweist sich als Problempunkt für den Datenschutz: Aufgrund des zentralistischen Staatsaufbaus gab und gibt es im Ostteil Berlins eine Vielzahl von Behörden, die Aufgaben wahrnehmen, die in der bisherigen Bundesrepublik von den Ländern durchgeführt werden.

Dazu gehört das *Zentrale Einwohnerregister (ZER)*, in dem sämtliche Meldedaten der 16 Mio. DDR-Bürger gespeichert, verarbeitet und übermittelt werden. Grundlage des ZER war ein Ministerratsbeschluß. Gesetzliche Regelungen - wie im Westteil Berlins das Meldegesetz - fehlen jedoch, ebenso (selbstverständlich) datenschutzrechtliche Regelungen. So gab es weder Zulässigkeitsvoraussetzungen noch Vorschriften zur Auskunft, Sperrung, Berichtigung und Löschung.

Allerdings war ein Datensicherungskonzept für das ZER durchaus vorhanden: Es ging um die Sicherung der Daten vor Ausspähung, Verlust und unbefugten Veränderungen. Es kommt hinzu, daß das ZER in die polizeiliche Tätigkeit eingebunden war und insbesondere für diesen Bereich als Informationsbasis diente. Auch das ZER wurde anhand des einheitlichen Ordnungsmerkmals PKZ geführt.

Zwar sieht der Einigungsvertrag vor, daß Einrichtungen, die bis zum Wirksamwerden des Beitritts Aufgaben erfüllt haben, die nach der Kompetenzordnung des Grundgesetzes von den Ländern wahrzunehmen sind, bis zu einer endgültigen Regelung als gemeinsame Einrichtungen der Länder weitergeführt werden. Sie unterstehen nach dem Einigungsvertrag den Ministerpräsidenten der neuen Länder, tatsächlich wird eine Dienst- oder Fachaufsicht jedoch nicht ausgeübt. In einer rechtlich ungeklärten Weise sind die jeweiligen Bundesministerien tätig, die vorübergehend auch für die Kosten der Einrichtungen aufkommen.

Dieser Zustand ist deshalb unhaltbar, weil er der Kompetenzzuordnung des Grundgesetzes nicht entspricht und einen rechtsfreien Raum entstehen läßt. Auch die datenschutzrechtliche Verantwortung für derartige Einrichtungen ist somit nicht klar geregelt. Aus allgemeinen Überlegungen ergibt sich jedoch, daß auch bei einem gemeinsamen Amt der Länder die Aufsicht letztlich einem Rechtsträger zugeordnet sein muß. Mangels ausdrücklicher (verfassungs-)rechtlicher Regelung kann dieser Rechtsträger nur das Land sein, in dem die Einrichtung ihren Sitz hat.

Für den Bereich des ZER lehnt die Senatsverwaltung für Inneres bisher eine Verantwortung des Landes ab mit dem Argument, dies hätte einer positiven Regelung im Einigungsvertrag bedurft.

Das ZER war Bestandteil der umfassenderen *Personendatenbank* (PDB).

Diese diente der zentralen Speicherung von Daten für die Schutz- und Sicherheitsorgane der ehemaligen DDR und war für die Deckung des Informationsbedarfs anderer Staatsorgane, staatlicher Institutionen und gesellschaftliche Einrichtungen gedacht. In der PDB wurde ein Katalog von Daten zentral gespeichert, für die in der Bundesrepublik die jeweiligen Fachbehörden zuständig sind. Dazu gehörten bei der PDB u. a.

- Strafregister der Generalstaatsanwaltschaft (dieses ist bereits jetzt in das Bundeszentralregister übernommen worden)
- Strafvollzugsverwaltung
- Kader- und Personalverwaltung
- Reiseanträge
- Sozialversicherung
- Rentenauszahlung
- Nationale Volksarmee
- Arbeit und Lohn (gesellschaftliches Arbeitsvermögen)
- Wehrüberwachung.

Auch Ausreisesperren, Führerscheinentzüge, die Zugehörigkeit zu bewaffneten Organen, Sommerwohnungen, Waffenscheine usw. wurden in der PDB festgehalten.

Mit der PDB war der umfassende Zugriff des Staates - durch die Polizei - auf den Bürger, der in allen Lebenslagen registriert wurde, gesichert. Neben den Aspekten der Fürsorge (Rente, Sozialversicherung) tritt deutlich die Überwachung in den Vordergrund.

Es ist selbstverständlich, daß diese Daten entweder gelöscht oder soweit ihre Fortführung nach der neuen gesetzlichen Situation erforderlich ist - an die jeweiligen Fachbereichsverwaltungen übermittelt werden. Dementsprechend ist im Einigungsvertrag geregelt, daß diese Daten von den Meldedaten getrennt zu speichern und zum frühestmöglichen Zeitpunkt, spätestens bis zum 31. Dezember 1992, zu löschen oder an die zuständigen Behörden zu übermitteln sind.

Anläßlich unserer Überprüfung konnten wir feststellen, daß die entsprechenden Daten bereits vom Gesamtbestand separiert worden sind und getrennt aufbewahrt werden, so daß einer ordnungsgemäßen Übergabe nichts entgegensteht.

Privatisierung

Eine besondere Herausforderung für den Datenschutz ist mit der noch keineswegs abgeschlossenen *Privatisierung* staatlicher Einrichtungen der ehemaligen DDR verbunden. Noch vor der Vereinigung der beiden Stadthälften gab es starke Bestrebungen, z. B. das Rechenzentrum des Magistrats von Berlin, in dem die Meldedaten aller Einwohner Ostberlins verarbeitet wurden, oder das mit der Verarbeitung von Steuerdaten beauftragte staatliche Rechenzentrum zu privatisieren. Damit wären sensible personenbezogene Informationen (im Fall des Magistratsrechenzentrums z. B. sogar Daten aus der ehem. DDR über Gewerkschaftszugehörigkeit oder Ausreiseanträge) dem öffentlichen Bereich entzogen worden und im privaten Bereich „versickert".

Die Treuhandanstalt hat dieser Problematik bei ihren Entscheidungen offenbar wenig Bedeutung beigemessen. Sie scheint sich auf den Standpunkt gestellt zu haben, mit den bisher öffentlichen Rechenzentren könnten auch die dort für öffentliche Zwecke verarbeiteten personenbezogenen Daten an private Interessenten verkauft werden; es sei dann deren Angelegenheit, die erforderlichen Datensicherungsmaßnahmen zu treffen.

Diese Haltung wäre nicht angemessen. Es kann nicht angehen, daß Daten, die im Rahmen der öffentlichen Verwaltung erhoben und verarbeitet worden sind, auf dem Wege der Privatisierung an nichtöffentliche Stellen übermittelt und den neuen Eigentümern zur Verwertung zur Verfügung gestellt werden.

Datenaustausch Ost/West

Ein zwar erledigtes, aber für die allgemeine Situation in der Übergangszeit charakteristisches Problem war die Frage, in welchem Umfang nach der Öffnung der Mauer personenbezogene Daten zwischen dem Ost- und dem Westteil Berlins ausgetauscht werden dürfen.

Anlaß für Prüfungen war der *Austausch personenbezogener Daten* zwischen Polizisten aus Berlin (West) und den Grenzorganen der DDR: Eine vergewaltigte Frau aus Ost-Berlin konnte einige Angaben über den Straftäter machen; diese Daten wurden an die DDR-Mitarbeiter an der betroffenen Grenzübergangsstelle mit der Bitte übermittelt, aufgrund der damals noch geführten Zählkarten die Person zu ermitteln; dies gelang.

Das dahinter stehende Problem war die fehlende Rechtsgrundlage für derartige Datenübermittlungen. Zu diesem Zeitpunkt war die DDR noch als Ausland zu betrachten und damit nach den Berliner Bestimmungen ein Gesetz, zumindest aber eine völkerrechtlich bindende Vereinbarung eine Voraussetzung für den rechtmäßigen Datenaustausch. Hinzu kam eben der Umstand, daß die DDR über keine angemessenen Datenschutzregelungen verfügte und damit die übermittelten Daten nicht mehr in der gleichen Weise geschützt waren wie im Bundesgebiet.

Nur für eingehende Rechts- und Amtshilfeersuchen enthielt das Gesetz über die innerdeutsche Rechts- und Amtshilfe in Strafsachen entsprechende Regelungen. Wir haben sehr früh auf die damit verbundenen Probleme der zunehmenden Übermittlung personenbezogener Informationen in die DDR hingewiesen und schon vor dem Abschluß des Staatsvertrages gefordert, daß das in der Bundesrepublik und in den meisten Staaten des Europarates erreichte Datenschutzniveau nicht unterlaufen werden dürfe.

Zu diesem Zweck haben wir die öffentlichen Stellen in Berlin (West) aufgefordert, vor einer Übermittlung personenbezogener Daten in die DDR die Verhältnismäßigkeit einer solchen Maßnahme von einer zentralen Stelle prüfen zu lassen und die Zweckbindung der übermittelten Daten sowie die Transparenz der Datenverarbeitung beim Empfänger in der DDR durch Zusicherung von Auskunftsrechten in einer entsprechenden Vereinbarung mit dem Datenempfänger sicherzustellen. Das Abgeordnetenhaus von Berlin hat[17] entsprechende Grundsätze beschlossen und den Senat aufgefordert, diese beim Austausch personenbezogener Daten zu beachten. Zugleich wurde der Berliner Datenschutzbeauftragte aufgefordert, den personenbezogenen Datenaustausch zu kontrollieren.

Wir haben stichprobenhaft die Praxis der datenverarbeitenden Stellen im Land Berlin überprüft. Beanstandungen mußten nicht ausgesprochen werden.

Am stärksten betroffen war die Jugendverwaltung. Im Bereich der Familienfürsorge gab es schon vor dem 9. November 1989 Kontakte zu Ostbehörden bei der Rückführung und der Zusammenführung.

Bei der Rückführung fand kein Datenaustausch mit den Ostbehörden statt, da den West-Berliner Behörden von den Ostbehörden mitgeteilt wurde, daß ein Kind aus West-Berlin in der ehemaligen DDR aufgegriffen wurde. Dann ist nur die Übergabe vereinbart worden.

Bei der Zusammenführung von Familien wurde wie folgt verfahren:

Den Ostbehörden wurde die Zuständigkeit des Bezirksamtes mitgeteilt. Dann wurde bei dem betreffenden Elternteil in Berlin-West eine Einwilligung eingeholt, daß dessen Daten zur Zusammenführung der Familie an die Ostbehörden im erforderlichen Umfang übermittelt werden dürfen. In diesen Fällen ging die Stellungnahme des Bezirksamtes an die Ostbehörde, wobei nur Informationen verwendet wurden, die für die Abwicklung der Zusammenführung unbedingt notwendig waren. Diese Verfahrensweise war nicht zu beanstanden.

Schwieriger war die Situation bei Amtsvormundschaft und Standesamt. Hier konnte nicht in allen Fällen die Einwilligung eingeholt werden; gleichwohl waren Datenübermittlungen erforderlich - etwa zur Klärung von Unterhaltsverpflichtungen oder Testamentsangelegenheiten. Seit Jahren vorbereitete Abkommen zwischen den beiden deutschen Staaten waren nicht abgeschlossen worden.

Im Einzelfall mußte ebenfalls keine Beanstandung ausgesprochen werden.

2.2 Kein Datenschutz 2. Klasse für Ausländer

Am 1. Januar 1991 ist das neue *Ausländergesetz* in Kraft getreten. Es setzt ausländerpolitische Zielsetzungen um, die bisher nur in einem undurchsichtigen Geflecht von untergesetzlichen Vorschriften und Rechtsprechung niedergelegt waren. Die Frage, unter welchen Voraussetzungen Aufenthaltsgenehmigungen in ihren verschiedenen Ausprägungen zu erteilen, zu verlängern oder zu entziehen sind, sowie wann Ausländerinnen und Ausländer auszuweisen und abzuschieben sind, wird normenklarer als zuvor geregelt. Kritik hieran mag geübt werden können, ist aber nicht Sache des Datenschutzes.

Schon bisher waren Ausländerinnen und Ausländer in einem erheblichen Maße Gegenstand der Verarbeitung personenbezogener Daten durch die Ausländerbehörde einerseits, durch Behörden, die Daten an die Ausländerbehörde übermitteln, andererseits. Die Verpflichtung hierzu ergab sich ebenfalls mehr aus der Verwaltungspraxis als aus klaren Regelungen. Dies wird nunmehr durch gesetzliche Regelungen ersetzt.

Generalklauselartig werden die Ausländerbehörden ermächtigt, die für ihre Aufgabenstellung erforderlichen Daten bei öffentlichen und nichtöffentlichen Stellen zu erheben (§ 75), eine klare Eingrenzung dieser Daten oder zumindest eine Verord-

[17] Drucksache 11/743

nungsermächtigung hierfür fehlt. Es bleibt also im Dunkeln, welche Daten tatsächlich für die Entscheidungen der Behörde benötigt werden.

Diese Unklarheit erhält ihre Brisanz durch die folgende Vorschrift, die alle öffentlichen Stellen verpflichtet, auf Ersuchen der Ausländerbehörde alle ihr bekannten Daten (also die ganzen Akten?) dieser mitzuteilen (§ 76 Abs. 1); ja mehr noch: Auch ohne Ersuchen sollen alle öffentlichen Stellen Daten mitteilen, wenn Sie für bestimmte Entscheidungen der Ausländerbehörden von Belang sind (§ 76 Abs. 2).

Dies bedeutet in der Konsequenz, daß die Behörden künftig, wenn Sie mit einem Ausländer in Kontakt kommen, stets die Belange der Ausländerbehörde mit zu berücksichtigen haben. Aus dem Ausnahmefall, nämlich daß Daten nur im nachgewiesen erforderlichen Fall weitergegeben werden dürfen, wird eine Verdachtsregel: Weitergegeben werden darf, was von Belang sein könnte.

Für den gerade bei Ausländern wichtigen Bereich der Sozialbehörden werden die Offenbarungsbefugnisse des *Sozialgesetzbuches* erheblich erweitert, wobei unklar bleibt, in welchem Verhältnis diese zu den recht engen Befugnissen des Kinder- und Jugendhilfegesetzes stehen, das gleichzeitig mit dem Ausländergesetz in Kraft getreten ist. Jedenfalls sieht das Ausländergesetz gerade bei Kindern und Jugendlichen weitgehende Offenbarungen vor: Es geht so weit, Prognosen über das künftige soziale Verhalten ausländischer Jugendlicher zu verlangen.

Diese Bestimmungen liegen an der Grenze zur Verfassungswidrigkeit. Nur wenn der Gesetzeswortlaut durch Rechtsverordnungen hinreichend konkretisiert wird und den Datenfluß auf das Unerläßliche beschränkt, ist eine verfassungskonforme verwaltungspraxis möglich.

Die angekündigten *bundeseinheitlichen Ausführungsvorschriften* fehlen noch immer. Um eine einheitliche Anwendung sicherzustellen, folgt Berlin dem Hamburger Beispiel und plant – jedenfalls für die Übergangszeit – landeseigene Anwendungshinweise. Die bis Ende des Jahres bekanntgewordenen Texte lassen hoffen, daß jedenfalls in Berlin eine akzeptable Praxis erreicht werden kann. In Zusammenarbeit mit der Ausländerbeauftragten werden wir energisch hierauf hinwirken.

Um einen datenschutzrechtlichen Umgang mit dem neuen Ausländergesetz sicherzustellen, sind insbesondere folgende Regelungslücken zu schließen:

Klarzustellen ist, daß nicht-öffentliche Stellen (kirchliche Einrichtungen, freie Wohlfahrtsverbände etc.) nicht zur Übermittlung von Informationen der von ihnen betreuten Ausländer verpflichtet sind – entsprechend den Bestimmungen des Bundesdatenschutzgesetzes müssen sie eine Abwägung des öffentlichen Interesses mit den Belangen der von ihnen betreuten Personen vornehmen.

Für öffentliche und nichtöffentliche Stellen gilt, daß Datenübermittlungen nur unter strikter Beachtung des Verhältnismäßigkeitsgrundsatzes erfolgen dürfen. Vor jeder Übermittlung ist zu prüfen, ob die damit verbundenen Nachteile für den Betroffenen so schwerwiegend sind, daß sie die öffentlichen Interessen an der Datenübermittlung überwiegen. Ist dies der Fall, hat die Weitergabe der Informationen an die Ausländerbehörde zu unterbleiben.

Damit die zur Übermittlung verpflichteten Stellen die datenschutzrechtliche Zulässigkeit der Informationsweitergabe überprüfen können, hat die Ausländerbehörde bei Anfragen darzulegen, zu welchem konkreten Zweck sie die Daten braucht und warum sie für ihre Aufgabenerfüllung erforderlich sind.

Da Datenübermittlungen nur zulässig sind, soweit sie erforderlich sind, kann eine Offenbarung personenbezogener Informationen – ob mit oder ohne Anfrage der Ausländerbehörde – nur dann erfolgen, wenn den zur Übermittlung verpflichteten Stellen eindeutig definierbare Fallgruppen vorgegeben worden sind. Ohne derartige Vorgaben ist es den für Ausländerfragen nicht zuständigen Stellen, wie z. B. den sozialen Einrichtungen, nicht möglich, die Frage der Erforderlichkeit zu beantworten.

Es ist klarzustellen, daß eine Übermittlungspflicht nur für Informationen besteht, die rechtmäßig im Rahmen der Aufgabenerfüllung erlangt wurden. Kenntnisse, die bei Gelegenheit anfallen, sind nicht zu übermitteln, da sonst eine allgemeine Ausforschungspflicht begründet würde.

Personenbezogene Daten, die als Geheimnisse z. B. einem Arzt oder einem Sozialarbeiter anvertraut werden, fallen nicht unter die weitgehende Offenbarungsbefugnis des neuen § 71 Abs. 2 SGB X. Derartige Erkenntnisse dürfen auch dann nicht offenbart werden, wenn sie sich in Dokumentationsunterlagen befinden, deren zuständiger Sachbearbeiter persönlich nicht auf ein besonderes Berufsgeheimnis verpflichtet ist. Zwar sieht das Ausländergesetz hier bereits eine allgemeine Regelung vor (§ 77), sie bleibt jedoch zu allgemein und ist ebenfalls zu konkretisieren.

Wegen des Vorrangs der Datenerhebung beim Betroffenen darf die Ausländerbehörde keine Daten bei anderen Stellen erheben, wenn der Ausländer die erforderlichen Informationen oder Unterlagen (z. B. Negativbescheinigungen des Arbeitsamtes) selbst beibringen kann. Die Ausnahmen im Gesetz sind restriktiv auszulegen.

Das derzeitige Regelungsdefizit hat zur Folge, daß bei den Mitarbeitern der betroffenen Behörden eine erhebliche Verunsicherung herrscht. Sie sind mangels genauerer Bestimmungen in der Regel nicht in der Lage, die Übermittlungsvoraussetzungen festzustellen. Solange es an Konkretisierungen zumindest durch Ausführungsvorschriften fehlt, die das informationelle Selbstbestimmungssrecht hinreichend berücksichtigen, dürfen Datenübermittlungen nach dem neuen Ausländergesetz nur äußerst restriktiv erfolgen. Die Mitarbeiter der Jugendämter, Sozialämter, Schulen und anderer öffentlicher Stellen sind gesetzlich verpflichtet, bei Unklarheiten dem informationellen Selbstbestimmungsrecht Vorrang einzuräumen. Dies ändert natürlich nichts an der Übermittlungspflicht, wenn an dem Vorliegen der Voraussetzungen etwa für eine Ausweisung kein Zweifel bestehen kann.

Trotz dieser Situation sollten Ausländerinnen und Ausländer keine unberechtigte Furcht haben. Wir gehen davon aus, daß die Berliner Verwaltung bis zur Klärung der Probleme Zurückhaltung übt und jedenfalls keine Verschlechterung des status quo eintritt.

Bei Zweifeln sollte der Rat der *Ausländerbeauftragten* gesucht werden: Das Ausländergesetz nimmt die Ausländerbeauftragten von den Übermittlungspflichten aus, wenn dadurch die Erfüllung eigener Aufgaben gefährdet wird – ein Grundsatz, der ohnehin eine grundsätzliche Einschränkung der Amtshilfepflicht darstellt. Die entsprechende Verordnung hat die Landesregierung bereits erlassen.

Daß das informationelle Selbstbestimmungsrecht der ausländischen Mitbürgerinnen und Mitbürger nicht nur von den Ausländerbehörden selbst, sondern auch von der Informationsverarbeitung anderer Stellen berührt ist, zeigt folgendes Beispiel:

Das *Akademische Auslandsamt der Technischen Universität* plant, eine „Schwarze Liste" von ausländischen Studierenden, die bisher manuell geführt wurde, zu automatisieren. Neben Namen, Vornamen, Geburtsdatum sollen die Daten des erstmaligen bzw. des zweitmaligen Nichtbestehens der Feststellungsprüfung gespeichert und an alle übrigen Hochschulen übermittelt werden. Dies soll dazu dienen, daß ausländische Studienbewerber, die die Feststellungsprüfung endgültig nicht bestanden haben und sich bei anderen Hochschulen dennoch um die Ablegung der Prüfung bewerben, dort abgewiesen werden können. Die Senatsverwaltung für Schule, Berufsbildung und Sport verweist hierzu auf Ziffer 18 Abs. 1 der Feststellungsprüfungsordnung, die die Weitergabe der Informationen über das Nichtbestehen der Feststellungsprüfung an die zuständigen Stellen in den anderen Bundesländern regelt.

Wir halten diese Regelung für unverhältnismäßig, weil nicht erforderlich und damit für verfassungswidrig. Sie führt dazu, daß an allen Hochschulen, an die die Meldungen gehen, auf Vorrat eine Datei von Personen entsteht, die die Prüfung nicht bestanden haben – ganz unabhängig davon, ob sich die Betroffenen tatsächlich nochmals bewerben. Demgegenüber haben wir vorgeschlagen, daß die Hochschule, bei der sich ein Ausländer bewirbt, zunächst diesen nach vorangegangenen Versuchen befragt. Sollte

die Frage nicht beantwortet werden oder aufgrund der eingereichten Unterlagen Zweifel an der Richtigkeit der Antwort oder der eingereichten Unterlagen bestehen, könnten in diesem Einzelfall die anderen Hochschulen befragt werden.

2.3 Datengigantomanie bei Telekommunikation und Medien

Seit 1980 führt der Berliner Datenschutzbeauftragte den Vorsitz im *Arbeitskreis Medien der Konferenz der Datenschutzbeauftragten des Bundes und der Länder.* Seit jeher bildete die datenschutzrechtliche Beobachtung der „Neuen Medien" daher einen Schwerpunkt der Arbeit, der national und auch international Anerkennung gefunden hat - unter anderem dadurch, daß die Internationale Konferenz in Berlin 1989 den Berliner Datenschutzbeauftragten ausdrücklich beauftragt hat, die Arbeit ihrer *Arbeitsgruppe Telekommunikation und Medien* zu intensivieren. Dies ist auch geschehen.

Im Mittelpunkt des Interesses stehen die gewaltigen Datensammlungen, die beim Betrieb von Telekommunikationsnetzen entstehen.

Das Grundrecht auf unbeobachtbare Kommunikation

Das in Art. 10 Grundgesetz garantierte Fernmeldegeheimnis steht in einem engen Zusammenhang mit dem Grundrecht auf informationelle Selbstbestimmung. Diese beiden Verfassungsgarantien sind ihrerseits Ausdruck der unantastbaren Menschenwürde, sie sichern jedem einzelnen das Recht, unbeobachtet und unregistriert mit anderen Menschen zu telefonieren oder mit anderen Mitteln der Telekommunikation (z. B. Telefax) in Verbindung zu treten. Das Grundrecht auf unbeobachtete Kommunikation[18] wird von der Deutschen Bundespost TELEKOM bei der Einführung des *digitalen diensteintegrierenden Telekommunikationsnetzes ISDN* nicht hinreichend geachtet.

Dieses Grundrecht kann jedoch - darauf ist in der Wissenschaft zu Recht hingewiesen worden - nur bei einer Technikgestaltung gewahrt werden, die durch eine strikte Begrenzung der Erhebung personenbezogener Daten von vornherein sicherstellt, daß Kommunikation unbeobachtbar bleibt.

Während der Benutzer eines herkömmlichen Telefons mit der gegenwärtig noch vorherrschenden analogen Technik nicht befürchten muß, daß sein Anruf irgendwelche Datenspuren hinterläßt, speichert die TELEKOM bei allen von ISDN-Universalanschlüssen geführten Gesprächen einen Kommunikationsdatensatz, der Datum, genaue Dauer der Verbindung, Diensteart und vor allem die Rufnummer des angerufenen Teilnehmers (Zielnummer) enthält, fast vier Monate lang zentral. Als Begründung führt sie dafür an, diese Daten würden zur Gebührenberechnung benötigt.

Dies ist nach Auffassung aller Datenschutzbeauftragten unzutreffend. Zur Berechnung der Gebühren ist allenfalls die Vorwahlnummer erforderlich. Im übrigen könnte die Gebührenabrechnung datenschutzfreundlich in der Weise organisiert werden, daß entweder die Berechnung während des Gesprächs im Telefon des anrufenden Teilnehmers mit einer dezentralen Zähleinrichtung durchgeführt oder die Post den Einsatz der datenschutzfreundlichen Telefonkarten auf Guthabenbasis auch bei privaten Telefonanschlüssen ermöglichen würde. Beides lehnt der Bundesminister für Post und Telekommunikation bisher ab. Stattdessen schickt sich die TELEKOM an, die *größte Sammlung personenbezogener Datensätze* anzuhäufen, die jemals in der Bundesrepublik existiert hat. Dies läßt sich weder auf die bestehende Telekommunikationsordnung noch auf eine Einwilligung des Telefonteilnehmers stützen, der einen ISDN-Universalanschluß beantragt hat. Denn in naher Zukunft wird es keine Alternative zu diesen Anschlüssen mehr geben, so daß von Wahlfreiheit keine Rede sein kann.

Der Bundesbeauftragte für den Datenschutz hat die Speicherungspraxis der TELEKOM deshalb als rechtswidrig beanstandet. Auch die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat eindringlich auf die Notwendigkeit hingewiesen, das Grundrecht auf unbeobachtete Kommunikation vor Gefährdungen durch die neue Technik zu sichern[19]. Dabei geht es nicht darum, den erhöhten Komfort der Telefonbenutzung, wie er mit der Einführung von ISDN ermöglicht wird, zu bestreiten oder zu verhindern. Es geht vielmehr darum, den einzelnen Bürgern, die in zunehmendem Maße das Telefon benutzen und zum Teil auch auf diese Kommunikationsmöglichkeit angewiesen sind, ein Kommunikationsnetz anzubieten, das auf ihre Persönlichkeitsrechte Rücksicht nimmt. Neben denjenigen Bürgern, die die Telefonseelsorge oder eine AIDS-Beratungsstelle anrufen, haben auch alle anderen Bürger ein grundsätzliches Recht auf Anonymität beim Telefonieren.

Der Bundesminister für Post und Telekommunikation sowie die TELEKOM, die sich bisher uneinsichtig gezeigt haben, müssen deshalb auch von den Ländern, die auf die Entscheidungen der Post über den Infrastrukturrat Einfluß nehmen können, zu einer datenschutzgerechten Technikgestaltung veranlaßt werden. Auch der Senat von Berlin sollte sich hierfür einsetzen.

Anstelle der Vollspeicherung der Verbindungsdatensätze muß folgendes Verarbeitungskonzept stehen:

- Alle - durch die computergesteuerte Vermittlungstechnik zwangsläufig entstehenden - *Verbindungsdaten* sind nach Herstellung der Verbindung sofort zu löschen, soweit sie nicht zur Gebührenermittlung erforderlich sind. Ihre Speicherung ist auf den hierfür verarbeitungstechnisch unerläßlichen Zeitraum begrenzt. Die Zweckbindung der Daten wird rechtlich so verankert, daß die Kontrollmöglichkeiten gegenüber dem gegenwärtigen Rechtszustand nicht erweitert werden.
- Nach Errechnung der Gebühren wird im Regelfall für jede Verbindung nur ein Datensatz gespeichert, in dem bei Ferngesprächen die Nummer des Angerufenen durch *Unterdrükkung der letzten Ziffern* so weit verkürzt ist, daß dieser nicht mehr erkannt werden kann. Zielnummern bei Ortsgesprächen werden überhaupt nicht gespeichert. Diese Datensätze können maximal in dem dafür durch Rechtsvorschrift vorgesehenen Zeitraum zur Aufklärung von Gebührenbeschwerden oder aber - auf Wunsch des Kunden - zur Erstellung von detaillierten Telefonrechnungen (Einzelgebührennachweisen) genutzt werden.
- Auf Wunsch des Kunden unterbleibt die Speicherung auch für den Reklamationszeitraum völlig.
- In besonders begründeten Einzelfällen, z. B. bei telefonischen Belästigungen, können auf Wunsch des Kunden für einen begrenzten Zeitraum die vollständigen Verbindungsdaten gespeichert werden.
- Soweit Rufnummern des Anrufers oder des Angerufenen am Telefon angezeigt werden können, muß dies von allen Betroffenen im Einzelfall unterdrückt werden können. Die gegenwärtig gegebene Möglichkeit des Anrufers, eine generelle *Unterdrückung der Rufnummernanzeige* beim Angerufenen zu beantragen, reicht nicht aus. Er muß die Entscheidungsmöglichkeit im Einzelfall erhalten. Umgekehrt muß der Angerufene die Möglichkeit erhalten, nur solche Anrufe entgegenzunehmen, bei denen sich der Anrufer identifiziert.
- Wenn ein Teilnehmer
  - nicht auf die Speicherung von Abrechnungsdaten für den Reklamationszeitraum verzichtet hat oder gar
  - die vollständige Speicherung bzw. den Einzelgebührennachweis beantragt hat oder
  - die Schaltung einer Anrufumleitung oder -weiterleitung veranlaßt hat oder
  - über einen ISDN-Anschluß verfügt, bei dem die Rufnummer des Anrufers angezeigt wird,

  so ist dies dem Anrufer, auch soweit er von einem analogen Telefon aus anruft, so rechtzeitig (durch Eintrag im Telefonbuch und einen entsprechenden Signalton) zu verdeutlichen, daß dieser gebührenfrei von dem Telefongespräch Abstand nehmen kann. Das gleiche gilt für Mitbenutzer eines ISDN-Anschlusses, die den Umfang der Datenspeicherung bei Gesprächen von diesem Anschluß aus nicht kennen. Umgekehrt sollte die Möglichkeit bestehen, generell gebührenfrei auf die Weiterleitung oder Anzeige der Rufnummer zu verzichten und dies auch im Telefonbuch kenntlich zu machen.

[18] vgl. 12. Tätigkeitsbericht des Bundesbeauftragten für den Datenschutz 1989, S.39
[19] vgl. Anlage 1.9

– Der Einsatz von vorausbezahlten *Telefonkarten auf Guthabenbasis* muß auch beim häuslichen Telefonapparat ermöglicht werden. Auf diese Weise kann nach Beendigung der Verbindung auf jede Speicherung von personenbezogenen Daten verzichtet werden.

Mobilfunk: Mehr Bewegung, weniger Datenschutz

Neue und zusätzliche Gefahren für das Grundrecht auf unbeobachtete Kommunikation ergeben sich in den schnell wachsenden *Mobilfunknetzen.* Schon in den bisher existierenden B- und C-Netzen hat die Post zur Unterbindung und Verfolgung von Mißbrauch von Funktelefonen auf eine Vollspeicherung von Verbindungsdaten bestanden, die beim Funktelefon immer auch die zusätzliche Information über den aktuellen Standort des Gesprächsteilnehmers enthält. Der Benutzer eines Funktelefons (in der Regel des Autotelefons) gibt der nächstgelegenen Vermittlungsstelle durch Einschieben seiner Berechtigungskarte zu erkennen, daß sein Gerät aktiviert und damit empfangsbereit ist. Schon deshalb hinterläßt er stets eine elektronische Spur, die allerdings erlischt, wenn er die jeweilige Zelle der Vermittlungsstelle verläßt und in die nächste Zelle wechselt. Längerfristig gespeichert wird die Position des mobilen Telefonbenutzers jedoch dann, wenn tatsächlich ein Gespräch geführt wird und damit auch Gebühren entstehen. Auch in diesem Fall ist die Vollspeicherung - ebensowenig wie im digitalen Telefonnetz - nicht zu rechtfertigen.

Das Funktelefon hat gerade in Berlin im Zuge der Vereinigung wegen des völlig überlasteten stationären Telefonnetzes besondere Bedeutung erlangt. Es wird auch nach einer Erhöhung der Zahl der Anschlüsse im Ostteil der Stadt weiter schnell wachsen. Als nächster Schritt soll bereits 1991 das europaweite digitale Funktelefonnetz in der Bundesrepublik unter dem Namen D-Netz eingeführt werden. Hier treten erstmals die Deutsche Bundespost TELEKOM und ein privates Firmenkonsortium unter Führung der Mannesmann Mobilfunk GmbH zueinander in Konkurrenz als Netzbetreiber. Wir haben frühzeitig versucht, auch das private Firmenkonsortium auf die Bedeutung einer datenschutzgerechten Konzipierung dieses neuen Funktelefonnetzes hinzuweisen. Diese datenschutzgerechte Ausgestaltung könnte durchaus den Wettbewerb positiv beeinflussen, wenn einer der beiden Netzbetreiber die datenschutzfreundlichere Technologie anbieten könnte und der Kunde nicht von einem Monopolisten gezwungen wäre, eine unverhältnismäßige Speicherung seiner Kommunikationsdaten in Kauf zu nehmen.

Seit Juni 1990 bietet die TELEKOM in Berlin das erste *Bündelfunknetz* CHEKKER an, mit dem Betriebe Kontakt zu ihren Außendienstmitarbeitern halten können. Wenngleich diese leistungsfähigere Form des bisherigen Betriebsfunks nicht alle Merkmale eines ISDN-Anschlusses aufweist, kann man durchaus von einer „beweglichen Nebenstellenanlage" sprechen, mit allen Problemen der Arbeitnehmerüberwachung, die sich daraus ergeben.

Parallel zum Funktelefon werden in zunehmendem Maße billigere und leichtere Funkempfänger auf den Markt gebracht, die eine beschränktere Übermittlung von Zeichen oder Signalen erlauben (z. B. City-Ruf)[20]. Dieses City-Ruf-System ermöglicht inzwischen über EUROMESSAGE eine Verbindung zu entsprechenden Funkrufnetzen in England, Frankreich, Italien und demnächst auch in der Schweiz. Dabei kann allerdings stets nur ein Empfänger in derjenigen Rufzone erreicht werden, in der er angemeldet ist. Demgegenüber erlaubt das Funktelefon im D-Netz dem Urlauber in Portugal, seine Freunde in Dänemark anzurufen, ohne daß er ihren Aufenthaltsort von vornherein kennt. Die dadurch ausgelösten Datenflüsse müssen auf das unerläßliche Maß beschränkt werden. Auch müssen speziell beim Funktelefon die Betreiber den Benutzer auf das erhöhte Risiko des Abhörens von Nachrichten hinweisen, wenn er ein Funktelefon anmelden will. Ihm sollte außerdem eine Punkt-zu-Punkt-Verschlüsselung als zusätzliche Dienstleistung angeboten werden. Auch hier gilt, daß der Anbieter von Telekommunikationsdienstleistungen dem Verbraucher keine Dienstleistung aufzwingen darf, die ihn in seiner Selbstbestimmung gravierend einschränkt.

[20] vgl. dazu Jahresbericht 1989, S. 2, S. 18

Nutzungsneutrale Alternativen

Immerhin gibt die Deutsche Bundespost TELEKOM bisher noch im Bereich der Zahlungsmittel in öffentlichen Telefonzellen ein positives Beispiel für echte Wahlfreiheit: Sie bietet sowohl eine *Telefonkarte auf Guthabenbasis* als auch neuerdings die *Telekarte* an, mit der unter Verwendung einer persönlichen Identifikationsnummer aus Telefonzellen telefoniert werden kann, wobei die Gebühren anschließend auf die Fernmelderechnung des Karteninhabers gesetzt werden. Solange diese beiden Karten alternativ angeboten werden, kann der Kunde sich entscheiden, ob er mit oder ohne Datenspur aus einer Telefonzelle telefonieren will. Sollte die Post allerdings die Telefonkarten auf Guthabenbasis in der Zukunft abschaffen - was einige Kritiker bereits befürchten -, so würde sie den Telefonkunden auch hier dazu zwingen, bestimmte Datenspuren zu hinterlassen. Das herkömmliche Münztelefon, bei dem man ebenfalls spurlos telefonieren kann, soll mittelfristig flächendeckend durch Kartentelefone ersetzt werden, weil man davon ausgeht, daß diese mangels Aussicht auf Beute seltener beschädigt werden.

Das weltweite elektronische Telefonbuch

Die Möglichkeit raumübergreifender Vernetzungen war schon immer eine der Risiken, auf die der Datenschutz besonders vehement reagierte: Ein verwaltungsübergreifendes Personenkennzeichen ist verfassungswidrig, ebenso der Aufbau eines gemeinde- oder gar länderübergreifenden Melderegisters durch entsprechende Verknüpfungen. Dem läuft die Entwicklung weltweiter *Teilnehmerverzeichnisse* für die Telekommunikation *(Directories)* in bemerkenswerter Weise zuwider.

Die Internationale Normungsbehörde der Postverwaltungen CCITT mit ihren X.500-Empfehlungen und die Internationale Standardisierungsorganisation ISO mit ihrem Standard ISO-9594 haben Ende 1988 mit identischem Text einen Basisstandard für Teilnehmerverzeichnisse in offenen Telekommunikationsnetzen (Directories) verabschiedet. Dabei handelt es sich um die Normierung eines globalen Directory-Dienstes auf dem in Zukunft wohl einzigen einheitlichen Telekommunikationsnetz, das weltweit verteilte Datenbanken verknüpft. Vorgesehen ist ein einziger Datenbestand, der neben Telekommunikationsanschlußnummern Informationen über Benutzer, Organisationen, Betreiber, verfügbare Dienste usw. bereithalten soll.

Erste Forschungsprojekte befassen sich jetzt mit der Realisierung des Directory-Dienstes innerhalb existierender Telekommunikationsnetze. In Berlin beschäftigt sich eine Forschungsgruppe der Gesellschaft für Mathematik und Datenverarbeitung mit dem Projekt *VERDI* (Verteiltes Directory), einem X.500-Directory im Deutschen Forschungsnetz (DFN). Die Berliner Gruppe hat sich erfreulich intensiv auch den anfallenden Fragen des Datenschutzes gestellt.

Einige davon:

Nicht die Betreiber der verteilten Datenbank bzw. deren lokale Elemente, sondern die Organisationen, die am Directory teilnehmen, sind als datenverarbeitende Stellen anzusehen. Sie bestimmen, welche Daten über ihre Anschlüsse im Directory bereitgehalten werden. Damit kommt auf sie, und nicht auf die Organisatoren des Directory die *Verantwortlichkeit* für die Gewährleistung des Datenschutzes zu. Hierzu gehört vor allem die Installation entsprechender Zugriffssicherungen, die von der X.500-Norm selbst nicht vorgeschrieben sind.

Es besteht Übereinstimmung, daß die Speicherung personenbezogener Daten im Directory nur mit *Einwilligung der Betroffenen* selbst erfolgen kann. Für diese Einwilligung ist es Voraussetzung, daß sie in Kenntnis aller Konsequenzen erfolgt, die mit der Aufnahme in das internationale Directory verbunden sind, so z. B. auch der Abruf der Daten in Staaten, die über keine vergleichbaren Datenschutzvorschriften verfügen.

Die Zulässigkeitsvoraussetzungen für die Erweiterung des Datenangebotes der Teilnehmerverzeichnisse sind differenziert zu betrachten, je nachdem, ob mit den Erweiterungen Zweckänderungen der Verzeichnisse verbunden sind oder nicht. Da das Verzeichnis allein die weltweite Erreichbarkeit der Teilnehmer zum Ziele hat, könnte die Ersteinwilligung auch die Ermächti-

gung zur Erweiterung des jeweils persönlichen Datensatzes im Directory darstellen, wenn die Möglichkeit zur Berichtigung und zum Widerspruch besteht und die Erweiterung allein dem Zweck des Verzeichnisses dient.

Pläne, dem Verzeichnis Angaben aus amtlichen Veröffentlichungen, etwa Veröffentlichungen zu Änderungen im Handelsregister hinzuzufügen, würden eine Zweckerweiterung darstellen, die der Einwilligung in jedem Fall bedürfte. Wir haben größte Zurückhaltung empfohlen, denn es ist rechtlich ein Unterschied darin zu sehen, ob Daten in amtlichen Mitteilungen veröffentlicht werden oder in allgemein zugänglichen Datenbanken zum Abruf bereitgehalten werden.

Es ist sicherlich naheliegend, die nötigen Einwilligungen mittels *elektronischer Post* (E-Mail) über das Telekommunikationsnetz zu übermitteln. Es bedarf jedoch noch der rechtlichen Klärung, ob eine in der Regel schriftlich zu klärende Einwilligung durch E-Mail abgegeben werden kann.

Am Beispiel der X.500-Directory-Empfehlungen der CCITT zeigt sich nicht zum ersten Mal, daß internationale Normungen sehr wohl Konsequenzen für den Datenschutz haben können.

Programmierpanne im Telefonnetz

Durch die Presse wurden der Bundesbeauftragte für den Datenschutz und wir im Mai davon unterrichtet, daß von Telefonapparaten in Nordrhein-Westfalen aus unter bestimmten Voraussetzungen Telefongespräche der Berliner Polizei mitgehört werden konnten. Es stellte sich heraus, daß der Fehler bereits seit einiger Zeit bekannt war, er aber von der TELEKOM und der Polizei weder entdeckt noch die von ihm verursachte Fehlfunktion wiederholt werden konnte. Schließlich stellte sich heraus, daß es nicht ein Problem der polizeilichen Telefonnebenstellenanlage war, sondern daß mehrere Nebenstellenanlagen im Zuständigkeitsbereich einer Teilnehmervermittlungsstelle in Charlottenburg, so auch das Bezirksamt Charlottenburg, davon betroffen waren. Bei dieser Teilnehmervermittlungsstelle handelt es sich um eine der ersten auf digitale Vermittlung umgestellten Vermittlungsstellen in Berlin.

Bei der Analyse des Fehlers durch die TELEKOM stellte sich heraus, daß dann mitgehört werden konnte, wenn eine nicht beschaltete Rufnummer einer Nebenstellenanlage gewählt wurde und die Verbindung über digitale Vermittlungsstellen aufgebaut worden war. In diesen Fällen konnte ein zufällig von einem Apparat dieser Nebenstellenanlage geführtes Gespräch mitverfolgt werden. Ein gezieltes Mithören war jedoch nicht möglich.

Ursache war ein Programmierfehler in einem Vermittlungsrechner der digitalisierten Vermittlungsstelle, der durch eine unvollständig durchgeführte Softwarekorrektur zu Beginn des Jahres 1990 bewirkt wurde.

Ein Fehlverhalten der Polizei konnte nicht festgestellt werden, da sie sofort das Notwendige veranlaßt hatte, um den Fehler zu entdecken. Bis die TELEKOM den Fehler beseitigt hatte, wurde zwischenzeitig bei Anwahl der zum Mithören verwendeten Rufnummer eine Ansage angeschaltet, so daß keine Gespräche mehr mitgehört werden konnten.

Gleichwohl zeigt der Fall, welche Auswirkungen bei der digitalen Vermittlung, die in Zukunft im Rahmen des ISDN die Regel sein wird, durch Programmierfehler bewirkt werden können und wie verletzlich auch die scheinbar so sichere ISDN-Welt ist.

Rahmendienstvereinbarung über den Einsatz digitalter Nebenstellenanlagen

Nicht nur die Datensammelwut beim Betrieb des ISDN muß kritisch hinterfragt werden, sondern auch das Datenaufkommen beim Einsatz *digitaler Nebenstellenanlagen.* Dabei handelt es sich um Daten der Teilnehmer der digitalen Nebenstellenanlage sowie der Angerufenen. Da die Teilnehmer digitaler Nebenstellenanlagen in der Regel Mitarbeiter der Stelle sind, die die Nebenstelle betreibt, handelt es sich bei diesen Daten um Personaldaten, die über das Telekommunikationsverhalten des einzelnen detaillierte Aussagen treffen können, somit auch zur Verhaltenskontrolle geeignet sind. Im Bereich der öffentlichen Verwaltung Berlins ist bisher kein Zweifel darüber aufgekommen, daß der Einsatz digitaler Nebenstellenanlagen mitbestimmungspflichtig ist und des Abschlusses von Dienstvereinbarungen bedarf, die den Umgang mit den personenbezogenen Daten, die beim Einsatz der Nebenstellenanlage abfallen, regeln.

Während hinsichtlich der Daten des angerufenen Teilnehmers meist Übereinkunft darüber erreicht werden kann, daß ihre Speicherung nach Beendigung der Verbindung nur in verkürzter Form erfolgen soll, bietet die Speicherung der Mitarbeiterdaten Grund zu Auseinandersetzungen. Da anders als herkömmliche analoge Systeme die Telekommunikationsvorgänge bei digitalen Systemen Datenspuren hinterlassen, lockt die Möglichkeit, solche Daten zur Abrechnung von privaten Telefongesprächen heranzuziehen. Diesem zweifellos berechtigten Interesse steht aber entgegen, daß solche Daten auch zu darüberhinausgehender Personalkontrolle mißbraucht werden können. Die Tatsache, daß die Organisationen ihren Mitarbeitern die Möglichkeit für Privatgespräche großzügig einräumen, soll dadurch erkauft werden, daß die gerade bei privaten Gesprächen wichtige Unbeobachtetheit der Telekommunikation durchbrochen wird.

In diesem Sinne haben wir uns auf Wunsch der Senatsverwaltung für Inneres und mit Einverständnis des Hauptpersonalrates an der Beratung des Entwurfs einer *Rahmendienstvereinbarung* über den Einsatz von digitalen Nebenstellenanlagen beteiligt. Im Ergebnis bestand Übereinstimmung darin, daß möglichst ein Verzicht auf die über die Verbindungsdauer hinausgehende Speicherung personenbezogener Daten erreicht werden sollte.

Zum Abschluß einer solchen datenschutzkonformen Rahmendienstvereinbarung ist es bisher noch nicht gekommen. Gleichwohl ist zwischen dem Bezirksamt Wilmersdorf und dem Hauptpersonalrat inzwischen eine Dienstvereinbarung für den Einsatz und den Betrieb einer digitalen Telefonnebenstellenanlage abgeschlossen worden, die auf dem datenschutzfreundlichen Entwurf der Rahmendienstvereinbarung beruht. Wir würden es sehr begrüßen, wenn auch die übrige Berliner Verwaltung sich dazu durchringt, den Verlockungen des Datenanfalls bei digitalen Nebenstellenanlagen zu widerstehen.

Bildschirmtext und Kabelpilotprojekt

Der Bildschirmtextdienst wurde im vergangenen Jahr erneut erweitert und durch neue Leistungsmerkmale verbessert.

So wurde Mitte des letzten Jahres eine neue *Mitteilungsseite* angeboten, die ein um vier auf achtzehn Zeilen verlängertes Textfeld für Nachrichten und ein verkürztes Adreßfeld, in dem nur noch der Name des Absenders ausgegeben wird, enthält.

Wir begrüßen diese Neuerung, da damit dem datenschutzbewußten Btx-Teilnehmer neben der bisherigen, erweiterten Mitteilungsseite eine zweite angeboten wird, die nur noch die Angaben aufnimmt, die für den eigentlichen Zweck erforderlich sind.

Im März 1990 eröffnete die TELEKOM den Probebetrieb des *Übergangs von Btx zu Telefax.* Damit können von Btx-Teilnehmern und Mitbenutzern Telefax-Mitteilungen ins In- und Ausland versandt werden, wenn sie berechtigt sind, nutzungsabhängige Btx-Gebühren zu verursachen.

In den vergangenen Monaten wurden wiederum Verstöße von Btx-Anbietern gegen Vorschriften des Btx-Staatsvertrages festgestellt.

Mit Hilfe von Negativlisten können sowohl Teilnehmer als auch Anbieter vom Zugang zu einem Angebot ausgesperrt werden. Ein Petent beschwerte sich über die unbefugte Kenntnisnahme seiner neuen Telefon-Geheimnummer durch zwei Btx-Anbieter. Die betreffenden Anbieter sind auf einem uns nicht bekannten Wege in den Besitz der Telefon-Geheimnummer des Petenten gelangt und verwehrten ihm durch einen Eintrag dieser Nummer in eine automatisierte Referenzliste den Zutritt zu ihrem Angebot.

In einem ähnlich gelagerten Fall kündigte ein Anbieter in seinem Angebot an, daß er sich die Möglichkeit offen hält, bei einer bestimmten Nutzergruppe überraschende und verdeckte Datenabfragen durchzuführen, um ihr den Zutritt zu seinem Angebot zu erschweren bzw. zu verweigern.

Diese Praxis verstößt gegen Art. 9 Abs. 8 Nr. 2 Btx-Staatsvertrag und die entsprechenden Vorschriften des § 24 BDSG, da die

Teilnehmer ihre personenbezogenen Daten nicht mehr eindeutig und bewußt im Rahmen der Zweckbestimmung des Vertragsverhältnisses übermitteln können.

Beim *Kabelpilotprojekt* gab es im Berichtszeitraum keinen Anlaß für eine Mängelfeststellung.

2.4 Computer als Schoßhündchen - Risiken und datenschutzrechtliche Anforderungen beim Einsatz von Laptops

Wir haben in den vergangenen Jahren im Jahresbericht als Schwerpunkt jeweils eine aktuelle informationstechnische Entwicklung aufgegriffen und deren besondere datenschutzrechtliche Risiken behandelt. Themen waren u.a. der PC-Einsatz, ISDN, die Vernetzung und die Bürokommunikation. Diesmal wenden wir uns den tragbaren Personalcomputern zu. Sie werden auch außerhalb des englischen Sprachraums inzwischen *Laptops* genannt - in Anspielung auf das englische Wort für „Schoßhündchen" (lap dog).

Überall dort, wo es die wechselnde Arbeitsplatzsituation verlangt, kommen Laptops dem Wunsch nach Flexibilität und Mobilität entgegen, ohne daß auf die Vorteile einer Automatisierung verzichtet werden muß. Auch in der öffentlichen Verwaltung wird verstärkt auf die Fähigkeiten von tragbaren Computern, die inzwischen zum Teil den Standard von den am Arbeitsplatz eingesetzten Personalcomputern erreichen, zurückgegriffen werden.

Der ortsungebundene Rechner-Einsatz führt jedoch zu einem in dieser Form bisher unbekannten Gefährdungspotential, wenn es um den Schutz personenbezogener Daten und um die Wahrung von Betriebs- und Geschäftsgeheimnissen geht.

Mit der Ausstattung von Sachbearbeitern mit tragbaren Computern behält die datenverarbeitende Stelle die Verantwortung für den datenschutzgerechten Einsatz und kann diese nicht auf diese Mitarbeiter abwälzen. Sie hat wie bei allen anderen automatisierten Verfahren für den bestimmungsgemäßen Einsatz und die datenschutzgerechte Ausstattung und Verwendung der Geräte zu sorgen.

Das Spektrum der tragbaren Computer reicht vom programmierbaren Pocket-Computer bis hin zu Hochleistungs-Laptops, die mit den leistungsfähigsten Betriebssystemen ausgestattet sind. Wir wollen uns hier mit den Laptops befassen, die mit Standard Betriebssystemen (z. B. MS/DOS oder UNIX) arbeiten, da diese es sein werden, die im Rahmen von ADV-Verfahren der Verwaltung, also nicht nur für die individuelle Datenverarbeitung, genutzt werden können.

Risiken beim Einsatz von Laptops

Während in der herkömmlichen Büroumgebung der Zugang zu den Geräten gesichert werden kann (z. B. durch Ausstattung der Türen mit Sicherheitsschlössern, getrennte Schließanlage, Organisation der Schlüsselvergabe und Zutrittsberechtigung), fallen diese Möglichkeiten beim Einsatz von Laptops außerhalb der Behörde weg. Beim mobilen Einsatz der tragbaren Rechner verlassen nicht nur die Daten den Kontrollbereich der Behörde, sondern gleichzeitig auch die Geräte.

Daraus ergibt sich, daß die Hauptgefahr im *Diebstahl* oder dem unbeabsichtigten *Verlust* des Gerätes liegt.

So kann ein Laptop in einem Auto unbeaufsichtigt liegengelassen oder in einem Sitzungssaal vergessen werden, so daß Unbefugte sich nicht nur die gespeicherten Daten aneignen können, sondern darüber hinaus noch die Möglichkeit erhalten, zeitlich unbegrenzt und unabhängig von Kompatibilitätsproblemen die Daten aus dem Gerät auszulesen, auf dem sie verarbeitet wurden. Das Rüstzeug wird ihnen gleichsam „mitgeliefert", installierte Sicherheitsmechanismen können ungestört ausprobiert und so möglicherweise umgangen werden.

Ein wegen der Unachtsamkeit des Benutzers möglicher kurzfristiger Zugriff bietet vielfältige Gelegenheiten zur unbefugten Kenntnisnahme schutzwürdiger Daten.

Für die *Zugriffssicherheit* von Laptops gilt zunächst das Gleiche wie bei anderen Personal Computern: Ohne zusätzliche Schutzmaßnahmen hat jeder, der das Gerät in die Hände bekommt, einen ungehinderten Zugriff auf die zur Verfügung gestellten Ressourcen. Er kann nahezu uneingeschränkt Daten eingeben, verarbeiten und wieder ausgeben, sofern er über entsprechende Kenntnisse verfügt.

Da darüber hinaus Laptops beim mobilen Einsatz fast ausschließlich in einer ungesicherten Umgebung benutzt werden, ist die Zahl derer, die in einem unbeobachteten Augenblick Einsicht auf den Bildschirm nehmen oder sich die gespeicherten Daten auf Diskette kopieren können, nicht eingrenzbar.

Dabei liegt die Gefahr nicht allein im unbefugten Auslesen von Daten, sondern auch in der Möglichkeit zur Manipulation von Hard- und/oder Software durch materielle Zerstörung oder das Einspielen von Viren, trojanischen Pferden o. ä., die später nicht nur den ordnungsgemäßen Programmablauf im Laptop, sondern beim etwaigen Einspielen der Daten in behördeneigene stationäre Systeme auch die dort verwendeten Verfahren nachhaltig stören können.

Da sich der Laptop beim Außeneinsatz außerhalb des kontrollierten Bereiches der datenverarbeitenden Stelle befindet, besteht leicht die Gefahr, daß das Gerät zweckentfremdet wird.

Dazu gehört die Verwendung für private Zwecke oder in privaten Räumen, aber auch das unbefugte Einspielen oder Ändern von Programmen.

Daten können unbefugt auf andere externe (behördenfremde) Rechner unbemerkt kopiert, auf Druckern ausgedruckt oder Programme unlizenziert weitergegeben werden.

In Laptops eingegebene Informationen bleiben meist nicht auf dem Gerät, sondern werden auf stationäre ADV-Systeme übertragen und dort weiterverarbeitet. Dies geschieht entweder unmittelbar am Arbeitsplatz oder von außerhalb über Modem, Akustikkoppler oder über ein Rechnerverbundsystem.

Über die dafür notwendigerweise zur Verfügung stehenden *Kommunikationsschnittstellen* können Daten entweder unbefugt oder falsch eingegeben oder in der entgegengesetzten Richtung Daten unbefugt ausgelesen werden. Wird eine Vielzahl von Laptops eingesetzt, so wird zudem die Zahl der Netzteilnehmer unüberschaubar.

Neben diesen Gefahren für die Integrität der Verfahren und Daten sind bei Laptops besondere Risiken für die Verfügbarkeit der Systeme und der auf ihnen befindlichen Daten zu beachten, die zwar nicht primär aus Datenschutzsicht zu berücksichtigen sind, aber dennoch für die Ordnungsmäßigkeit des Verwaltungshandelns eine Rolle spielen können. Hier seien erwähnt:

- besondere Risiken der Stromversorgung, insbesondere für die Daten im Arbeitsspeicher, bei stromnetzunabhängigem Betrieb;
- Fehlbedienung und -eingaben wegen ungewohnter, reduzierter und eng angeordneter Tastaturen;
- Datenzerstörungen durch Gewalteinwirkungen und Übertragungsfehler durch Verschmutzung von Schnittstellen.

Datenschutzgerechter Einsatz

Sollen mit Hilfe eines Laptops personenbezogene Daten datenschutzgemäß verarbeitet werden, so sind den beschriebenen Risiken entsprechende Maßnahmen entgegenzusetzen. Die folgenden *Anforderungen* beziehen sich auf den Einsatz von Laptops in automatisierten Verwaltungsverfahren, in denen die *Verfügbarkeit* der Systeme, Programme und Daten, die *Integrität* von Programmen und Daten sowie die *Vertraulichkeit* der Daten in angemessener Form sichergestellt werden müssen.

Organisatorische Maßnahmen:

- Wie bei Personal Computern sollte die *Auswahl und Beschaffung* der Laptops und der darauf einzusetzenden Programme zentral oder zumindest abgestimmt durchgeführt werden, damit die Kompatibilität zwischen Hard- und (Sicherheits)-Software gewährleistet ist und ein einheitliches Sicherheitskonzept als Mindeststandard umgesetzt werden kann. Bei der Anschaffung der Geräte sollte von vornherein auf eine gewisse Sicherheitsausstattung Wert gelegt werden. Dazu gehören z. B. das Vorhandensein eines Sicherheitsschlosses,

eines festen Behältnisses mit Zahlenschloßkombination für den Transport, aber auch Schutzvorrichtungen für empfindliche Geräteteile wie etwa die sich auf der Geräterückseite befindlichen Schnittstellen zur Aufrechterhaltung der Funktionssicherheit.

- Die im Einsatz befindlichen Laptops sind in das in § 19 Abs.4 Berliner Datenschutzgesetz geforderte *Geräteverzeichnis* aufzunehmen. Daneben ist bei einem personengebundenen Einsatz der mit dem Laptop ausgestattete Mitarbeiter, bei einem für ein Verfahren gewidmeten Einsatz das Datum und die Uhrzeit der Aushändigung sowie der Rückgabe und der betreffende Mitarbeiter zu registrieren.
- Nach Ende eines Arbeitstages sind die Laptops zur Dienststelle zurückzubringen und dort *verschlossen* aufzubewahren. Für Ausnahmesituationen, wie z. B. den Einsatz bei Dienstreisen, sind Regelungen mit entsprechender Wirksamkeit zu vereinbaren.
- Die Ausgabe und die Kontrolle der Geräte sollten ebenso wie die Einrichtung und Wartung zentral in der Dienststelle erfolgen. Die *Geräteverantwortung* sollte bei einem dafür mit besonderen Rechten ausgestatteten Systemverwalter liegen.
- Die für den mobilen Einsatz vorgesehenen Laptops sollten einem *formalen Freigabeverfahren* unterzogen werden. Es sollten nur für den Außendienst freigegebene Geräte verwendet werden. Mit der Freigabe bestätigt die verantwortliche Stelle, daß das Gerät den dienstlichen Erfordernissen entspricht und legt fest, wie die Laptops in die bereits vorhandene ADV-Konzeption einzubinden sind und für welche Aufgabenbereiche diese eingesetzt werden dürfen.
- Ebenso wie bei Personal-Computern dürfen auch bei Laptops nur Anwendungsprogramme auf Grund eines in der Verantwortung der datenverarbeitenden Stelle liegenden formalen Freigabeverfahrens angewendet werden, wenn das Verfahren in verbindlicher Weise abzuwickeln ist.

  Programme dürfen nur in compilierter oder versiegelter Form gespeichert werden, damit unautorisierte Veränderungen an den Programmen nicht vorgenommen werden können. Ferner ist sicherzustellen, daß nur die für die Aufgabenerledigung mit dem Laptop erforderlichen Programme eingesetzt werden. So sollten z. B. Dienstprogramme für die Systemverwaltung auf einem Laptop für die Arbeit unterwegs nicht zur Verfügung stehen. Sie sollten nur für die zentrale Wartung in der Dienststelle und nur für dafür besonders Berechtigte (Systemverwalter) verfügbar sein.
- Art und Umfang des Laptop-Einsatzes sind verbindlich und für jeden nachvollziehbar schriftlich in einer *Dienstanweisung* zu regeln. Dabei ist festzulegen, welche Geräte mit welchen Programmen verwendet, für welche Aufgabengebiete diese eingesetzt und welche Daten verarbeitet werden dürfen. Es sind gegebenenfalls Sanktionen für die Fälle vorzusehen, in denen gegen die Dienstanweisungen in grober Weise verstoßen wird.
- Mit den genannten Maßnahmen kann ein gewisser Sicherheitsgrad, aber kein vollständiger Schutz erzielt werden. Die mit Laptops ausgestatteten Mitarbeiter sind deshalb besonders auf die mit dem Einsatz tragbarer Rechner verbundenen Gefahren hinzuweisen und für eine strikte Einhaltung der erforderlichen datenschutzrechtlichen Maßnahmen zu *sensibilisieren.*

Technische Maßnahmen

Grundsätzlich sind für einen datenschutzgerechten Einsatz die von uns als Broschüre herausgegebenen *„Grundsätze zum Datenschutz - Isolierte Rechner/Personal Computer"* auch für Laptops anwendbar.

Darüber hinaus sind aber noch Maßnahmen zu treffen, die die besonderen Risiken des Laptop-Einsatzes berücksichtigen.

- Ein Laptop ist gegen *Hardwaremanipulationen,* etwa das Öffnen des Gehäuses und die Entnahme von Bausteinen, Steckkarten etc., durch geeignete Maßnahmen zu schützen (z. B. durch Verplombung des Rechners).
- Der Laptop ist mit *Sicherheitssoftware* auszustatten, die in der Lage ist, Authentizitäts- und Identitätsprüfungen vorzunehmen und Protokollierungs- und gegebenenfalls auch Verschlüsselungsfunktionen zur Verfügung zu stellen.

  Für den personengebundenen Betrieb ist nur ein Benutzer, für ein einem Verfahren gewidmetes Gerät ist die erforderliche Anzahl von Benutzern einzurichten, die jeweils über ein individuelles und von ihnen änderbares Paßwort verfügen müssen.

  Die Datenschutzsoftware soll gewährleisten, daß Paßwörter verschlüsselt und alle sicherheitsrelevanten Informationen, die für einen reibungslosen Einsatz des Sicherheitsproduktes erforderlich sind, so geschützt werden, daß eine Manipulation bzw. Umgehung des Schutzes ausgeschlossen werden kann.

  Auf dem Laptop sollte aus Gründen der Kompatibilität und des einheitlichen Sicherheitsstandards das gleiche Sicherheitssoftwareprodukt eingesetzt werden, das auch für die behördeninternen stationären ADV-Systeme verwendet wird.
- Alle Aktivitäten am Laptop sind mit Hilfe der einzusetzenden Datenschutzsoftware zu *protokollieren.* Die Protokolldateien sind in regelmäßigen Abständen stichprobenartig oder bei besonderen Anlässen zentral in der Dienststelle von einer damit beauftragten Person auszuwerten (z. B. interner Datenschutzbeauftragter). Die Protokolldateien dürfen für den Anwender nicht manipulierbar sein.

  Gemäß § 11 Abs. 5 BlnDSG dürfen erhobene personenbezogene Daten, die ausschließlich zu Zwecken der Datenschutzkontrolle, der Datensicherung oder zur Sicherstellung des ordnungsgemäßen Betriebes einer Datenverarbeitungsanlage gespeichert wurden, nicht für andere Zwecke verwendet werden.
- Um das Laden des Betriebssystems beim Start des Rechners über das Diskettenlaufwerk und damit die Umgehung der auf der Festplatte des Rechner installierten Sicherheitssoftware zu verhindern, muß das Diskettenlaufwerk des Laptops *gesperrt* werden. Damit verhindert man gleichzeitig das unbefugte Einspielen von Programmen und Daten über bewegliche Datenträger (Disketten). Der Einsatz beweglicher Datenträger, z. B. zum Zwecke der Datensicherung, sollte der Dienststelle vorbehalten bleiben, damit verhindert wird, daß nicht freigegebene Anwendungsprogramme oder Betriebssystemversionen eingesetzt werden, oder daß vor Ort zusätzliche Datenträger verwendet werden, deren Herkunft und Verbleib im Dunkeln bleiben und sich einer Kontrolle entziehen.
- Um die unbefugte Weitergabe von Programmen und Daten zu verhindern, sind unabhängig vom Diskettenlaufwerk auch die *Schnittstellen* des Laptops zu *sperren.* Bei Laptop-Netz-Kopplungen ist ein Datenaustausch in beiden Richtungen möglich. Es muß daher verhindert werden, daß Daten vom Laptop unbefugt auf externe Rechner überspielt oder aus externen Rechnern vom Laptop ausgelesen werden können.

  Werden tragbare Computer gerade zum Zwecke des Datenaustausches eingesetzt, so ist dafür Sorge zu tragen, daß nur die für den Datenaustausch vorgesehenen Daten im dafür erforderlichen Umfang kopiert werden dürfen. Beim Kopieren von Daten auf den Laptop ist auf die Gefahr der „Virenverseuchung" zu achten.

  Die Berechtigung zur Entsperrung der Schnittstellen zum Zwecke der internen Weiterverarbeitung der Daten sollte bei einem dafür berechtigten Benutzer (Systemverwalter) liegen. Es kann erforderlich sein, die gewonnenen Informationen am Arbeitsplatz sofort weiter zu verarbeiten, ohne daß ein Systemverwalter bemüht werden soll. In diesen Fällen muß die Berechtigungsprüfung zum Überspielen von Daten vom behördeninternen Rechner durchgeführt werden.
- In der Regel ist eine *Zugriffsmöglichkeit auf das Betriebssystem* für den „normalen" Anwender nicht erforderlich. Da irrtümliche oder nachlässige Eingaben auf Betriebssystemebene unbeabsichtigte Folgen für die Sicherheit des Gerätes

haben können, sollte dem Benutzer der Zugriff in diesen Bereich verwehrt werden. Der für die Datenverarbeitung notwendige Betriebssystembefehlsumfang sollte über die Sicherheitssoftware gesteuert werden.

- Zumindest wenn auf dem Laptop personenbezogene Daten verarbeitet werden, die einem besonderen Berufs- oder Amtsgeheimnis unterliegen oder einen hohen Grad an Schutzbedürftigkeit aufweisen, so sollten diese *verschlüsselt* werden. Damit soll erreicht werden, daß im Falle eines Diebstahls oder Verlustes des Gerätes die Daten für Dritte nicht mehr verwertbar sind.
- Programme und Daten auf für den Datenaustausch mit anderen Behörden vorgesehenen Laptops sollten einer regelmäßigen *Integritätsprüfung* unterzogen werden. Dabei geht es im wesentlichen um die Vorbeugung der Verbreitung von Viren u. ä. Aus Sicherheitsgründen sollten derartige Prüfungen vor jeder Anbindung an ein behördeninternes ADV-System stattfinden.

  Aus diesen Gründen sind auch für den Laptop-Einsatz vorgesehene bewegliche Datenträger besonders zu kennzeichnen und zu behandeln.

3. Berichte aus den Geschäftsbereichen

3.1 Bau- und Wohnungswesen

Automation im Bau- und Wohnungswesen

Im Bereich des Bau- und Wohnungswesens werden sowohl bei den zuständigen Senatsverwaltungen als auch in den Bezirken umfangreiche Dateien geführt. Darunter befinden sich so große Datensammlungen wie die Wohnungsdatei für Kataster, Fehlbelegung und Mietausgleich mit etwa einer halben Million Datensätzen, die Bewerberdatei für Sozialwohnungen mit ca. 70 000 Datensätzen und die bezirklichen Wohngelddateien mit ca. 170 000 Datensätzen (nur Westbezirke).

Diese Dateien wurden im vergangenen Jahr in eine umfassende datenschutzrechtliche Überprüfung der Datenverarbeitung bei der Senatsverwaltung sowie - stellvertretend für alle Bezirke - in den Bezirken Wilmersdorf, Tiergarten und Zehlendorf einbezogen.

In allen Fällen sind die Bezirke zuständig für die Durchführung dieser übertragenen Vorbehaltsaufgabe. Allerdings liegt die datenschutzrechtliche Verantwortung für die Führung der Wohnungsdatei sowie der Datei für Sozialwohnungsbewerber bei der Senatsverwaltung für Bau- und Wohnungswesen. Sie stellt die technischen Mittel für die Durchführung des ADV-Verfahrens zur Verfügung,

Auch das *Wohnungswesen,* für das die bezirklichen Wohnungsämter datenverarbeitende Stellen sind, wird bei der Senatsverwaltung für Bau- und Wohnungswesen zentral koordiniert.

Innerhalb der Senatsverwaltung ist die fachliche Zuständigkeit von der Abteilung für die technische Umsetzung des Verfahrens getrennt.

Die Systeme entsprechen den datenschutzrechtlichen Anforderungen. Festzuhalten ist jedoch, daß die zentrale Führung der Dateien „Wohnungskataster" und „Bewerber für Sozialwohnungen" durch die Senatsverwaltung nichts an der Zuständigkeit der Bezirke für die Durchführung der Verfahren ändert. Insoweit bleiben auch die Bezirke für die Verfahren zuständig.

Auch im Bereich des *Grundstückswesens* werden umfangreiche Datensammlungen für die Administration des Grund und Bodens in Berlin geführt. So enthält das *Automatisierte Liegenschaftsbuch* (ALB) ca. 330 000 Datensätze. Das ALB sowie die *Bodenwirtschaftliche Datei* (BOWIDA), die *Sanierungsdatei* des Bezirks Tiergarten und die *Stadtplanungs-Informationsdateien* in den Bezirken Wilmersdorf und Zehlendorf wurden ebenfalls überprüft. Bei dieser Überprüfung ging es um die Abgrenzung der verschiedenen Grundstücksdateien hinsichtlich ihrer Daten, ihrer Verwendung sowie um die Gewinnung einer Übersicht über die verschiedenen Zuständigkeiten für diese Datensammlungen.

Während das ALB-Verfahren ein zwar zentral von der Senatsverwaltung für Bau- und Wohnungswesen koordiniertes und mit einheitlichen Vorgaben versehenes Verfahren in der datenschutzrechtlichen Verantwortung der bezirklichen Vermessungsämter ist, ist für die BOWIDA allein die Senatsverwaltung zuständig. Die BOWIDA diente ursprünglich dazu, unbebaute Grundstücke nachzuweisen, jedoch wird jetzt daran gedacht, sämtliche Grundstücke zu erfassen. Zusätzlich erfaßt auch die Stadtplanungsdatei der Senatsverwaltung für Stadtentwicklung und Umweltschutz sämtliche Grundstücke der zwölf westlichen Bezirke. Einige Bezirke wie die geprüften Bezirke Tiergarten, Wilmersdorf und Zehlendorf haben eigene Sanierungs- und Planungsdateien aufgebaut.

Die genannten Dateien sind miteinander nicht verknüpfbar, da sie zu unterschiedlichen Zeiten und mit unterschiedlicher Technik entstanden.

In den Dateien werden z. T. identische Daten geführt. So wird die Grundstücksgröße, der Eigentümer bzw. die Eigentümer-Art und die Art der tatsächlichen Nutzung in allen Dateien gleichermaßen geführt.

Die parallele Speicherung ist dann gerechtfertigt, wenn es für die jeweilige Aufgabenerfüllung erforderlich ist. In diesem Fall können gleiche Daten für unterschiedliche Aufgaben in verschiedenen Dateien gespeichert werden.

Jedoch überdecken sich die Aufgaben teilweise. Insbesondere sind in den Bezirken Angaben aus dem Bebauungssplan identisch mit solchen in der BOWIDA sowie Angaben aus dem Flächennutzungsplan identisch mit solchen in der Stadtplanungsdatei. Hier ist die Erforderlichkeit einer parallelen Datenspeicherung nicht ohne weiteres ersichtlich. Allerdings ist bekannt, daß Planungen zu einer Vereinheitlichung bzw. Integration der Verfahren bestehen.

Sowohl für die BOWIDA als auch für das ALB fehlt es an ausreichenden bereichsspezifischen Rechtsgrundlagen.

Vor allem beim ALB wird deutlich, daß die Gesetzgebung mit dem Ausbau der ADV nicht Schritt hält: Das Vermessungsgesetz enthält keinerlei Bestimmungen zur ADV und beruht auf der längst überholten Vorstellung von traditioneller Karteiarbeit. Dies führt u. a. dazu, daß die Zulässigkeit von Auskünften aus dem ALB nur schwer überprüfbar ist. Während beim manuellen Verfahren eine Einzelauskunft im Vordergrund stand, ergeben sich aus den nunmehr vorhandenen technischen Möglichkeiten auch Wünsche nach umfassenden bzw. in bestimmter Art aufbereiteten Auskünften. Eine Regelung des Verfahrens, die sich auch auf die Auskunftsarten erstreckt, ist daher dringend erforderlich.

Obwohl bereits für die Führung der BOWIDA eine Rechtsgrundlage schon seit Jahren von uns angemahnt wird, wurde beabsichtigt, den Senatsverwaltungen für Finanzen, für Wirtschaft und für Stadtentwicklung und Umweltschutz Online-Anschlüsse an die BOWIDA einzurichten. Dies ist - auch unter den Voraussetzungen des alten Berliner Datenschutzgesetzes - nur aufgrund einer expliziten Rechtsgrundlage zulässig. Den zur Rechtfertigung vorgetragenen Hinweis, die genannten Senatsverwaltungen hätten schon immer regelmäßig vollständige Ausdrucke der BOWIDA erhalten, nahmen wir zum Anlaß einer datenschutzrechtlichen Überprüfung, die zu einer formellen Beanstandung dieser unzulässigen regelmäßigen Übermittlungen führte. Keine Bedenken bestehen natürlich, wenn ein Direktzugriff auf jene Datensätze ermöglicht wird, in denen das Land Berlin Eigentümer der Grundstücke ist, weil in diesen Fällen die Eigentümerangaben keinen Personenbezug begründen.

Weitere Automatisierungsvorhaben

In zwei Stufen soll die *Automatisierte Liegenschaftskarte* (ALK) eingeführt werden. In der ersten Stufe soll innerhalb von sieben Jahren ein digitaler Datenbestand erstellt werden, in denen die bisher schriftlich geführten Kartenwerke und die zugrundeliegenden Koordinatenverzeichnisse der Landesvermessung und des Liegenschaftskatasters in automatisierter Form geführt werden Sollen. Für die zweite Stufe ist die Integration weiterer Verfahren des Grundstückswesens geplant.

Das Verfahren selbst besteht aus zwei Teilen: dem ALK-Datenbankteil, der einheitliche Grundlage für die Vermessungsaufgaben in Berlin sein soll und dem Verarbeitungsteil zur Antragsbearbeitung und zur graphisch-interaktiven Erfassung, Fortführung und Weiterverarbeitung von raumbezogenen Daten. Die Daten der beiden Teile werden untereinander ausgetauscht, indem der Datenbankteil die Daten des Verarbeitungsteils in Form von Aufträgen übernimmt.

Das uns vorgelegte Konzept läßt keine präzise Regelung für die Übermittlung von Daten erkennen. Es wird zwischen Primär- und Sekundärdaten unterschieden, die in insgesamt vier Benutzerklassen unterteilt werden. Sofern dabei für interne Benutzer Online-Anschlüsse eingerichtet werden sollen, bedarf es auch hier einer normenklaren bereichsspezifischen gesetzlichen Regelung im Vermessungsgesetz.

Es ist eine Verknüpfung der ALK-Daten mit den Fachdateien der außenstehenden Benutzer vorgesehen. Auch diese Verknüpfung ist nicht vom Vermessungsgesetz gedeckt. Dies hat insbesondere Bedeutung für die Verknüpfung mit dem Grundbuch:

Zum einen ist der Umfang der zulässigen Speicherung von personenbezogenen Daten für das Grundbuch und das Liegenschaftskataster unterschiedlich geregelt. Das Grundbuch muß Angaben zu den Grundstückseigentümern enthalten, während dies für das Liegenschaftskataster nicht zwingend vorgeschrieben ist.

Zwar wird auf die besondere rechtliche Relevanz der Katasterdaten und der daraus folgenden erhöhten Anforderungen bezüglich der Zugriffsberechtigungen hingewiesen. Auch bei der Beschreibung des Datenbankverwaltungssystems werden kurz einige Zugriffskontrollmöglichkeiten erläutert, ohne festzulegen, welche konkret für das Verfahren ergriffen werden sollen.

Rechtliche Bedenken ergeben sich ferner aus der vorgesehenen Doppelspeicherung des digitalen Datenbestandes. Die 12 westlichen bezirklichen Vermessungsämter sollen einen Bezirksdatenbestand erhalten und bei der Senatsverwaltung für Bau- und Wohnungswesen soll eine vollständige zentrale ALK-Datenbank errichtet werden. Begründet wurde dies lapidar mit arbeitstechnischer Notwendigkeit. Dies kann nicht akzeptiert werden.

Es ist geplant, das *Wohngeldverfahren* zu dialogisieren. Bei einem derartigen Dialogverfahren, welches bezirkliche Aufgaben und übertragene Vorbehaltsaufgaben vereint, ist sicherzustellen, daß die Bezirke nur auf die ihrer eigenen Zuständigkeit unterliegenden Daten zugreifen können. Es sind bei einem zentralen System wie diesem Softwaresicherungen zu installieren, die die Abschottung der Bezirke untereinander gewährleisten.

Der Online-Zugriff der Bezirke auf Daten der anderen Bezirke bedarf nach § 15 Berliner Datenschutzgesetz einer eigenen Rechtsgrundlage.

Die Senatsverwaltung für Bau- und Wohnungswesen sieht in § 69 Abs. 1 Nr. 1 SGB X eine Rechtsgrundlage für den Online-Zugriff der Bezirke auf Daten anderer Bezirke.

Diesem Argument können wir uns nicht anschließen. Zunächst ist jedes Wohnungsamt für sich zuständig für die gesetzliche Aufgabe der Durchführung des Wohngeldgesetzes in seinem Bezirk. Mit den Daten anderer Bezirke werden mangels Zuständigkeit keine gesetzlichen Aufgaben vollzogen.

Gegen einen Online-Zugriff auf die Daten, die Vorgänge des eigenen Bezirks betreffen, ist dagegen nichts einzuwenden, da das Wohnungsamt datenverarbeitende Stelle für diese Daten ist, eine Übermittlung also nicht stattfindet.

Wenn es im Einzelfall erforderlich ist, für die Bearbeitung eines in eigener Zuständigkeit liegenden Vorgangs Daten anderer Bezirke zu erhalten, so wäre diese Übermittlung im Einzelfall nach § 69 Abs. 1 Nr. 1 SGB X zulässig. Dies ist aber nur die Ausnahme. Für die Übermittlung ist das übermittelnde Wohnungsamt datenschutzrechtlich verantwortlich und daher zur Überprüfung der rechtlichen Voraussetzungen verpflichtet.

Fragebögen für Wohnungsbewerber

Bürgerinnen und Bürger aus den östlichen Bezirken der Stadt sind empört darüber, daß sie bei der Wohnungssuche nun plötzlich Fragen beantworten sollen, die ihnen früher nie gestellt wurden: Wohnungsbaugesellschaften, aber auch einzelne Vermieter legen Mietbewerbern vor Vertragsschluß umfangreiche Fragebögen vor. Dazu gehören auch (ehemals) staatliche Wohnungsbau-Gesellschaften in Berlin (Ost).

Darin müssen Fragen nach Arbeitgeber, Einkommen, pünktlicher Mietzahlung, laufenden Pfändungen und Mietprozessen beantwortet werden. Es gibt aber auch Fragebögen, die weit über diese Fragen hinausgehen, indem nach Fernsehgeräten, Fahrrädern oder Mopeds geforscht wird.

In einem Fragebogen will die Wohnungsbau-Gesellschaft auch Namen und Adressen sämtlicher Vermieter wissen, bei denen der Bewerber in den letzten fünf Jahren gewohnt hat.

Es ist nicht zu beanstanden, daß die Vermieter bzw. Wohnungsbau-Gesellschaften Daten abfragen, die für die Abwicklung des Mietvertrages erforderlich sind. Dazu gehören die Angaben zum Einkommen. Ausführungen dazu, warum die Wohnung gewechselt werden soll und zu den Vermietern der vergangenen Jahre sind dagegen für die Abwicklung des Vertrages nicht erforderlich.

Gleichwohl ist der Mieter hier in einer denkbar schlechten Position, da er als Bewerber ausscheidet, falls er die Fragen nicht beantwortet.

Wenn die Fragebögen von öffentlichen Stellen ausgegeben würden, hielte § 10 Berliner Datenschutzgesetz seit neuem eine Regelung bereit, nach der die freiwillige Erhebung dann unzulässig ist, wenn ungesetzliche Nachteile angedroht werden oder keine Aufklärung über die Bedeutung der Einwilligung erfolgt ist. Nach dem neuen Bundesdatenschutzgesetz muß die Datenerhebung nach Treu und Glauben erfolgen (§ 28 Abs. 1 Bundesdatenschutzgesetz). Gegen beide Grundsätze wird verstoßen, wenn nicht erforderliche Daten erhoben werden.

Sollten die Vermieter sich hier nicht selbst Beschränkungen auferlegen, wird der Gesetzgeber etwa in einer bereichsspezifischen Regelung im Bürgerlichen Gesetzbuch tätig werden müssen.

Schlüsselzahl macht obdachlos

Ein Bürger hatte, obwohl er im Besitz eines gültigen Wohnberechtigungsscheins war und eine feste Anstellung hatte, von mehreren Wohnungsbaugesellschaften eine Absage erhalten. Auf Anfrage wurde ihm mitgeteilt, aus der auf der Überlassungsmitteilung der Wohnungsämter unter „verwaltungsinterne Angaben" enthaltenen Schlüsselzahl „85" gehe hervor, daß er seine letzte Wohnung aufgrund einer erfolgten Räumung hatte verlassen müssen.

Es ist offensichtlich, daß diese Praxis eine unangemessene Benachteiligung der Bürger darstellt. Die Senatsverwaltung für Bau- und Wohnungswesen berief sich darauf, daß eine Verfahrensänderung dem Prinzip der Verhältnismäßigkeit zwischen Aufwand und angestrebtem Schutzzweck entgegenstehe, weil mit der Änderung ein zeitlicher Mehraufwand und eine Erhöhung des Personalbedarfs einhergehe. Außerdem bestanden aus Sicht der Senatsverwaltung keine Bedenken dagegen, daß dem potentiellen Vermieter die Zugehörigkeit des Wohnungsbewerbers zur Berechtigungsgruppe „85" bekannt wird, da zu dieser Berechtigungsgruppe nicht nur Personen gehören, die nach Vorlage eines gerichtlichen Räumungstitels ausziehen mußten, sondern auch solche, die aufgrund eines bau- oder wohnungsaufsichtlichen Benutzungsverbots oder anderer Umstände die Wohnung räumen mußten.

Die Offenbarung der Berechtigungsgruppe „85" gegenüber einem potentiellen Vermieter ist demgegenüber weder durch eine gesetzliche Regelung geboten noch aus sonstigen Gründen erforderlich ist. Für die Vergabe der Dringlichkeit eines WBS ist es auch unerheblich, zu welcher Berechtigungsgruppe der Betroffene konkret gehört. Die Offenbarung der Berechtigungsgruppe „85" entfaltet jedenfalls benachteiligende Wirkung, da sie ganz überwiegend auf eine Zwangsräumung hinweisen, denn die übrigen in der Berechtigungsgruppe aufgeführten Gründe spielen in der Praxis nur eine untergeordnete Rolle.

Dementsprechend wurde das Verfahren von uns datenschutzrechtlich beanstandet und empfohlen, die Berechtigungsgruppen auf der Überlassungsmitteilung nicht mehr auszudrucken.

Die Senatsverwaltung für Bau- und Wohnungswesen hat sich daraufhin entschlossen, auf den Ausdruck verwaltungsinterner Angaben auf den Überlassungsmitteilungen zu verzichten.

Gleichwohl zeigt der Fall exemplarisch, daß die überflüssige und beiläufige Offenbarung verschlüsselter „verwaltungsinterner Hinweise", die zu vielfältigen Interpretationen Anlaß geben, in einer Wohnungsmangelsituation wie in Berlin in existenzgefährdender Weise schutzwürdige Belange verletzen kann.

Überflüssige Kontonummern

Ein Bürger mußte für die Berechnung der Fehlbelegungsabgabe auch die Kontonummern seiner Sparbücher angeben. Er berief sich demgegenüber darauf, daß die Sparsummen ordnungsgemäß angegeben worden waren und durch die Vorlage der Sparbücher ein Zweifel an der Richtigkeit der Angaben ausgeschlossen war. Die Notierung der Kontonummern empfand er als überflüssig.

Auf unsere Nachfrage bei dem betroffenen Bezirk sowie bei der Senatsverwaltung für Bau- und Wohnungswesen, warum die Notierung der Kontonummern von Sparbüchern bei der Fehlbelegungsabgabe erforderlich sei, wurde uns mitgeteilt, daß es sich in Einzelfällen zur Nachvollziehbarkeit und Prüfbarkeit als erforderlich erwiesen habe, daß die Kontonummern notiert werden, wenn keine anderen Unterlagen (z. B. Steuerbescheid oder Zinsbescheinigung des Bankinstituts) vorgelegt werden. Dieses Verfahren beruhe auf einer Forderung des Berliner Rechnungshofs, daß auch Einkünfte aus Kapitalvermögen zu berücksichtigen und Belege zu verlangen sind.

Allerdings wurde eingeräumt, daß ein generelles Notieren von Sparbuch- bzw. Kontonummern unter datenschutzrechtlichen Gesichtspunkten fragwürdig ist. Die Bezirke wurden daher angewiesen, Sparbuch- bzw. Kontonummern nur dann einzutragen, wenn es im Einzelfall unabdingbar ist, um Angaben des betroffenen Bürgers nachweisen zu können.

Der Fall macht deutlich, daß auch in Massenverfahren wie der Berechnung der Fehlbelegungsabgabe jeweils zu prüfen ist, welche einzelnen Daten beim Bürger erhoben werden. Es geht nicht an, daß Behörden aus Vereinfachungsgründen Angaben erheben und speichern, die nur möglicherweise interessant sind.

3.2 Finanzen

Die Finanzbehörden gehören zu den größten Datenverarbeitern der Berliner Verwaltung. Die drei Dateien, die die Oberfinanzdirektion bisher nur zum Besonderen Dateienregister zu melden hatte (Steuerfestsetzung, Kontoführung, Adreßverwaltung), enthalten über 4 Millionen Datensätze.

Eingeführt wird derzeit ein neues maschinelles Lohnsteuer-Anmeldeverfahren. Damit sollen die Überwachung des rechtzeitigen und vollständigen Eingangs der Lohnsteuerdaten, die rechnerische Prüfung von Festsetzungen und Steueranmeldungen sowie die Weitergabe der Daten an das Erhebungsverfahren abgewickelt werden. Dieses Verfahren wird von uns im laufenden Jahr geprüft werden.

Ganz besondere Probleme bringt hier die Vereinigung der Stadt mit sich. Die Umstellung der Finanzverwaltung der früheren DDR auf das Bundesrecht wirft auch im Hinblick auf die Informationsverarbeitung erhebliche Probleme auf. Zunächst sind hier die zuständigen Stellen, insbesondere die Oberfinanzdirektion gefordert. Eine datenschutzrechtliche Überprüfung wird zur angemessenen Zeit erfolgen.

Dezentrale Computerleistungen

Die traditionelle Form der Groß-Datenverarbeitung, die ursprünglich als Stapelverarbeitung betrieben wurde, wird derzeit erheblich erweitert mit dem Ziel, Computerleistung an den Arbeitsplatz der Sachbearbeiter zu bringen. Das Konzept wird von der Finanzverwaltung *DCL-Verfahren* (Dezentrale Computerleistung in den Finanzämtern) genannt. Es wurde im Berichtsjahr erprobt. Netzkonzept und Zugangs- und Zugriffsregelungen waren Gegenstand von Beratungsgesprächen.

Bei dieser Anwendung erfolgt der Einsatz von Computern in drei Stufen:

In den Finanzämtern werden PCs in der Kasse, der Datenerfassungsstelle, der Kanzlei und zum Teil auch in der Vollstreckungsstelle eingesetzt. Die Sachbearbeiter in den einzelnen Raten haben derzeit noch keine Terminals an ihrem Arbeitsplatz; alle Abfragen (u. a. auch Sofortauskünfte) werden über diese Stellen abgewickelt. Die meisten Auskünfte werden daher nach wie vor über die beim Sachbearbeiter befindlichen Akten erteilt.

In jedem Finanzamt (und auch bei der Oberfinanzdirektion) ist ein Vermittlungsrechner installiert, der die Verbindung zum Hauptrechner (Host) herstellt.

Im Host-Rechner werden die Dateien „Speicherkonten" und „AV-Konten" (für Einkommensteuer = Festsetzungs- und Einzelwertangaben, für Lohnsteuer = Anschrift und Bankverbindung) geführt, die sämtliche Daten der Lohn- und Einkommensteuer beinhalten.

Das DCL-Verfahren ist als Oberbegriff für mehrere dezentrale Anwendungen (z. B. Festsetzungsspeicher, Einzelwerteingabe, Vollstreckung) zu sehen. Zur Zeit sind insgesamt 400 Terminals (PCs) angeschlossen, wobei ca. 70 auf die OFD entfallen. Im Endstadium, d. h. 1995 sollen 1600 Terminals angeschlossen sein, so daß jeder Sachbearbeiter an seinem Arbeitsplatz mit dem Rechner in Dialog treten kann.

Der Umstellung der Verfahrensteile Datenerfassung und Abfragen werden in diesem Jahr die Bereiche Vollstreckung und Steuerfahndung folgen.

Die erforderliche Datensicherungs- und Datenschutz-Software wurde in der Zwischenzeit implementiert. Bei der Datenerfassungsstelle und der Maschinenbedienung wurden keine Mängel festgestellt.

Auch die Organisation der Zugriffssicherung entspricht den hohen Anforderungen, die an einen derart sensiblen Bereich wie die Finanzverwaltung zu stellen sind.

Ein offenes Problem bleibt allerdings - wie übrigens in anderen Verwaltungen auch - der Umfang der Protokollierung des Zugriffs.

Die Rache des Geschiedenen

Ein geschiedener Ehemann, der bei einem Finanzamt beschäftigt ist, rächt sich an der Familie seiner Ehemaligen auf seine Weise: Von dem Terminal aus, zu dem er Zugangsberechtigung hat, ruft er die Steuerdaten aus der Einkommensteuererklärung seines früheren Schwiegervaters sowie die Kfz-Steuerdaten seiner früheren Frau ab. Er nimmt zur Kenntnis, daß diese noch erhebliche Zuwendungen von ihrem Vater erhält und sich sogar ein neues Auto leisten konnte. Dies mindert seine Lust erheblich, Unterhaltszahlungen in der bisherigen Höhe zu leisten.

Selbstverständlich handelte der Beamte rechtswidrig. Die Frage ist nur, wie der Nachweis zu führen ist. Er bestreitet natürlich, sein Wissen mit einem unbefugten Abruf erworben zu haben - Petzer gibt es immer und überall. Das Finanzamt kann den Nachweis auch nicht führen. Es prüft nur die allgemeine Berechtigung (etwa des Zugriffs zu den Kfz-Daten), protokolliert aber nicht jeden einzelnen Abruf, sondern nur stichprobenweise. Die künftige Steuerdaten-Abrufverordnung will an dieser Situation nichts ändern.

Nochmals Betriebsprüfer und ihre Privat-PCs

In der Stellungnahme des Senats zu unserem Jahresbericht 1989 ist auf unsere Feststellungen über private Computer in der Steuerverwaltung eingegangen worden. Dabei wurde unsere Auffassung, daß durch die *Nutzung privater PCs in der Wohnung der Betriebsprüfer* das Steuergeheimnis gefährdet sei, zurückgewiesen.

Der Senat stützt in der Stellungnahme seine Auffassung erstens darauf, daß das Steuergeheimnis durch strafbewehrte Vorschriften ausreichend geschützt sei, zweitens darauf, daß die Betriebsprüfer seit Jahrzehnten ihre Zuverlässigkeit bezüglich der Wahrung des Steuergeheimnisses unter Beweis gestellt hätten und drittens darauf, daß bisher keine Fälle bekannt geworden seien, die unsere Befürchtungen begründen könnten.

Diese Argumentation überzeugt nicht. Vorschriften allein stellen keine Schutzmaßnahmen für das Steuergeheimnis dar, sondern die Kontrolle ihrer Befolgung. Diese stellt aber, wie der Senat mit dem Hinweis auf Artikel 13 GG und Artikel 19 Abs. 2 Verfassung von Berlin richtig feststellt, einen schwerwiegenden Eingriff in Grundrechte dar, wenn sie in der Privatwohnung stattfindet, und ist mangels hinreichender Befugnisnorm ohnehin nur mit Einwilligung der Betroffenen möglich. Damit verliert auch die Strafbewehrung ihren Sinn.

Es geht auch nicht um die vorsätzliche oder die leichtfertige Offenbarung von Steuerdaten, sondern darum, ob die Daten in der Privatwohnung des Betriebsprüfers in einer dem Schutzbedürfnis der Steuerdaten angemessenen Weise dem Zugriff oder der beiläufigen Kenntnisnahme durch Familienangehörige oder Gäste jederzeit entzogen sind.

Wir zweifeln die Zuverlässigkeit der Betriebsprüfer bezüglich der Wahrung des Steuergeheimnisses nicht an, sehen aber andererseits in dem Vertrauen auf diese Zuverlässigkeit weder eine technisch-organisatorische Maßnahme für die Wahrung des Steuergeheimnisses noch eine Entbindung von der Kontrollpflicht.

Gegen die Mitnahme von Unterlagen aus den Diensträumen zu den geprüften Betrieben haben wir keine Einwände, soweit dies für die Durchführung der Prüfung erforderlich ist. Gleiches würde auch für dienstlich beschaffte tragbare Computer gelten. Während der Prüftätigkeit am Prüfungsort gehen wir ohnehin davon aus, daß der Prüfer seine Unterlagen oder Daten im Auge hat. Anders als in seiner Privatwohnung muß am Prüfungsort auch damit gerechnet werden, daß der leichtfertige Umgang mit Steuerunterlagen von Dritten bemerkt wird.

Es ist zu begrüßen, daß nunmehr eine einheitliche ADV-Unterstützung für die Betriebsprüfer mit dem Programmsystem *BPPLAN* eingeführt werden soll. Es ist zu hoffen, daß damit der Einsatz privater PCs unterbunden werden kann, ohne daß auf den Komfort automatisierter Datenverarbeitung verzichtet werden muß.

Das Verfahren BPPLAN ist für den bundesweiten Einsatz konzipiert und geht nur bedingt auf landesspezifische Lösungen ein, da die Hard- und Software-Gegebenheiten zu unterschiedlich sind; es umfaßt sowohl eine Unterstützung des Innendienstes als auch des Außendienstes. In den Außenprüfungsbereichen sollen auch tragbare PCs und programmierbare Taschenrechner zum Einsatz kommen.

In Berlin liegt BPPLAN als Testversion in einer stand-alone-Lösung vor. Schnittstellen zu anderen Verfahren bzw. Systemen sind geplant. In Berlin soll die Anbindung von BPPLAN an das DCL-Verfahren innerhalb des nächsten Jahres realisiert werden.

Steuergeheimnis und Mikroverfilmung

Formulare begleiten den Bürger von der Wiege bis zur Bahre. Die Unterbringung der dabei bei Behörden entstehenden Papiermengen, insbesondere bei Massenverfahren bereitet zunehmend Platzprobleme, so daß viele Behörden dazu übergegangen sind, abgeschlossene Vorgänge der *Mikroverfilmung* zuzuführen. Dies wird üblicherweise im Auftrag der Behörden von Privatfirmen erledigt, die sich auf diese Tätigkeit spezialisiert haben.

Damit verlassen sensible Daten den abgeschlossenen Behördenbereich und gelangen nach außen. Beispiele für die Problematik ergeben sich bei der Fehlbelegungsabgabe, bei deren Berechnung häufig Steuerdaten anfallen, wenn die Einkommensverhältnisse mit Hilfe des Steuerbescheids nachgewiesen werden. Obwohl dies nicht vorgeschrieben ist, entspricht es der Behördenpraxis, eine Kopie des Steuerbescheids zu den Akten zu nehmen.

Diese Daten werden nicht unmittelbar durch die Vorschriften zum Steuergeheimnis geschützt, da diese nur gelten, wenn es sich um ein Besteuerungsverfahren handelt oder die Vorlage des Bescheides gesetzlich vorgeschrieben ist (§ 30 Abs. 2 Ziff. 1 c Abgabenordnung). Diese Situation führt zu folgender, dem Bürger kaum zu vermittelnder Konsequenz: Die Mikroverfilmung von Steuerunterlagen, die aufgrund einer gesetzlichen Verpflichtung vorgelegt wurden, außerhalb des Finanzamtes ist rechtswidrig, weil die Abgabenordnung keine Offenbarungsbefugnis an Fremdfirmen vorsieht. Wird der Bescheid jedoch ohne Verpflichtung zu den Akten genommen, entfällt dieser Schutz und die Mikroverfilmung ist aufgrund der allgemeinen Vorschriften zulässig. Diese Ungleichbehandlung muß dadurch aufgefangen werden, daß die Verlängerung des Steuergeheimnisses in jedem Fall gilt.

Trotz Empörung alles in Ordnung

Zu den Eigenheiten der Finanzverwaltung gehört, daß sich Bürger häufig auch über rechtmäßiges Handeln der Beamten empören, insbesondere dann, wenn der Fiskus sozusagen aus dem Hinterhalt zuschlägt: Jemand bezahlt die Rechnung für eine (aus seiner Sicht überflüssige) Umsetzung nach einem Falschparken nicht und findet ein halbes Jahr später sein Bankkonto gepfändet; einem anderen Bürger, der es für angemessen hält, dem Finanzamt die Hundesteuer wenn überhaupt, dann jedenfalls erheblich zu spät zu zahlen, widerfährt das gleiche mit dem Sparkonto, auch beim Arbeitgeber (den er bisher, da er keinen Lohnsteuerjahresausgleich beantragt hat, vor dem Finanzamt glaubte geheimhalten zu können) wird eine unangenehme Pfändung vorgenommen.

Den Bürgern, die sich wegen dieser oder ähnlicher Begebenheiten an den Datenschutzbeauftragten wenden, ist nicht klar, daß den Steuerbehörden eine Reihe von Informationsquellen rechtmäßig zur Verfügung stehen. So kann das Finanzamt aus den eigenen Akten, wenn auch aus anderem Zusammenhang Daten aus Bankkonten erheben, ja Schulden und Guthaben miteinander verrechnen. Das Sozialgesetzbuch verpflichtet Sozialbehörden, etwa die Allgemeine Ortskrankenkasse, die Adresse des Arbeitgebers zu übermitteln. Auch die Steuerfahndung kann sich Informationsquellen auf der Grundlage der Abgabenordnung, aber auch der Strafprozeßordnung erschließen.

Dieses kann nicht beanstandet werden, wenn auch die Regelungen in einiger Hinsicht die erforderliche Klarheit vermissen lassen.

3.3 Frauen, Familie und Jugend

In diesem Geschäftsbereich besteht als einziges großes EDV-Verfahren die automatisierte Verarbeitung von Daten zum Unterhaltsvorschußverfahren (ZVK/UVK), über das schon mehrfach berichtet wurde. Im Vordergrund datenschutzrechtlicher Erörterungen standen hier zwei Gesetzgebungsvorhaben, eines des Bundes und eines des Landes.

Der verlorene Sohn

Kurz nach der Wende verließ ein Jugendlicher Ost-Berlin. Eine Dienststelle der ehemaligen DDR trat an die Senatsverwaltung für Frauen, Jugend und Familie mit folgender Bitte heran: Die Eltern suchten nach dem Jungen. Da er homosexuell veranlagt sei, bitte man, eine Beschreibung in allen Beratungsstellen und „Schwulentreffs" auszuhängen mit der Aufforderung, daß sich der Junge selbst meldet oder sein Aufenthaltsort mitgeteilt wird.

Bei allem Verständnis für die Situation der Eltern muß hier die Frage gestellt werden, unter welchen rechtlichen Voraussetzungen die Beratungsstellen Daten des gesuchten Jungen hätten veröffentlichen dürfen. Nach dem damals noch geltendem Jugendwohlfahrtsgesetz wäre dies allenfalls aus Gründen des Kindeswohls zulässig gewesen. Diese Offenbarungsbefugnis hätte aber nur dann bestanden, wenn der Junge aufgrund seines Alters und seiner Einsichtsfähigkeit noch nicht in der Lage gewesen wäre, über sich selbst und damit auch über die Preisgabe seiner Daten zu bestimmen. Minderjährige gelten bereits ab dem vollendeten 14. Lebensjahr als grundrechtsmündig. Wenn diese Altersgrenze noch nicht überschritten war, dann hätte die Einwilligung des Gesuchten durch die seiner Eltern ersetzt werden können. Das tatsächliche Vorliegen der elterlichen Einwilligung hätte die DDR-Dienststelle aber nachweisen müssen.

Kinder- und Jugendhilfegesetz

Das Jugendwohlfahrtsgesetz ist inzwischen durch das neue Kinder- und Jugendhilfegesetz ersetzt worden, das als 8. Buch in

das Sozialgesetzbuch eingefügt wurde[21]. Dieses zu Beginn des Jahres 1991 in Kraft getretene Gesetz definiert erstmals erfreulich klar die Aufgaben der Jugendhilfe und enthält längst überfällige Datenschutzregelungen, die dem informationellen Selbstbestimmungsrecht von Kindern, Jugendlichen und Eltern ebenso Rechnung tragen wie den praktischen Bedürfnissen der Jugendhilfe.

Insbesondere unterscheidet der Gesetzgeber bei den Aufgaben der Jugendhilfe klar zwischen „Leistungen" mit Angebotscharakter und „anderen Aufgaben" mit Eingriffscharakter. Dies hat Konsequenzen für die zweckgebundene Verwendung der Daten: Informationen, die bei der Scheidungsberatung erhoben worden sind, dürfen nicht für die Familiengerichtshilfe verwandt werden. Auch dürfen Daten selbst zur Erfüllung einer Aufgabe der Jugendhilfe nur offenbart werden, wenn dadurch der Erfolg einer zu gewährenden Leistung nicht in Frage gestellt wird.

Schließlich enthält das neue Kinder- und Jugendhilferecht ein besonderes Amtsgeheimnis, das jeder einzelne Mitarbeiter eines Trägers der öffentlichen Jugendhilfe bezüglich der personenbezogenen Daten zu wahren hat, die ihm zum Zweck der persönlichen und erzieherischen Hilfe anvertraut worden sind. Dies erfordert Änderungen in der Aktenführung und organisatorischen Struktur der Jugendämter.

Für die Frau – gegen den Datenschutz?

Nach dem *Landesantidiskriminierungsgesetz* (LADG) vom 31. Dezember 1990[22] sind auch unerwünschte Bemerkungen, Kommentare oder Witze über das Äußere von Beschäftigten sexuelle Belästigungen, über die betroffene Frauen sich bei den in jeder Einrichtung des Landes Berlin zu wählenden Frauenvertreterin beschweren können. Diese berät die Betroffenen und leitet Mitteilungen über sexuelle Belästigungen mit Einverständnis der betroffenen Frau der Amts-, Anstalts- oder Betriebsleitung zu (§ 16 Abs. 4 LADG). Es ist nicht zu bestreiten, daß das Problem der sexuellen Belästigung am Arbeitsplatz lange Zeit verschwiegen und nicht entschieden genug bekämpft wurde. Das neue Gesetz geht jedoch von einem sehr weiten Begriff der sexuellen Belästigung aus („unnötiger Körperkontakt, von der Betroffenen unerwünschte Bemerkungen sexuellen Inhalts, unerwünschte Bemerkungen, Kommentare oder Witze über das Äußere von Beschäftigten, Zeigen pornographischer Darstellungen am Arbeitsplatz sowie Aufforderungen zu sexuellen Handlungen" – § 12 Abs. 2 LADG). Außerdem verpflichtet das Gesetz die Frauenvertreterin dazu, mit Einverständnis der betroffenen Frau Mitteilungen über sexuelle Belästigungen der Amtsleitung zuzuleiten.

Ich habe im Gesetzgebungsverfahren darauf hingewiesen, daß in dieser Situation neben den Rechten der belästigten Frau auch das informationelle Selbstbestimmungsrecht des Belästigers betroffen ist. Damit wäre es nicht zu vereinbaren, wenn die Frauenvertreterin schematisch alle Beschwerden über sexuelle Belästigungen mit Einwilligung der belästigten Frauen der Amtsleitung mitteilen würde. Sie muß vielmehr im Einzelfall prüfen, ob eine solche Mitteilung gerade angesichts des konkreten Verhaltens, das Anlaß zu der Beschwerde gegeben hat, verhältnismäßig wäre. Das neue Gesetz sollte in diesem Punkt mit Augenmaß angewandt werden, um es nicht von vornherein zu diskreditieren.

Das neue Landesantidiskriminierungsgesetz regelt in erfreulicher Klarheit (auch wesentlich eindeutiger als das Hochschulgesetz) die Befugnisse der Frauenvertreterin, die eine Offenbarung personenbezogener Daten erforderlich machen. Insbesondere werden durch die ausdrückliche Regelung, daß die Frauenvertreterin an Bewerbungsgesprächen teilnehmen kann, Unsicherheiten, wie sie im Personalvertretungsrecht bestehen, beseitigt.

Jede Einrichtung muß Mitte 1992 eine Analyse der Beschäftigtenstruktur erstellen und dem Senat als Grundlage für einen Bericht über die Durchführung dieses Gesetzes zuleiten. Dabei sind bestimmte Daten zu erheben, die in der Anlage zum Gesetz aufgeführt sind. Es handelt sich jedoch in erster Linie um aggregierte Daten. Soweit in Einzelfällen personenbezogene Daten in die Analyse der Beschäftigtenstruktur eingehen (z. B. weil es nur eine Frau als Abteilungsleiterin gibt), sind die betroffenen Personen im Rahmen der Zielsetzung des Landesantidiskriminierungsgesetzes zur Duldung der Offenbarung verpflichtet.

3.4 Gesundheit und Soziales

Im *Gesundheitswesen* befinden sich im Westteil der Stadt die großen Datensammlungen in den Kliniken und Krankenhäusern; sie waren Gegenstand umfangreicher Prüfungen und Berichte. Da es sich hier um die sensibelsten Datenbestände der Verwaltung überhaupt handelt, wird die Informationsverarbeitung der medizinischen Einrichtungen im Ostteil der Stadt einer der vordringlichsten Prüfgegenstände sein müssen. Der Beginn wurde mit einer ersten Einschätzung großer epidemiologischer Register sowie des Verbleibs von Daten aus Einrichtungen gemacht, die nicht mehr fortbestehen werden.

In der *Sozialverwaltung* steht die Umwandlung der Großverfahren, mit denen die Sozialleistungen des Landes bearbeitet werden, im Vordergrund: Auch hier soll künftig die Arbeit am Arbeitsplatz in den Sozialämtern direkt unterstützt werden.

Das nationale Krebsregister der DDR

Eine der interessantesten, aber auch der problematischsten medizinischen Datensammlungen in der ehemaligen DDR ist das *nationale Krebsregister.* Es wird vom „Institut für Krebsforschung" der Akademie der Wissenschaften in Ost-Berlin geführt. Der Einigungsvertrag bestimmt, daß die Forschungsinstitute als Einrichtungen der Länder fortbestehen, wenn sie nicht aufgelöst oder umgewandelt werden (Artikel 38 Abs. 2). Damit steht das Land Berlin in der Verantwortung für diesen Datenbestand.

Das Krebsregister wurde Mitte der 50er Jahre angelegt und gilt unter Epidemiologen wegen der Meldepflichten als eines der aussagekräftigsten derartigen Register in der Welt. Hier wurden seit 1956 Daten zu allen behandelten Krebserkrankungen, zur Therapie und zu Krankheitsverläufen gespeichert. Jeder behandelnde Arzt war verpflichtet, entsprechende Meldungen mit Name, Anschrift und Personenkennzahl des Patienten an das Institut für Krebsforschung abzugeben, wobei die Meldungen ohne Kenntnis oder gar Einverständnis der Patienten erfolgte. Als Rechtsgrundlage für diese Meldepflicht existierte bis zum Sommer 1990 eine „Verordnung" des Ministerrats und eine „Richtlinie" des Gesundheitsministers[23]. Seit Juli 1990 schreibt das Statistikgesetz der DDR die Meldepflichten gesetzlich fest.

Nach der deutschen Einigung ist das Krebsregister an den Regelungen des Einigungsvertrages und des Grundgesetzes zu messen. Der Einigungsvertrag enthält keine spezifischen Sonderbestimmungen; da der Bundesgesetzgeber von seiner Gesetzgebungszuständigkeit auch ansonsten keinen Gebrauch gemacht hat, könnten die Vorschriften allenfalls als Landesrecht fortbestehen, allerdings nur dann, wenn die vorliegenden Meldungen mit dem Grundgesetz vereinbar sind (Artikel 9 Abs. 1 Einigungsvertrag).

Die Meldungen greifen in das informationelle Selbstbestimmungsrecht der betroffenen Krebspatienten sowie in die ärztliche Schweigepflicht in einem Maße ein, das ganz erheblich gegen das Übermaßverbot verstößt und damit verfassungswidrig ist. Akzeptabel sind bei nationalen Epidemiologieregistern nur anonymisierte oder auf die Einwilligung der Betroffenen gestützte Melde- und Verarbeitungsverfahren.

Wir verkennen nicht die wissenschaftliche Bedeutung dieses Registers. Ferner kann das Register aufgrund der erheblichen Umweltbelastungen, denen die Menschen in der ehemaligen DDR ausgesetzt waren und sind, möglicherweise auch eine sehr persönliche Bedeutung für die betroffenen Familien (z. B. als Informationsquelle für die Geltendmachung von Entschädigungsansprüchen) erlangen.

[21] GVBl. 1990, S. 1391 ff

[22] GVBl. 1991, S. 8 ff

[23] Verordnung des Ministerrats der DDR vom 17. Mai 1956 zur Verbesserung der Behandlung von Geschwulsterkrankungen, Gesetzblatt der DDR 1956 I, S. 477 f.;
Richtlinien des Ministeriums für Gesundheitswesen vom 21. Dezember 1986 zur frühzeitigen Erkennung von Geschwulstkrankheiten und zur Betreuung von Geschwulstkranken, Verfügungen und Mitteilungen des Gesundheitsministeriums 1987, S. 9 ff.

Dies kann jedoch einen so schwerwiegenden übermäßigen Eingriff in das informationelle Selbstbestimmungsrecht, wie er in der Vergangenheit durch die Krebsregistrierung erfolgte, nicht rechtfertigen. Vielmehr sind umgehend Schritte einzuleiten, die einerseits durch eine Anonymisierung der vorhandenen Bestände, andererseits durch eine grundgesetzkonforme Ausgestaltung der Meldewege einen Zustand herstellen, der mit dem informationellen Selbstbestimmungsrecht vereinbar ist. Erste Verhandlungen sind hierzu bereits geführt worden, wobei auch die Pläne einer bundesweiten Krebsregistrierung einbezogen wurden.

AIDS-Kartei

Es ist geradezu selbstverständlich, daß der „fürsorgende Staat" der DDR auch alle *AIDS-Kranken* erfaßte. Im Ost-Berliner Bezirks-Hygiene-Institut wurde aufgrund einer Weisung des Gesundheitsministers Mitte der 80er Jahre eine entsprechende Kartei angelegt. Hier wurden nicht nur die persönlichen Daten wie Name und Anschrift der Infizierten gesammelt, sondern auch Informationen wie „Anlaß der Untersuchung", „Partnerlabilität", „Sexualpraktiken" und „Arbeitsstelle". Die Namen der Betroffenen waren bei unserer Prüfung zwar unkenntlich gemacht, jedoch wäre es möglich, aus den Restdaten wie Arbeitsstelle, behandelnder Arzt etc. die Betroffenen wieder ausfindig zu machen.

Das Bezirks-Hygiene-Institut hatte diese Meldungen auf Formularen von dem jeweils behandelnden Arzt bzw. Labor erhalten und zwar ohne Kenntnis oder Einverständnis des Betroffenen.

Die ministerielle Anweisung kann unter den Bedingungen des Grundgesetzes keine geeignete Rechtsgrundlage für diese Datenspeicherung sein. Somit ist auch die fortdauernde Speicherung derartiger Erkenntnisse durch die staatliche Stelle ein rechtswidriger Eingriff in das Recht auf informationelle Selbstbestimmung der Betroffenen. Wir haben daher die Vernichtung empfohlen.

Vom Ost-Berliner Hygiene-Institut wurde uns versichert, daß es seit Schaffung der Datei - abgesehen von der Meldung an das Zentrale Hygiene-Institut - keine offizielle Weitergabe der Informationen an andere Stellen (Polizei, Stasi) und auch keinerlei dahingehende Gesuche gegeben habe.

Umstrukturierung des Gesundheitswesens der DDR

Journalisten einer West-Berliner Zeitung fanden in einer Wohnstraße aufgerissene Mülltüten, angefüllt mit ärztlichen Gutachten, Protokollen und Befunden mit Name, Adresse, Arbeitsstelle und Lebenslauf der Patienten. Die Unterlagen stammen aus einer ärztlichen Begutachtungsstelle.

Der Vorfall hat zu einer energischen Untersuchung geführt. Er macht deutlich, daß die Umgestaltung des Gesundheitswesens im Ostteil der Stadt in datenschutzrechtlicher Hinsicht besondere Sorge bereitet.

Es geht dabei um die Frage, wie mit Patientendaten verfahren werden soll, wenn weite Bereiche der Gesundheitsdienste privatisiert werden.

Die Gesundheitsversorgung wurde bisher fast ausschließlich von staatlichen Stellen erbracht, sowohl in Apotheken, ambulanten „Polikliniken", Arztpraxen als auch in Krankenhäusern. Mit der Vereinigung wird das Gesundheitswesen in Ost-Berlin der bundesdeutschen Situation angeglichen. Zwar ist den staatlichen Einrichtungen durch den Einigungsvertrag eine Übergangszeit eingeräumt, aber dort ist auch festgelegt, daß die Niederlassung von Ärzten in freien Praxen zu fördern ist. Mit der Umwandlung von staatlichen Einrichtungen in private ist bereits begonnen worden.

Dadurch taucht auch das Problem auf, was mit den über die Jahre hinweg entstandenen Patientendaten einer staatlichen Arztpraxis geschehen soll, wenn diese Stelle privatisiert wird. In den Unterlagen befinden sich Informationen, die nur dem behandelnden Arzt anvertraut wurden.

Die Problematik ist vergleichbar der in der Bundesrepublik seit Jahren diskutierten beim Verkauf von Arztpraxen. Bereits beim Privatverkauf einer Arztpraxis geht man mittlerweile überwiegend davon aus, daß die Übergabe der Patientendaten ohne Einwilligung der Betroffenen unzulässig ist. Denn die ärztliche Schweigepflicht des behandelnden Arztes besteht auch gegenüber medizinischen Kollegen, die der Patient nicht konsultiert. Dies muß erst recht gelten, wenn die Weitergabe von einer staatlichen Stelle erfolgt.

Das bedeutet im Ergebnis, daß eine Übernahme der Patientenunterlagen nur dann unproblematisch ist, wenn der oder die Ärzte, die die Patienten zuvor betreut haben, selbst die Praxis übernehmen. In allen anderen Fällen können die Unterlagen nur mit Einwilligung der Patienten an den Erwerber übergeben werden.

Für die Vielzahl der Fälle, in denen medizinische Einrichtungen ohne Nachfolge aufgelöst werden, müssen Regelungen geschaffen werden, die Fälle wie den geschilderten ausschließen. Soweit die Unterlagen vernichtet werden können, muß dies auf eine Weise geschehen, die eine Offenbarung an Unbefugte ausschließt. Für die anderen Unterlagen muß die Gesundheitsverwaltung für eine angemessene Unterbringung sorgen, die für künftige Nachfragen den Zugriff sicherstellt.

Automatisierte Sozialhilfedateien

Die bezirklichen Sozialämter haben, nachdem sie lange ohne IuK-Unterstützung am Arbeitsplatz auskommen mußten (das automatisierte Sozialhilfeverfahren ist ein zentrales Batchverfahren), ihr Bemühen verstärkt, die bisher in den einzelnen Bezirken unterschiedlich und unabhängig voneinander manuell geführten Sozialhilfedateien (auch Fürsorge- oder Sozialleistungskarteien - FÜKA, SOLEIKA -) mit dem Ziel der Vereinheitlichung zu automatisieren.

Mit Hilfe der im Rahmen des SODA-Verfahrens geführten *Sozialhilfedateien* soll den bezirklichen Jugend- und Sozialämtern das Auffinden von Vorgängen erleichtert, die Zuordnung von Vorgängen ohne Aktenzeichen ermöglicht, die Zuständigkeit von Sachgebieten festgestellt und Doppelbearbeitungen und Doppelzahlungen vermieden werden. Darüber hinaus soll das eingesetzte Programm zur Erstellung von Statistiken, für die Fertigung von Serienbriefen und der Beantwortung von parlamentarischen Anfragen herangezogen werden. Zur Verhinderung der betrügerischen Mehrfachbeantragung von Sozialleistungen ist in einer späteren Phase ein überbezirklicher Datenträgeraustausch zum Zwecke des Datenabgleichs vorgesehen.

Die Federführung bei der Erprobung des Verfahrens hat das Bezirksamt Wedding übernommen.

Die in der Sozialhilfedatei gespeicherten Daten kommen aus dem Jugend- und Sozialamt. Beide Abteilungen sollen berechtigt sein, Daten telefonisch abzufragen, woraufhin Mitarbeiter der Sozialhilfedateiverwaltung mündlich die entsprechenden Auskünfte erteilen. Die Auskünfte werden in den Fällen bereichsübergreifend erteilt, in denen die Zuständigkeit für einen Hilfeempfänger zwischen den Abteilungen wechselt. Für den in einer späteren Phase geplanten überbezirklichen Datenabgleich zur Verhinderung des Unterstützungsbetruges sollen Disketten mit den verschlüsselten Daten aller seit dem letzten Abgleich neugemeldeten Hilfeempfänger ausgetauscht werden. Während des Abgleiches werden nur die bei verschiedenen Bezirksämtern doppelt gemeldeten Hilfeempfänger ausgeworfen.

Ob und in welchem Umfang dieses Modell von den anderen Bezirksämtern übernommen wird, ist zum jetzigen Zeitpunkt noch nicht abschließend geklärt.

Obwohl weder die Notwendigkeit noch die Befugnis zur Erhebung und Speicherung der unter das Sozialgeheimnis nach § 35 SGB I fallenden personenbezogenen Daten und zur Automatisierung des Verfahrens durch die Bezirksämter bestritten werden kann, stößt jedoch die Handhabung der Dateien auf datenschutzrechtliche Bedenken.

Datenverarbeitende Stelle ist jede Behörde oder sonstige öffentliche Stelle, die Daten für sich selbst verarbeitet oder durch andere verarbeiten läßt; nimmt diese unterschiedliche gesetzliche Aufgaben wahr, gilt diejenige Organisationseinheit als datenverarbeitende Stelle, der die Aufgabe zugewiesen ist.

Zwar handelt es sich bei der Sozialhilfedateiverwaltung um ein bei der Abteilung Sozialwesen angesiedeltes eigenständiges Arbeitsgebiet, jedoch werden dort Datenbestände zweier Ämter

mit unterschiedlichen gesetzlichen Aufgabenzuweisungen gespeichert, die nach dem funktionalen Behördenbegriff voneinander abgeschottet werden müssen. Eine Auskunft an eine Abteilung aus dem Datenbestand der anderen stellt deshalb datenschutzrechtlich eine Übermittlung dar. Dies setzt voraus, daß die übermittelnde Stelle im Einzelfall über die Zulässigkeit der Übermittlung entscheidet. Diese Entscheidung kann nur die Fachabteilung, in der Regel der zuständige Sachbearbeiter nach Prüfung der gesetzlichen Voraussetzungen treffen, nicht jedoch die allein mit der Verwaltung der Sozialhilfedatei betrauten Mitarbeiter.

Vorbehaltlich späterer Regelungen zur datenschutzrechtlichen Abgrenzung von Sozialleistungen, die auf unterschiedlichen Rechtsgrundlagen beruhen, halten wir es für unbedenklich, daß die Datenbestände der Abteilungen Jugend und Sozialwesen gemeinsam geführt werden, solange die Daten durch ein Ordnungsmerkmal, wie z. B. dem Aktenzeichen, einer der beiden Stellen eindeutig zugeordnet und getrennt verarbeitet werden können. Da die Sozialhilfedateiverwaltung organisatorisch der Abteilung Sozialwesen angegliedert ist, speichert diese die Daten der Abteilung Jugend im Rahmen der Auftragsdatenverarbeitung nach § 80 SGB X. Für diese Auftragsdatenverarbeitung müssen Weisungen des Auftraggebers, also der Abteilung Jugend, vorliegen, die Art und Umfang der Auskunftserteilung regeln.

Während Auskünfte an die betreffenden Abteilungen aus den eigenen Datenbeständen im Rahmen der Aufgabenerfüllung jederzeit zulässig sind, ist von der Sozialhilfedateiverwaltung bei abteilungsübergreifenden Anfragen nur auf den zuständigen Sachbearbeiter zu verweisen, damit dieser im Einzelfall die Rechtmäßigkeit der Offenbarung gemäß § 69 SGB X prüfen kann.

Der von den Bezirken in diesem Zusammenhang angestrebte regelmäßige *Datenabgleich zur Feststellung betrügerischer Mehrfachbeantragung von Sozialhilfe* ist allerdings gegenwärtig mangels einer fehlenden hinreichend konkreten Rechtsgrundlage unzulässig. Warnmeldungen vor Unterstützungsbetrügern aus Gründen der Vorbeugung vor ungerechtfertigtem Sozialhilfebezug sind im Einzelfall durchaus zulässig, jedoch darf in Not geratenen Hilfeempfängern nicht von vornherein ein gesetzwidriges Verhalten unterstellt werden. Bereits 1985 wurde Einvernehmen mit der Senatsverwaltung für Gesundheit und Soziales darüber erzielt, daß die Weitergabe zielloser Warnmeldungen mangels gesetzlicher Grundlage unzulässig ist. Die gegenseitige Unterrichtung der Sozialleistungsträger ist nur im Einzelfall und aus konkretem Anlaß zulässig.

Mittlerweile wird unter der Federführung der Senatsverwaltung für Gesundheit und Soziales die Einführung eines in allen 23 Bezirken einzusetzenden, vernetzten *Berliner Automatisierten Sozial- und Jugendhilfe-Interaktions-Systems (BASIS)* zur Bearbeitung von Sozial- und Jugendhilfeanträgen geplant. Vorgesehen ist dafür die Übernahme und Anpassung eines Verfahrens, welches für die Sozialhilfebearbeitung in westdeutschen Kommunen bereits erprobt wird. Eine Entscheidung darüber, welches Verfahren letztlich ausgewählt werden soll, steht noch aus, solange die in Frage kommenden Verfahren (PROSOZ-Bremen, PROSOZ-Herten) noch in ausgewählten Bezirken erprobt werden.

Hinsichtlich der Zuständigkeitsregelungen für die Sozial- und Jugendhilfe unterscheidet sich die Berliner Verwaltung z. B. von Bremen dadurch, daß die Zuständigkeit in der Hand der 23 Bezirke und nicht in der Hand eines zentralen Amtes liegt. Dies bedeutet, daß die bei PROSOZ vorgesehene zentrale Datenhaltung für alle Bezirke dann wegen mangelnder Rechtsgrundlage unzulässig ist, wenn bezirksübergreifend zugegriffen werden kann oder in der Zentrale ein Abgleich zwischen Daten verschiedener Bezirke zwecks Feststellung von mißbräuchlichen Mehrfachbeantragungen erfolgt.

Da wir uns beratend an der Lenkungsgruppe für das BASIS-Projekt beteiligen, werden wir unmittelbar auf die datenschutzgerechte und rechtmäßige Gestaltung des Verfahrens Einfluß nehmen können.

Datenschutz contra Denkmalschutz

Auf ungeahnte Schwierigkeiten stieß die Umsetzung von Sicherheitsmaßnahmen einer im Zuständigkeitsbereich der Senatsverwaltung für Gesundheit und Soziales angesiedelten Dienststelle, in der im großen Umfang wichtige und sensible personenbezogene Unterlagen verwaltet werden.

Bei einer bereits 1989 durchgeführten technisch-organisatorischen Prüfung wurden unzureichende *Gebäudesicherungsmaßnahmen* festgestellt, obwohl nach zwei erfolgten Einbrüchen bereits umfangreiche Sicherheitsvorkehrungen getroffen wurden. Mit Ausnahme eines Neubaus fehlte es bei allen übrigen Gebäuden an einer ausreichenden Zugangssicherung. Sicherheitsmängel bestanden im wesentlichen in allen im Erdgeschoß befindlichen Räumen, da diese lediglich über einfache und unvergitterte Fensterfronten und zum Teil veraltete, leicht zu öffnende Außentüren verfügten. Über das Gerüst einer privaten Firma bestanden darüber hinaus noch Einstiegsmöglichkeiten für die darüber liegenden Stockwerke, so daß auch diese als nicht gesichert angesehen werden mußten. Das aufgrund der Einbrüche zur Geländesicherung eingesetzte Wachpersonal konnte wegen der Unüberschaubarkeit und Größe des Grundstückes eine ausreichende Sicherheit nicht gewährleisten.

Wir haben dieser Dienststelle dringend empfohlen, zumindest die Fensterfronten zu vergittern und die äußeren Zugänge zu sichern sowie die Sicherheit der inneren Bereiche zu überprüfen. Einige Forderungen wurden inzwischen erfüllt.

Die Empfehlung hinsichtlich der Fenstervergitterung stieß jedoch aus Gründen des Denkmalschutzes auf den Widerstand des *Landeskonservators*. Die von ihm gebilligte Alternative, das Gebäude mit einbruchssicherem Glas auszustatten, würde eine Investition in Millionenhöhe bedeuten. Die dafür notwendigen Mittel könnten aller Voraussicht nach nicht zur Verfügung gestellt werden.

Da die von uns empfohlenen gebäudetechnischen Außensicherungen nicht umgesetzt wurden, haben wir dies gegenüber der Senatsverwaltung für Gesundheit und Soziales beanstandet. In der Stellungnahme der Senatsverwaltung wurde abermals darauf verwiesen, daß sie sich nicht in der Lage sehe, die erforderlichen Mittel bereitzustellen, zumal auch Bundesbehörden daran beteiligt werden müßten.

Eine zu Rate gezogene Sachverständigengruppe für technische Sicherheitseinrichtungen der Polizei hat inzwischen eine Reihe von Empfehlungen zur Gebäudesicherung ausgesprochen. Unter anderem wurde eine elektronische Freigeländesicherung vorgeschlagen, die, wenn dieses durch entsprechende personelle Ausstattung zur Überwachung des Systems ergänzt wird, eine ausreichende Sicherheit bieten würde. Die betreffende Dienststelle geht jedoch davon aus, daß zusätzliches Personal nicht eingestellt werden kann, so daß das vorgeschlagene elektronische Überwachungssystem nicht die erwünschte Sicherheit im vollen Umfang gewährleisten kann.

Aufgrund der bis jetzt ungeklärten Situation ergibt sich für uns die Schlußfolgerung, daß das unter Denkmalschutz stehende Gebäude ganz offensichtlich für die sichere Unterbringung der sensiblen Unterlagen völlig ungeeignet ist, da selbst minimale Forderungen für eine Außensicherung des Gebäudes nicht erfüllt werden können.

3.5 Inneres

Polizei und Verfassungsschutz

Im Mittelpunkt der polizeilichen Datenverarbeitung steht nach wie vor das Informationssystem Verbrechensbekämpfung (ISVB), das von der Polizei als zentrales Großrechnerverfahren betrieben wird. Dieses Informationssystem dient der Aktenverwaltung und Dokumentation polizeilichen Handelns sowie der vorbeugenden Straftatenbekämpfung. Im ISVB werden alle im Zusammenhang mit der Verbrechensbekämpfung anfallenden Informationen gespeichert, verarbeitet und den Polizeibeamten unmittelbar zur Verfügung gestellt. Daten über Verdächtige und andere Personen (Geschädigte, Anzeigenerstatter) werden gemeinsam gespeichert. Unsere Forderung nach einer deutlicheren Trennung des Zugriffs auf diese Personenkreise[24] hat der Polizeipräsident bisher nicht umgesetzt.

[24] vgl. JB 1985, S. 10

Nach einer Bereinigung der Bestände wurden in das System die Ost-Berliner Datensätze aus dem Informationssystem DORA (Dialogorientiertes Rechen- und Auskunftssystem) der ehemaligen Volkspolizei übernommen. Damit enthält ISVB am Ende des Berichtszeitraums etwa 1 800 000 Datensätze. Eine Überprüfung des Verfahrens wurde eingeleitet.

Neben diesem zentralen Verfahren gewinnen für die Berliner Polizei anwendungsspezifische IuK-Anwendungen immer mehr Bedeutung. In zwei umfangreichen Überprüfungen wurden im Berichtszeitraum gemeldete PCs der Polizei sowie das letztlich gescheiterte neue Einsatzleitsystem überprüft.

Personalcomputer im Dienst der Strafverfolgung

Für die Bewältigung inhaltlich eingrenzbarer Aufgabenbereiche der Polizei ist der Personalcomputer besonders geeignet. Seine Funktionen können auf die Bedürfnisse des einzelnen Anwenders flexibel zugeschnitten werden, ohne daß die Bedienung dieser Geräte besonderer EDV-Kenntnisse bedürfte.

Allerdings bergen Personalcomputer spezielle Risiken hinsichtlich der Sicherheit der Verarbeitung, auf die wir in früheren Jahresberichten ausführlich eingegangen sind.[25] So fehlen ohne zusätzliche Maßnahmen Möglichkeiten zur Zugriffs- und Benutzerkontrolle, zur Protokollierung, zur Funktionentrennung und zur sicheren Datenträgerverwaltung. Diese Risiken haben uns veranlaßt, den Einsatz lokaler Systeme bei der Polizei zu überprüfen. Insgesamt wurden davon 22 automatisierte Verfahren erfaßt, die auf 15 MS-DOS-Einplatzrechnern und zwei UNIX-Mehrplatzsystemen verarbeitet wurden.

Rechtlich war zu prüfen, ob sich angesichts fehlender verfassungsgemäßer Rechtsgrundlagen für die Verarbeitung personenbezogener Daten durch die Polizei Anwendungen auf den lokalen Systemen in dem Rahmen halten, der noch durch den Übergangsbonus (der nach dem Berliner Datenschutzgesetz spätestens am 31. 12. 1991 abläuft) gedeckt ist oder ob die Eingriffe in das informationelle Selbstbestimmungsrecht der Bürger damit bereits eine neue Qualität erreichen.

In der derzeitigen rechtlichen Situation hat sich die polizeiliche Datenverarbeitung auf die für ihre Aufgabenerfüllung unerläßliche Datenverarbeitung zu beschränken. Dabei ist konkret auf den jeweiligen Zweck der Datenverarbeitung abzustellen: Die Vorgangsverwaltung hat sich auf die für die Dokumentation unerläßlichen Daten zu beschränken, zur Gefahrenabwehr dürfen nur die zur Bekämpfung der jeweils konkreten Gefahrenlage unerläßlichen Daten verarbeitet werden und bei Ermittlungsverfahren ist die Datenverarbeitung auf die Daten zu beschränken, die für das konkrete Ermittlungsverfahren unerläßlich sind.

Die *organisatorische Prüfung* erstreckte sich auf Fragen des Einsatzgebietes der Rechner, auf die technische Verantwortlichkeit (Systemadministration), auf die Arbeitsplatzsituation, auf die Zugriffsberechtigungen zum System, Fragen der räumlichen und organisatorischen Systemsicherung und auf die Ordnungsmäßigkeit der Datenverarbeitung (Programmdokumentation, Freigabeverfahren, Einhaltung formeller Pflichten etc.).

Die *technische Prüfung* umfaßte Fragen der Ausstattung und Sicherheit der Hardwarekomponenten, die Verwendung von Softwareprogrammen und Sicherheitsprodukten, die damit erreichte Zugriffssicherheit sowie die Zuverlässigkeit des Paßwortverfahrens, der Benutzerberechtigungen und Eingabekontrollen.

Aus der Prüfung ergaben sich folgende Erkenntnisse:

Im Gegensatz zu manuellen Karteien bestehen beim PC vielfältige Verknüpfungs- und Auswertungsmöglichkeiten. Die personenbezogenen Daten können durch Verknüpfung mit Daten anderer Personen oder mit Sachzusammenhängen zu vollkommen anderen Bewertungen und Aussagen führen. Listen und Zusammenstellungen über bestimmte Personen, differenziert nach den verschiedensten Merkmalen, können mit einem Knopfdruck erstellt werden und zur Konstruierung und Gewinnung eines Straftatverdachts genutzt werden.

Diese Gefahr zeigt sich besonders deutlich bei PCs, auf denen mehrere Dateien zur Aufklärung einer Reihe gleichartiger Strafverfahren verarbeitet werden. Hier verschärfen sich die von Spurendokumentationssystemen (SPUDOK) bekannten Probleme, die in der Speicherung vieler nicht Tatverdächtiger und der prinzipiellen Möglichkeit liegen, daß Unschuldige aufgrund der Nutzung der umfangreichen Speicherungs- und Verknüpfungsmöglichkeiten sowie des Datenabgleichs mit anderen Datenbeständen durch eine „Verdachtsverdichtung" zu Verdächtigen werden können. Wenn eine Vielzahl von Verfahren über einen längeren Zeitraum in einer Datei geführt werden, können prinzipiell sämtliche, zu den verschiedenen Ermittlungsverfahren gespeicherten Personen, miteinander abgeglichen und verknüpft werden.

Die Prüfung hat ergeben, daß die Datenverarbeitung zur vorbeugenden Straftatenbekämpfung sich bei den meisten Dateien nicht im Rahmen der verfassungsrechtlich während der Übergangszeit gebotenen Beschränkungen hält. Bei mehreren Dateien war festzustellen, daß Daten über Unbeteiligte („andere Personen") in unzulässigem Umfang gespeichert werden. Bei einigen Dateien war die Speicherung Tatverdächtiger und Beschuldigter zu weitgehend: Entweder wurde die Datensammlung nicht wie vorgesehen auf schwerwiegende Delikte beschränkt, es wurden nicht erforderliche Angaben zu einem Tatverdächtigen gespeichert oder die Speicherung erfolgte nur aufgrund von „Warnhinweisen".

Bei den Dateien der Polizeitechnischen Untersuchungsstelle, die zum Zweck der Begutachtung bestimmter Tatmittel oder Tatspuren geführt werden, ist als grundsätzliches datenschutzrechtliches Problem festzustellen, daß hier personenbezogene Daten über Verdächtige oder Geschädigte gespeichert werden, ohne daß dies für die Aufgabenerfüllung unmittelbar erforderlich ist. Hier sind für die verwaltungstechnische Abwicklung der Gutachtenaufträge Verfahrensweisen ohne Personenbezug zu finden.

Bei mehreren der geprüften Dateien wurden die Daten zu lange gespeichert. Entweder wird der Fristbeginn auf einen späteren Termin gelegt als in den Richtlinien zur Führung kriminalpolizeilicher personenbezogener Sammlungen (KpS-Richtlinien) vorgeschrieben oder sind die Löschungsfristen mangels Datumseingabe nicht feststellbar oder sind die Aufbewahrungsfristen ohnehin zu lang bemessen.

Ein bereits seit Jahren gerügter Mangel ist, daß bei vielen der überprüften Dateien, die der vorbeugenden Straftatenbekämpfung dienen sollen, der Ausgang des staatsanwaltschaftlichen oder gerichtlichen Verfahrens nicht in Erfahrung gebracht wird. Es ist deshalb davon auszugehen, daß in den Dateien Personen erfaßt sind, bei denen kein Tatverdacht mehr besteht.

Die Administration und Betreuung der in verschiedenen Bereichen der Polizei eingesetzten lokalen Systemen erfolgt in gutem Zusammenwirken zwischen der Abteilung Datenverarbeitung der Polizei und den lokalen Anwendern und entspricht den Anforderungen, die ein ordnungsgemäßer PC-Einsatz stellt.

Dennoch wurden Mängel der ordnungsgemäßen Datenverarbeitung festgestellt:

Meist fand kein ordnungsgemäßes Freigabeverfahren durch den Anwender statt. Programmdokumentationen waren nicht entsprechend interner polizeilicher Anweisungen bei den Anwendern verfügbar. Auch die Verwaltung externer Datenträger (Disketten) wies Mängel auf, da in der Regel weder die Vollständigkeit der vorhandenen Datenträger noch deren Authentizität in Bezug auf die jeweilige Anwendung nachweisbar waren. Zwar werden in der Regel bei Einplatz-PCs zusätzliche Sicherheitssysteme eingesetzt, jedoch meist nicht in einer Weise, die die Sicherheitsfunktionen dieser Systeme voll zur Geltung bringt.

Bei den geprüften Mehrplatzsystemen mit UNIX-Betriebssystemen wurden Mängel hinsichtlich der Programm-, Datei- und Benutzerverwaltung festgestellt. Da die genannten Betriebssysteme hinreichende Sicherheitsfunktionen zur Verfügung stellen, liegen hier die Ursachen hauptsächlich in der unzureichenden Systemverwaltung. Die festgestellten Defizite reichen von mangelhaft differenzierten Benutzerprofilen (gemeinsames Paßwort für alle Benutzer), nicht erforderlichen Zugriffsmöglichkeiten auf die Betriebssystemebene durch die Benutzer bis zur fehlenden Dokumentation.

[25] zuletzt im Jahresbericht 1989, S. 15 ff.

Die Überprüfung zeigt, daß bei allem Gewinn, den der Einsatz lokaler Anwendungen für die polizeiliche Arbeit bringen kann, sowohl den Aspekten der Rechtmäßigkeit des verarbeiteten Datenumfangs als auch der Ordnungsmäßigkeit noch mehr Beachtung geschenkt werden muß, als dies bisher geschehen ist.

Einsatzleitsystem ELSY

Zur Ablösung der veralteten technischen Ausstattung der Funkbetriebszentrale plante der Polizeipräsident die Einführung eines modernen computergesteuerten Einsatzleitsystems (ELSY). Im Auftrag des Unterausschusses Datenschutz des Ausschusses für Inneres, Sicherheit und Ordnung des Abgeordnetenhauses von Berlin haben wir eine Überprüfung des Konzeptes und des bereits installierten und im Test befindlichen Systems durchgeführt.

Eine detaillierte Darlegung der Prüfergebnisse, die im März 1990 dem Polizeipräsidenten und dem Unterausschuß Datenschutz mitgeteilt wurden, erübrigt sich deshalb, weil der Polizeipräsident von der Inbetriebnahme von ELSY mittlerweile Abstand nehmen mußte. Unabhängig davon, daß generell die rechtlichen Voraussetzungen für ELSY fehlten, zeigte sich, daß es trotz langjähriger Entwicklungsarbeit nicht gelungen war, ein funktionstüchtiges System zu entwickeln. Im übrigen hatte der Vertreter des Polizeipräsidenten vor dem Unterausschuß erklärt, daß die Erweiterung Von ELSY auf alle 23 Bezirke nicht möglich wäre.

In unserem Prüfbericht wurde der Sinn, die Erforderlichkeit und das Vorhandensein der rechtlichen Voraussetzungen für die Erfassung und Speicherung bestimmter personenbezogener Daten, deren Auswertbarkeit durch flexible relationale Datenbanksysteme sowie das Zusammenwirken mit anderen Systemen der Verwaltung problematisiert. Es wurden Empfehlungen zur Bereinigung kritischer Feststellungen abgegeben. Ferner wurden technische Verbesserungen für die Zugriffs- und Benutzerkontrolle am System angeregt.

Die von uns vorgebrachten Gesichtspunkte sollten bei den nun erforderlichen Neuplanungen Berücksichtigung finden. Insbesondere muß jedenfalls für die geplanten Verknüpfungen mit anderen Verfahren, die erst den eigentlichen Rationalisierungsgewinn ausmachen, rechtzeitig für eine ausreichende Rechtsgrundlage gesorgt werden.

Keine Rechtsgrundlagen für die polizeiliche Datenverarbeitung

Obwohl wir dies seit Jahren anmahnen[26], fehlen für die polizeiliche Datenverarbeitung noch immer die erforderlichen gesetzlichen Grundlagen. Mehr als 7 Jahre nach dem Volkszählungsurteil des Bundesverfassungsgerichts ist zweifelhaft, ob für die Erhebung und Nutzung personenbezogener Daten durch die Polizei noch der Übergangsbonus strapaziert werden kann. Für das Land Berlin haben wir bereits mehrfach darauf hingewiesen, daß der Übergangsbonus aus unserer Sicht mit dem Ende der letzten Legislaturperiode abgelaufen ist[27]. Der Gesetzgeber muß unverzüglich das Allgemeine Sicherheits- und Ordnungsgesetz (ASOG) novellieren, um endlich Rechtsklarheit in diesem Bereich zu schaffen.

Dies bestätigen auch zwei Urteile des Bundesverwaltungsgerichts vom 20. Februar 1990[28], wenn sich auch die Ausführungen des Gerichts streckenweise unbeeindruckt von der Entwicklung des Datenschutzrechts zeigen. Obwohl das Bundesverfassungsgericht unmißverständlich gesetzliche Rechtsgrundlagen gefordert hat, die präzise die Voraussetzungen und den Umfang der Datenverarbeitung regeln, und obwohl Landes- und Bundesgesetzgeber dieser Forderung zunehmend durch bereichsspezifische Gesetze nachkommen, hält das Bundesverwaltungsgericht die allgemeinen Aufgabenzuweisungsnormen des ASOG (wie auch des alten Bundesverfassungsschutzgesetzes) für hinreichend bestimmte Gesetzesgrundlagen: eine nicht nur wegen des Bestimmtheitsgebots, sondern auch wegen der verfassungsrechtlich gebotenen Trennung von Aufgabenzuweisungs- und Befugnisnormen mehr als bedenkliche Feststellung. Der Schluß von der Aufgabe auf die Befugnis ist eine verfassungsrechtlich nicht haltbare Konstruktion. Sie ist schon vor über 90 Jahren von Otto Mayer, dem Gründer der deutschen Verwaltungsrechtslehre, als „Folgerungsweise des Polizeistaats" gekennzeichnet und abgelehnt worden, weil sie mit dem Rechtsstaatsprinzip unvereinbar ist. Das Bundesverwaltungsgericht zieht denn auch noch sicherheitshalber den Übergangsbonus als Rechtfertigung für die Datenverarbeitung bei.

Das Bundesverwaltungsgericht hat in diesen Urteilen auch weitere Thesen vertreten, die der Bedeutung der informationellen Selbstbestimmung nicht gerecht werden. Es hat aus dem Grundgesetz ein Geheimhaltungsrecht der Polizei und des Verfassungsschutzes abgeleitet und damit nicht nur die Rechtsprechung des Bundesverfassungsgerichts, sondern auch die Entwicklung der neueren Gesetzgebung im Polizeibereich ignoriert.

Im Gegensatz zum Bundesverfassungsgericht, das den Auskunftsanspruch des Bürgers als einen wesentlichen Bestandteil des Rechts auf informationelle Selbstbestimmung ansieht, räumt das Bundesverwaltungsgericht dem Geheimhaltungsinteresse pauschal Vorrang ein und läßt Auskünfte an Bürger nur in Ausnahmefällen – für die der Bürger darlegungspflichtig ist – zu. Damit nicht genug: Auch eine Begründung, warum Auskunft verweigert wird, brauchen Polizei und Verfassungsschutz dem Bürger nicht zu geben.

Das Bundesverfassungsgericht hat demgegenüber im Volkszählungsurteil klargestellt, daß das Auskunftsrecht zu den grundlegenden Datenschutzrechten des Bürgers gehört, da eine Gesellschaftsordnung, in der die Bürger nicht mehr wissen können, wer was wann und bei welcher Gelegenheit über sie weiß, nicht mit dem Grundrecht auf informationelle Selbstbestimmung zu vereinbaren wäre. Entgegen der Auffassung des Bundesverwaltungsgerichts hat der Betroffene – auch gegenüber den Sicherheitsbehörden – einen aus dem allgemeinen Persönlichkeitsrecht folgenden Anspruch auf Auskunftserteilung, der nach Einzelfallabwägung nur eingeschränkt werden darf, soweit es zum Schutz öffentlicher Interessen unerläßlich ist.

In dieser Situation ist es umso dringlicher, daß ein ASOG das informationelle Selbstbestimmungsrecht der Berliner Bürgerinnen und Bürger gegenüber unangemessenen Einschränkungen sichert.

Polizeiliche Registrierung von Prostituierten

Die Prostituiertenorganisation „Hydra" machte auf folgenden Fall aufmerksam: Eine Frau war wegen Zuhälterei angeklagt worden, weil sie Prostituierten telefonisch Hausbesuche bei Freiern vermittelt habe. Im Zuge der Ermittlungen wurde ihr Adreßbuch beschlagnahmt. Daraus suchte die Polizei drei Zeuginnen heraus. Kein Zufall, wie sich später bei der gerichtlichen Zeugenvernehmung herausstellte. Alle drei Zeuginnen hatten ehemals als Prostituierte gearbeitet. Ein vor Gericht vernommener Polizeibeamter gab an, daß die Polizei die Namen aus dem Adreßbuch mit Daten von Prostituierten abgeglichen hat, die die Kripo in einer Kartei sammelt.

Wir haben diese Kartei, die den Namen „Zuhälterei, Menschenhandel und ähnliche Delikte" hat, geprüft. Darin sind etwa 5 000 Prostituierte registriert. Es werden auch undifferenziert Daten von Frauen gesammelt, die keiner Straftat verdächtig sind und lediglich der Prostitution nachgehen. Diese Speicherungen sind rechtswidrig. Wir haben den Innensenator aufgefordert, die Kartei umgehend zu bereinigen. Der Unterausschuß Datenschutz des Abgeordnetenhauses hat sich ebenfalls mit dieser Problematik befaßt. Eine Einigung mit der Polizei konnte jedoch bisher nicht erreicht werden.

Die Senatsverwaltung für Inneres lehnt die Löschung der Daten dieser Frauen ab, da sie zur vorbeugenden Straftatenbekämpfung erforderlich seien. Als Begründung wird angeführt, daß die Prostitution regelmäßig in einem Milieu stattfinde, das von Straftaten wie Zuhälterei, Menschenhandel, Förderung der Prostitution und der damit einhergehenden Begleitkriminalität gekennzeichnet sei. Wegen der fehlenden Anzeige- und Aussagebereitschaft müßten bereits im Vorfeld der Strafverfolgung Strukturen des Milieus bekannt sein. Prostituierte müßten polizeilich registriert werden, da sie den Kontakt zwischen Tatverdächtigen herstellen und in das kriminelle Milieu eingebunden seien.

[26] erstmals JB 1983, Ziff. 2.5.
[27] vgl. JB 1988, Ziff. 1.2 und JB 1987, Ziff. 5.3.
[28] 1 C 29/86 und 1 C 42/83.

Demgegenüber halten wir daran fest, daß die Daten aller Personen in dieser Kartei zu löschen sind, die keiner Straftat verdächtig sind.

Die Registrierung dieses Personenkreises hält sich nicht im Rahmen der rechtmäßigen Aufgabenerfüllung der Polizei. Die Daten der Frauen werden weder zur Strafverfolgung im Rahmen eines konkreten Ermittlungsverfahrens gespeichert, noch dienen sie der Gefahrenabwehr. Die Ausübung der Prostitution ist weder ausreichend für die Annahme einer im Einzelfall unmittelbar bevorstehenden Gefahr, noch ein Anhaltspunkt für die künftige Begehung einer Straftat durch die Betroffene. Die Frauen werden ohne Einzelfallprüfung aufgrund einer pauschalen Entscheidung lediglich wegen der (nicht strafbaren) Prostitution registriert. Mit der gleichen Begründung könnten die verschiedensten Personen (z. B. Angestellte, Betreiber oder Gäste von Nachtbars, Kunden von Prostituierten, Besucher einer Boxkampfveranstaltung) erfaßt werden. Die polizeiliche Inanspruchnahme von Personen, die nicht „Störer" im polizeirechtlichen Sinn sind, d.h., von Personen, die keine Gefahr für die öffentliche Sicherheit und Ordnung verursachen, ist aber nach den Prinzipien des Polizeirechts nur in den Fällen des Notstandes zulässig. Ausnahmen sind abschließend gesetzlich geregelt (z. B. die Identitätsfeststellung gem. § 15 ASOG). Soweit - wie hier der Fall - konkrete gesetzliche Regelungen fehlen, die bei Datenspeicherungen vom Erfordernis der konkreten Gefahr absehen und Eingriffsvoraussetzungen sowie den betroffenen Personenkreis selbständig regeln, ist die Inanspruchnahme von „Nichtstörern" unzulässig. Dahinter steht der anerkannte Grundsatz, daß unbescholtenen Bürgern, die weder durch eine Straftat noch durch Störung der öffentlichen Sicherheit oder Ordnung Anlaß zu polizeilichen Eingriffen geboten haben, grundsätzlich das Recht zusteht, vom Staat in Ruhe gelassen zu werden. Frauen, die der Prostitution nachgehen, haben da keine geringeren Rechte.

Erkennungsdienstliche Behandlung: schnelle Strafe?

Eine 17jährige junge Frau wurde bei dem Diebstahl eines Schokoladenriegels ertappt. Die Polizei sah sich veranlaßt, sie durch Abnahme von Fingerabdrücken und Foto-Aufnahmen erkennungsdienstlich zu behandeln und eine Kriminalakte über sie anzulegen.

Ein 14jähriger Junge, der sich mit zwei Freunden auf dem Nachhauseweg befand, wurde von der Polizei angehalten und einer erkennungsdienstlichen Behandlung unterzogen, weil sie sich in einer Gegend befanden, in der Jugendbanden aktiv sind. Konkrete Anhaltspunkte dafür, daß der Junge einer Jugendbande angehört, bestanden nicht.

Zwei Fälle von Überreaktionen der Polizei, die nicht zu rechtfertigen sind.

Bei der jungen Frau wurde die erkennungsdienstliche Behandlung nach § 81 b 2. Alt. StPO angeordnet. Diese erheblich in das Persönlichkeitsrecht eingreifende Maßnahme kommt auch nach der ständigen Rechtsprechung des Bundesverwaltungsgerichts nur in Betracht, wenn eine entsprechend schwere Straftat begangen wurde und Wiederholungsgefahr besteht. Die erkennungsdienstliche Behandlung wegen eines Bagatelldelikts, wie Diebstahl eines Schoko-Riegels, verstößt eklatant gegen den verfassungsrechtlichen Grundsatz der Verhältnismäßigkeit. Es drängt sich der Verdacht auf, daß die erkennungsdienstliche Behandlung zur Bestrafung und Disziplinierung der jungen Frau mißbraucht werden sollte.

Der 14jährige Junge wurde nach § 16 Abs.1 Nr.3 ASOG zur Verhütung von Straftaten erkennungsdienstlich behandelt. Die Eingriffsvoraussetzung dieser Norm ist sehr weit gefaßt und setzt keine konkrete Gefahr voraus. Deshalb ist eine rechtsstaatliche Begrenzung und strikte Beachtung des Übermaßverbots bei der Anordnung dieser Maßnahme erforderlich. Die Durchführung der erkennungsdienstlichen Behandlung nach § 16 Abs. 1 Nr. 3 ASOG muß sich auf einen konkreten, in der Person des Betroffenen begründeten Anlaß stützen. Ein derartiger Anlaß kann nur ein Verhalten des Betroffenen sein, das auf die Begehung bestimmter Straftaten abzielt oder mit solchen konkret in Zusammenhang steht. Solche Anhaltspunkte lagen nicht vor.

Sammlungen und Wandlungen beim Landesamt für Verfassungsschutz

Nach den vielen Prüfungen beim Landesamt für Verfassungsschutz, an denen auch wir beteiligt waren, haben sich erhebliche Änderungen in dieser Behörde ergeben. Gleichwohl hat sich die Zahl der vom Berliner Landesamt gespeicherten Datensätze im Berichtszeitraum nicht verringert, sondern eher erhöht. Dies liegt an dem im Zusammenhang mit der Arbeit des Untersuchungsausschusses in der vergangenen Legislaturperiode ergangenen Löschungsverbot. Es führt zunehmend zu Beschwerden und Unverständnis bei betroffenen Bürgern. Es ist den Betroffenen nicht vermittelbar, daß ihre zu löschenden Daten, die in keinem Zusammenhang mit dem Auftrag des damaligen Untersuchungsausschusses stehen, weiter beim Landesamt gespeichert werden müssen. Wir halten diesen Zustand nicht mehr für tragbar und empfehlen eindringlich, das Verbot zumindest insoweit aufzuheben, als hierdurch die inhaltlichen Fragen des Untersuchungsausschusses des Abgeordnetenhauses nicht betroffen sind.

Dessen ungeachtet waren erhebliche Wandlungen in der Arbeit des Landesamtes für Verfassungsschutz zu registrieren, die wichtige Schritte zu mehr Transparenz und Vertrauensbildung bei der Bevölkerung darstellen.

So wurde unserer Empfehlung nachgekommen und eine Fachaufsicht bei der Senatsverwaltung für Inneres eingerichtet und das Landesamt in eine nachgeordnete Behörde umgewandelt. Die Einrichtung einer inneren Revision im Verfassungsschutz, die gleichzeitig die Aufgaben des behördlichen Datenschutzbeauftragten wahrnimmt, ist in Vorbereitung.

Von wesentlicher Bedeutung ist die Änderung des Verfahrens bei Auskunftsersuchen von Bürgern. Eine Arbeitsanweisung zur Auskunftserteilung (vgl. JB 89, Ziff. 2.2, S. 8) wurde vorläufig in Kraft gesetzt. Diese im Bundesgebiet einmalige Auskunftsanweisung ist ausdrücklich zu begrüßen. Die Praxis der Auskunfterteilung und Akteneinsicht beim Landesamt hat sich offenbar eingespielt und bewährt. An uns wurde im Berichtszeitraum nur ein Fall herangetragen, in dem das Landesamt die Auskunft wegen vorrangiger Geheimhaltungsinteressen verweigert hat.

Auch auf anderen Gebieten wurden erhebliche Anstrengungen unternommen, daß auch bei unserer Prüfung festgestellte Vorschriftendefizit zu beheben.

Weitere von uns geforderte Maßnahmen, insbesondere eine umfassende Aktion zur Bereinigung der umfänglichen nicht (mehr) rechtmäßig geführten Unterlagen und die Entwicklung einer Anweisung zur ordnungsgemäßen Aktenführung, wurden noch nicht realisiert. Wir gehen aber davon aus, daß dies demnächst erfolgen wird.

So begrüßenswert diese Ansätze sind, sie ersetzen auch hier nicht die erforderlichen gesetzlichen Regelungen zum Umgang mit personenbezogenen Daten beim Landesamt. Es ist eine vordringliche Aufgabe für die kommende Legislaturperiode, auch im Land Berlin ein das informationelle Selbstbestimmungsrecht hinreichend berücksichtigendes Verfassungsschutzgesetz zu verabschieden.

Einwohnerwesen, Wahlen, Statistik

Im Mittelpunkt dieser sich in besonderem Maße dem Bürger zuwendenden Verwaltungsbereiche steht die Registrierung des Einwohners durch die Meldebehörde, in Berlin das Landeseinwohneramt.

Zu diesem Zweck führt die Meldebehörde das Melderegister, das folgende Zwecke erfüllt:

- Feststellung und Nachweis der Grunddaten wie z. B. Familienname, Vorname, Anschrift, Staatsangehörigkeit;
- Feststellung und Nachweis der Daten, die unmittelbar an die Identität und Wohnung anknüpfen, z. B. das Vorliegen von Paßversagungsgründen, Name und Anschrift des Wohnungsgebers und Angaben, ob der Betroffene erwerbstätig ist;
- Die Erreichbarkeit der Bürger untereinander sicherzustellen und Auskünfte an Private zu erteilen.

Mit Stand vom Dezember 1990 sind in der Einwohnerdatenbank 2 805 999 Datensätze gespeichert.

Im Laufe dieses Jahres wird der Einwohnerbestand der Ostberliner Bezirke in die Einwohnerdatenbank zu übernehmen sein, der bisher noch im oben beschriebenen ZER gespeichert ist. Wir werden eine umfassende Prüfung des Bestandes beim Landeseinwohneramt vornehmen, sobald die Übernahme abgeschlossen ist.

Novellierungsbedarf des Meldegesetzes

In der neuen Legislaturperiode wird das Meldegesetz in einigen Punkten zu ändern sein. Im folgenden werden einige Fallkonstellationen dargestellt, die neu geregelt werden sollten.

Die vermißte Großmutter

Anfang des Jahres meldete eine Berliner Zeitung folgenden Text: Eine alte Dame wird bewußtlos in ein Krankenhaus eingeliefert. Die Angehörigen hatten bereits Vermißtenanzeige bei der Polizei erstattet und könnten angeblich „wegen des Datenschutzes" nicht unterrichtet werden.

Hier wurde der Datenschutz einmal wieder für etwas verantwortlich gemacht, das von anderer Seite zu vertreten ist.

Bereits 1985 während des Gesetzgebungsverfahrens zur Novellierung des Berliner Meldegesetzes haben wir auf diese Problematik hingewiesen. Wir haben damals den Vorschlag gemacht, daß jeder Bürger die Möglichkeit erhalten sollte, im Melderegister die Information speichern zu lassen, wer benachrichtigt werden soll, falls er bei einem Unglücksfall schwer verletzt oder gar getötet wird. Dieser Vorschlag wurde abgelehnt.

Auf Grund der Vorgaben des Melderechtsrahmengesetzes erhalten im Melderegister volljährige Personen einen eigenen Datensatz, der getrennt ist von denen ihrer Eltern. Es ist denkbar, daß jemand bei einem Unfall mit tragischen Folgen zunächst nicht die nächsten Verwandten damit konfrontiert sehen möchte, sondern daß engste Freunde zuerst darüber Mitteilung erhalten sollen. Gerade in einer Zeit, in der es viele nicht-eheliche Lebensgemeinschaften gibt, muß den Bürgern diese Möglichkeit eingeräumt werden.

Bei der anstehenden Novellierung des Berliner Meldegesetzes sollte unser Vorschlag wieder aufgegriffen werden.

Gegen die Regelungen über die *Krankenhaus- und Hotelmeldepflicht* sind ebenfalls schon seit Jahren erhebliche Bedenken vorgetragen worden. Hier handelt es sich um materielles Polizeirecht, dessen Regelung im Melderecht verfehlt ist. Polizeiliche Datenverarbeitung setzt voraus, daß Gefahren abgewendet oder Straftaten verfolgt bzw. verhütet werden sollen. Es kann nicht unterstellt werden, daß bei Hotelgästen und Krankenhauspatienten diese Voraussetzungen regelmäßig vorliegen.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat sich im Oktober 1990 eindeutig gegen diese Meldepflichten ausgesprochen.*) Bei der Novellierung des Berliner Meldegesetzes sind diese Regelungen ersatzlos zu streichen; für konkret beschriebene Einzelfälle könnte das künftige ASOG angemessene Regelungen enthalten.

Nach § 28 Abs. 3 Satz 1 Berliner Meldegesetz darf das Landeseinwohneramt eine Melderegisterauskunft über eine Vielzahl nicht namentlich bezeichneter Einwohner *(Gruppenauskunft)* nur erteilen, soweit sie im öffentlichen Interesse liegt. Die Meldebehörde hat der Senatsverwaltung für Inneres gem § 28 Abs. 3 Satz 5 Berliner Meldegesetz den Antrag auf Gruppenauskunft zur Entscheidung über das Vorliegen des öffentlichen Interesses vorzulegen.

Bei einem Auskunftsersuchen eines Vermieters (Grundstücks- oder Wohnungseigentümers bzw. Hausverwalters) über die Namen der in seinem Gebäude wohnhaften Mieter liegt nach Auffassung der Senatsverwaltung für Inneres das öffentliche Interesse vor, weil nach § 13 Berliner Meldegesetz der Wohnungsgeber oder sein Beauftragter verpflichtet sei, bei der An- oder Abmeldung mitzuwirken. Durch die Nebenmeldepflicht entstehe ein öffentlich-rechtliches Verhältnis zwischen Wohnungsgeber und Meldebehörde. Die Gruppenauskunft diene der Motivation des Wohnungsgebers zur Erfüllung seiner Mitwirkungspflicht und sei darüber hinaus ein geeignetes und rechtlich nicht zu beanstandendes Instrument, um aufgrund entsprechender Anzeigen der Wohnungsgeber Unrichtigkeiten des Melderegisters berichtigen zu können. Demgegenüber liege bei einem Auskunftsersuchen über die Namen bzw. Anzahl bei den Mietern gemeldeten Untermietern kein öffentliches Interesse vor, weil das Auskunftsersuchen in diesen Fällen vornehmlich unter zivilrechtlichen Gesichtspunkten erfolge.

Diese Auffassung teilen wir nicht. Diese Begründung bestätigt nicht nur die auch von uns im Gesetzgebungsverfahren vorgebrachte Befürchtung, über die Bestimmung des § 13 Meldegesetz sollten die Vermieter zu Erfüllungsgehilfen der Ordnungsbehörden gemacht werden, sondern gestattet dem Vermieter darüber hinaus auch die Nutzung der Meldedaten zu eigenen Zwecken.

Will der Gesetzgeber derartige Datenübermittlungen gestatten, muß er sie in Form eines speziellen Auskunftsanspruchs in § 13 Meldegesetz regeln.

Diese und eine Reihe anderer Fragen, bei denen ein Regelungsbedarf besteht, sind der Senatsverwaltung für Inneres bekannt. Wir gehen davon aus, daß im künftigen Meldegesetz angemessene Regelungen gefunden werden.

Unerwünschte Geburtstagsgrüße

Ein Petent hat verwundert vorgetragen, daß seine Mutter von zwei großen Parteien Glückwunschbriefe zu ihrem 85. Geburtstag erhalten hat. Weil seine Mutter in keiner Partei und auch nicht in einer Sozialkommission oder sonst auf kommunaler Ebene tätig ist, war der Familie völlig unklar, wie die Parteien Kenntnis von dem anstehenden Geburtstag haben konnten. Auf entsprechende Nachfragen des Petenten hat der Kreisverband der einen Partei erklärt, sie entnimmt die Geburtstage alten Wählerlisten, der Kreisverband der anderen, sie erhalte sie vom Sozialamt.

Wir haben beim zuständigen Bezirksamt festgestellt, daß aufgrund einer Anfang der 70er Jahre getroffenen Festlegung des Sozialausschusses den beiden Parteien sowie einer Kirchengemeinde jeweils monatlich die anstehenden Geburtstage der Bewohner des Bezirks durch die Abt. Sozialwesen mitgeteilt werden. Dabei handelt es sich um die 80sten, 85sten, 90sten und die folgenden Geburtstage.

Dieses Verfahren haben wir beanstandet. Nach § 26 Abs. 2 Meldegesetz i. V. m. § 3 Nr. 1 DVO-Meldegesetz und der Nr. 1 der Anlage zu § 3 Nr. 1 DVO-Meldegesetz werden den zuständigen Stellen der Bezirksämter bei bestimmten Anlässen u.a. das Geburtsdatum sowie Namen und Anschriften von betreffenden Einwohnern des Bezirks übermittelt. Die Zwecke und die Empfänger dieser Daten sind in Nr. 1 der Anlage zu § 3 DVO-Meldegesetz festgeschrieben. Zu diesen Zwecken gehört die Ehrung von Altersjubilaren (der Vollendung des 80sten, 85sten, 90sten und jeweils weiteren Lebensjahres) durch die zuständige Stelle des Bezirksamtes. Empfänger ist ausschließlich die zuständige Stelle des Bezirksamtes, hier die Abt. Sozialwesen. Eine Weitergabe dieser Daten an Dritte ist mit dem Zweckbindungsgebot nach § 25 Meldegesetz nicht vereinbar und daher unzulässig.

Das Bezirksamt hat dieses Verfahren mit Beginn des Jahres 1990 eingestellt.

Unabhängig davon hat eine der beiden Parteien auch gegenüber der Senatsverwaltung für Inneres bestätigt, daß für die Gratulationsschreiben der Kreisverbände Auszüge aus den Wählerlisten verwendet werden, die den Parteien für die Wahl 1979 zur Verfügung gestellt wurden. Diese enthielten noch die Geburtsdaten und waren noch nicht mit den seit der Novellierung des Berliner Meldegesetzes im Jahre 1985 vorgeschriebenen Auflagen des § 29 verbunden.

Dieser Fall belegt exemplarisch, wie wichtig und richtig das Festschreiben des Zweckbindungsgebotes und der Auflagen ist, die Listen innerhalb einer Woche nach dem Wahltag zu vernichten.

Meldestelle beschwert sich beim Chef

Ein Bürger will sich bei seiner Meldestelle melden und gerät in eine Auseinandersetzung mit dem Meldestellenleiter. Am nächsten Tag spricht ihn sein Vorgesetzter auf diese Sache an und teilt ihm mit,

*) vgl. Anlage 1.10

der Meldestellenleiter habe ihn angerufen und sich über ihn beschwert. Die Kenntnis über den Vorgesetzten des Bürgers hatte der Meldestellenleiter aus seinen Akten. Darin war nämlich eine Auskunftssperre enthalten, die wegen der dienstlichen Aufgaben des Bürgers verfügt wurde. In diesem Zusammenhang war auch seine Dienststelle angegeben.

Die Nutzung dieser Angaben zu persönlichen Zwecken, nämlich um sich über einen Bürger bei seinem Vorgesetzten zu beschweren, ist unzulässig. Diese Angabe über die Dienststelle darf nur für die Entscheidung über die Auskunftssperre verwertet werden. Jede andere Nutzung ist eine unzulässige Zweckentfremdung dieser Angaben.

Das Landeseinwohneramt hat eingeräumt, daß keine dienstlichen Belange vorgelegen hatten, die diese Vorgehensweise zugelassen hätten. Der Mitarbeiter wurde eingehend über die Sach- und Rechtslage belehrt und ist aufgefordert worden, künftig solche Anrufe zu unterlassen.

Wahlen zum Deutschen Bundestag und zum Abgeordnetenhaus

Wie schon bei den vergangenen Wahlen wurde wiederholt die Frage an uns herangetragen, wie die *Parteien* an die Anschriften der Wahlberechtigten gelangt seien.

Nach dem Berliner Meldegesetz darf die Meldebehörde Parteien im Zusammenhang mit den Wahlen zum Abgeordnetenhaus in den 6 Monaten vor der Wahl die Namen und Anschriften von Wahlberechtigten mitteilen. Dies kann dazu führen, daß Parteien, mit deren politischen Zielsetzung sich die Einwohner möglicherweise in keiner Weise identifizieren wollen, komplette Register der Wahlberechtigten erhalten. Wir hatten daher bei den Beratungen zum Meldegesetz 1985 gefordert, den Bürgern ein Widerspruchsrecht gegen die Weitergabe ihrer Daten an Parteien einzuräumen, damit sie selbst über die Zusendung von Wahlwerbung entscheiden können. Diese Lösung ist in § 29 Abs. 1 Meldegesetz umgesetzt worden. Es ist ferner ausdrücklich vorgesehen, daß die übermittelten Daten nur für die Wahlwerbung verwandt werden dürfen und innerhalb einer Woche nach dem Wahltag zu vernichten sind.

Das Landeseinwohneramt hat, wie bei den letzten Wahlen auch, 1990 durch öffentliche Bekanntmachung darauf aufmerksam gemacht, daß die Wahlberechtigten ein Widerspruchsrecht innerhalb einer bestimmten Frist gegen die Weitergabe der Daten an die politischen Parteien zum Zwecke der Wahlwerbung haben.

Eine Übermittlung der Wählerdaten vor Ablauf der festgesetzten Widerspruchsfrist ist datenschutzrechtlich unzulässig, da damit das Recht der betroffenen Bürger, die Herausgabe ihrer Daten zu untersagen, mißachtet würde. Die Meldebehörde ist zwar an die gesetzte Frist nicht gebunden, sie kann sie unter Berücksichtigung des durch die Veröffentlichung geschaffenen Vertrauenstatbestandes verkürzen. Der Vertrauensschutz kann jedoch nur entfallen, wenn die Fristverkürzung oder -aufhebung rechtzeitig und in geeigneter Weise – mindestens im Amtsblatt, wie die ursprüngliche Veröffentlichung – bekannt gemacht wird, damit die Wahlberechtigten die Möglichkeit haben, sich darauf einzustellen.

Aufgrund einer Bürgerbeschwerde haben wir allerdings festgestellt, daß das Landeseinwohneramt die Listen bereits am 12. Oktober 1990, also vor Fristablauf zusammengestellt hat. Die danach bis zum Fristablauf eingehenden Widersprüche wurden nicht mehr berücksichtigt. Diese Vorgehensweise haben wir beanstandet.

Schwierigkeiten warf die Aufstellung eines *Wählerverzeichnisses* für ganz Berlin auf. Der Landeswahlleiter stand bereits im September, also vor der Vereinigung, vor dem Problem, Doppelstimmabgabem zu verhindern, um Wahlanfechtungsgründe auszuschließen.

Viele Bürger, die im Zuge der Grenzöffnung den Ostteil der Stadt verlassen und sich im Westteil niedergelassen haben, wurden auch nach der Anmeldung im Westen im Osten noch mit dem Hauptwohnsitz geführt und hätten damit zweimal wählen können. Um dies zu vermeiden, wollte das Statistische Landesamt den Einwohnerdatenbestand Ost mit dem Melderegister abgleichen. Dazu wurde zwischen dem Statistischen Amt der DDR und dem Landeswahlleiter unter Beteiligung des Ministeriums des Innern der DDR vereinbart, einen Abzug von wahlrelevanten Teilen des Einwohnerdatenspeichers für Berlin (Ost) (Personenkennzahl, Familienname, Vorname, Titel, akademische Grade, Geburtsort, -kreis, -land, Hauptwohnung, Staatsbürgerschaft, Hauptwohnung, Wohnbezirks-, Straßennummer, Prüfziffer) an das Statistische Landesamt zu geben, das im Auftrag des Landeswahlleiters arbeitet. Diese Auszüge sollten vom Statistischen Landesamt mit dem Berliner Melderegister abgeglichen werden.

Die Durchführung der Wahlen, insbesondere die Erstellung der Wählerlisten und das Ausdrucken der Wahlbenachrichtigungskarten obliegt nach den Wahlvorschriften den Gemeinden, in Berlin den Bezirkseinwohnerämtern (§ 3 Landeswahlgesetz, § 2 Abs. 2 Meldegesetz, Nr. 3 Abs. 18 DVO-AZG). Die Durchführung eines Abgleichs der Meldedaten Ost und Meldedaten West zur Erstellung des Wählerverzeichnisses und zum Zweck der Vermeidung doppelter Stimmabgaben kann dem Statistischen Landesamt ausschließlich im Rahmen der auftragsweisen Datenverarbeitung von den 23 Bezirksämtern bzw. Stadtbezirken – für Ost-Berlin durch das Statistische Amt der DDR (§ 91 a Abs. 2 Nr. 5 der Bundeswahlordnung) – förmlich übertragen werden. Den hierfür erforderlichen Auftrag hat der Landeswahlleiter nicht eingeholt. Wir sehen hierin einen Verstoß gegen die Vorschriften zur Auftragsdatenverarbeitung.

Verfassungswidrig wäre auch die ursprünglich geplante Nutzung der Personenkennzahl für den Abgleich der Daten durch den Landeswahlleiter gewesen. Der Einigungsvertrag läßt zwar vorübergehend die weitere Verwendung der PKZ zu, wenn dies für den Verwaltungsablauf unerläßlich ist. Dies kann aber nur für die Fortführung der früheren DDR-Verfahren gelten, nicht aber für neu einzuführende. Im Ergebnis wurde ein Verfahren gefunden, bei dem die PKZ nicht in den Westen übermittelt werden mußte.

Amtliche Statistik

Das *Statistische Landesamt* gehört zu den öffentlichen Stellen Berlins, die am umfangreichsten personenbezogene Daten verarbeiten. Da diese Behörde die *Volkszählungsdaten* aller Bewohner der westlichen Stadtbezirke zum Stichtag der Volkszählung 1987 gespeichert hat, handelt es sich mindestens um 2,3 Millionen personenbezogene Datensätze. Hinzu kommen eine Vielzahl von Datensätzen aus anderen Einzelstatistiken (z. B. Mikrozensus, Handels- und Gaststättenzählung und viele andere). Insgesamt hat das Statistische Landesamt 128 automatisierte Dateien zum Dateienregister gemeldet. Es muß noch einmal betont werden, daß alle diese Daten trotz der gesetzlich vorgeschriebenen Maßnahmen zur Anonymisierung nach der Rechtssprechung des Bundesverfassungsgerichts dennoch personenbezogene Daten bleiben und ihre Nutzung daher dem bereichsspezifischen Datenschutzrecht in Form des Bundesstatistikgesetzes sowie dem Berliner Datenschutzgesetz unterliegen.

Der Bundesgesetzgeber hat seine ursprüngliche Absicht, ein Gebäude- und Wohnungsstichprobengesetz zu verabschieden,[29] fallengelassen. Stattdessen sind kurz vor Ablauf der Legislaturperiode das *Mikrozensusgesetz* und *Bundesstatistikgesetz* geändert worden[30]. Dadurch wird die Mikrozensuserhebung in den Jahren 1991–1995 fortgesetzt, wobei der Fragenumfang geringfügig reduziert und bei einzelnen Fragen auf die Auskunftspflicht verzichtet wurde.

Die Befugnis zur Führung von Adreßdateien im Bundesstatistikgesetz wurde ergänzt um eine Befugnis, Datensätze aus verschiedenen Wirtschafts- und Umweltstatistiken zusammenzuführen. Dabei müssen jedoch zunächst zusätzliche Anonymisierungsmaßnahmen für jede Erhebungseinheit getroffen werden, damit ein Bezug zwischen den zusammengeführten Datensätzen und einzelnen Personen oder Unternehmen nicht hergestellt werden kann.

Auch die *Straßenverkehrsunfallstatistik* des Bundes ist auf eine neue gesetzliche Grundlage gestellt worden[31]. Damit ist dieser

[29] dazu Jahresbericht 1989, 4.4, S. 28 ff

[30] Gesetz vom 17. 12. 1990, BGBl. I, S. 2837 ff

[31] Straßenverkehrsunfallstatistikgesetz vom 15. 6. 1990, BGBl. I, S. 1347 ff

Statistikbereich ebenfalls entsprechend den Anforderungen des Bundesverfassungsgerichts auf eine normenklare gesetzliche Grundlage gestellt. Zudem wurde eine Lücke des alten Gesetzes geschlossen, so daß jetzt auch unter bestimmten Voraussetzungen Unfallforschung mit den für Zwecke der Statistik erhobenen Daten unter Wahrung des Statistikgeheimnisses durchgeführt werden kann.

Der Polizeipräsident hatte dem Statistischen Landesamt in der Vergangenheit die Daten für die Unfallstatistik auf einer Durchschrift der polizeilichen Unfallanzeige übermittelt. Dabei wurden ursprünglich auch Namen, Anschriften und andere persönliche Angaben der Unfallbeteiligten weitergegeben, obwohl dies für die Statistik gar nicht erforderlich war. Erst 1987 wurden die Vordrucke der Unfallanzeige so geändert, daß auf der Durchschrift für das Statistische Landesamt Überschußinformationen über die Beteiligten nicht mehr lesbar waren. Dennoch hat der Polizeipräsident zunächst weiterhin auch Einzelangaben über Unfälle mit leichten Sachschäden an das Statistische Landesamt übermittelt, obwohl das Straßenverkehrsunfallstatistikgesetz von 1982 hierfür keine rechtliche Grundlage enthielt. Erst aufgrund unseres Hinweises wurde diese unzulässige Datenübermittlung im Juni 1990 eingestellt.

Bereits seit einiger Zeit plante der Polizeipräsident, das Verfahren der Straßenverkehrsunfallstatistik zu automatisieren. Dabei sollten die von der Polizei bei der Aufnahme des Unfalls erhobenen Daten automatisiert erfaßt werden und dem Statistischen Landesamt lediglich ein Datenträger mit denjenigen Daten übermittelt werden, die nach dem Straßenverkehrsunfallstatistikgesetz von der amtlichen Statistik zu erheben sind. Dieses Verfahren steht kurz vor der Einführung. Es führt insofern zu einer Verbesserung des Datenschutzes, als statt der Durchschriften von Verkehrsunfallanzeigen nur noch diejenigen Daten auf Datenträgern der Statistik zur Verfügung gestellt werden, für die das Bundesrecht die Übermittlung vorschreibt. Allerdings ist zu beachten, daß der Polizeipräsident für die eigene Erhebung personenbezogener Daten im Zusammenhang mit Straßenverkehrsunfällen bisher keine bereichsspezifische Rechtsgrundlage hat. Insofern ist hier eine ähnliche Situation wie bei der Hochschulstatistik gegeben: Der Bundesgesetzgeber hat angeordnet, daß bestimmte Daten aus dem Verwaltungsvollzug für eine Sekundärstatistik verwendet werden, bevor der Landesgesetzgeber die Erhebung und Verarbeitung dieser Daten für den Verwaltungsvollzug selbst geregelt hat. Dies muß auch im Bereich der Polizei im Rahmen der Novellierung des allgemeinen Sicherheits- und Ordnungsgesetzes so schnell wie möglich nachgeholt werden. Das neue Berliner Datenschutzgesetz bietet auch hierfür nur noch eine übergangsweise Rechtsgrundlage, die spätestens Ende dieses Jahres entfällt.

Die Verordnung des EG-Ministerrates über die Übermittlung von unter die Geheimhaltungspflicht fallenden Informationen an das Statistische Amt der Europäischen Gemeinschaften[32] ist inzwischen in Kraft getreten[33]. Die Konferenz der Datenschutzbeauftragten hatte noch im Oktober 1989 den ursprünglichen Entwurf dieser Verordnung kritisiert und datenschutzrechtliche Verbesserungen verlangt. Sie war darin auch vom Innenausschuß des Deutschen Bundestages unterstützt worden. Die jetzt in Kraft getretene Fassung der Verordnung entspricht diesen Forderungen nur zum Teil. Dabei ist allerdings zu berücksichtigen, daß die Verordnung zwar unmittelbar gilt, aber nur einen Rahmencharakter hat, weil jede Gemeinschaftsstatistik durch einen besonderen Rechtsakt der Gemeinschaft angeordnet werden muß. Auch in diesem Bereich ist es bisher allerdings nicht gelungen, eine unabhängige Kontrollinstanz auf Gemeinschaftsebene zu installieren, die die Einhaltung des Statistikgeheimnisses überwacht.

Personalwesen

Das *Landesverwaltungsamt* als nachgeordnete Behörde der Senatsverwaltung für Inneres ist verantwortlich für vier große Dateien im Rahmen des Personalbezügeverfahrens für die gesamte Berliner Verwaltung: Hierin werden erhebliche Datenmengen verarbeitet. Einschließlich der Versorgungsfälle handelte es sich in der Westberliner Verwaltung um über 300 000 Datensätze, die übernommenen Mitarbeiterinnen und Mitarbeiter aus dem östlichen Teil der Stadt werden im Laufe des Jahres noch hinzukommen. Bemerkenswert ist auch die Menge der einzelnen Felder in den Datensätzen: So werden etwa bei den Beamten 377, bei den Lohnempfängern 665 und bei den Angestellten gar 750 Felder vorgehalten (die natürlich nicht in jedem Fall belegt sind).

Personalfragebögen für übernommene Verwaltungsmitarbeiter der ehemaligen DRR

Zu zahlreichen Anfragen und Beschwerden hat die Befragung übernommener Mitarbeiter der ehemaligen DDR-Behörden geführt. Auf der Grundlage des Einigungsvertrages sind zahlreiche Behörden und Einrichtungen aus dem Ostteil Berlins mit den dort beschäftigten Dienstkräften auf das Land Berlin überführt worden. Die bestehenden Arbeitsverhältnisse der dort beschäftigten Arbeitnehmer bestanden zunächst fort. Beim Aufbau einer Gesamtberliner Verwaltung muß soweit wie möglich sichergestellt werden, daß nicht solche Personen in den öffentlichen Dienst übernommen werden und hoheitliche Funktionen etwa als Richter, Polizei- oder Verwaltungsbeamte ausüben, die in der ehemaligen DDR das System der Bespitzelung durch Partei und Staatssicherheit mitgetragen haben.

Deshalb ist nach dem Einigungsvertrag eine außerordentliche Kündigung möglich, wenn der Arbeitnehmer

- gegen die Grundsätze der Menschlichkeit oder Rechtsstaatlichkeit verstoßen hat oder
- für das frühere Ministerium für Staatssicherheit/Amtes für Nationale Sicherheit tätig war

und deshalb ein Festhalten am Arbeitsverhältnis unzumutbar erscheint.

Um dies zu prüfen, haben sämtliche Arbeitnehmer einen umfangreichen *Personalfragebogen* auszufüllen. Dieser Personalfragebogen wird auch an Dienstkräfte ausgegeben, die in Einrichtungen tätig waren, die abgewickelt werden, sofern sie an einer Weiterbeschäftigung in anderen Verwaltungseinrichtungen interessiert sind. Auch Bewerber um einen Arbeitsplatz in auf das Land Berlin überführten Einrichtungen haben diesen Personalfragebogen als Voraussetzung für die Einstellung auszufüllen. Bei der Durchführung dieser umfassenden Personaldatenerhebung kommt es wesentlich auch auf die Einhaltung datenschutzrechtlicher Grundsätze an.

Erst nachdem wir von dritter Seite auf die bevorstehende Fragebogenaktion hingewiesen worden waren, leitete uns die Senatsinnenverwaltung, auf unsere Bitte hin, einen Fragebogenentwurf zu. Bei der inhaltlichen Überprüfung dieses Entwurfs haben wir akzeptiert, daß bei der Entscheidung über die Weiterbeschäftigung z. B. als Polizist weitergehende Fragen gestellt werden können als im allgemeinen Verwaltungsdienst.

Soweit der Personalfragebogen Fragen in bezug auf mögliche Verstöße gegen Grundsätze der Menschlichkeit oder Rechtsstaatlichkeit oder bezüglich einer früheren Tätigkeit für das Ministerium für Staatssicherheit/Amtes für Nationale Sicherheit beinhaltet, sind diese grundsätzlich durch den Einigungsvertrag gedeckt. Dabei ist allerdings schon die Art der Fragestellung datenschutzrechtlich von Bedeutung.

Im ersten Entwurf dieses Personalfragebogens waren Fragen vorgesehen, bei deren Beantwortung sich der Befragte möglicherweise der Begehung einer Straftat bezichtigen würde, die u. U. eine strafrechtliche Verfolgung nach sich ziehen würde (Fragen nach Beteiligung an Folterungen bzw. Einweisungen in Internierungslager). Durch die faktische Auskunftspflicht gerät der Befragte in die Konfliktsituation, sich entweder selbst einer strafbaren Handlung zu bezichtigen oder die Frage falsch zu beantworten. Dies war verfassungsrechtlich nicht hinnehmbar.

Der faktische Zwang zur Auskunftserteilung stellt wegen der geschilderten Folgen einen schwerwiegenden Eingriff in das Persönlichkeitsrecht dar. Ein Zwang zur Selbstbezichtigung berührt zugleich die Würde des Menschen, dessen Aussage als Beweismittel gegen ihn selbst verwendet wird. Deshalb wurden Schutz-

32) vgl. dazu Jahresbericht 1989, 4.4 S. 29

33) Amtsblatt der EG Nr. 151/1 v. 15. 6. 1990

vorkehrungen vor allem dort entwickelt, wo die Aussage speziell strafrechtlichen Zwecken dient. So besteht ein Schweigerecht nicht nur in strafrechtlichen, sondern auch in Disziplinarverfahren und anderen berufsgerichtlichen Verfahren. Aufgrund unserer verfassungsrechtlichen Bedenken wurden die Fragen wieder aus dem Fragebogen herausgenommen. Wir haben zwar akzeptiert, daß der Betroffene gefragt wird, ob gegen ihn Vorwürfe wegen Verstößen gegen Grundsätze der Menschlichkeit und Rechtsstaatlichkeit erhoben worden sind, jedoch nur dann, wenn er zugleich Gelegenheit erhält, zu diesen Vorwürfen Stellung zu nehmen.

Außerdem wurden befragte ehemalige Volkspolizisten aufgefordert, Mitarbeiter (auch Vorgesetzte) anzugeben, die nach dem 9. November 1989 oder nach dem 18. März 1990 in ihrer Dienststelle umgesetzt („versteckt") wurden. Wir haben in diesem Zusammenhang darauf hingewiesen, daß eine solche Frage schon rein sachlich nicht in einen Personalfragebogen gehört. Im übrigen wird dadurch zur Denunziation Dritter aufgefordert. Auch auf diese Frage verzichtete die Senatsverwaltung für Inneres deshalb.

Ferner enthielt der Entwurf des Personalfragebogens Fragen nach strafrechtlichen Verurteilungen, anhängigen Strafverfahren, getroffenen Disziplinarmaßnahmen und anhängigen Disziplinarverfahren. Der Fragebogen enthielt jedoch zunächst keinen Hinweis auf Tilgungsfristen, nach deren Ablauf die ehemaligen Mitarbeiter der DDR-Verwaltung bestimmte Tatbestände rechtmäßig verschweigen dürfen. Über Verurteilungen, die im Bundeszentralregister getilgt waren, brauchen keine Angaben gemacht zu werden. Über diese Tilgungsfristen sind auch die Befragten aufzuklären. Eine Auskunftspflicht besteht nur hinsichtlich solcher Verurteilungen, die zwar tilgungsreif, aber noch nicht getilgt sind. Dies gilt auch für verhängte Disziplinarmaßnahmen. Der Fragebogenentwurf wurde entsprechend abgeändert.

Der Personalfragebogen beinhaltete ferner eine Frage nach der Mitgliedschaft in der SED, in einer anderen Blockpartei und in Massenorganisationen.

Man kann alle diese Organisationen zwar nach unserem Rechtsverständnis als verfassungsfeindlich einstufen. Angesichts der Tatsache, daß viele Menschen in der ehemaligen DDR aufgrund des politischen und sozialen Drucks und nicht aus persönlicher Überzeugung Mitglieder der SED, der Blockparteien und anderer Massenorganisationen waren, ist diese Frage jedoch nicht geeignet, Anhaltspunkte für die Prognose der zukünftigen Verfassungstreue des Befragten zu gewinnen.

Anders verhält es sich jedoch mit Fragen nach einer Funktion in einer solchen Partei oder Massenorganisation. Wer wichtiger Funktionsträger in den genannten Parteien oder Massenorganisationen war, betätigte sich als Stütze des SED-Regimes. Hieraus können sich Zweifel an einer künftigen Verfassungstreue des übernommenen Mitarbeiters der ehemaligen DDR-Verwaltung ergeben, die zumindest zu Rückfragen bei diesem führen werden.

Die Senatsverwaltung für Inneres hat unsere datenschutzrechtlichen Bedenken inzwischen berücksichtigt.

Ferner beinhaltete der Fragebogen für ehemalige Volkspolisten Fragen nach einer evtl. Alkohol- oder Drogenabhängigkeit und möglichen therapeutischen Maßnahmen. Abgesehen davon, daß die Frage nach der Drogenabhängigkeit eine unzulässige Aufforderung zur Selbstbezichtigung sein kann, haben wir darauf hingewiesen, daß Fragen nach Krankheiten allenfalls von einem Arzt zu stellen sind, der die medizinische Untersuchung durchführt. Bei Eignung des Bewerbers ist der auftraggebenden Dienststelle dann das Ergebnis mitzuteilen. Ausführungen zur Krankengeschichte sind bei Eignung des Bewerbers nicht erforderlich und haben deshalb zu unterbleiben. Aufgrund unserer Einwände verzichtete die Innenverwaltung auf die Frage nach einer Alkohol- oder Drogenabhängigkeit und beschränkte sich auf eine Frage nach der gesundheitlichen Einsatzfähigkeit.

Zur Form der Datenerhebung haben wir vorgeschlagen, den Fragebogen in verschiedene Komplexe aufzuteilen und getrennt zu erheben. Dies hätte zur Folge gehabt, daß Fragen zu Disziplinarmaßnahmen und Verurteilungen sowie sogenannte Gesinnungsfragen getrennt vom allgemeinen Personalfragebogen erfragt und aufbewahrt worden wären. Diese Empfehlung ist jedoch nicht berücksichtigt worden.

Bezüglich der *Aufbewahrung der Fragebögen* und der evtl. in diesem Zusammenhang entstandenen Vorgänge haben wir empfohlen, diese in einer Beiakte der Personalakte aufzubewahren. Dies ist jedoch nur bis zum Abschluß des Überprüfungsverfahrens möglich. Danach wären die Fragebögen zu vernichten. Sofern eine weitere Nutzung der Personalfragebögen als mögliches Beweismittel für eine Rücknahme der Ernennung erforderlich sein sollte, halten wir die Aufbewahrung in einer Sachakte für geboten, in die nur zu diesem Zweck Einsicht genommen werden dürfte. Die Fragebögen von gekündigten bzw. entlassenen Mitarbeitern sind nach Kündigung bzw. Entlassung (spätestens nach rechtskräftigem Abschluß eines Kündigungsschutzprozesses) dem Betroffenen herauszugeben. Ferner bedarf es einer Regelung, wie mit den von den Personalkommissionen angefertigten Niederschriften der Anhörung von „vorbelasteten" Mitarbeitern umgegangen wird.

Bewerben sich in normalen Stellenbesetzungsverfahren auch Bürger aus der ehemaligen DDR, so dürfen ihnen spezielle Fragen zu ihrer politischen Vergangenheit erst dann gestellt werden, wenn alle übrigen Anstellungsvoraussetzungen gegeben sind.

Bevor nicht eindeutige Regelungen über die Nutzung der Daten geschaffen werden, hatten wir die Verwendung der erhobenen Informationen für unzulässig erachtet. Diese sollten insbesondere enthalten:

- genaue Festlegung der Zwecke, zu denen die Daten genutzt werden dürfen;
- Bestimmung der Personen, die auf die Daten zugreifen dürfen;
- besondere Bestimmungen über die Offenbarung der Daten;
- keine Aufbewahrung des Fragebogens in der Personalakte;
- Art des Verschlusses und Dauer der Aufbewahrung.

Ursprünglich sollte die Fragebogenaktion ohne derartige Feststellungen beginnen. Der Unmut und die Verunsicherung bei den Betroffenen wie bei den Personalstellen waren deshalb nur zu verständlich.

Durch das Rundschreiben II Nr. 82/1990 der Senatsverwaltung für Inneres sind unsere wesentlichen Forderungen zur Verwendung der Daten aus den Fragebögen inzwischen erfüllt worden.

Darin ist auch geregelt, welche Personen auf die Daten zugreifen dürfen. Danach werden die Personalfragebögen von der Stelle in der jeweiligen Verwaltung ausgewertet, die die personalrechtlichen Entscheidungen vorbereitet.

Die ausgewerteten Personalfragebögen sowie das Protokoll des Gesprächs mit der Personalkommission werden nach Abschluß des Verfahrens in verschlossenem und versiegeltem Umschlag (in einer Beiakte) zur Personalakte genommen. Der Umschlag enthält die Aufschrift „Personalvorgänge aus Anlaß der Weiterbeschäftigung nach der Vereinigung. Nur vom Leiter der Personalabteilung oder dem ausdrücklich Bevollmächtigten zu öffnen." Die Vorgänge dürfen, nachdem sie zur Personalakte genommen worden sind, nur noch aus Anlaß der Überprüfung bei begründeten Zweifeln über die Richtigkeit der Angaben im Personalfragebogen und den dazu entstandenen Vorgängen, die zur Weiterbeschäftigung geführt haben, von den Leitern der Personalabteilung oder den von ihnen ausdrücklich Bevollmächtigten geöffnet werden. Dies bedeutet, daß Personalfragebögen z. B. nicht bei Beförderungsentscheidungen herangezogen werden dürfen.

Offen ist allerdings noch die Frage, wie lange die Fragebögen aufzubewahren sind. In keinem Fall dürfen die Fragebögen ebenso lange wie die Personalakten aufbewahrt werden. Für den Bereich der Polizei will die Senatsverwaltung eine Vernichtung nach zehn Jahren vorsehen. Dies wäre als Aufbewahrungsdauer noch hinnehmbar. Umso unverständlicher ist es, daß der allgemeine Personalfragebogen, der außerhalb des Polizeibereichs verwandt wird, unbeschränkt aufbewahrt werden soll. Auch ist es

nicht hinnehmbar, daß Arbeitnehmern in abgewickelten Einrichtungen, die den Personalfragebogen ausgefüllt haben, aber nicht erneut beim Land Berlin beschäftigt werden, der Personalfragebogen nur auf Wunsch ausgehändigt werden soll. Dies würde dazu führen, daß Fragebogen solcher Bewerber, die nicht von sich aus die Aushändigung wünschen, auf Dauer aufbewahrt werden, obwohl sie noch nicht einmal Bedienstete des Landes Berlin sind.

Wir werden die Aufbewahrung und Verwendung der Personalfragebögen überprüfen. Es ist nach wie vor erforderlich, daß der Senat eine allgemeine Verwaltungsvorschrift nach § 6 AZG zur Durchführung dieses Teils des Einigungsvertrages beschließt, an die alle Senatsverwaltungen gebunden sind. Es ist von entscheidender Bedeutung, daß diese Sammlung hochsensibler Informationen von vornherein auf das unerläßliche Maß beschränkt und ihre Verwendung in datenschutzgerechter Weise sichergestellt wird.

Der Wettlauf zwischen Bewerber und Personalakte - die Personalakte ist immer schon da

Ein Angestellter der Fachhochschule für Wirtschaft Berlin, dessen Stelle dort mit einem „KW-Vermerk" („künftig wegfallend") versehen ist, erhielt vom Landesverwaltungsamt einen Anruf, daß dort eine Stelle nach BesGr. A 8 zu besetzen ist. Als er dort zum Bewerbungsgespräch erschien, erfuhr er, daß bereits seine Personalakte angefordert und aus dieser Auszüge angefertigt worden seien.

Jede Stelle der Berliner Verwaltung ist verpflichtet, Inhaber von „KW-Stellen" auf die nächste besetzbare Stelle zu übernehmen.

Dienstkräfte im Personalüberhang, die nicht innerhalb von 6 Monaten vom Tage ihrer Zugehörigkeit an in geeignete besetzbare Stellen übernommen werden können, sind der Senatsverwaltung für Inneres zur Aufnahme in die *Personalüberhangslisten* zu melden.

Eine jederzeitige Übersendung der Personalakten dieser öffentlichen Bediensteten ohne Kenntnis des Betroffenen ist nicht datenschutzgerecht.

Auf unseren Hinweis hat die Senatsverwaltung für Inneres mit Rundschreiben vom 9. März 1989 mitgeteilt, daß eine Aktenanforderung zwar zulässig, aber nicht in jedem Fall erforderlich ist, so daß eine differenzierte Prüfung zu erfolgen hat.

So sollen zunächst die Personalwirtschaftsstellen eine erste Grobauswahl anhand der in der Personalüberhangsliste enthaltenen Amts- und Berufsbezeichnungen, der Besoldungs-, Vergütungs- oder Lohngruppen sowie der derzeitigen Beschäftigungsdienststelle treffen. Dadurch könnte ein Großteil der Personalüberhangskräfte von vornherein vom Auswahlverfahren ausgenommen werden. Ferner sollen Informationen durch persönliche Kontaktaufnahme mit den entsprechenden Dienststellen selbst eingeholt werden. Erst wenn Überhangskräfte nicht sofort zu erreichen oder zu kurzfristigen Auskünften bereit sind, wird empfohlen, entscheidungsrelevante Informationen über den beruflichen Werdegang bei der Dienstbehörde der Überhangskräfte direkt einzuholen, ohne die Personalakte anzufordern. Hierzu sollen die Dienststellen auf Anforderung von anderen Dienstbehörden in konkreten Stellenbesetzungsfällen formularmäßig festgelegte Informationen an Stelle der Personalakten übersenden. Dabei sind diese Angaben ebenso vertraulich zu behandeln wie die Personalakten selbst. Nach Abschluß des Stellenbesetzungs- oder Auswahlverfahrens sind diese Unterlagen zu vernichten.

3.6 Justiz

Auch im Bereich der Berliner Justiz hat die Automation von Verwaltungvorgängen mittlerweile fast alle Bereiche erfaßt. Allein das ADV-Verfahren ASTA (Amts- und Staatsanwaltschaften) enthält weit mehr als 2 Millionen Datensätze über Personen in Strafverfahren. Neben diesem Großverfahren finden sich ADV-Anwendungen etwa zur Unterstützung von Ermittlungsverfahren, für Verwaltungsaufgaben in den Strafvollzugsanstalten und bei den Gerichtsvollziehern. Insgesamt liegen derzeit aus dem Geschäftsbereich der Senatsverwaltung für Justiz 118 Meldungen automatisierter Dateien zum Allgemeinen und Besonderen Dateienregister vor.

ADV-Verfahren in der Strafjustiz

Damit aber nicht genug: Um auch die private Investitionsbereitschaft und wohl auch die Computerbegeisterung seiner Bediensteten zu dienstlichen Zwecken ausnutzen zu können, hat der Generalstaatsanwalt beim Landgericht einen Bericht vorgelegt, der die Nutzung *privater Arbeitsplatzcomputer* für dienstliche Zwecke der Dezernenten im Dienst, vor allem aber auch in deren Privatwohnung vorbereiten soll.

Zwar wird die Genehmigung des Einsatzes privateigener Computer zur Erledigung dienstlicher Aufgaben von Voraussetzungen abhängig gemacht, die die Vertraulichkeit der Daten sicherstellen sollen. Die Beachtung dieser Regeln ist in der Privatwohnung jedoch vom Generalstaatsanwalt bei dem Landgericht nicht sicherzustellen und zu kontrollieren. Er kann insoweit daher für seinen Geschäftbereich die Ausführung der datenschutzrechtlichen Bestimmungen nicht gewährleisten. Dies würde gegen § 19 Abs. 1 Satz 1 Berliner Datenschutzgesetz verstoßen und wäre gem. § 26 Abs. 1 Berliner Datenschutzgesetz bei der Senatsverwaltung für Justiz formell zu beanstanden.

Die im Bericht angeführten Gründe für die Verarbeitung dienstlicher Zwecke in der Privatwohnung sind nicht zwingend und heben letztlich darauf ab, daß es den Dezernenten bequemer ist, ihre Arbeit zu Hause statt in den Diensträumen zu verrichten. Die als Zulassungsvoraussetzung genannte Billigung der Praxis durch die Behörde ist schon deshalb unerheblich, weil sie aus obengenannten Gründen rechtswidrig ist.

Im *Registraturbereich der Sozialen Dienste* soll das ADV-Verfahren *ADSoDi* eingeführt werden. Wir haben dagegen keine grundsätzlichen Bedenken erhoben, jedoch verschiedene Hinweise zur Realisierung technischer und organisatorischer Datenschutzmaßnahmen gegeben.

ADV-Verfahren in der Ziviljustiz

Auch die *Automation des Handelsregisters* im Rahmen des Projektes *HAREG* haben wir weiterhin beratend begleitet. Nachdem die Fragen über die Art des Betriebssystems und die Vollständigkeit der Dokumentation für die Phase 1 (Firmendatei) geklärt waren, haben wir uns das Verfahren im Amtsgericht Charlottenburg erläutern lassen und dabei folgende Probleme erörtert:

Für das Verfahren wird das Betriebssystem UNIX eingesetzt. Die UNIX-immanenten Sicherheitsfunktionen unterstützen bei ordnungsgemäßer Anwendung eine sichere Verfahrensabwicklung. Auch die im Rahmen der Präsentation des Verfahrens zur Sprache gekommenen Fragen zur Datensicherheit und zum Datenschutz (u. a. Zugangs- und Zugriffskontrolle, Benutzerprofil), die zum Teil auch in der Geschäftsanweisung für die automatisierte Führung des Namenverzeichnisses zum Handels- und Genossenschaftsregister festgeschrieben sind, werden von uns als datenschutzgerecht geregelt angesehen.

Die noch offenen Fragen der zweiten Projektstufe im Zusammenhang mit der Verfahrenserweiterung, wie z. B. die Übermittlungen an die Industrie- und Handelskammer, die Eingabeprotokollierung und die Datenträgervernichtung werden nach Vorliegen der Unterlagen näher zu untersuchen sein.

Eine bisher umstrittene Frage hat der Gesetzgeber mit der Novellierung des Berliner Datenschutzgesetzes beantwortet: In § 24 Abs. 2 Satz 2 ist nunmehr eindeutig geregelt, daß die Gerichte unbeschadet der richterlichen Unabhängigkeit bei Erfüllung ihrer gesetzlichen Aufgaben mit automatischen Datenverarbeitungsanlagen der Kontrolle des Datenschutzbeauftragten für die Ordnungsmäßigkeit und Rechtmäßigkeit der Verfahren unterliegen. Daraus folgt, daß auch das HAREG-Verfahren zum Dateienregister gemeldet werden muß, was die Senatsverwaltung für Justiz bisher abgelehnt hatte. Auch im Zivilverfahren ist der Bundesgesetzgeber weiterhin gefordert. Noch immer steht eine datenschutzgerechte Ausgestaltung des Schuldnerverzeichnisses nach § 915 Zivilprozeßordnung aus[34].

[34] vgl. dazu Jahresbericht 1989, 4.5, S. 31

Auch die bisherige Praxis der *Mitteilungen in Zivil- und Strafsachen* kann nach dem Ende des Übergangsbonus nicht länger auf bloße Verwaltungsvorschriften gestützt werden, sondern bedarf jetzt einer normenklaren bereichsspezifischen Rechtsgrundlage in einem Justizmitteilungsgesetz.

Für das *automatisierte gerichtliche Mahnverfahren AUMAV* soll eine *Fernwartung* durchgeführt werden, zu deren Vereinbarungen mit dem Hersteller wir beratend aus der Sicht des Datenschutzes Stellung beziehen sollten. Hier muß durch eine gesonderte schriftliche Anweisung für die Sicherheit der personenbezogenen Daten vor dem unbefugten und unbeobachteten Zugriff durch Mitarbeiter des wartenden Unternehmens gesorgt werden.

Noch immer keine datenschutzgerechte Strafprozeßordnung

Die Aufnahme von bereichsspezifischen Datenschutzbestimmungen in die *Strafprozeßordnung* ist überfällig. Auch der Bundesminister der Justiz hat die Notwendigkeit einer Anpassung der Strafprozeßordnung an die Rechtsprechung des Bundesverfassungsgerichts anerkannt. Sein Referentenentwurf für ein Strafverfahrensänderungsgesetz (StVÄG) vom Juni 1989 ist allerdings in der abgelaufenen Legislaturperiode nicht mehr ins Parlament eingebracht worden. Verfassungskonforme Regelungen für die Datenverarbeitung im Strafverfahren, für die die Datenschutzkonferenz bereits 1989 detaillierte Vorschläge gemacht hat[35], müssen jetzt zügig verabschiedet werden. Dafür sollte sich auch der Senat über den Bundesrat energischer als bisher einsetzen. Mehr als sieben Jahre nach dem Volkszählungsurteil ist der Übergangsbonus verbraucht, den das Bundesverfassungsgericht dem Gesetzgeber zugebilligt hat.

Statt der dringend notwendigen Datenschutznovelle zur Strafprozeßordnung überwiegen gegenwärtig allerdings Bestrebungen, einzelne Probleme des Strafverfahrensrechts nach Art eines Flickenteppichs zu lösen.

Wanzen, Peilsender und andere Instrumente der Verdachtsschöpfung

Auf Initiative der Länder Bayern und Baden-Württemberg wurde im Bundesrat der *„Entwurf eines Gesetzes zur Bekämpfung des illegalen Rauschgifthandels und anderer Erscheinungsformen der organisierten Kriminalität"*, kurz „OrgKG" genannt, eingebracht. Der Bundesrat hat im Mai 1990 diese Gesetzesinitiative beschlossen, möglicherweise ohne sich der vollen Tragweite dieses Gesetzes bewußt zu sein. Die Bezeichnung des Gesetzentwurfs erweckt zwar den Eindruck, daß er ausschließlich den Bereich der organisierten Kriminalität betrifft, inhaltlich geht er aber weit darüber hinaus und stellt eine einschneidende Revision des gesamten Strafrechts dar.

Diese „Mogelpackung" sieht auch für den Bereich der mittelschweren Kriminalität in besorgniserregendem Umfang geheime Ermittlungsmethoden für die Polizei vor. Datenschutzrechtliche Essentials, wie Akteneinsichtsrechte für Betroffene und differenzierte Regelungen über die Verarbeitung personenbezogener Daten fehlen völlig. Richterliche Kontrollen werden in dem Entwurf verfassungsrechtlich bedenklich zugunsten polizeilicher Eilanordnungen eingeschränkt. Damit nicht genug: Seit Jahren umstrittene polizeiliche Ermittlungsmethoden sollen gesetzlich abgesegnet werden. So soll das heimliche Abhören von Telefongesprächen erleichtert werden, die Rasterfahndung und der Einsatz verdeckter Ermittler bei einer Vielzahl von Delikten außerhalb der organisierten Kriminalität ermöglicht werden. Gegen unverdächtige Personen sollen Wanzen und Peilsender eingesetzt werden dürfen, wenn eine „Verbindung" mit dem Täter vermutet wird.

Die Bekämpfung der organisierten Kriminalität kann zwar besondere Ermittlungsmethoden erforderlich machen. Das darf jedoch nicht dazu führen, daß die Polizei in die Privatsphäre unbescholtener Bürger eindringen kann und diese zum Objekt geheimer staatlicher Beobachtung macht.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat gegen diesen Gesetzentwurf im Juni 1990 eindeutig Stellung bezogen und hat den Bundestag aufgefordert, den Entwurf wegen erheblicher Eingriffe in die Bürgerrechte abzulehnen*). Auch die Bundesregierung hat in ihrer Stellungnahme diese Gesetzesinitiative skeptisch beurteilt. Glücklicherweise ist dieses Werk mit Ablauf der Legislaturperiode der Diskontinuität zum Opfer gefallen. Die Länder Bayern und Baden-Württemberg haben allerdings inzwischen im Bundesrat beantragt, diesen Gesetzentwurf erneut einzubringen.

Schutz von Zeugen im Strafverfahren

Ein Bürger beobachtet in einer Parkanlage die Straftat einer Jugendbande und ruft daraufhin die Polizei, die einen der Täter dingfest machen kann. Bald darauf erhält der Bürger Drohanrufe, in denen ihm Rache für die Anzeige bei der Polizei angedroht wird.

Uns sind mehrere Fälle bekannt geworden, in denen Anzeigeerstatter später Repressionen übler Art ausgesetzt waren. Daher stellt sich in letzter Zeit auch in Berlin zunehmend das Problem des Schutzes der Opfer bzw. Zeugen, die eine Straftat angezeigt haben.

Dabei ergibt sich die Frage, auf welche Weise verhindert werden kann, daß der Beschuldigte an die Wohnadresse des Anzeigeerstatters bzw. Opfers gelangt.

Grundsätzlich müssen Zeugen nach § 68 Satz 1 Strafprozeßordnung (StPO) - in der Hauptverhandlung - ihren Wohnort nennen.

In § 222 Abs. 1 Satz 1 StPO ist festgelegt, daß in der Ladungsmitteilung u. a. dem Angeklagten die vom Gericht geladenen Zeugen rechtzeitig namhaft zu machen sind und ihr Wohn- oder Aufenthaltsort anzugeben ist.

Dies verpflichtet allerdings nur zur Angabe der politischen Gemeinde als Wohnort, nicht aber zur Preisgabe der genauen postalischen Anschrift[36].

Insoweit kann aus Gründen des *Zeugenschutzes* auf die Angabe der genauen Wohnanschrift verzichtet werden.

Gleiches muß gelten für die Angabe der „Beweismittel", die nach § 200 Abs. 1 Satz 2 StPO für die Anklageschrift und nach § 409 Abs. 1 Nr. 5 StPO für den Strafbefehl vorgeschrieben sind. Hier wird teilweise die Auffassung vertreten, daß zu diesen Beweismitteln auch die Anschriften der Zeugen gehören. Das Schutzbedürfnis eines Zeugen verbietet jedoch auch hier die genaue Anschrift anzugeben.

Die Senatsverwaltung für Justiz ist ebenfalls der Auffassung, daß dem Zeugenschutz im Strafverfahren eine erhebliche Bedeutung zukommt, der durch die derzeitige Gesetzeslage nicht in allen Bereichen hinreichend Rechnung getragen wird. Auch auf der Grundlage des geltenden Rechts muß dem Zeugenschutz soweit wie möglich Genüge getan werden.

Wie eine Umfrage der Senatsverwaltung für Justiz ergeben hat, hat sich auch die gerichtliche Praxis in diesem Sinne geäußert. Auch die Staatsanwaltschaft ist um Überprüfung gebeten worden, ob künftig in Strafbefehlsanträgen und Anklageschriften auf die Angabe der vollen Wohnanschrift verzichtet werden kann.

Es bleibt abzuwarten, ob aufgrund dieser begrüßenswerten Haltung der Justiz künftig für einen besseren Schutz gefährdeter Zeugen gesorgt wird. Eine Klarstellung in der Strafprozeßordnung, daß die Wohnanschriften von Zeugen nicht in Ladungen, Anklageschriften und Strafbefehlen aufzunehmen sind, ist in jedem Fall wünschenswert.

Das Risiko, daß sich ein Täter die Anschrift durch einen Blick ins Telefonbuch oder auf sonstige Weise verschafft, ist damit allerdings nicht auszuschalten.

Genomanalyse im Strafprozeß

Das *genetische Personenkennzeichen***) in Gestalt des sogenannten genetischen Fingerabdrucks spielt sowohl in Strafverfahren als auch in Verfahren zu Vaterschaftsfeststellungen eine zunehmende Rolle.

---

*) vgl. Anlage 1.8

35) Jahresbericht 1989, Anlage 1.1

36) BGH Beschluß v. 26. 1. 1990 - 3 StR 428/89 -

**) vgl. dazu Jahresbericht 1989, 2.3, S. 9 ff.

Der Bundesgerichtshof hat sich im Berichtszeitraum erstmals mit der Frage auseinandergesetzt, ob der genetische Fingerabdruck nach der geltenden Strafprozeßordnung ein zulässiges Beweismittel ist[37]. Er hat diese Frage für den Fall bejaht, daß die Genomanalyse als Methode zur Identifikation eines Täters oder zur Entlastung eines Verdächtigen benutzt wird, weil bei diesem Verfahren nach dem gegenwärtigen Erkenntnisstand nur der „stumme" Teil der Erbinformation des Betroffenen untersucht wird. Ausdrücklich offen gelassen hat der Bundesgerichtshof die Frage, ob eine Verwertung von „sprechenden" Teilen der Erbinformation eines Menschen, die z. B. über äußerlich sichtbare Körpermerkmale oder gar über Krankheiten bzw. Veranlagungen hierzu Auskunft geben können, im Strafprozeß verwertet werden dürfen. Auch nach dieser Entscheidung ist eine spezifische Regelung des Einsatzes dieser neuen Beweismethode in der Strafprozeßordnung unerläßlich.

Der Bundesminister der Justiz hat zur Verwendung des genetischen Fingerabdrucks im Strafprozeß einen Diskussionsentwurf vorgelegt, der eine Ergänzung der Strafprozeßordnung vorsieht. Danach soll die Genomanalyse im Strafverfahren sich auf den „stummen" Teil der menschlichen Erbinformationen beschränken, der bestimmte unverwechselbare Strukturen aufweist, mit deren Hilfe Tatverdächtige identifiziert oder entlastet werden können. Andererseits eröffnet der Diskussionsentwurf ausdrücklich die Möglichkeit, diejenigen Teile der Erbinformationen genomanalytisch zu untersuchen, die auf „äußerlich sichtbare Körpermerkmale" schließen lassen. Damit wird die Grenze zwischen dem „stummen" (nicht kodierenden) und dem „sprechenden" (kodierenden) Bereich des menschlichen Genoms durchbrochen. Eine effektive Beschränkung der Untersuchungsmethoden im kodierenden Bereich auf diejenigen Teile der Erbinformationen, die für äußerlich sichtbare Körpermerkmale verantwortlich sind, ist nicht möglich. Persönlichkeitsrelevante „Überschußinformationen" z. B. über genetische Defekte, die nicht äußerlich erkennbar sind, werden unvermeidlich anfallen, wenn der „sprechende" Teil des menschlichen Genoms analysiert wird. Damit wäre die Grenze zur verfassungswidrigen Registrierung der gesamten Erbinformationen eines Menschen überschritten.

Der Gesetzgeber sollte außerdem ausdrücklich klarstellen, daß auch in einem Strafverfahren gentechnische Methoden, die nach gegenwärtigem Erkenntnisstand nur Aussagen über die Identität eines Tatverdächtigen oder eines Spurenlegers zulassen, nur als ultima ratio zuzulassen sind. Diese Methode darf nur auf richterliche Anordnung angewandt werden, wobei der Richter auch die konkrete Gensonde bezeichnen muß, die eingesetzt werden soll. Der Einsatz von sog. Single-Locus-Sonden ist gesetzlich auszuschließen, weil bei ihnen das Risiko besteht, daß indirekt Informationen aus dem kodierenden Bereich des Genoms anfallen.

Die Datenschutzbeauftragten haben empfohlen[38], die einzelnen bei gentechnischen Untersuchungen anzuwendenden Sonden einem besonderen Zulassungsverfahren zu unterwerfen. Daneben sollen auch die Institute, in denen solche Sonden angewendet werden dürfen, nur nach besonderer Zulassung tätig werden können. Der Diskussionsentwurf des Bundesjustizministers sieht ein solches zweistufiges Zulassungsverfahren bisher nicht vor. Damit entsteht in der Praxis die Gefahr, daß Sonden eingesetzt werden, die über die bloße Identifikation hinaus Erbinformationen entschlüsseln, die nicht in den Strafprozeß eingeführt werden dürfen. Der Bundesgesetzgeber hat im neuen Gentechnikgesetz[39] ein solches Zulassungsverfahren lediglich bei gentechnischen Anlagen für Forschungszwecke (z. B. Freilandversuche) vorgeschrieben. Im Strafprozeß kann nur die besondere Zulassung der Sonden und der untersuchenden Institute sicherstellen, daß die Erhebung der Daten auf das erforderliche Minimum beschränkt bleibt und ihre Verwendung streng zweckgebunden erfolgt. Solange ein solches Zulassungsverfahren fehlt, sollte die Polizei (in Berlin: die Polizeitechnische Untersuchungsstelle) nicht mit gentechnischen Untersuchungen für Zwecke der Strafverfolgung beauftragt werden. Zumindest muß bis zu einer gesetzlichen Regelung sichergestellt werden, daß die Polizeitechnische Untersuchungsstelle anonymisiertes Untersuchungsmaterial mit einer Code-Nummer und ohne Hinweis auf den jeweiligen Tatvorwurf erhält.

Auch muß der Gesetzgeber eine Umwidmung von gentechnischen Untersuchungsergebnissen für präventiv-polizeiliche Zwecke und zur Vorsorge für künftige Strafverfolgung ausdrücklich ausschließen. Die Verwendung der Ergebnisse einer gentechnischen Untersuchung ist ausschließlich auf das konkrete Strafverfahren zu beschränken, in dessen Rahmen sie vom Richter angeordnet worden ist. Schließlich sollte die Erhebung und Verwertung von genetischen Überschußinformationen aus dem „sprechenden" Bereich des menschlichen Genoms ausdrücklich verboten und mit Strafe bedroht werden.

Das inzwischen in Kraft getretene Gentechnikgesetz klammert ebenso wie das *Embryonenschutzgesetz*[40] Fragen der Genomanalyse am Menschen völlig aus. Nach wie vor ist vor allem ein effektives Verbot der Genomanalyse an Arbeitnehmern und Stellenbewerbern zu fordern. Auch die Anwendung der Genomanalyse durch Krankenversicherungs- und Lebensversicherungsgesellschaften muß dringend gesetzlich begrenzt werden.

In einer weiteren Entscheidung zum Strafverfahren hat der Bundesgerichtshof sich zum Problem der *Telefonüberwachung* geäußert. In einem Strafprozeß hatte ein Gericht die Telefonüberwachung eines Entlastungszeugen angeordnet, weil es diesen Zeugen für unglaubwürdig hielt. Das Ergebnis der Überwachung entlastete den Angeklagten sogar. Dennoch wurde in der Hauptverhandlung die Abhörmaßnahme nicht erwähnt. Erst nachdem der Angeklagte zu 6 Jahren Freiheitsstrafe verurteilt worden war, benachrichtigte die Staatsanwaltschaft ihn, daß man bei einem Zeugen ergebnislos das Telefon abgehört habe. Der Bundesgerichtshof sah dadurch den Grundsatz des fairen Verfahrens verletzt und hob das Urteil auf. Das Gericht betonte, daß dem Angeklagten und seinem Verteidiger die Tatsache und das Ergebnis der Telefonüberwachung eines Zeugen hätte mitgeteilt werden müssen, obwohl es dieses Ergebnis nicht für entscheidungserheblich hielt[41].

Auch das Bundesverfassungsgericht hat sich im Berichtszeitraum zu Fragen der informationellen Selbstbestimmung im Strafprozeß geäußert. Es hat einen formularmäßig ausgefüllten Haftbefehl gegen einen Demonstrationsteilnehmer für verfassungswidrig erklärt, in dem der Richter u. a. angekreuzt hatte, der Festgenommene sei von der Polizei angehört worden, habe aber keine Angaben gemacht. Das Bundesverfassungsgericht sah hierin eine Verletzung des Anspruchs auf rechtliches Gehör (Art. 103 Abs. 1 GG) und betonte, ein Dritter könne dieses Gehör nur vermitteln, wenn er das Vertrauen des Betroffenen genieße oder einer besonderen rechtsstaatlichen Objektivitätspflicht unterworfen sei. Der Betroffene müsse außerdem von der stellvertretenden Entgegennahme von Informationen und der Abgabe von Erklärungen in seinem Namen wissen. Im Regelfall eines nicht eilbedürftigen Gerichtsverfahrens könne das rechtliche Gehör nicht durch die Behörde vermittelt werden, deren Maßnahme in dem Gerichtsverfahren überprüft werden solle. Eine Aussage vor der Polizei entspreche daher selbst in Eilverfahren nur dem Grundrecht auf rechtliches Gehör, wenn der Betroffene wisse, daß seine Äußerung für das Gericht bestimmt sei[42].

Akteneinsicht zu Forschungszwecken

Die Senatsverwaltung für Justiz hat auf unsere Anregung hin alle aktenführenden Stellen in ihrem Bereich angewiesen, Richtlinien der Hamburgischen Justizverwaltung zur *Auswertung von Akten* (vor allem Gerichtsakten und Gefangenenpersonalakten) *für Forschungszwecke* entsprechend anzuwenden. Diese Richtlinien enthalten recht detaillierte Kriterien für die Entscheidung, wann für ein bestimmtes Forschungsprojekt Akteneinsicht in diese sensiblen Informationssammlungen gewährt werden darf. Damit ist auch für Wissenschaftler ein höheres Maß an Rechtssicherheit erreicht, die sich inzwischen außerdem an der Forschungsklausel (§ 30) des novellierten Berliner Datenschutzgesetzes orientieren können.

[37] BGH Urteil v. 21. 8. 1990 – 5 StR 145/80 –

[38] vgl. Anlage 1.4

[39] BGBl. 1990 I, S. 1349

[40] BGBl. 1990 I, S. 2746 – vgl. dazu Jahresbericht 1989, 4.3, S. 23

[41] Urteil vom 29. November 1989 – 2 StR 264/89 –

[42] Beschluß vom 30. Oktober 1990 – 2 BvR 562/88 –

3.7 Schule, Berufsbildung und Sport

Datenverarbeitung im Schulbereich

Noch immer werden über Berliner Lehrer bei der Senatsverwaltung für Schulwesen, Berufsbildung und Sport zahlreiche Daten in der *Lehrerindividualdatei* (LID) verarbeitet. Diese Datei enthält jeweils ca. 19 000 Datensätze für den Westteil und neuerdings auch für den Ostteil der Stadt, wobei jeder einzelne Datensatz u. a. Informationen über Geburtsdatum, Geschlecht, Staatsangehörigkeit, Beschäftigungsumfang, Zahl der Pflichtstunden, Zeiten der Vertretungsbereitschaft, Stundenermäßigungen und deren Gründe, die zu unterrichtenden Fächer, den Schulzweig, das derzeitige Rechtsverhältnis und die Dienstbezeichnung des Lehrers oder der Lehrerin enthält.

Diese Informationen dienen zwar nur statistischen Zwecken, sie werden aber noch immer auf problematische Weise bei der Senatsschulverwaltung verarbeitet[43], weil nur die Bezirke datenverarbeitende Stellen für diese Personaldaten sein können. Dies hatte die Senatsschulverwaltung bereits 1988 eingeräumt und mit der Entwicklung eines dezentralen Lehrer-Informations- und Verwaltungssystems (LIV) begonnen, das sie den Bezirken zur Verfügung stellen wollte und aus dem sie lediglich einen anonymisierten Statistikabzug erhalten soll. Das Schicksal und insbesondere die Finanzierung der LIV ist gegenwärtig ungewiß. Eine datenschutzgerechte Verarbeitung von Lehrerdaten im Land Berlin kann jedoch nicht mehr auf die lange Bank geschoben werden.

Die Verarbeitung von *Schülerdaten* verlagert sich zusehends aus den Schulen in die Wohn- und Arbeitszimmer von Lehrern. Diese Entwicklung, die durch die Ausführungsvorschriften über Schülerunterlagen notdürftig rechtlich abgesichert worden ist, findet bisher praktisch keinen Niederschlag in den Meldungen zum allgemeinen Dateienregister. Es ist davon auszugehen, daß die wenigen zu diesem Register gemeldeten Schülerdateien, die Lehrer auf ihrem privaten PC zu Hause führen, nur die Spitze des Eisberges sind. Wir haben der Verarbeitung von Schülerdaten auf privaten Rechnern der Lehrer seinerzeit zugestimmt, weil wir der Auffassung sind, daß ein völliges Verbot der Verarbeitung solcher Daten auf privaten Rechnern, wie es in einigen Bundesländern gilt, diese Datenverarbeitung nicht effektiv unterbinden würde; sie würde vielmehr unkontrolliert stattfinden.

Schulgesetzgebung

Die *Schulgesetzgebung* weist nach wie vor erhebliche datenschutzrechtliche Defizite auf. Immerhin hat die Senatsverwaltung für Schule, Berufsbildung und Sport uns im letzten Jahr zum ersten Mal den Entwurf einer Datenschutznovelle zum Schulgesetz zugeleitet, die wir bereits seit langem für erforderlich halten[44]. Allerdings ist dieser erste Entwurf in mehreren Punkten änderungs- und ergänzungsbedürftig.

Es genügt insbesondere nicht, dem für das Schulwesen zuständigen Senatsmitglied die pauschale Ermächtigung zu erteilen, irgendwann nähere Regelungen über die Verarbeitung personenbezogener Daten durch Rechtsverordnung zu treffen. Der Gesetzgeber kann nach der Rechtsprechung des Bundesverfassungsgerichts die wesentlichen Regelungen zur verfahrensrechtlichen Absicherung des Rechts auf informationelle Selbstbestimmung nicht dem Verordnungsgeber überlassen. Vielmehr muß er selbst den Umfang der Erhebung und Verarbeitung personenbezogener Daten zumindest im Grundsatz regeln und darüber hinaus entscheiden, in welchen Punkten Einsichtsrechte sowie Löschungs- und Berichtigungsansprüche Betroffener über das Berliner Datenschutzgesetz hinaus oder abweichend von diesem gewährt werden sollen. Lediglich Regelungen über den konkreten Umfang der Datenverarbeitung kann der Verordnungsgeber treffen. Der Entwurf einer entsprechenden Rechtsverordnung sollte gleichzeitig mit dem Entwurf eines Schulgesetzes in das Abgeordnetenhaus eingebracht werden, da nur so Art und Umfang von Schülerdaten im Zusammenhang erkennbar werden.

Der Schulgesetzgeber sollte selbst folgende prinzipiellen Entscheidungen treffen:

- In welchem Umfang und in welchen Schulstufen dürfen Leistungsdaten, insbesondere Zensuren automatisiert verarbeitet werden?
- Welche besonders sensiblen Informationen (z. B. zur Gesundheit der Schüler) dürfen in keinem Fall automatisiert verarbeitet werden?
- Unter welchen Voraussetzungen dürfen wissenschaftliche Forschungsvorhaben in der Schule durchgeführt werden?
- An welche öffentliche (insbesondere außerschulischen) Stellen dürfen Schülerdaten übermittelt werden? Die bloße Mitwirkung an der Erfüllung von Aufgaben nach dem Schulgesetz kann hierfür nicht ausreichen.
- Unter welchen Voraussetzungen dürfen schülerbezogene Daten an Privatpersonen (z. B. Eltern von Mitschülern) zur Durchsetzung von Schadensersatzansprüchen und zur Stellung von Strafanträgen weitergegeben werden?

Auch geplante Änderungen des *Schulverfassungsgesetzes* führten im Berichtszeitraum zu datenschutzrechtlichen Fragen.

Der Landesschulbeirat hatte vorgeschlagen, daß Schüler- und Elternvertreter an allen Klassenkonferenzen beteiligt werden sollen. Die Senatsschulverwaltung hatte hiergegen datenschutzrechtliche Bedenken. In der Tat kommt es darauf an, daß auch ein erweiterter Kreis der Teilnehmer an Klassenkonferenzen Verschwiegenheit über die dabei erörterten personenbezogenen Informationen bewahrt. Hierzu sind alle Gremienmitglieder nach dem Schulverfassungsgesetz verpflichtet. Soweit sie gegen diese Pflicht verstoßen, kann das betreffende Gremium sie zeitweise oder ganz von der weiteren Teilnahme ausschließen. Darüber hinaus machen sich Eltern und Schüler, die in ihrer Eigenschaft als Gremienmitglieder gegen das Beratungsgeheimnis verstoßen, ebenso wie sämtliche Lehrer strafbar, weil sie dadurch ein besonderes Amtsgeheimnis verletzen. Allerdings sollte die Möglichkeit geschaffen werden, Schüler unter 14 Jahren, die noch nicht strafrechtlich verantwortlich sind, von Klassenkonferenzen auszuschließen, soweit fremde Geheimnisse im Sinne des Strafrechts erörtert werden.

Auch ist darauf zu achten, daß schriftliche Unterlagen mit personenbezogenen Daten über Schüler oder Eltern, die zur Vorbereitung von Klassenkonferenzen verteilt werden, nur entweder an das ordentliche Mitglied der Konferenz oder seinen jeweiligen Vertreter ausgegeben werden. Eine pauschale Verteilung von Kopien an Gremienmitglieder und alle Vertreter würde zu einer unkontrollierbaren Streuung der Informationen führen.

Diese beiden Empfehlungen beziehen sich bereits auf das geltende Schulverfassungsgesetz und sind unabhängig davon, ob der Kreis der Teilnehmer an Klassenkonferenzen erweitert wird oder nicht.

Ein Personalrat hatte uns darauf hingewiesen, daß alle *Bewerbungen von Lehrern* bei den Bezirksämtern für den Schuldienst ohne Einwilligung der Betroffenen an die Senatsverwaltung für Schulwesen weitergeleitet und dort in einer Zentralen Bewerberkartei gespeichert wurden. In dieser Bewerberkartei wurden u. a. auch das Ergebnis der Zweiten Staatsprüfung und die Bezirke, bei denen sich der Betroffene beworben hatte, aufgenommen. Zunächst plante die Senatschulverwaltung, diese Kartei PC-gestützt weiterzuführen. Sie lehnte anfangs auch unsere dringende Empfehlung ab, die betroffenen Lehramtsbewerber um Einwilligung für die Übermittlung ihrer Bewerberdaten zu bitten, da für die Übermittlung ansonsten keine Rechtsgrundlage bestand. Lediglich zu einem entsprechenden nachträglichen Hinweis an die Betroffenen mit einem Widerspruchsrecht erklärte sie sich bereit. Inzwischen hat uns die Senatsschulverwaltung mitgeteilt, daß die Arbeiten an der EDV-gestützten zentralen Bewerberdatei eingestellt worden sind und auch keine Meldungen von den Bezirken über eingehende Bewerbungen verlangt werden.

Integration und Förderung behinderter Schüler

Ein behinderter Schüler, der bisher auf die Sonderschule ging, soll in eine Klasse der Grundschule mit nichtbehinderten Schülern aufgenommen werden. Hierzu wird ein Förderausschuß gebildet, dem der Schulleiter der zukünftigen Grundschule, der Klassenlehrer der

[43] vgl. Jahresbericht 1986, 4.4, S. 22 f.

[44] vgl. zuletzt Jahresbericht 1989, 4.7 S. 32

1. Klasse, der Leiter der schulpsychologischen Beratungsstelle, ein Sonderpädagoge und die Eltern des Kindes angehören. Außerdem werden der Jugendgesundheitsdienst für Schüler und das Jugendamt beteiligt und die Erzieher der besuchten Kindertagesstätte sowie die behandelnden Fachärzte hinzugezogen und befragt. Der Förderausschuß erstellt ein umfangreiches Fördergutachten und empfiehlt bestimmte Maßnahmen zum besonderen Förderbedarf und zur Einschulung des Schülers. Dieses Fördergutachten wird in die Schülerpersonalakte, den Schülerbogen, aufgenommen.

Jeder spätere Klassenlehrer wird das Fördergutachten lesen und seine Schlüsse daraus ziehen können. Diese können einerseits im Interesse des behinderten Schülers liegen. Andererseits dokumentieren sie auch auf Dauer seine Behinderung und wirken damit einer Integration geradezu entgegen.

Dieses Beispiel verdeutlicht, wie wichtig es ist, gerade bei dem ohne Frage sinnvollen Bemühen, behinderte Schüler unter bestimmten Umständen mit nichtbehinderten Schülern zusammen zu unterrichten, bei der Datenerhebung und Verarbeitung mit Augenmaß vorzugehen.

Der am 1. Februar 1991 in Kraft getretene neue § 10 a des Schulgesetzes regelt die *Integration von Schülern mit sonderpädagogischem Förderbedarf*. Danach umfaßt der Unterrichts- und Erziehungsauftrag der allgemeinen Schule nunmehr auch Schülerinnen und Schüler mit sonderpädagogischem Förderbedarf. Die Senatsverwaltung für Schulwesen wird ermächtigt, durch Rechtsverordnung weitere Regelungen insbesondere über die Feststellung des sonderpädagogischen Förderbedarfs und über das Verfahren zu treffen.

Aus datenschutzrechtlicher Sicht ist diese Regelung, an der wir nicht mitgewirkt haben, unzureichend. Zwar hat der Gesetzgeber dem Förderausschuß eine bestimmte Aufgabe zugewiesen. Eine Befugnis zur Verarbeitung personenbezogener Daten und damit zum Eingriff in das informationelle Selbstbestimmungsrecht des Schülers und seiner Eltern enthält das Gesetz jedoch nicht. Auch wird kein dem neuen Berliner Datenschutzgesetz vergleichbarer Datenschutz gewährleistet. Deshalb können die Förderausschüsse Daten über den Schüler ausschließlich auf der Grundlage einer informierten Einwilligung der Eltern erheben und verarbeiten. Dies gilt ohnehin für solche Tatsachen, die dem Berufsgeheimnis von Ärzten, Schulpsychologen, Sozialarbeitern und Erziehern unterliegen. Es kann auch nicht genügen, daß die Eltern, die eine Integration ihres Kindes in eine Klasse mit nichtbehinderten Kindern wünschen, pauschal alle diese Stellen von ihrer Schweigepflicht entbinden. Dies würde zu einem unüberschaubaren Informationsfluß – an den Eltern vorbei – führen, so daß diese nicht mehr wissen könnten, wer was wann wo über ihr Kind gesagt und geschrieben hat und wo diese Informationen letztlich landen.

Es dürfte deshalb schwer sein, die Eltern in der erforderlichen Weise über die Bedeutung ihrer Einwilligung aufzuklären, gerade weil zu Beginn der Beratungen des Förderausschusses noch gar nicht absehbar ist, welche schweigepflichtigen Personen zu welchen Teilen der „Kind-Umfeld-Diagnose" befragt werden müssen. Im Grunde können die Eltern wirksam nur in der Weise ihre schriftliche Einwilligung erklären, daß sie zunächst Gelegenheit erhalten, das jeweilige Gutachten oder die Information zur Kenntnis zu nehmen, die in den Förderausschuß eingebracht werden sollen. Letztlich wird man nicht umhin können, den Umfang der Datenerhebung und -verarbeitung genauer gesetzlich festzulegen. Dabei ist auch sicherzustellen, daß das Fördergutachten nicht offen im Schülerbogen aufbewahrt wird und ständig überprüft wird, ob es verzichtbar ist.

3.8 Stadtentwicklung und Umweltschutz

Die größten automatisierten Dateien bei der Senatsverwaltung für Stadtentwicklung und Umweltschutz sind die Stadtplanungsdatei mit ca. 115 000 Grundstücksdatensätzen und ca. 150 000 Gebäudedatensätzen und das Emissionskataster mit insgesamt über 200 000 Datensätzen. Für das Emissionskataster werden Daten aus dem „Belastungsgebiet Berlin" erhoben, die Auskunft über die zeitliche und räumliche Verteilung der Emissionen luftfremder Stoffe aus den Emittentengruppen Hausbrand, Industrie, Kleingewerbe und Verkehr geben. Alle diese Dateien enthalten auch personenbezogene Informationen z. B. über Einfamilienhäuser und Einzelkaufleute.

Ein Gewässerverschmutzer entdeckt den Datenschutz

Ein Unternehmen hat von der Wasserbehörde die Genehmigung erhalten, in bestimmtem Umfang Abwässer in die Spree einzuleiten. Diese Genehmigung enthält bestimmte Höchstwerte, die nicht überschritten werden dürfen. Sie werden ebenso wie die von Zeit zu Zeit tatsächlich festgestellte Abwassermenge in das Wasserbuch eingetragen. In dieses Wasserbuch kann jeder Einsicht nehmen, der ein berechtigtes Interesse darlegt. Ein Nachbar, dem die täglich an seinem Grundstück vorbeitreibende Brühe zu sehr stinkt, macht hiervon Gebrauch und geht zur Wasserbehörde, um in das Wasserbuch einzusehen. Der Sachbearbeiter ruft den Datensatz des Unternehmens an seinem Computer auf und läßt den wütenden Nachbarn am Bildschirm Einsicht in das Wasserbuch nehmen. Er selbst holt sich erst einmal einen Kaffee. Der Unternehmer erfährt hiervon und beschwert sich empört bei der Wasserbehörde und beim Datenschutzbeauftragten.

Dieser fiktive Fall verdeutlicht das Verhältnis zwischen Datenschutz und Informationsfreiheit in einer speziellen Situation. Das *Wassergesetz* räumt jedem Bürger, der ein berechtigtes Interesse darlegen kann, ein Recht auf Einsichtnahme ein. Die Aufbewahrung, Einsichtnahme und Fertigung von Auszügen ist jetzt durch die neugefaßte *Wasserbuchverordnung* geregelt worden. Die betroffenen Unternehmen haben zwar im Grundsatz Anspruch darauf, daß ihre Betriebs- und Geschäftsgeheimnisse von der für das Wasserbuch verantwortlichen Wasserbehörde gewahrt werden. Entsprechende Informationen müssen deshalb vor der Einsichtnahme aus dem Wasserbuch entfernt oder für den Zugriff gesperrt werden.

Diejenigen Informationen, die für den Nachbarn häufig jedoch besonders interessant sind, nämlich die von der Wasserbehörde festgesetzten Grenzwerte und die gemessenen Ist-Werte, also das was die Behörde selbst festgestellt hat, sind keine Betriebs- oder Geschäftsgeheimnisse. Sie lassen auch keinen Rückschluß auf bestimmte Produktionsverfahren des Unternehmens zu. Bei einer Abwägung zwischen dem Unternehmensinteresse an der Geheimhaltung dieser Informationen und dem Informationsinteresse der Nachbarn und anderer betroffener Bürger wird das Unternehmen die Bekanntgabe der Ist- und Soll-Werte hinzunehmen haben. Überdies geben die genehmigten Grenzwerte und die tatsächlich gemessenen Ist-Werte auch Auskunft über Entscheidungen und die Überwachungspraxis der Wasserbehörde, für deren Geheimhaltung es ohnehin keine Rechtfertigung gibt.

Der Beispielsfall führt noch zu einem anderen Problem, das mit Sicherheit an praktischer Bedeutung gewinnen wird. Die Wasserbehörde plant tatsächlich, zumindest Teile des Wasserbuches auf elektronischen Datenträgern zu führen und Bürgern, die ein berechtigtes Interesse dargelegt haben, auch auf dem Bildschirm die Einsichtnahme in das Wasserbuch zu ermöglichen. Dies ist datenschutzrechtlich allerdings nur dann zulässig, wenn sichergestellt ist, daß der Einsichtnehmende die Daten nur lesen und nicht verändern kann. Technisch läßt sich dies am besten in der Weise sicherstellen, daß der Bürger auf einem sog. abgesetzten Bildschirm möglichst auch in einem gesonderten Raum nur einen bestimmten Bildschirminhalt zu sehen bekommt. Über diesen abgesetzten Bildschirm kann er nicht auf die Datei selbst zugreifen oder sie gar verändern.

Gesetzgebung

Auch im *Umweltbereich* läuft die Uhr für die Verarbeitung personenbezogener Daten im gesetzesfreien Raum ab. Das Berliner Datenschutzgesetz gestattet sie nur noch übergangsweise im Rahmen der Erforderlichkeit für die Aufgabenerfüllung der jeweils datenverarbeitenden Stelle bis zum Ende dieses Jahres. Gerade im Interesse eines effektiven Umweltschutzes müssen deshalb bereichsspezifische Regeln für die Verarbeitung von personenbezogenen Daten auch in diesem Bereich baldmöglichst geschaffen werden.

Dies gilt auch für das flächendeckende rechnergestützte *Altlastenverdachtsflächenkataster*, das die Senatsverwaltung für Stadtentwicklung und Umweltschutz im Rahmen eines gemein-

sam mit dem Umweltbundesamt durchgeführten Projektes „Ökologisches Planungsinstrumentarium Berlin" aufgebaut hat. Es bietet die Möglichkeit, zunächst im Westteil der Stadt eine Übersicht über die Verteilung der Altlasten zu erhalten.

Dies ist aus datenschutzrechtlicher Sicht unproblematisch, soweit Grundstücke des Landes Berlin (z. B. der Berliner Stadtreinigung) oder juristischer Personen des Privatrechts betroffen sind. Darauf soll sich das Kataster jedoch nicht beschränken, sondern es sollen auch personenbezogene Daten anderer Grundstückseigentümer verarbeitet werden. Dies ist nur auf der Grundlage einer bereichsspezifischen gesetzlichen Regelung zulässig, die die Verwendung entsprechender personenbezogener Daten für die Zwecke der Altlastenkartierung regeln muß. Da das europäische Gemeinschaftsrecht inzwischen im Umweltrecht die Mitgliedsstaaten zu einer verstärkten Transparenz ihrer Verwaltungsentscheidungen und Datensammlungen verpflichtet, liegt es nahe, Dritten auch das Recht auf Auskunft oder Einsichtnahme in das Altlastenverdachtsflächenkataster ebenso wie in das Wasserbuch zu eröffnen. Auch hierfür ist eine normenklare Regelung erforderlich, die den schützenswerten Belangen der Betroffenen Rechnung trägt. Insbesondere muß auch diese Regelung festlegen, wann ein geheimzuhaltendes Betriebs- und Geschäftsgeheimnis vorliegt und wann nicht. Auch ist die schwierige Frage zu beantworten, welche Daten des Katasters überhaupt einen Personenbezug aufweisen. Der Umstand, daß sich auf einem bestimmten Grundstück eine Altlast befindet oder von einem Grundstück eine bestimmte Schmutzfahne im Grundwasser herrühren könnte, verweist nämlich nicht nur oder evtl. überhaupt nicht auf den gegenwärtigen Grundstückseigentümer, sondern auch oder in erster Linie auf frühere Eigentümer oder Nutzer dieses Grundstücks. Hier ergeben sich völlig neuartige datenschutzrechtliche Fragestellungen, die einer gesetzlichen Klärung bedürfen. Die Senatsverwaltung für Stadtentwicklung und Umweltschutz hat inzwischen ihre Absicht erklärt, die notwendigen datenschutzrechtlichen Vorschriften zum Altlastenverdachtsflächenkataster in ein geplantes Bodenschutzgesetz aufzunehmen.

Aufgrund einer Änderung des Berliner Wassergesetzes ist die sog. *Indirekteinleiter-Verordnung* erlassen worden. Danach bedarf jeder, der gefährliche Stoffe in bestimmtem Umfang oder bestimmter Konzentration in die öffentlichen Abwasseranlagen einleitet (z. B. der Zahnarzt, der Amalgamreste wegspülen läßt) einer Genehmigung durch die Wasserbehörde.

Diese hat uns um Rat gefragt, wie die Namen und Anschriften der betroffenen Indirekteinleiter ermittelt werden könnten, damit sie über diese Genehmigungspflicht und mögliche rechtliche Auswirkungen informiert werden könnten. Eine direkte Adressenübermittlung durch die Ärztekammer, die Zahnärztekammer, die Handwerksinnungen oder die Bezirksämter (Abt. Wirtschaft) schied aus, da eine Rechtsgrundlage für die Übermittlung dieser Daten fehlt. Allerdings können die betroffenen Kammern oder Körperschaften ihre Mitglieder über die neue Rechtslage informieren. Lediglich in die Handwerksrolle und das Verzeichnis der Inhaber handwerksähnlicher Betriebe bei der Handwerkskammer kann bei Nachweis eines berechtigten Interesses auch von der Wasserbehörde Einsicht genommen werden.

Zur Durchsetzung der Indirekteinleiter-Verordnung wollten die Berliner Wasserbetriebe auf die Daten der Wasserbehörde zugreifen, um z. B. ihr Personal bei der Begehung des Abwasserrohrnetzes schützen zu können. Umgekehrt war auch die Wasserbehörde an Daten der Wasserbetriebe z. B. über die Abwassermenge bei einzelnen Einleitern interessiert. Diese gegenseitige Übermittlung von personenbezogenen Daten ist jetzt möglich, nachdem die Verordnung über die Genehmigungspflicht für das Einleiten gefährlicher Stoffe und Stoffgruppen in öffentliche Abwasseranlagen und ihre Überwachung (VGS) entsprechend unserem Vorschlag um eine Regelung ergänzt worden ist, die die gegenseitige Übermittlung personenbezogener Daten im jeweils erforderlichen Umfang zuläßt. Sie beschränkt sich auf Namen und Anschrift des Indirekteinleiters, Herkunftsbereich des betreffenden Abwassers, Ergebnisse vorliegender Abwasseruntersuchungen sowie Anforderungen nach dem Stand der Technik, die im Genehmigungsbescheid aufgegeben wurden. Soweit die datenverarbeitende Stelle die übermittelten Daten zur rechtmäßigen Erfüllung ihrer Aufgabe nicht mehr benötigt, sind sie zu löschen.

3.9 Wirtschaft und Verkehr

Die Informationsverarbeitung in diesen Geschäftsbereichen wird vor allem von den kommerziellen Anwendungen der nachgeordneten Stellen geprägt, seien dies die von der Senatsverwaltung für Wirtschaft beaufsichtigten großen Anstalten des öffentlichen Rechts wie etwa die Berliner Sparkasse (die Datenverarbeitung auf einem sehr hohen technischen und Sicherheitsniveau betreibt), seien es die verschiedenen Eigenbetriebe oder Kammern. Demgegenüber ist die Automation der Wirtschaftsverwaltung selbst eher langsam vorangeschritten. Die wichtigsten Verfahren sind hier die in der Einführung begriffenen dezentralen, aber einheitlich strukturierten bezirklichen Gewerbedatenbanken.

Gewerbedatenbank

Das *ADV-Verfahren Gewerbedatenbank (GEWDAT)*, mit dem jetzt die Führung der Datei der Gewerbeanzeigen und die Durchführung der in der Gewerbeordnung vorgesehenen Benachrichtigungen automatisiert werden sollen, ist als Pilotanwendung in einem Bezirksamt auf der Basis eines lokalen PC-Netzes erprobt worden.

Es werden nur diejenigen Daten gespeichert, die für die gesetzmäßige Aufnahme, Weiterführung und Beendigung eines Gewerbebetriebes benötigt werden. Im Gegensatz zu früher, als die Bearbeiter zum Teil mehr Informationen erlangten als für ihre Aufgabe erforderlich war, ist nunmehr ein vom System gesteuerter, differenzierter Zugriff möglich.

Automationsunterstützung der betriebsärztlichen Betreuung

Der *TÜV* nimmt für einige Bezirksämter die Aufgaben der durch das Arbeitssicherheitsgesetz gebotenen *betriebsärztlichen Betreuung* wahr. Dafür speichert er die bei der arbeitsmedizinischen Betreuung der Mitarbeiter der Bezirksämter anfallenden Daten. Diese betriebsärztliche Betreuung beruht auf dem Arbeitssicherheitsgesetz, nach der der Betriebsarzt verpflichtet ist, alle Untersuchungen zu erfassen und auszuwerten.

Für die elektronische Datenverarbeitung wird ein PC-Netz von drei Sachbearbeiterinnen genutzt, die jeweils für verschiedene zu betreuende Dienststellen bzw. Firmen zuständig sind, sich aber untereinander vertreten. Betriebsärzte greifen selbst nicht auf die Dateien zu, sondern erhalten jeweils von der Sachbearbeiterin einen Ausdruck, der für die jeweilige Untersuchung benötigt wird.

Es muß dabei sichergestellt werden, daß die in der ärztlichen Berufsordnung vorgesehenen Abschottungen einzuhalten sind. § 2 Abs. 6 der Berufsordnung der Ärztekammer Berlin sieht vor, daß die Ärzte, die gleichzeitig oder nacheinander den gleichen Patienten untersuchen oder behandeln, untereinander nur dann von der Schweigepflicht befreit sind, wenn ein Einverständnis des Patienten anzunehmen ist. Anderenfalls muß sichergestellt sein, daß nicht jeder Arzt des betriebsärztlichen Dienstes des TÜV Patientendaten seiner Kollegen zur Kenntnis nehmen kann. Wir haben ferner darauf hingewiesen, daß die Sachbearbeiterinnen berufsmäßig tätige Gehilfen des Arztes im Sinne der §§ 203 Abs. 3 StGB, 2 Abs. 3 Berufsordnung der Ärztekammer Berlin sind, die ebenso wie der Arzt selbst der Pflicht zur Verschwiegenheit unterliegen. Für diese muß ebenso wie für den betreffenden Arzt sichergestellt sein, daß der Zugriff nur auf die erforderlichen Datenbestände möglich ist. Ein generelles Zugriffsrecht aller das PC-Netz benutzenden Mitarbeiterinnen auf den gesamten Datenbestand muß ausgeschlossen werden.

Während der TÜV in anderen Bundesländern die Probanden lediglich darüber informiert, daß die von ihnen erfaßten Daten nur für Zwecke der medizinischen Untersuchung im Rahmen des Arbeitssicherungsgesetzes elektronisch gespeichert werden, hat sich der TÜV Berlin für eine datenschutzfreundlichere Lösung entschieden. Danach sollen die Daten nur dann elektronisch gespeichert werden, wenn der Betroffene seine Zustimmung hierfür erteilt. Darüber hinaus wird sich der TÜV in den Verträgen mit den Behörden, die ihm die Aufgaben des betriebsärztlichen Dienstes übertragen, der Kontrolle durch den Berliner Datenschutzbeauftragten unterwerfen. Ein datenschutzgerechtes Ver-

fahren bei der Einführung der elektronischen Datenverarbeitung im Zusammenhang mit der arbeitsmedizinischen Betreuung von Dienstkräften der Bezirksämter ist somit ebenso wie dessen Überwachung sichergestellt worden.

Verbraucherkreditgesetz

Am 1. Januar 1991 ist das neue *Verbraucherkreditgesetz* in Kraft getreten[45]. Trotz der verbraucherfreundlichen Tendenz dieses Gesetzes hat es der Bundesgesetzgeber versäumt, die Anregungen der Datenschutzbeauftragten zur Stärkung des informationellen Selbstbestimmungsrechts der Kreditnehmer aufzugreifen. Insbesondere läßt das Gesetz eine Regelung der wichtigen Frage vermissen, welche Negativmerkmale in Kreditinformationssystemen (z. B. der Schufa) verarbeitet werden dürfen. Das bisher praktizierte Einwilligungsmodell der Banken haben wir mehrfach kritisiert, weil es in der Bundesrepublik keine Bank gibt, die ein „schufaloses" Konto anbietet. Auch sind die Voraussetzungen und Grenzen der Erhebung, Speicherung und Übermittlung personenbezogener Kreditdaten bisher nicht bereichsspezifisch festgelegt. Die Informationsrechte des Verbrauchers über die möglichen Empfänger von Kreditdaten und die Löschungsfristen sollten ebenfalls gesetzlich präzisiert werden. Der Bundesgesetzgeber hat eine wichtige Gelegenheit verpaßt, den Zusammenhang zwischen Verbraucherschutz und Datenschutz deutlich zu machen. Viele Bürger empfinden die massenhafte Datenverarbeitung durch private Auskunfteien und das Risiko ihrer Zweckentfremdung als einen mindesten ebenso gravierenden Eingriff in ihr informationelles Selbstbestimmungsrecht wie die Datenverarbeitung öffentlicher Stellen.

Im Bereich der *Eigenbetriebe* zeigt ein Fall, mit wie wenig Aufwand ein erheblicher Erfolg für den Schutz vor informationeller Diskriminierung erreicht werden kann.

Zeitkarten für Arbeitslose und Sozialhilfeempfänger bei der BVG

Viele Arbeitslose und Sozialhilfeempfänger haben es als unnötige Diskriminierung empfunden, daß ihre leuchtend grünen und doppelt so großen BVG-Zeitkarten sie bis Mitte des Jahres dem Personal der BVG und auch allen Umstehenden beim Vorzeigen sofort als Sozialleistungsempfänger erkennbar machten und daß sie somit ein Sozialgeheimnis offenbaren mußten.

Unsere Empfehlung, die Karten neutral zu gestalten, lehnte die BVG zunächst ab. Erst nach zähen Verhandlungen und wachsendem öffentlichen Unmut hat die BVG sämtliche persönliche Zeitkarten farblich einheitlich gestaltet, also auch das Schülerticket, das Ausbildungsticket und die Seniorenkarte. Außerdem haben jetzt alle Zeitkarten das einheitliche Format DIN A 7.

Unnötige und erniedrigende Bloßstellungen werden damit in diesem Bereich vermieden.

3.10 Wissenschaft und Forschung

Die Senatsverwaltung für Wissenschaft und Forschung hat selbst nur wenige personenbezogene Dateien zum Dateienregister gemeldet. In großem Umfang werden dagegen personenbezogene Daten von den Berliner Hochschulen (Freie Universität, Technische Universität) und den übrigen Großforschungseinrichtungen verarbeitet. Aus dem gesamten Geschäftsbereich der Senatsverwaltung für Wissenschaft und Forschung liegen derzeit insgesamt 140 Meldungen zum Allgemeinen Dateienregister vor – eine Zahl, die sicherlich angesichts der Vielfalt von Forschungsaktivitäten nicht der Realität entspricht und deswegen künftig erhebliche Nachfragen erforderlich machen wird.

Hochschulgesetz

Bei der *Novellierung des Berliner Hochschulgesetzes* hätte die Möglichkeit bestanden, erstmals die Verarbeitung personenbezogener Daten insbesondere der Studenten, aber auch des Personals auf eine verfassungskonforme Rechtsgrundlage zu stellen. Trotz unserer detaillierten Vorschläge für entsprechende Regelungen, denen die Senatsverwaltung für Wissenschaft und Forschung grundsätzlich zugestimmt hatte, ist diese Möglichkeit vom Gesetzgeber zum zweiten Mal in Folge seit 1986[46] nicht genutzt worden. Auch das novellierte Berliner Hochschulgesetz[47] enthält eine unveränderte Vorschrift über Erhebungen für statistische Zwecke, die in dieser Form verfassungswidrig ist. Auf diese Vorschrift kann keine Erhebung personenbezogener Daten an den Berliner Hochschulen gestützt werden. Statistische Erhebungen, die über die Hochschulstatistik des Bundes hinausgehen, bedürfen vielmehr einer gesetzlichen Grundlage, die Zweck und Umfang der Datenerhebung normenklar festlegt. Dagegen können weder die Senatsverwaltung für Wissenschaft und Forschung noch das Kuratorium einer Hochschule die Erhebung personenbezogener Daten für Zwecke der Hochschulstatistik und -planung mit Auskunftspflicht anordnen.

Sehr viel gravierender ist jedoch der Umstand, daß das neue Hochschulgesetz nicht die verfassungsrechtlich gebotene Befugnis zur Verarbeitung von *Studentendaten* enthält. Dies hat zur Folge, daß die gegenwärtig stattfindende Verarbeitung von Studentendaten nur noch übergangsweise, nämlich längstens bis zum 31. Dezember 1991 auf der Grundlage des § 34 Abs. 1 BlnDSG rechtmäßig erfolgen kann, soweit sie zur Erfüllung der Aufgaben der jeweiligen Hochschule erforderlich ist. Nach Ablauf dieser Frist würde die Verarbeitung von Studentendaten an allen Berliner Hochschulen ohne gesetzliche Grundlage erfolgen, wenn das Berliner Hochschulgesetz nicht rechtzeitig um eine entsprechende Verarbeitungsbefugnis ergänzt wird. Diese Frage darf deshalb auch nicht bis zu der in der Koalitionsvereinbarung festgelegten Gesamtrevision des Berliner Hochschulgesetzes aufgeschoben werden, die für Ende 1992 vorgesehen ist.

Auch die Formulierung der Befugnisse der *Frauenbeauftragten* in Bewerbungsverfahren an den Hochschulen ist mißverständlich und umschreibt die Rechte der Frauenbeauftragten auf Einsicht in Bewerbungsunterlagen und auf Teilnahme an Bewerbungsgesprächen nicht mit derselben Deutlichkeit wie z. B. das Landesantidiskriminierungsgesetz.

Schließlich muß das Hochschulgesetz um eine Regelung der Verarbeitung personenbezogener Daten der *Bibliotheksbenutzer* ergänzt werden. Dies kann nicht den Bibliotheks- bzw. Benutzungsordnungen der einzelnen Hochschulbibliotheken überlassen bleiben.

Hochschulstatistikgesetz

Die eindeutige gesetzliche Regelung der Verarbeitung personenbezogener Daten an den Hochschulen ist auch deshalb vordringlich, weil am 1. Juni 1992 das neue *Hochschulstatistikgesetz* des Bundes in Kraft tritt, das nach langjährigen Beratungen die gesamte Hochschulstatistik endlich auf eine verfassungskonforme Grundlage stellt[48]. Das neue Gesetz sieht vor, daß die erforderlichen Daten für die Hochschulstatistik nicht mehr durch Befragung der betroffenen Studenten oder Hochschulmitarbeiter erhoben werden sollen, sondern diese Daten als Sekundärstatistik von den Hochschulen, Prüfungsämtern und Studentenwerken an die Statistischen Landesämter übermittelt werden. Lediglich die Schüler in Abschlußklassen von Bildungseinrichtungen der Sekundarstufe II werden selbst danach gefragt, welches Studium sie an welchem Ort aufnehmen wollen. Diese Befragung ist jedoch freiwillig. Mit dieser Regelung ist ein echter Fortschritt im Bereich der Hochschulstatistik erreicht worden, zumal ursprüngliche Pläne für eine Studienverlaufsstatistik, bei der ein Profil des einzelnen Studenten vom Anfang bis zum Ende seines Studiums erstellt worden wäre, fallengelassen wurden.

Allerdings wird dieser Fortschritt in Berlin solange gefährdet sein, wie der Landesgesetzgeber das Hochschulgesetz nicht dem Hochschulstatistikgesetz des Bundes anpaßt. Da die Hochschulstatistik in Zukunft nur noch aus Daten gespeist wird, die von den Hochschulen erhoben werden, müssen die Hochschulen ihrerseits die Befugnis zur Erhebung und Verarbeitung der entsprechenden personenbezogenen Daten erhalten. Solange dies nicht geschieht, kann auch keine Hochschulstatistik nach dem neuen Modell durchgeführt werden. Insbesondere muß der Umfang der Daten, den die Hochschulen für eigene Verwaltungszwecke benö-

[45] BGBl. 1990 I, S. 2830 ff.

[46] Vgl. Jahresbericht 1986, S. 22.

[47] GVBl. 1990, S. 2165 ff.

[48] Hochschulstatistikgesetz vom 2. November 1990, BGBl. I, S. 2414.

tigen, definiert und mit den Merkmalen verglichen werden, die die Hochschulen nach dem Hochschulstatistikgesetz an die amtliche Statistik liefern müssen. Dem Studenten oder Hochschulmitarbeiter, dessen Daten verarbeitet werden sollen, muß eindeutig gesagt werden, für welche Zwecke seine Daten erhoben werden. Sollten Daten ausschließlich für Zwecke der Hochschulstatistik, aber nicht der Hochschulverwaltung, benötigt werden, so ist durch das Erhebungsverfahren sicherzustellen, daß derartige Daten getrennt von der Hochschulverwaltung erhoben und direkt dem Statischen Landesamt übermittelt werden, ohne daß sie für Verwaltungszwecke genutzt werden können.

Bei der letzten Erhebung des wissenschaftlichen und künstlerischen Personals schickte das Statistische Landesamt den Befragten mit den Erhebungsunterlagen ein Rücksendekuvert, das den Zusatz „über Freie Universität Berlin - II E 20 -" enthielt. Dadurch wurde bei den Auskunftspflichtigen der unzutreffende Eindruck erweckt, sie müßten ihre statistischen Angaben auf dem Fachpostweg über die Hochschule an das Statistische Landesamt schicken. In Wirklichkeit konnten sie sich entscheiden, ob sie diesen Weg wählen wollten oder ihre Angaben auf dem direkten Postweg an das Statistische Landesamt schicken wollten. Auf dieses Wahlrecht wurden die Auskunftspflichtigen im Erhebungsbogen nur versteckt hingewiesen. Außerdem waren die Hilfsmerkmale auf einem weiteren Adreßaufkleber direkt auf dem Erhebungsbogen angebracht, so daß der betroffene Bürger Zweifel daran haben mußte, wie die amtliche Statistik ihrer Verpflichtung nachkommen wollte, die Hilfsmerkmale unverzüglich nach Abschluß der Prüfung auf Vollständigkeit und Schlüssigkeit von den Erhebungsmerkmalen zu trennen und zu vernichten.

Das zuerst genannte Problem wird in dieser Form schon deshalb nicht mehr auftreten, weil eine unmittelbare Befragung des wissenschaftlichen und künstlerischen Personals der Hochschulen nach dem neuen Hochschulstatistikgesetz nicht mehr vorgesehen ist. Unsere Empfehlungen zur Fragebogengestaltung will das Statistische Landesamt „im Rahmen der technischen und haushaltsmäßigen Rahmenbedingung" bei der Neugestaltung der Erhebungsunterlagen berücksichtigen. Dies wird in Zukunft nur noch bei der Befragung der Schüler in Abschlußklassen von Bedeutung sein, die als einzige nach dem neuen Hochschulstatistikgesetz selbst befragt werden. Auch in diesem Fall dürfen jedoch „haushaltsmäßige Rahmenbedingungen" nicht zu Lasten einer datenschutzgerechten Gestaltung der Erhebungsbogen gehen.

Bei der letzten Erhebung des wissenschaftlichen und künstlerischen Personals nach dem alten Hochschulstatistikgesetz hat das Statistische Landesamt auf die förmliche Zustellung von Aufforderungsbescheiden und Zwangsmaßnahmen gegen die Auskunftspflichtigen verzichtet, da die Rücklaufquote auch ohne derartige Maßnahmen aus statistischer Sicht ausreichend war. Eine förmliche Zustellung auf dem Dienstweg wäre auch unzulässig gewesen, da auf diese Weise die Hochschule von der Tatsache erfahren hätte, daß einer ihrer Mitarbeiter seiner Auskunftspflicht nicht genügt hat.

Wissenschaftsklausel im Berliner Datenschutzgesetz

Das neue Berliner Datenschutzgesetz enthält erstmals eine allgemeine *Wissenschaftsklausel* (§ 30 BlnDSG). Sie ändert nichts an dem Grundsatz, daß Forscher personenbezogene Daten in aller Regel nur mit Einwilligung der betroffenen Personen verarbeiten dürfen. Überdies wird diese Regelung den Besonderheiten einzelner Forschungsbereiche (z. B. Justizforschung, zeitgeschichtliche Forschung) nicht gerecht. Sie kann nur ein erster Schritt auf dem Weg zu einer bereichsspezifischen Datenschutzgesetzgebung für einzelne Forschungszweige sein, die ihrerseits durch Richtlinien und Verhaltenscodices ergänzt werden sollten, die von den Forschern und ihren Berufsvereinigungen selbst entwickelt werden müssen.

Berliner Altersstudie

Aus der Vielzahl von Forschungsvorhaben, die uns zur Begutachtung vorgelegt worden sind, ist ein Projekt der Akademie der Wissenschaften zu Berlin besonders anschaulich:

Sie führt in Zusammenarbeit mit dem Max-Planck-Institut für Bildungsforschung und medizinischen Einrichtungen der Freien Universität Berlin eine *Berliner Altersstudie* durch. Ziel der Studie ist es, ein wissenschaftlich fundiertes Gesamtbild der Lebenssituation älterer Menschen in Berlin zu erhalten. Im Rahmen dieser Studie werden Interviews, Tests, Befragungen und medizinische Untersuchungen vorgenommen.

Über jede befragte Person wird ein außerordentlich umfangreicher und sensibler Datensatz aufgebaut, der umfassende Informationen über den physischen und psychischen Zustand des Betroffenen enthält.

Die in Betracht kommenden Studienteilnehmer sind in deutlicher Form auf die Freiwilligkeit der Teilnahme, auf die geplante Speicherungsdauer der zu erhebenden Daten, auf geplante Übermittlungen und auf ihren zu jeder Zeit bestehenden Löschungsanspruch hinzuweisen. Darüberhinaus ist eine Einwilligung erforderlich, wenn Daten des Befragten nach dessen Tod weiter verarbeitet werden sollen. Anderenfalls wäre eine Anonymisierung der Daten geboten.

Für die Nutzung der erhobenen Daten durch andere Wissenschaftler soll eine Makrodatenbank aufgebaut werden, die aus verschiedenen Dateien besteht, die auch getrennt abgefragt werden können. Dabei sollte der unterschiedliche Datenzugriff durch Paßwörter geregelt werden. Insbesondere sollten die Mikrodaten versiegelt werden, so daß sie für externe Forscher nicht sichtbar sind.

Bei dieser Studie werden von verschiedenen Instituten der Freien Universität Daten erhoben, die auch dort zwischengelagert werden und die die dort tätigen Forscher zur Eigenforschung weiterverwenden wollen. Vom Hochschulgesetz ist diese Eigenforschung zwar gedeckt, der befragte alte Mensch, der seine Einwilligung nur gegenüber der Akademie abgegeben hat, kann jedoch nicht wissen, daß seine Daten auch an Hochschulinstituten für andere Forschungszwecke versandt werden sollen. Auch diese anderweitige Verwendung der Daten ist deshalb nur zulässig, wenn die Betroffenen ihr nach vorheriger Information zustimmen.

Die Forscher wollen auch dann bestimmte Daten der Betroffenen erheben, wenn diese an der Studie nicht teilnehmen wollen. So soll u. a. die Forschungsassistentin ihre Beobachtungen bei der Kontaktaufnahme dokumentieren (Geruch, Aussehen, psychische Auffälligkeiten). Wir haben darauf hingewiesen, daß es sich hierbei auch um die Erhebung personenbezogener Daten handelt. Diese dürften mangels Einwilligung in einen Beobachtungsbogen nur in anonymisierter Form eingehen (Geburtsjahr, ID-Nr., Geschlecht, Familienstand, Bezirk, statistisches Gebiet und Teilnahmeintensität). Bei dem Merkmal Teilnahmeintensität soll ferner gespeichert werden, ob es sich bei der Person um einen „Verweigerer" handelt, eine Person, die die Beendigung der Befragung wünschte, sowie die Begründung dieses Wunsches.

Bei Zweifeln an der Einwilligungsfähigkeit der befragten Person soll die Forschungsassistentin den möglichen Grund dokumentieren. Dabei soll sie den Betroffenen fragen, ob sie beim nächsten Mal einen Arzt mitbringen könne. Dieser solle feststellen, ob die befragte Person einwilligungsfähig ist und den Grund benennen. Auch hierfür ist schon anfangs der Personenbezug zu beseitigen. Ferner ergibt sich hier das Problem, daß der Arzt der ärztlichen Schweigepflicht unterliegt, von der er von einem nicht-einwilligungsfähigen Befragten auch nicht wirksam entbunden werden kann, so daß der Arzt zur Offenbarung der erhobenen Daten gar nicht befugt wäre.

3.11 Technik, Organisation und Geschäftsordnung

Ergebnisse weiterer Prüfungen von PC-Anwendungen

Die im vorigen Berichtsjahr begonnene schwerpunktmäßige *Prüfung von PC-Anwendungen* wurde fortgeführt. Dabei lag das Hauptaugenmerk auf bezirks- bzw. behördenübergreifenden Verfahren und solchen, bei denen besonders sensible personenbezogene Daten verarbeitet werden.

Der steigende Beratungsbedarf in datenschutzrechtlichen Fragen bei PC-Anwendungen deutet an, daß die datenschutzrechtliche und sicherheitstechnische Problematik bei PC-gestützten Verfahren zunehmend erkannt wird. Das Ziel, durch eine im

Vorfeld zum Echtbetrieb stattfindende oder verfahrensbegleitende Beratung Fehler zu vermeiden, die einem datenschutzgerechten Einsatz von Einzelplatzsystemen entgegenstehen würden, ist jedoch noch nicht erreicht. So wurde bei der Prüfung bereits laufender Verfahren eine Vielzahl von typischen, aber meist auch vermeidbaren technisch-organisatorischen Mängeln festgestellt, die im wesentlichen auf Nachlässigkeit oder fehlendes „know-how" zurückzuführen sind.

Einsatz von Sicherheitssoftware

Positiv zu vermerken ist, daß speziell für Einzelplatzsysteme entwickelte *Datenschutzprogramme* auch in der Berliner Verwaltung verstärkt eingesetzt werden. Hier hat sich nicht zuletzt durch die Beratungstätigkeit des Landesamtes für Elektronische Datenverarbeitung ein Produkt als Quasi-Standard für die Berliner Verwaltung etabliert, das vom Hersteller stetig weiterentwickelt und damit den meisten datenschutzrechtlichen Anforderungen angepaßt wurde.

Mit der Komplexität der zur Verfügung gestellten Sicherheitsfunktionen sind aber auch die Anforderungen gestiegen, die an die verantwortliche Person für eine ordnungsgemäße und datenschutzgerechte Installation gestellt werden. Die Ergebnisse der Prüfungen haben jedoch gezeigt, daß es in Unkenntnis der Gefahrenquellen und der gesetzlichen Anforderungen oft als ausreichend erachtet wurde, die Einzelplatzsysteme lediglich gegen einen unbefugten Zugriff außenstehender Dritter zu schützen. Dabei wird verkannt, daß die größte Gefahr von den Mitarbeitern ausgehen kann, die die Zugriffsberechtigung für das System besitzen.

Obwohl in diesen Fällen die geforderte Datenschutzsoftware eingesetzt wurde, mußten die unzureichenden Speicher-, Benutzer-, Zugriffs- und Eingabekontrollen sowie Verstöße gegen die Organisationskontrolle bemängelt werden.

Kontrolle eines *PC-gestützten Verfahrens einer bezirklichen Ausbildungsleitung* ergab, daß alle Benutzer nicht nur die gleiche Zugriffsberechtigung besaßen, sondern sich darüber hinaus die Benutzerkennungen und die dazugehörenden Berechtigungen selbst einrichten durften. Jeder Benutzer hatte über das eingesetzte Anwendungsprogramm uneingeschränkten Zugriff auf das Betriebssystem und war so zumindest theoretisch in der Lage, umfangreiche Manipulationen einschließlich des Ausschaltens der Sicherheitssoftware durchzuführen. Eingaben am System wurden zwar protokolliert, die Protokolldatei wurde aber aufgrund fehlender Kenntnisse nicht ausgewertet.

Bei anderen Prüfungen konnte nachgewiesen werden, daß ein installiertes Sicherheitssystem von einem berechtigten Benutzer ausgeschaltet werden konnte, indem über einen Seiteneinstieg eines Anwendungsprogramms auf das Betriebssystem zugegriffen und dort die Programmdateien der Datenschutzsoftware gelöscht wurden. Ebenso war es möglich, die von der Sicherheitssoftware erstellten Protokolle zu manipulieren.

In einem in einer *bezirklichen Personalverwaltung* eingesetzten PC war keine Datenschutzsoftware installiert, die eine mögliche unbefugte Eingabe sowie Kenntnisnahme, Veränderung oder Löschung gespeicherter personenbezogener Daten verhindern konnte. Ein „selbstprogrammierter Zugriffsschutz" war unzureichend und entsprach nicht den Anforderungen an ein ordnungsgemäßes Paßwortverfahren. Das Zugriffsschutzverfahren war in einer Programmdatei eingebunden, deren Abarbeitung durch einen einfachen Befehl unterbrochen werden konnte. Danach befand man sich im Betriebssystem und hatte ungehinderten Zugriff auf alle relevanten Programmteile und Daten. Unabhängig davon wurde das Paßwort bei der Eingabe auf dem Bildschirm sichtbar, so daß auch ein Ausspähen nicht ausgeschlossen werden konnte. Es wurde nur ein Paßwort verwendet, das jedem Mitarbeiter bekannt war und zudem im Klartext in einer Datei abgespeichert war. Da das Diskettenlaufwerk gegen einen unbefugten Systemstart und das Einspielen von Programmen, mit deren Hilfe Daten physikalisch ausgelesen werden können, nicht geschützt war, war auch ohne Auslesen oder Kenntnis des Paßwortes ein ungehinderter Zugriff auf die personenbezogenen Daten möglich. Darüber hinaus war ein Protokollierungssystem zur Eingabekontrolle nicht vorhanden.

Hinzu kamen schwerwiegende organisatorische Mängel. Es existierte weder eine Programmdokumentation, die die Verfügbarkeit einer Anwendung dann sichern soll, wenn der Programmierer oder Systemverwalter für diese Aufgabe nicht mehr zur Verfügung steht, noch eine Dienstanweisung, die verbindlich und für jeden nachvollziehbar regelt, in welchem Umfang die datenverarbeitende Stelle den PC-Einsatz billigt und damit verantwortet. Darüber hinaus wurde weder ein Freigabeverfahren durchgeführt noch ein Systemverwalter für die technische Betreuung des Rechners und die Pflege und Wartung der Anwendung benannt. Mängel wurden auch in der Raumsicherung festgestellt: Der Schlüssel zum Rechnerraum wurde zentral vom Pförtner verwaltet und ausgegeben, der aber nicht die Zugangsberechtigung zum Rechnerraum kontrollierte. Da das Gerät auch für Schulungszwecke genutzt werden sollte und darüber hinaus Reinigungsarbeiten durch eine Fremdfirma ohne Aufsicht durch zuständige Mitarbeiter durchgeführt wurden, war der Personenkreis nicht wirksam eingrenzbar, der Zugriff zum Rechner nehmen konnte, so daß die Entwendung des Gerätes oder eine Manipulation der Anwendung nicht ausgeschlossen werden konnte.

Gemäß § 5 Abs. 3 Nr. 10 BlnDSG ist die innerbehördliche oder innerbetriebliche Organisation so zu gestalten, daß sie den besonderen Anforderungen des Datenschutzes gerecht wird (Organisationskontrolle). Auf Grund der festgestellten schwerwiegenden technischen und organisatorischen Mängel wurde das Verfahren von uns beanstandet. Die aufgezeigten Mängel sind inzwischen beseitigt.

Dieser exemplarisch geschilderte Fall verdeutlicht zweierlei:

Die vorgefundenen „selbstprogrammierten" Zugriffsschutzsysteme erfüllten in keinem einzigen Fall die hohen datenschutzrechtlichen Anforderungen, die an eine Sicherheitssoftware gestellt werden. Selbst ein professionell programmiertes Paßwortverfahren gewährleistet noch nicht alle notwendigen Sicherheitsfunktionen wie differenzierte Identifizierungsprozeduren, Eingabekontrollen, Verschlüsselungstechniken oder ein Betriebssystemschutz. Zur Sicherung der PC sollte auf marktgängige und bewährte Produkte zurückgegriffen werden.

Prüfung des Einsatzes eines UNIX-Systems

Auf der Grundlage eines neuen Prüfkonzeptes, welches anhand der im Jahresbericht 1990 veröffentlichten „Empfehlungen für den datenschutzgerechten Einsatz von UNIX-Systemen" in Zusammenarbeit mit der Technischen Universität entwickelt wurde, haben wir mit der Prüfung von UNIX-Systemen im Berichtszeitraum begonnen.

Erster Prüfgegenstand war ein SINIX-System, welches seit Jahren in einem bezirklichen Vermessungsamt betrieben wird.

Neben den Daten des Vermessungsamtes werden auch noch Daten der Friedhofsverwaltung und der Personalstelle der Abt. Bau- und Wohnungswesen mit diesem Rechner verwaltet.

Wegen der völlig unterschiedlichen Aufgabenstellungen der Bereiche führt das Vermessungsamt die Verarbeitung personenbezogener Daten im Auftrag der Friedhofsverwaltung und der Personalstelle nach § 3 BlnDSG durch, obwohl alle drei Bereiche der gleichen Abteilung angehören.

Da diese verteilte Datenverarbeitung in Zukunft üblich sein wird, haben wir der Überprüfung besonderen grundsätzlichen Wert beigemessen.

Bei der Prüfung wurden besonders im Bereich der Benutzer- und Programmverwaltung Mängel festgestellt.

Der größte Mangel war das Fehlen von Dokumentationen über das Benutzerprofil. So konnte selbst der Systemverwalter nicht angeben, warum einige Benutzer einen Zugang zur Betriebssystemebene hatten und wie die jeweiligen Gruppenberechtigungen – in einer Gruppe können mehrere Benutzer mit gleichen Zugriffsrechten auf die entsprechenden Daten zugreifen – zusammengestellt worden waren. Ohne eine solche Dokumentation ist eine ordnungsgemäße Datenverarbeitung gemäß § 19 Abs. 1 BlnDSG ebensowenig sicherzustellen wie eine datenschutzgerechte Zugriffskontrolle gemäß § 5 Abs. 3 Nr. 5 BlnDSG. Inwie-

weit von der Personalstelle Vorgaben für die Benutzerberechtigungen getroffen worden waren, konnte bei der Prüfung nicht nachvollzogen werden.

Die vorliegende Programmdokumentation war unvollständig oder überhaupt nicht vorhanden, so daß eine Überprüfung kaum oder nicht möglich war.

Bei einigen Dateien waren Zugriffberechtigungen vergeben worden, die auch Zugriffe von Anwendern zuließen, die dafür keine Berechtigung erhalten durften, ein Mangel, der von den Verantwortlichen zum größten Teil noch während der Prüfung abgestellt wurde.

Um nach Beseitigung der aufgezeigten Mängel den Datenschutz weiter zu verbessern, haben wir dem Vermessungsamt empfohlen, eine marktgängige und erprobte Sicherheitssoftware zu beschaffen, um eine wesentlich bessere Zugriffssicherheit erreichen.

Um die Echtdatenverarbeitung von der Programmierung zu trennen, haben wir dem Bezirksamt vorgeschlagen, nach der vorgesehenen Installation eines größeren und moderneren Rechners den vorhandenen Rechner als Entwicklungssystem weiter zu nutzen.

Einsatz von Telefaxgeräten

Die Zahl der *Telefaxgeräte* als Mittel der schnellen Bürokommunikation steigt zunehmend in der Berliner Verwaltung. Wurden die Geräte ursprünglich nur beim Versand von Eil- und Schnellbriefen eingesetzt, ersetzen die Fernkopien immer stärker auch einfache Schreiben, was durch die Gebührenstruktur der Post, nach der innerhalb Berlins Fernkopien preiswerter als der Briefversand sind, erleichtert wird. Durch die neue Technik muß aber - soweit es sich um Telekopien mit personenbezogenem Inhalt handelt - der gleiche Datenschutzstandard sichergestellt werden, wie beim herkömmlichen Postversand, für den die absendende Stelle verantwortlich ist.

Weil die Telekopie nicht kuvertiert beim Empfänger ankommt, müssen besondere Sicherungsmaßnahmen beim Empfänger getroffen sein. Gerade hier liegt das zentrale Problem, weil der Absender regelmäßig nicht wissen kann, wie das Gerät beim Empfänger aufgestellt ist und wer im einzelnen auf die Fernkopien zugreifen kann. Selbstverständlich können nicht nur Telefaxsendungen bei einem anderen als dem beabsichtigten Empfänger ankommen. Das Risiko eines Verwählens bei einer Fernkopie ist jedoch ungleich höher als bei der Adressierung eines Briefes*). Darüber hinaus muß der falsch adressierte Brief nicht vom Empfänger in jedem Fall geöffnet und somit der Inhalt des Schreibens zwangsläufig von einem Dritten zur Kenntnis genommen werden. Bei einem falsch adressierten Telefax ist die Quote ungleich höher. Darüber hinaus scheiden besondere Adressierungssätze beim Fernkopieren ohne zusätzlichen technischen Aufwand aus. Hinzu kommt, daß aus Kostengründen regelmäßig mehrere Verwaltungseinheiten ein Gerät benutzen und diese frei zugänglich aufgestellt sind. Somit kann jeder Mitarbeiter die eingehenden Schreiben einsehen.

Nach alledem muß als Ergebnis festgehalten werden, daß keine Schriftstücke mit personenbezogenem Inhalt über die Fernkopierer versandt werden dürfen, wenn der Absender die Gegebenheiten beim Empfänger nicht kennt und er somit seiner Verantwortung nicht gerecht werden kann.

Sofern in begründeten Einzelfällen davon abgewichen werden soll, dann ist sicherzustellen, daß Unbefugte die Schreiben nicht lesen können. Eine denkbare Möglichkeit wäre beispielsweise, mit dem Empfänger einen konkreten Zeitpunkt zu vereinbaren, an dem er dann persönlich neben dem Gerät steht und die Fernkopie an sich nehmen kann. Eine weitere denkbare Variante wäre, daß das Gerät in einem Raum aufgestellt ist, der nur vom Empfangsberechtigten betreten werden kann. Dabei erwarten wir unabhängig davon, daß die Geräte selbstverständlich immer so untergebracht sind, daß unbefugte Dritte nicht auf die eingehenden Fernkopien zugreifen können. Im übrigen muß beobachtet werden, was von den Anbietern an technischen Sicherungsmaßnahmen auf den Markt gebracht wird.

*) vgl. dazu auch den JB 1988, S. 21.

Datenträgervernichtung

Eine Fülle von Anfragen betraf die datenschutzgerechte *Vernichtung von Akten und sonstigen Unterlagen,* die personenbezogene Daten enthalten.

Das *Löschen* personenbezogener Angaben gemäß § 4 Abs. 2 BlnDSG ist eine Phase der Datenverarbeitung und meint das Beseitigen gespeicherter Daten (§ 4 Abs. 2 Nr. 6 BlnDSG). Hinweise über die Vernichtung von Altakten finden sich auch in der Gemeinsamen Geschäftsordnung für die Berliner Verwaltung - Allgemeiner Teil - (GGO I).

Für die Datenträgervernichtung von Bedeutung ist die 1985 in Kraft getretene DIN-Norm 32757, die zwar keine Rechtsnorm darstellt, jedoch über die dort genannten fünf Sicherheitsstufen Anhaltspunkte für eine datenschutzgerechte Vernichtung gibt.

Nach einer mit den Datenschutzbeauftragten des Bundes und der Länder abgestimmten Forderung gelten Informationsträger der öffentlichen Verwaltung, die personenbezogene Daten enthalten (Akten, bewegliche Datenträger, Carbonbänder etc.) dann im Sinne des Gesetzes als gelöscht, wenn die Anforderungen der Sicherheitsstufe 3 des DIN-Blattes 32757 erfüllt sind.

Die Sicherheitsstufe 3 definiert, daß die Informationsträger so vernichtet werden müssen, daß eine Reproduktion der auf ihnen wiedergegebenen Informationen nur unter erheblichen Aufwand (Personen, Hilfsmittel, Zeit) möglich ist.

Viele marktgängige Büroaktenvernichter tragen diesen Anforderungen mittlerweile Rechnung. Schwierigkeiten tauchen dagegen bei der Vernichtung von Massengut auf, da nach Auskunft verschiedener Hersteller bei den dafür konzipierten Industrieaktenvernichtern die nach der Sicherheitsstufe 3 erforderlichen technischen Umrüstungen nur schwer realisierbar und deshalb für den Kunden nur mit erheblichen Preisaufschlägen verbunden seien.

Kann die Sicherheitsstufe 3 durch die Vernichtung der Akten mit Hilfe eines herkömmlichen Aktenvernichters nicht oder nur unzureichend erreicht werden, so müssen andere bzw. weitergehende Maßnahmen ergriffen werden, die eine Kenntnisnahme der unvollständig vernichteten Daten durch Dritte mittels Rekonstruktion verhindern. Dies wäre gegeben, wenn das Datenmaterial direkt oder unmittelbar nach Vernichtung auf einer niedrigeren Stufe in den Recycling- oder Verbrennungsprozeß überführt wird. In den Fällen, in denen eine sofortige Überführung nicht möglich ist, ist die Sicherheit der Zwischenlagerung (Aufbewahrung in verschlossenen Räumen oder Behältern) und des Transportes (z. B. in verschlossenen Containern) zu gewährleisten. Aus datenschutzrechtlicher Sicht entscheidend ist, daß am Ende des Vernichtungsprozesses die Sicherheitsstufe 3 erreicht wird.

Die datenverarbeitende Stelle trägt die volle Verantwortung dafür, daß die zur Löschung bestimmten Datenträger bis zur endgültigen Vernichtung in geeigneter Form gesammelt und verwahrt werden.

Wird die *Vernichtung* von der datenverarbeitenen Stelle nicht selbst durchgeführt, so handelt es sich um eine Datenverarbeitung *im Auftrag.* In diesen Fällen ist nach § 3 Abs.1 BlnDSG der Auftragnehmer unter besonderer Berücksichtigung der Eignung der von ihm getroffenen technischen und organisatorischen Maßnahmen (§ 5 Abs.1) sorgfältig auszuwählen. Die Auftragsvergabe sollte auf vertraglicher Vereinbarung beruhen, die u. a. die Pflicht zur Ausstellung eines Vernichtungsprotokolles durch den Auftragnehmer und das Recht zur Durchführung auf Stichproben des Auftraggebers beim Auftragnehmer beinhaltet. Darüber hinaus ist der Auftraggeber gemäß § 3 Abs. 4 BlnDSG verpflichtet, vertraglich sicherzustellen, daß der Auftragnehmer die Vorschriften des Berliner Datenschutzgesetzes befolgt und sich, sofern die Vernichtung im Geltungsbereich des Berliner Datenschutzgesetzes durchgeführt wird, der Kontrolle des Berliner Datenschutzbeauftragten unterwirft.

Die *Berliner Stadtreinigungsbetriebe (BSR)* haben in Abstimmung mit uns ein mobiles Entsorgungskonzept entwickelt, das den Anforderungen an eine datenschutzgerechte Vernichtung im vollen Umfang Rechnung trägt.

Die BSR stellt dafür einen *mobilen Aktenvernichter* zur Verfügung, der entweder in Form einer Ganztagsentsorgung (der Aktenvernichter wird beim Kunden für eine vereinbarte Zeit abgestellt), einer Filialentsorgung (die BSR fährt von Kunde zu Kunde) oder einer Betriebsentsorgung (die BSR stellt den Aktenvernichter zu vorgegebenen Terminen an bestimmten Orten bereit) eingesetzt wird.

Das Konzept sieht vor, daß die zu vernichtenden Unterlagen bis zum Zeitpunkt der Vernichtung von der datenverarbeitenden Stelle in verschließbaren Aktencontainern aufbewahrt werden, die bei der BSR angemietet oder käuflich erworben werden können.

Für jede Entsorgung wird von der BSR ein Entsorgungsvertrag und ein Datenvernichtungsprotokoll ausgefertigt. Die datenverarbeitende Stelle hat das Recht, die Vernichtung durch einen eigenen Mitarbeiter kontrollieren zu lassen.

Durch die Betriebsentsorgung, für die die BSR jeweils Zeitpunkt und Aufstellungsort über die Presse mitteilen will, besteht erstmals die Möglichkeit, daß auch Privatpersonen ihre persönlichen Unterlagen sachgerecht vernichten lassen können. Damit wurde einer langjährigen Forderung des Datenschutzbeauftragten nachgekommen.

Die persönliche Not in der Öffentlichkeit

Neben fernen Urlaubsgrüßen besser gestellter Bekannter und verschlossenen „persönlichen" Schreiben werbender Losverkäufer findet ein Bürger eine Postkarte seines Sozialamtes im Briefkasten, in der er gebeten wird, im Zusammenhang mit seinem Bekleidungsantrag die Kopie seiner letzten Mieterhöhung zu übersenden.

Ob der Bürger tatsächlich soviel Post empfangen hat, das wissen wir nicht, aber sein Problem kannten wir schon, hat er sich doch bereits einige Jahre zuvor bei uns darüber beschwert, daß ihm sein Sozialamt auf einer offenen Postkarte mitteilt, daß im Zusammenhang mit seinem Antrag auf Frühjahrs- und Sommerbekleidung sein Widerspruch nicht bearbeitet werden konnte, da die Akten nicht verfügbar waren.

Seinerzeit hatten wir den Vorgang beanstandet, weil die offene Versendung einen Verstoß gegen das Sozialgeheimnis nach § 35 SGB I sowie gegen § 6 Bundesdatenschutzgesetz darstellt. Durch die offene Versendung haben unbefugte Dritte die Möglichkeit, Rückschlüsse auf die Beziehungen eines Bürgers zu einem Sozialleistungsträger zu ziehen. Somit ist eine unbefugte Offenbarung persönlicher Geheimnisse nicht auszuschließen. Die Postkarten dürfen keine geheimzuhaltenden Angaben und keine Hinweise enthalten, aus denen auf Geheimzuhaltendes geschlossen werden kann (§ 58 Abs. 1 GGO I).

Das Bezirksamt hatte seinerzeit in einer Arbeitsanweisung festgelegt, daß künftig keine Versendung von offenen Postkarten mehr erfolgen soll. Sofern Postkarten verwandt werden, sind sie zu kuvertieren.

Dieser neue Vorgang belegt exemplarisch, wie sorglos in Einzelfällen immer wieder mit den Belangen des Datenschutzes und somit des Bürgers umgegangen wird. Nicht nur, daß gegen die interne Arbeitsanweisung verstoßen wird, es werden offensichtlich auch die besonderen Amtsgeheimnisse (§ 35 SGB I) nicht besonders ernst genommen.

Das Bezirksamt will mit einer erneuten Arbeitsanweisung, wonach die Postkarten nicht mehr verwandt werden dürfen und anderenfalls die Poststelle diese Karten künftig nicht mehr weiterleiten wird, Wiederholungen entgegenwirken.

4. Aus der Arbeit der Dienststelle

Nach mehr als zehn Jahren endete am 30. November 1989 die Amtszeit des ersten Berliner Datenschutzbeauftragten Dr. Hans-Joachim Kerkau. Ihm kommt das Verdienst zu, die Dienststelle des Datenschutzbeauftragten nicht nur aufgebaut, sondern diese Institution auch in der Berliner Verwaltung verankert zu haben. Sein stets um Vermittlung divergierender Interessen bemühter Ehrgeiz richtete sich vor allem auf eine Integration der im Datenschutz mitunter heftig aufeinander prallenden rechtlichen und technischen Gesichtspunkte. Der Technik einen verfassungskonformen und sozialverträglichen Weg vorzuzeichnen, aber auch dem technischen Denken bei juristischen Fragestellungen hinreichend Berücksichtigung zu verschaffen, ist auch die Zielsetzung unserer Arbeit in der neuen Amtsperiode.

Die Dienststelle

Die Größe der Dienststelle blieb wie in den vergangenen Jahren trotz des erheblichen Aufgabenzuwachses gleich: Ihr gehören 15 Mitarbeiterinnen und Mitarbeiter an, die in unterschiedlichem Umfang von Ausbildungskräften unterstützt werden. Bereits Dr. Kerkau hatte seit Jahren darauf hingewiesen, daß eine angemessene Kontrolle der Informationsverarbeitung im Land Berlin auch in den damaligen Grenzen nicht möglich war. Zwar wurden die von ihm bereits zuvor vorgetragenen Stellenwünsche für das Haushaltsjahr 1991 erneut vorgetragen; sie wurden aber wiederum zurückgewiesen.

Die Erstreckung der Zuständigkeit auf die östlichen Teile Berlins verschärft die Situation natürlich erheblich. Zwar wurden uns im Rahmen des Beschlusses der Landesregierung vom 27. November 1990 drei Stellen zugewiesen, die mit Ostberlinerinnen bzw. Ostberlinern besetzt werden können. Auch dies kann den bestehenden Bedarf aber in keinster Weise abdecken.

Hinzu kommt, daß alleine die geografische Ausdehnung Berlins sowie die seit der Wende bestehende Verkehrssituation für eine Behörde mit Kontrollaufgaben einen erheblichen zusätzlichen Zeitaufwand mit sich bringt. Die Bitte an die Senatsverwaltung für Inneres, zumindest aus dem ja vorhandenen Reservoir des Magistratsfuhrparks einen Wagen zur Verfügung zu stellen, stieß auf schroffe Ablehnung.

Ändert sich diese Situation nicht deutlich, kann eine angemessene Sicherstellung des Datenschutzes in der neuen Berliner Verwaltung nicht gewährleistet werden.

Aufgabengebiete

Angesichts der Bedeutung, die wir den einzelnen Bürgerinnen und Bürgern als Subjekte des informationellen Selbstbestimmungsrechts beimessen (vgl. oben 1.1), wurde die Organisation der Dienststelle noch deutlicher auf die Bürgerberatung und die Öffentlichkeitsarbeit ausgerichtet: Neben den Bereichen für Recht und Verwaltung sowie Technik und Organisation wurde ein Bereich Bürger und Öffentlichkeit eingerichtet.

Wie wichtig dieser Schritt war, erwies sich gerade auf dem Hintergrund der Einigung: Bereits vor dem 3. Oktober mußten in erheblichem Umfang Auskünfte an Bürgerinnen und Bürger aus dem Ostteil der Stadt erteilt werden; hierzu wurde zusätzliches Informationsmaterial erstellt. Die Beteiligung an den Tagen der offenen Tür im Roten Rathaus, Veröffentlichungen in Ostberliner Zeitungen und Informationssendungen im Rundfunk dienten der Werbung für die Idee des Datenschutzes. Im Roten Rathaus stellte die Präsidentin der Stadtverordnetenversammlung, die für den Zuständigkeitsbereich des Magistrats bis zum Januar 1991 die Dienstaufsicht über den Datenschutzbeauftragten hatte, einen Raum zur Verfügung, in dem bis zum Jahresende vom Bereich Bürger und Öffentlichkeit eine datenschutzrechtliche Beratung angeboten wurde. Die hier vorgetragenen Probleme (z. B. die weitere Verwendung der Personenkennzahl) wurden zum Anlaß erster Prüfungen im neuen Zuständigkeitsbereich genommen.

Für ganz Berlin wurde die Öffentlichkeitsarbeit durch die Einrichtung eines unregelmäßig erscheinenden Informationsdienstes verstärkt. Eine Aufkleberaktion („Schnüffeln verboten") bediente sich auch dieses modernen Mediums, um die Bedeutung des Datenschutzes auch im Alltag anzumahnen. Die Aktion stieß bei allen Abnehmern auf große Begeisterung. Wenige Skeptiker fürchteten, ein derartiger Aufkleber könne das Vertrauen in die Berliner Verwaltung beeinträchtigen - eine ungerechtfertigte Furcht, denn die sorgfältige Beachtung des Datenschutzes ist gerade eine Voraussetzung für dieses Vertrauen.

Die Zahl der Beschwerden und Beratungsersuchen bestätigte den Trend der vergangenen Jahre: Während die Zahl der Eingaben in etwa gleich blieb, nahm der Umfang der Beratungsersuchen erheblich zu. Dies zeigt, daß die Bereitschaft der Verwal-

tung, datenschutzrechtliche Probleme zu erörtern, nach wie vor steigt ; hinzu kommen natürlich die Beratungsersuchen aus den östlichen Bezirken. Bei den Ostberliner Bürgern scheint eine gewisse Scheu vorhanden zu sein, die Probleme schriftlich vorzutragen; Beschwerden gelangten hier vor allem in persönlichen Rücksprachen oder telefonisch zu uns.

Die meisten Beschwerden stammten aus dem Geschäftsbereich der Innenverwaltung (in erster Linie aus dem Bereich von Polizei und Verfassungsschutz sowie dem Meldewesen), es folgen die Gesundheits- und Sozialverwaltungen, der Bereich Wirtschaft/ Verkehr/Betriebe und die Schulverwaltung. Bemerkenswert ist, daß die Zahl der Eingaben mit Hilfe eines neuen Telekommunikationsdienstes (Bildschirmtext, Telefax) erheblich gestiegen ist. Erneut erreichte uns eine Vielzahl von Beschwerden aus dem privaten Bereich, die wegen der oben beschriebenen Zuständigkeitsverteilung an die Senatsverwaltung für Inneres abgegeben wurden.

Bei den Beratungsersuchen stehen die Bereiche Bildung und Forschung sowie Gesundheitswesen ganz vorne. Dies mag damit zusammenhängen, daß einerseits der Wunsch hier besonders stark ist, die eigene Vorgehensweise gut abzusichern (etwa bei großen Forschungsprojekten), daß andererseits die Sensibilität der Daten etwa im Gesundheitsbereich besondere Aufmerksamkeit erfordert.

Auch der Bereich Technik und Organisation beriet die Gesundheits- und Sozialverwaltung besonders intensiv, wenn auch hier der Geschäftsbereich der Innenverwaltung ebenfalls die meiste Aufmerksamkeit beanspruchte. Zum Dateienregister waren am Jahresende 1954 Dateien von 565 Stellen gemeldet.

Abgeordnetenhaus

Der Berliner Datenschutzbeauftragte unterliegt der Dienstaufsicht des Präsidenten des Abgeordnetenhauses; er hat dem Abgeordnetenhaus jährlich einen Bericht über das Ergebnis seiner Tätigkeit vorzulegen und auch sonst Hinweisen aus dem Abgeordnetenhaus nachzugehen und Gutachten zu fertigen. Aus dieser Nähe zum Parlament ergeben sich besondere Verpflichtungen. Im Mittelpunkt stand die Beratung des Jahresberichtes 1989, aber auch verschiedener anderer Fragen im Unterausschuß Datenschutz des Ausschusses für Inneres, Sicherheit und Ordnung. Hier wurde auch das neue Berliner Datenschutzgesetz beraten und in seine schließlich verabschiedete Form gebracht.

Neben dem Ausschuß für Inneres, Sicherheit und Ordnung bedienten sich auch andere Ausschüsse (z. B. der Petitionsausschuß, der Rechtsausschuß und der Verfassungsschutzausschuß) unserer Fachkunde.

Kooperation

Der Datenschutzbeauftragte ist nicht nur auf Grund des Gesetzes verpflichtet, mit allen Stellen zusammenzuarbeiten, deren Aufgabe die Kontrolle und Weiterentwicklung des Datenschutzes ist. Dies ist schon allein aufgrund der geringen Personalstärke erforderlich, die es unmöglich macht, zu allen aufgeworfenen Fragen alleine Lösungen zu entwickeln.

Eine zentrale Bedeutung hat dabei die Konferenz der Datenschutzbeauftragten des Bundes und der Länder, die im Berichtszeitraum unter dem Vorsitz Schleswig-Holsteins zwei ordentliche und eine außerordentliche Sitzung abhielt. Die dort gefaßten Beschlüsse sind im Anhang abgedruckt. Insbesondere die Zusammenarbeit in den Arbeitskreisen der Konferenz hat große Bedeutung für die Alltagsarbeit.

Der Arbeitskreis Medien tagte zweimal unter Berliner Vorsitz; er war vor allem an der Ausarbeitung einer grundsätzlichen Entschließung zum Grundrecht auf unbeobachtete Kommunikation beteiligt.

Im Jahr 1991 führt der Bundesbeauftragte für den Datenschutz den Vorsitz; in den darauffolgenden Jahren geht der Vorsitz in alphabetischer Reihenfolge wieder auf die Länder unter Einschluß der neuen Länder über.

Berlin führt auch mit einigem Erfolg den Vorsitz in der Arbeitsgruppe Telekommunikation und Medien der Internationalen Konferenz der Datenschutzbeauftragten; in zwei Sitzungen wurde ein Resolutionsentwurf für das Plenum der Internationalen Konferenz erarbeitet, die im Oktober in Paris das Papier annahm (vgl. Anhang 2.2).

Die gute Zusammenarbeit mit der Aufsichtsbehörde für den Datenschutz bei der Senatsverwaltung für Inneres wurde nicht nur fortgesetzt, sondern intensiviert. In der Arbeitsgruppe für grenzüberschreitenden Datenverkehr des Düsseldorfer Kreises (der Entsprechung für die Datenschutzkonferenz im privaten Bereich) vertraten wir die Belange des Europaarbeitskreises der Konferenz.

Aus- und Fortbildung

Große Bedeutung kommt der Aus- und Fortbildung auf dem Gebiet des Datenschutzes zu. Die geringe Zahl der Mitarbeiterinnen und Mitarbeiter kann nur dadurch ausgeglichen werden, daß ständig Multiplikatoren für die Verbreitung der datenschutzrechtlichen Kenntnisse ausgebildet werden. Hierzu erreicht uns eine Vielzahl von Anfragen.

Die Auslastung der Mitarbeiterinnen und Mitarbeiter verbietet allerdings eine Beteiligung an Aus- und Fortbildung im Rahmen der dienstlichen Obliegenheiten im Regelfall. Wir sind vielmehr darauf verwiesen, daß diese sich bereitfinden, in der Freizeit entsprechende Lehrveranstaltungen durchzuführen. Glücklicherweise ist ihr Engagement so groß, daß in einem bestimmten Umfang an den Hochschulen, der Verwaltungsakademie, aber auch an anderen Fortbildungsstätten Datenschutzkurse angeboten werden können.

Berlin, 6. März 1991

Dr. Hansjürgen Garstka

Berliner Datenschutzbeauftragter

Anlagen zum Jahresbericht 1990 (Übersicht)

1. Entschließungen der Konferenz der Datenschutzbeauftragten des Bundes und der Länder sowie der Datenschutzkommission Rheinland-Pfalz

1.1 Entschließung der 38. Konferenz am 26./27. Oktober 1989 zum Entwurf eines Schengener Zusatzübereinkommens über den schrittweisen Abbau der Grenzkontrollen

1.2 Entschließung der 38. Konferenz am 26./27. Oktober 1989 über den Datenschutz in der Europäischen Gemeinschaft

1.3 Entschließung der 38. Konferenz am 26./27. Oktober 1989 zum Entwurf einer EG-Statistikverordnung

1.4 Entschließung der 38. Konferenz am 26./27. Oktober 1989 über Genomanalyse und informationelle Selbstbestimmung

1.5 Beschluß der 39. Konferenz am 22./23. März 1990 zum Datenschutz im deutsch-deutschen Verhältnis

1.6 Beschluß der 39. Konferenz am 22./23. März 1990 zum Bundesdatenschutzgesetz und zum Bundesverfassungsschutzgesetz

1.7 Beschluß der 39. Konferenz am 22./23. März 1990 zur Einrichtung eines Arbeitskreises Europäische Gemeinschaft

1.8 Entschließung der Sonderkonferenz am 27. Juni 1990 zum Entwurf eines Gesetzes zur Bekämpfung des illegalen Rauschgifthandels und anderer Erscheinungsformen der organisierten Kriminalität

1.9 Beschluß der 40. Konferenz am 4./5. Oktober 1990 zur Stärkung des Schutzes des Brief-, Post- und Fernmeldegeheimnisses sowie des nichtöffentlich gesprochenen Wortes

1.10 Beschluß der 40. Konferenz am 4./5. Oktober 1990 zur Neuregelung des Melderechtsrahmengesetzes

1.11 Beschluß der 40. Konferenz am 4./5. Oktober 1990 zur Erarbeitung von Krebsregistergesetzen in Bund und Ländern

2. Entschließungen der Internationalen Konferenz der Datenschutzbeauftragten

2.1 Entschließung der 12. Internationalen Konferenz am 19. September 1990 über Datenschutz und die Europäische Gemeinschaft

2.2 Beschluß der 12. Internationalen Konferenz am 19. September 1990 zu Problemen öffentlicher Telekommunikationsnetze und des Kabelfernsehens

---

1. Entschließungen der Konferenz der Datenschutzbeauftragten des Bundes und der Länder sowie der Datenschutzkommission Rheinland-Pfalz

1.1 Entschließung der 38. Konferenz am 26./27. Oktober 1989 zum Entwurf eines Schengener Zusatzübereinkommens über den schrittweisen Abbau der Grenzkontrollen

1. Am 14. Juni 1985 unterzeichneten die Regierungen Frankreichs, der Bundesrepublik Deutschland und der Beneluxstaaten in Schengen/Luxemburg ein Abkommen über den schrittweisen Abbau der Grenzen zwischen ihren Ländern. Dabei knüpften sie den Wegfall der Grenzkontrollen an eine Reihe von Maßnahmen, die die befürchteten Sicherheitsdefizite ausgleichen sollen. Die Maßnahmen sollen in einem Zusatzübereinkommen festgehalten werden. Hierzu gehört die Errichtung eines gemeinsamen automatisierten Informationssystems für den Bereich der Fahndung (Schengener Informationssystem – SIS). Dieses System dient vor allem der Ausschreibung zur Festnahme und zur Zurückweisung an der Grenze, der verdeckten Registrierung und der Ermittlung des Aufenthalts von Zeugen im Strafverfahren. Überdies sollen der Informationsaustausch zum Zwecke der Bekämpfung bestimmter Formen der Kriminalität verstärkt, die ausländer- und asylrechtlichen Entscheidungen vereinheitlicht und ein gemeinsames Verfahren für intensivierte Kontrollen an den Außengrenzen festgelegt werden.

2. Die Vertragsstaaten verpflichten sich in dem Entwurf zum Zusatzübereinkommen, Datenschutzvorschriften für das Schengener Informationssystem entsprechend den Grundsätzen der Datenschutzkonvention des Europarates und der Empfehlung des Ministerkomitees des Europarats an die Mitgliedsstaaten über die Nutzung personenbezogener Daten im Polizeibereich als Mindeststandard zu erlassen. Die Konferenz begrüßt dies und stellt zugleich fest, daß nach dem gegenwärtigen Stand der Verhandlungen auch die in der Erklärung der Datenschutzorgane Frankreichs, Luxemburgs und der Bundesrepublik Deutschland vom 16. März 1989 enthaltenen Forderungen in wesentlichen Bereichen erfüllt werden sollen. Der Vertragsentwurf sieht für das Schengener Informationssystem vor: Auskunfts-, Berichtigungs- und Klagerechte für die Betroffenen; Kontrollorgane auf nationaler und internationaler Ebene; eine Zweckbindung der Daten. Diese Elemente müssen Bestandteile des Zusatzübereinkommens bleiben, bedürfen aber noch der Verbesserung und Ergänzung, damit sich durch den grenzüberschreitenden Datenaustausch keine gravierenden Verschlechterungen für den Datenschutz ergeben.

2.1 Die Datenschutzbeauftragten fordern für das SIS insbesondere die

- Festlegung der Voraussetzungen, nach denen unter Berücksichtigung der Verhältnismäßigkeit (zum Beispiel nach der Schwere der Straftaten) Informationen aus dem nationalen in den internationalen Fahndungsbestand übernommen werden sollen,
- Festlegung, unter welchen Voraussetzungen und in welchem Umfang die verschiedenen Inlandsbehörden auf die Daten zugreifen dürfen,
- konkrete Beschreibung der Voraussetzungen, unter denen verdeckte Registrierungen erlaubt werden sollen (Straftatenkatalog),
- präzisere Beschreibung der Kriterien, nach denen Zweckdurchbrechungen zur Verhütung einer Straftat mit erheblicher Bedeutung sowie aus schwerwiegenden Gründen der Staatssicherheit erlaubt werden sollen, und
- Aufnahme einer Verpflichtung, Zweckänderungen zu Kontrollzwecken zu dokumentieren.

2.2. Die Regelungen über den Datenschutz – insbesondere die Rechte der Betroffenen und die Datenschutzkontrolle – müssen auf die im Zusatzübereinkommen vorgesehene konventionelle Verarbeitung personenbezogener Daten ausgedehnt werden. Dies gilt vor allem für den Informationsaustausch in den Bereichen des Ausländerrechts und des Asylverfahrens.

3. Der Entwurf des Zusatzübereinkommens enthält eine pauschale Verpflichtung der Vertragsparteien, daß ihre nationalen Sicherheitsdienste sich untereinander unter Berücksichtigung des nationalen Rechts und nach Maßgabe ihrer jeweiligen Zuständigkeit bei der Abwehr von Nachteilen für die Staatssicherheit Hilfe leisten.

   Die Datenschutzbeauftragten weisen vorsorglich darauf hin, daß eine solche Bestimmung nach deutschem Verfassungsrecht keine tragfähige Grundlage für einen umfassenden Datenaustausch der Geheimdienste darstellt.

4. Der Vertragsentwurf verpflichtet jeden Vertragsstaat, Ausländer aus dritten Staaten an der Grenze zurückzuweisen, wenn ein anderer Vertragsstaat ihn „zur Einreiseverweigerung" ausgeschrieben hat. Es ist nicht vorgesehen, daß der vollziehende Staat die Gründe der Ausschreibung zur Kenntnis nimmt und rechtlich überprüft.

Die Datenschutzbeauftragten fordern die verbindliche Festlegung der sachlichen Voraussetzungen solcher Ausschreibungen und die Ermöglichung einer Überprüfung.

5. Die Datenschutzbeauftragten machen darauf aufmerksam, daß das Zusatzübereinkommen den deutschen Gesetzgeber nicht von der dringenden Notwendigkeit enthebt, vor Inkrafttreten des Zusatzübereinkommens für die polizeiliche Datenverarbeitung verfassungskonforme Rechtsgrundlagen zu schaffen.

6. Bevor die einzelnen Vertragsstaaten ihre im Entwurf des Zusatzübereinkommens vorgesehene Verpflichtung, spezielle nationale Regelungen für das Erheben und Nutzen von Daten zu erlassen, nicht erfüllt haben, dürfen Daten an diese Staaten auf der Grundlage des Zusatzübereinkommens nicht übermittelt werden.

1.2 Entschließung der 38. Konferenz am 26./27. Oktober 1989 über den Datenschutz in der Europäischen Gemeinschaft

Angesichts der für das Jahr 1993 zu erwartenden Errichtung eines Binnenmarktes in der Europäischen Gemeinschaft zählt der grenzüberschreitende Datenaustausch zu den drängenden, ungelösten Problemen des Datenschutzes.

Eine internationale Datenverarbeitung ist nicht nur eine Grundbedingung für eine gemeinschaftsweite privatwirtschaftliche Tätigkeit. Auch für den öffentlichen Bereich gewinnt die Problematik zunehmend an Bedeutung. Der Abbau der Grenzkontrollen in der Euroäischen Gemeinschaft und das vor diesem Hintergrund geschlossene „Schengener Übereinkommen" über die verstärkte informationelle Zusammenarbeit der Polizeibehörden Frankreichs, der Bundesrepublik Deutschland und der Benelux-Staaten sind dafür ein signifikantes Beispiel.

Ebenso werden die technischen Voraussetzungen für internationale Datenübermittlungen immer weiter verbessert. Schon 1993 soll europaweit das digitale, diensteintegrierende Kommunikationsnetz (ISDN) zur Verfügung stehen.

In der Europäischen Gemeinschaft wird die Dynamik der wirtschaftlichen Integration die Entwicklung zu einem „informationellen Großraum" nachhaltig fördern. Dies hat zur Folge, daß die Informationsverarbeitung insbesondere in den Bereichen Umweltschutz, Forschung, Arbeitsmarkt, soziale Sicherung, Statistik und öffentliche Sicherheit erheblich zunehmen wird.

Die Beratungen der Internationalen Konferenz der Datenschutzbeauftragten im August 1989 in Berlin haben erneut gezeigt, daß die auf supranationaler Ebene vorhandenen Regelungen, wie etwa die Europaratskonvention von 1981, zwar wichtige Prinzipien für einen fairen Datenumgang enthalten, aber keineswegs ausreichen, den etwa in der Bundesrepublik Deutschland oder Frankreich durch das nationale Datenschutzrecht erreichten Stand der Sicherung des informationellen Selbstbestimmungsrechts des Bürgers zu gewährleisten, abgesehen davon, daß eine Reihe von Mitgliedsstaaten der Gemeinschaft die Konvention noch nicht ratifiziert hat.

Besonders bedenklich ist die Untätigkeit der EG im Bereich des Datenschutzes. Rechtsakte der EG verpflichten in zunehmendem Umfang die Mitgliedsländer zur Erhebung, Verarbeitung und Übermittlung personenbezogener Daten, etwa im Bereich der Statistik. Die Telekommunikationspolitik der EG ist auf einen forcierten Ausbau europaweit standardisierter und operierender Telekommunikationsdienste und -netze gerichtet. Zwischen den verschiedenen nationalen Datenschutzrechten der Mitgliedsstaaten bestehen im Hinblick auf Verarbeitungsvoraussetzungen, Rechte der betroffenen Personen und Kontrollmöglichkeiten große Unterschiede.

Die Konferenz bekräftigt daher die auf der Internationalen Konferenz in Berlin einmütig erhobenen Forderungen,

- daß bei der Entwicklung und Nutzung grenzüberschreitender Datennetze und Datendienste dem Datenschutz der gleiche Stellenwert zukommen muß, wie der Förderung der technischen Infrastruktur,
- daß die EG ein Gesamtkonzept für die Sicherung des Datenschutzes sowohl in den Mitgliedsländern als auch bei ihren eigenen Aktivitäten entwickeln muß, das insbesondere die Gleichwertigkeit des Schutzniveaus in der gesamten Gemeinschaft herstellt, und
- daß auf der EG-Ebene eine unabhängige Datenschutzinstanz einzurichten ist, die die Institution der Gemeinschaft in allen Datenschutzfragen berät, die Verarbeitung personenbezogener Daten durch die EG-Gremien überwacht, Eingaben von Bürgern entgegennimmt und mit den nationalen Datenschutzorganen zusammenarbeitet.

Die Konferenz der Datenschutzbeauftragten erklärt ihre ausdrückliche Bereitschaft, ihre Kenntnisse und Erfahrungen bei der Realisierung dieser Maßnahmen einzubringen. Ansprechpartner sind dabei zum einen die Organe der Gemeinschaft, insbesondere das Europäische Parlament, zum anderen die an der Willensbildung der EG beteiligten deutschen Behörden des Bundes und der Länder.

1.3 Entschließung der 38. Konferenz am 26./27. Oktober 1989 zum Entwurf einer EG-Statistikverordnung

Die Kommission der Europäischen Gemeinschaften hat den Entwurf einer Verordnung des Rates über die Übermittlung von unter die Geheimhaltungspflicht fallenden Informationen an das Statistische Amt der Europäischen Gemeinschaften vorgelegt.

Diese Verordnung darf nicht hinter dem datenschutzrechtlichen Standard der amtlichen Statistik in der Bundesrepublik Deutschland zurückbleiben.

Die nationalen Statistikämter sollen nach dem Vorschlag der EG-Kommission die Befugnis erhalten, vertrauliche statistische Daten dem Statistischen Amt der Europäischen Gemeinschaften auch dann zu übermitteln, wenn sie einen Personenbezug aufweisen. Es ist nicht auszuschließen, daß auf nationaler Ebene kurzfristig für bestimmte statistische Zwecke vorgehaltene personenbezogene Datenbestände (z. B. noch nicht anonymisierte Daten aus dem Mikrozensus) durch das Statistische Amt der EG abgerufen werden. Deshalb muß in der EG-Verordnung festgelegt werden, daß die Übermittlung personenbezogener Einzelangaben nur ausnahmsweise durch einen weiteren Rechtsakt der EG für bestimmte statistische Zwecke (z. B. für die Produktions-, Industrie- und Außenhandelsstatistik) zugelassen werden darf und daß eine möglichst frühzeitige Anonymisierung stattfindet sowie notwendige organisatorisch-technische Maßnahmen der Datensicherung getroffen werden.

Die unabhängige Datenschutzkontrolle auf Gemeinschaftsebene ist bisher nicht gewährleistet. Der geplante Beratende Ausschuß kann diese Kontrolle nicht ersetzen.

Im Gemeinschaftsrecht sind bisher für die Verletzung des Statistikgeheimnisses keine ausreichenden Sanktionen vorgesehen. Nicht einmal alle Mitgliedsstaaten stellen einen derartigen Verstoß unter Strafe.

Die Teilnehmer der 11. Internationalen Konferenz der Datenschutzbeauftragten in Berlin haben am 30. August 1989 diesen Fragenkreis diskutiert und sind übereingekommen, sich auf nationaler und internationaler Ebene für eine stärkere Berücksichtigung datenschutzrechtlicher Belange im Verordnungsentwurf einzusetzen.

Die Konferenz der Datenschutzbeauftragten appelliert daher an die Bundesregierung und den Ministerrat, vor einer Verabschiedung des Verordnungsentwurfs die aufgezeigten Mängel zu beseitigen, damit den Persönlichkeitsrechten der Gemeinschaftsbürger auch bei der ständig zunehmenden Zahl europäischer Statistiken und bei der für 1990 in den meisten anderen EG-Mitgliedsstaaten vorgesehenen Volkszählung Rechnung getragen wird.

1.4 Entschließung der 38. Konferenz am 26./27. Oktober 1989 über Genomanalyse und informationelle Selbstbestimmung

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder sowie der Datenschutzkommission Rheinland-Pfalz hat den Abschlußbericht der Enquête-Kommission des Deutschen Bundestages „Chancen und Risiken der Gentechnologie" (Drucksache 10/6775) zum Anlaß genommen, die Risiken für die informationelle Selbstbestimmung jedes Betroffenen abzuwägen gegenüber den Chancen, die die Genomanalyse bringt. Durch die Offenlegung genetischer Daten eines Menschen kann dieser in seinem Persönlichkeitsrecht und sonstigen schutzwürdigen Belangen nachhaltig beeinträchtigt werden. Informationen aus dem Kernbereich der Privatsphäre, die dem Betroffenen selbst bisher unbekannt waren, können ihn zu einem an sich ungewollten Verhalten in seiner Lebens- oder Berufsgestaltung veranlassen; ihre Kenntnis kann zu einer psychischen und sozialen Zwangslage für den Betroffenen führen. Wegen der genetischen Bedingtheit solcher Informationen können sich daher auch entsprechende Auswirkungen auf dritte Personen, insbesondere die Familie, ergeben. Das Bekanntwerden solcher Informationen kann den Betroffenen in seinem sozialen Umfeld diskriminieren mit der möglichen Folge gesellschaftlicher Ausgrenzung.

Um den besonderen Risiken bei der Anwendung der Genomanalyse zu begegnen, bedarf es der gesetzlichen Absicherung folgender Grundsätze:

1. Die Genomanalyse darf grundsätzlich nur auf freiwilliger Basis nach umfassender Aufklärung der Betroffenen vorgenommen werden; ausgenommen sind Straf- und Abstammungsverfahren.
2. Die jederzeit widerrufliche Einwilligung muß sich auch auf die weitere Verwendung der genetischen Informationen erstrecken. Im Falle eines Widerrufs sind die gewonnenen Informationen zu löschen oder an den Betroffenen herauszugeben.
3. Jede Genomanalyse muß zweckorientiert vorgenommen werden. Es ist diejenige genomanalytische Methode zu wählen, die keine oder die geringste Menge an Überschußinformationen bringt. Überschußinformationen sind unverzüglich zu vernichten.
4. Es ist zu prüfen, inwieweit genomanalytische Untersuchungsmethoden einer staatlichen Zulassung bedürfen. Für DNA-Sonden ist dies jedenfalls zu bejahen.
5. Die Genomanalyse im gerichtlichen Verfahren muß auf die reine Identitätsfeststellung beschränkt werden; es dürfen keine genomanalytischen Methoden angewandt werden, die Überschußinformationen zur Person liefern. Die Nutzung der Genomanalyse im Strafverfahren setzt eine normenklare gesetzliche Ermächtigung voraus. Präzise Regelungen müssen u. a. sicherstellen, daß genomanalytische Befunde einer strengen Zweckbindung unterworfen werden.
6. Im Arbeitsverhältnis sind die Anordnung von Genomanalysen oder die Verwendung ihrer Ergebnisse grundsätzlich zu verbieten. Ausnahmen bedürfen der gesetzlichen Regelung. Eine bloße Einwilligung des Arbeitnehmers ist wegen der faktischen Zwangssituation, der er im Arbeitsleben häufig unterliegt, nicht ausreichend.
7. Genomanalysen im Versicherungswesen sind grundsätzlich nicht erforderlich und mit dem Prinzip der Versicherungen, Risiken abzudecken und nicht auszuschließen, unvereinbar. Dies sollte durch eine Klarstellung im Versicherungsvertragsgesetz deutlich gemacht werden.
8. Im Rahmen der pränatalen Diagnostik dürfen nur Informationen über das Vorhandensein oder Fehlen von Erbanlagen erhoben werden, bei denen eine Schädigung heilbar ist oder die zu einer so schwerwiegenden Gesundheitsschädigung des Kindes führen würden, daß ein Schwangerschaftsabbruch straffrei bliebe.

   Reihenuntersuchungen an Neugeborenen dürfen sich nur auf solche Erbkrankheiten erstrecken, die bei frühzeitiger Erkennung eines genetischen Defekts geheilt oder zumindest spürbar therapeutisch begleitet werden können.

   Die Eltern müssen nach umfassender fachkundiger Beratung in voller Freiheit über die Anwendung genomanalytischer Methoden entscheiden können. Jegliche Beeinflussung, insbesondere jeder individuelle und gesellschaftliche Druck, muß vermieden werden.

   Die informationelle Selbstbestimmung Dritter, zu der auch das Recht auf Nichtwissen gehört, muß berücksichtigt werden.

Die Konferenz versteht ihre Stellungnahme als Beitrag zur Diskussion mit allen Institutionen, die an den Fragen der Genomanalyse arbeiten. Sie legt Wert darauf, den Dialog mit der Wissenschaft fortzusetzen und dabei neue wissenschaftliche Erkenntnisse einzubeziehen.

1.5 Beschluß der 39. Konferenz am 22./23. März 1990 zum Datenschutz im deutsch-deutschen Verhältnis

1. Das Engagement der Bevölkerung in der DDR für den Schutz ihrer personenbezogenen Daten z. B beim Staatssicherheitsdienst zeigt, wie elementar die Persönlichkeitsrechte von den Bürgern in der DDR verstanden werden und daß sie das Recht auf informationelle Selbstbestimmung als Teil des allgemeinen Selbstbestimmungsrechts wahrnehmen.

   Die Konferenz der Datenschutzbeauftragten begrüßt Bemühungen, auch in der DDR angemessene Datenschutzregelungen zu schaffen.
2. Obwohl in der DDR keine hinreichenden Datenschutzregelungen bestehen, werden bereits jetzt mehr personenbezogene Daten als früher ausgetauscht. Dieser Datentransfer wird noch zunehmen. Aktuelle Anlässe, wie der Austausch von Daten bei Verkehrsunfällen, sowie im Rahmen der Gefahrenabwehr und der Strafverfolgung haben in der Öffentlichkeit besondere Aufmerksamkeit gefunden.

   Der Prozeß der sozialen, wirtschaftlichen und politischen Einigung führt zu verstärktem grenzüberschreitenden Datenverkehr, z. B. im Sozialrecht, im Melderecht, im Versicherungs- und Kreditrecht. Dies wirft Fragen des Datenschulzes auf. Für die Bundesrepublik gelten das allgemeine Datenschutzrecht und besondere Gesetze wie z. B. das Gesetz über die innerdeutsche Rechts- und Amtshilfe in Strafsachen vom 2. Mai 1953 sowie Vereinbarungen.

   Bei der Verwirklichung technischer Maßnahmen insbesondere bei dem Ausbau der Telekommunikationsdienste und bei der automatisierten Datenverarbeitung muß der Datenschutz beachtet werden.
3. Die Datenschutzkonferenz hält es für geboten, daß der Austausch personenbezogener Daten zwischen Behörden und öffentlichen Stellen in der Bundesrepublik Deutschland und in der Deutschen Demokratischen Republik erst durchgeführt wird, wenn gewährleistet ist, daß nach folgenden Grundsätzen verfahren wird:
   - Die Grundsätze des Übereinkommens des Europarates über den Schutz des Menschen bei der Verarbeitung personenbezogener Daten vom 28. Januar 1981 sind zu beachten.
   - Die Übermittlung personenbezogener Informationen unterbleibt, soweit Grund zu der Annahme besteht, daß dadurch gegen den Zweck eines Gesetzes der Bundesrepublik Deutschland verstoßen würde oder schutzwürdige Belange bei den betroffenen Personen beeinträchtigt würden. Die Übermittlung personenbezogener Informationen unterbleibt insbesondere dann, wenn Grund zu der Annahme besteht, daß die Verwendung der übermittelten Informationen nicht in Einklang mit rechtsstaatlichen Grundsätzen steht oder dem Betroffenen aus der Verwendung der Informationen erhebliche Nachteile erwachsen, die im Widerspruch zu rechtsstaatlichen Grundsätzen stehen.

- Der Empfänger darf personenbezogene Informationen nur zu dem durch die übermittelnde Stelle angegebenen Zweck und unter den von ihr vorgeschriebenen Bedingungen nutzen.
- Personenbezogene Informationen dürfen ausschließlich an die in den Abkommen oder Absprachen genannten Behörden übermittelt werden. Eine Übermittlung an andere Stellen darf nur mit vorheriger Zustimmung der übermittelnden Stelle erfolgen.
- Der Empfänger unterrichtet die übermittelnde Stelle und den zuständigen Datenschutzbeauftragten auf Ersuchen über die Verwendung der übermittelten Informationen und über die dadurch erzielten Ergebnisse.
- Die übermittelnde Stelle ist verpflichtet, auf die Richtigkeit der zu übermittelnden Informationen zu achten. Erweist sich, daß unrichtige oder zu vernichtende personenbezogene Informationen übermittelt worden sind, so ist dies dem Empfänger unverzüglich mitzuteilen. Dieser ist verpflichtet, die Berichtigung oder Vernichtung vorzunehmen.
- Dem Betroffenen ist auf Antrag über die zu seiner Person vorhandenen Informationen sowie über den vorgesehenen Verwendungszweck Auskunft zu erteilen. Eine Verpflichtung zur Auskunftserteilung besteht nicht, soweit eine Abwägung ergibt, daß eine Auskunft den Verwendungszweck oder schutzwürdige Interessen Dritter gefährden würde.
- Die Übermittlung und der Empfang personenbezogener Informationen sind aktenkundig zu machen.
- Zur Gewährleistung dieser Grundsätze sind die verfahrensmäßigen Sicherungen vorzusehen. Dazu kann es gehören, besondere Stellen mit der Datenübermittlung zu beauftragen. Die Kontrolle der Datenübermittlung durch unabhängige Datenschutzbeauftragte muß gewährleistet sein.

4. Die Verarbeitung personenbezogener Daten bei den Sicherheitsbehörden der Bundesrepublik Deutschland muß im Hinblick auf die politischen Veränderungen in der DDR und im übrigen Mittel- und Osteuropa über die bereits getroffenen Maßnahmen hinaus überprüft werden. Diese Notwendigkeit besteht u. a. bei:
   - dem Verfahren der Sicherheitsüberprüfung,
   - der Datenerhebung und Datenübermittlung des Bundesgrenzschutzes anläßlich von Grenzkontrollen an die Nachrichtendienste,
   - der Bereinigung der Datensammlungen der Verfassungsschutzbehörden.

1.6 Beschluß der 39. Konferenz am 22./23. März 1990 zum Bundesdatenschutzgesetz und zum Bundesverfassungsschutzgesetz

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder und der Datenschutzkommission Rheinland Pfalz (gegen die Stimme Bayerns) begrüßt die mit den am 13. März 1990 vorgelegten Vorschlägen der Koalitionsfraktionen verbundene Absicht, die längst fällige Novellierung des Bundesdatenschutzgesetzes und des Bundesverfassungsschutzgesetzes noch rechtzeitig vor dem Ende der Legislaturperiode zu verabschieden.

Die Vorschläge zum *Bundesdatenschutzgesetz* beseitigen eine Reihe von Schwächen des Regierungsentwurfes. Hervorzuheben ist insoweit

- daß nunmehr für den öffentlichen Bereich die Verarbeitung personenbezogener Daten in Akten und die Datenerhebung durch öffentliche Stellen in den Geltungsbereich des Bundesdatenschutzgesetzes einbezogen werden,
- daß künftig der Bundesbeauftragte für den Datenschutz durch das Parlament gewählt werden soll,
- daß der Betroffene bei Ablehnung der Auskunftserteilung darauf hingewiesen wird, daß er sich an den Bundesbeauftragten für den Datenschutz wenden kann.

Demgegenüber weisen auch die Vorschläge noch Schwächen und Defizite auf. Dazu gehören u. a.:

- Die unzureichende Kontrollbefugnis des Bundesbeauftragten für den Datenschutz bei der Datenverarbeitung in Akten,
- ein Widerspruchsvorbehalt für die Betroffenen gegen eine Kontrolle ihrer Daten durch den Bundesbeauftragten für den Datenschutz, der systematische Prüfungen gefährdet und deshalb entbehrlich ist, weil es für die Datenschutzbeauftragten schon immer selbstverständlich war, die Daten von Betroffenen nicht gegen deren erklärten Willen in Kontrollen einzubeziehen,
- die verfassungswidrige Erstreckung des Widerspruchsvorbehaltes in der Neufassung auf die Landesbeauftragten für den Datenschutz,
- das Fehlen eines gesonderten Gesetzesvorbehaltes für die Einrichtung von Direktzugriffsverfahren in besonders sensiblen Bereichen,
- der zu weite Katalog erlaubter Zweckänderungen und die unzureichende Unterrichtung des Betroffenen über die Zweckänderung.

Im Bereich der Datenverarbeitung durch nichtöffentliche Stellen verschlechtern einzelne vorgeschlagene Regelungen die Rechte der Betroffenen im Vergleich zum geltenden Gesetz, etwa bei der Übermittlung von Daten an den Adressenhandel. Sie bleiben im übrigen weit hinter den Vorschlägen für den öffentlichen Bereich zurück. Weder die Verarbeitung in Akten noch die Datenerhebung werden einbezogen. Auch die höchst unzureichenden Kontrollbefugnisse der Datenschutzaufsichtbehörden sind nicht wesentlich verbessert worden.

Schließlich erinnern die Datenschutzbeauftragten an ihre früheren Forderungen nach bereichsspezifischen Regelungen für die Verarbeitung von Arbeitnehmerdaten sowie von Regelungen für den Kredit- und Versicherungsbereich.

Zu den Vorschlägen der Koalition für das *Bundesverfassungsschutzgesetz* stellen die Datenschutzbeauftragten des Bundes und der Länder fest:

Die Vorschläge bringen gegenüber dem Vorentwurf der Bundesregierung Verbesserungen. Dies gilt insbesondere für:

- Den Schutz des in Wohnungen nichtöffentlich gesprochenen Wortes vor heimlichem Mithören und Aufzeichnen,
- die Einschränkung der Speicherung von Daten über Minderjährige,
- die konkretisierenden und einschränkenden Regelungen für den Einsatz nachrichtendienstlicher Mittel,
- die präzise Definition der „Bestrebungen" gegen die freiheitlich-demokratische Grundordnung,
- die Anknüpfung der Sammlung und Verarbeitung von Daten an das Vorliegen tatsächlicher Voraussetzungen.

Hingegen sind u. a. folgende datenschutzrechtliche Anforderungen noch nicht erfüllt:

- Die Befugnisse zur Datenverarbeitung müssen differenziert den unterschiedlichen Aufgaben zugeordnet werden.
- Die Datenspeicherung ist nicht so präzise geregelt, daß der Bürger dem Gesetz entnehmen kann, unter welchen in seiner Person liegenden Voraussetzungen der Verfassungsschutz über ihn Daten speichern darf.
- Die Zweckbindung der Daten innerhalb des Verfassungsschutzes ist nicht gewährleistet.
- Das Auskunftsrecht des Bürgers auch gegenüber den Verfassungsschutzbehörden wird zwar nunmehr erstmals anerkannt.

  Die vorgeschlagene Regelung schränkt aber den Auskunftsanspruch zu sehr ein. So wird dem Bürger eine Pflicht zur Begründung seines Auskunftsersuchens auferlegt, während die ablehnung der Auskunft unter keinen Umständen begründet werden muß.

– Die vorgesehenen Regelungen zur Sicherheitsüberprüfung ersetzen nicht eine bereichsspezifische, präzise Rechtsgrundlage in einem Geheimschutzgesetz für das Überprüfungsverfahren.

Die Datenschutzbeauftragten gehen davon aus und halten es für notwendig, daß die bestehenden Mängel der Gesetzentwürfe in den anstehenden Parlamentsberatungen behoben und ihre Anregungen aufgegriffen werden.

1.7 Beschluß der 39. Konferenz am 22./23. Märzt 1990 zur Einrichtung eines Arbeitskreises Europäische Gemeinschaft

1. Der Arbeitskreis EG (AK EG) hat die Aufgabe, zum frühestmöglichen Zeitpunkt Informationen über Entwürfe, Vorschläge und Projekte der EG-Organe und des Europarats mit datenschutzrelevantem Inhalt zu beschaffen und diese umgehend allen Datenschutzbeauftragten zuzuleiten. Der AK EG verfolgt die weitere Behandlung dieser Vorhaben in den Institutionen auf EG/Europarats-Ebene sowie auf Bundes- und Landesebene (Bundesrat).
2. Zu den unter 1. genannten Aufgaben knüpft bzw. koordiniert der AK EG Kontakte zu den mit Datenschutzfragen befaßten Institutionen und Personen auf den Ebenen EG, Europarat, Bundesregierung, Bundestag(sfraktionen), Bundesrat, Landesregierungen usw. Gleiches gilt für die Datenschutzinstitutionen in den EG-Nachbarländern.
3. Der AK EG hält Kontakt zur Arbeitsgruppe „Internationaler Datenverkehr" des Düsseldorfer Kreises und lädt im Regelfall einen ihrer Vertreter zu seinen Sitzungen ein.
4. Vorhaben, die in den Aufgabenbereich eines bestehenden Arbeitskreises der DSB-Konferenz gehören, werden inhaltlich dort behandelt. Soweit dies nicht der Fall ist, insbesonder bei übergreifenden oder Querschnittsthemen (z. B. Entwurf einer Rahmenrichtlinie zum Datenschutz in der EG), werden diese im AK EG behandelt.
5. Der Vorsitz des AK EG wechselt jährlich. Im ersten führt der Hessische Datenschutzbeauftragte (HDSB) den Vorsitz. Im darauffolgendem Jahr wird der Vorsitz vom Bundesbeauftragten (BfD) wahrgenommen. Je ein Mitarbeiter von BfD und HDSB bilden gemeinsam das „Sekretariat" des AK EG.

1.8 Entschließung der Sonderkonferenz am 27. Juni 1990 zum Entwurf eines Gesetzes zur Bekämpfung des illegalen Rauschgifthandels und anderer Erscheinungsformen der organisierten Kriminalität

Die Konferenz der Datenschutzbeauftragten hat schwerwiegende datenschutzrechtliche Bedenken gegen die Ausweitung der polizeilichen Ermittlungsbefugnisse in der Strafprozeßordnung, wie sie mit dem vom Bundesrat vorgelegten Gesetzentwurf zur Bekämpfung des illegalen Rauschgifthandels und anderer Erscheinungsformen der organisierten Kriminalität (OrgKG) beabsichtigt ist.

Erstmals werden in die Strafprozeßordnung Regelungen zur Rasterfahndung, zum Einsatz verdeckter Ermittler sowie von Wanzen und Richtmikrofonen und heimlichen Film- und Fotoaufnahmen eingefügt. Die Konferenz der Datenschutzbeauftragten verkennt nicht, daß bestimmte Erscheinungsformen von Kriminalität im Interesse des Schutzes der Bürger besondere Ermittlungsmethoden erforderlich machen können. Der vorgelegte Entwurf regelt jedoch nicht nur neue Eingriffsbefugnisse zur Bekämpfung des illegalen Rauschgifthandels und sonstiger organisierter Kriminalität - die im übrigen nicht definiert wird - sondern soll tief in die Privatsphäre der Bürger eingreifende Fahndungs- und Ermittlungsmethoden in das Strafverfahrensrecht allgemein einführen.

Gegen den vorliegenden Entwurf bestehen insbesondere folgende datenschutzrechtliche Bedenken:

– Die vorgesehenen Eingriffsbefugnisse der Strafverfolgungsbehörden werden an den konturenlosen Begriff „Straftaten von erheblicher Bedeutung" geknüpft. Damit dürfte nach der Begründung in der Praxis allenfalls die Kleinkriminalität ausscheiden. So soll z. B. auf die *Rasterfahndung* für eine Vielzahl von Delikten außerhalb organisierter Kriminalität zugelassen werden. Dies erscheint besonders bedenklich, weil gerade die Form der Fahndung unbescholtene Bürger in großer Zahl unvermeidlich mit einbezieht und sie in der Folge Ziel weiterer Ermittlungen werden können.
– Tief in die Privatsphäre eindringende Ermittlungsmethoden werden nicht hinreichend präzisiert und sind großenteils unverhältnismäßig: So dürfen ohne Wissen des Betroffenen zur Aufklärung *jeder Straftat* - sogar in Wohnungen hinein - „Lichtbilder und Bildaufzeichnungen" aufgenommen sowie „besondere Sichthilfen" eingesetzt werden.
– Maßnahmen, wie Einsatz von Peilsendern, Richtmikrofonen, Wanzen und sonstiger Überwachungstechniken können sich auch gegen dritte *unverdächtige Personen* richten, wenn „auf Grund bestimmter Tatsachen" anzunehmen ist, „daß sie mit dem Täter in Verbindung stehen oder eine solche Verbindung hergestellt wird". Es bleibt völlig offen, wie das Tatbestandsmerkmal der „Verbindung" eingegrenzt werden soll. Foto- und Filmaufnahmen von Unbeteiligten sind bereits zulässig, wenn sie für Ermittlungen „geeignet" sind. Damit kann kein Bürger vorhersehen, ob und wann er hiervon betroffen sein kann. Ohne Kenntnis der gegen ihn gerichteten Eingriffe kann er im Regelfall nicht einmal Rechtsschutz erlangen.
– Die Möglichkeiten der Telefonüberwachung werden über das vertretbare Maß hinaus ausgeweitet.
– Bedenken richten sich ferner dagegen, bei besonderen Ermittlungsmaßnahmen auf die vorherige *richterliche Kontrolle* zu verzichten und durch Eilkompetenzen die Entscheidung der diese Maßnahmen selbst durchführenden Polizei zu übertragen. Nicht einmal die nachträgliche richterliche Kontrolle ist in jedem Fall zwingend vorgesehen.

Im Gegensatz zu den erweiterten Befugnissen der Strafverfolgungsbehörden sind Regelungen zum Schutz oder im Interesse der Betroffenen nur unzureichend vorgesehen. Die mit besonderen Ermittlungsmethoden für besondere Strafverfolgungszwecke erhobenen Daten dürfen für zu weitgehende andere Zwecke verwendet werden. So sind z. B. die Begriffe „Zwecke der staatsanwaltlichen Vorgangsverwaltung" und „Zwecke der Rechtspflege" zu unbestimmt. Es fehlen weiterhin ausreichende Bestimmungen zum Auskunftsrecht des Betroffenen und zur Löschung.

Zusammenfassend ist festzustellen, daß dieser Entwurf selbst hinter den datenschutzrechtlichen Ansätzen, wie sie etwa noch im Entwurf des Strafverfahrensänderungsgesetzes 1989 enthalten waren, zurückbleibt.

Die Konferenz der Datenschutzbeauftragten fordert den Deutschen Bundestag auf, diese Vorschläge des Gesetzentwurfs abzulehnen und die unterbrochenen Arbeiten an der umfassenden datenschutzrechtlichen Novellierung der Strafprozeßordnung, die dringend geboten ist, wieder aufzunehmen. Hierzu haben die Datenschutzbeauftragten wiederholt konkrete Vorschläge vorgelegt.

1.9 Beschluß der 40. Konferenz am 4./5. Oktober 1990 zur Stärkung des Schutzes des Brief-, Post- und Fernmeldegeheimnisses sowie des nichtöffentlich gesprochenen Wortes

Wegen der dynamischen technischen Entwicklung auf dem Gebiet der Telekommunikation ist es dringlich, das Grundrecht auf freie Entfaltung der Persönlichkeit gegen neue Gefährdungen zu schützen. Den Risiken für das Recht auf unbeobachtete Kommunikation muß rechtzeitig begegnet werden:

– Die Einführung von ISDN macht es möglich, daß auch nach Beendigung von Telefongesprächen über einen bestimmten Zeitraum gespeichert wird, wer wann mit wem wie lange telefoniert hat.

- Der zunehmende Einsatz von Funkdiensten im Telekommunikationsverkehr (z. B. mobile Telefone, Satellitenkommunikation) ist mit der Speicherung von noch mehr Daten über die Telefonverbindungen verbunden und erleichtert die Möglichkeit des Abhörens und Aufzeichnens der Gesprächsinhalte.
- Zunehmend stehen Abhöranlagen zur Verfügung, mit denen aus der Masse der geführten Telefongespräche bestimmte Telefonate gezielt herausgegriffen, aufgezeichnet und nach bestimmten Gesichtspunkten ausgewertet und gespeichert werden können.

Das Grundgesetz läßt Einschränkungen des Fernmeldegeheimnisses unter gewissen Voraussetzungen auf gesetzlicher Grundlage zu. In den vergangenen Jahren hat der Gesetzgeber diese Eingriffsmöglichkeiten mehrmals erweitert und hierbei alle Telekommunikationsdienste (wie z. B. Telefax und Btx) einbezogen. Zudem hat die Rechtsprechung den Anwendungsbereich extensiv ausgelegt. Vor diesem Hintergrund ist es erforderlich:

- Die gesetzlichen Regelungen präziser und enger zu fassen,
- bei Entwicklung, Auswahl und Einsatz von Telekommunikationstechniken darauf zu achten, daß bei deren Betrieb die Speicherung personenbezogener Daten nach Dauer und Umfang auf das wirklich Notwendige beschränkt wird,
- erlaubte Eingriffe in das Grundrecht nach Artikel 10 auf das unerläßliche Maß zu beschränken und eine strenge Zweckbindung der dabei gewonnenen Daten sicherzustellen,
- eine wirksame Kontrolle solcher Eingriffe durch geeignete technisch-organisatorische Maßnahmen zu gewährleisten.

Neben die Ausweitung der Möglichkeit der Überwachung der Telekommunikation treten zunehmend weitere Techniken der heimlichen Datenerhebung (z. B. durch Videoaufnahmen, Abhörgeräte, Richtmikrofone), durch die das Recht auf ungestörte Kommunikation auch außerhalb des Fernmeldebereiches gefährdet ist.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder erwartet, daß der Gesetzgeber diesen Gefährdungen des Rechts auf informationelle Selbstbestimmung seine Aufmerksamkeit zuwendet. Sie unterstützt in diesem Zusammenhang die Einwände der Bundesregierung in deren Stellungnahme zum Gesetzentwurf des Bundesrates zur Bekämpfung der organisierten Kriminalität. Die Datenschutzbeauftragten sehen in der Stärkung des Schutzes des Brief-, Post- und Fernmeldegeheimnisses sowie des nichtöffentlich gesprochenen Wortes einen Schwerpunkt ihrer weiteren Arbeit.

Enthaltung: Bayern

1.10 Beschluß der 40. Konferenz am 4./5. Oktober 1990 zur Neuregelung des Melderechtsrahmengsetzes

Der dem Deutschen Bundestag vorliegende Entwurf eines Ersten Gesetzes zur Änderung des Melderechtsrahmengesetzes hält weiter an der Hotel- und Krankenhausmeldepflicht fest. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder und der Datenschutzkommission Rheinland-Pfalz hat erhebliche Bedenken, ob dem Bund die Gesetzgebungskompetenz zur Regelung dieser Frage zusteht. In jedem Fall ist zu bedenken:

Zweck der allgemeinen Meldepflicht ist es, die Identität der Einwohner und deren Wohnungen festzustellen und diese Basisinformation für die Bewältigung einer vielzahl von Verwaltungsaufgaben zur Verfügung zu stellen. Bei einem kurzfristigen Aufenthalt in einem Hotel oder Krankenhaus entfällt dieser Zweck. Lediglich die Polizei hat ein Interesse an der Feststellung dieser Tatsachen. Schon deshalb paßt die Hotel- und Krankenhausmeldepflicht nicht in die Systematik des Melderechts, es handelt sich vielmehr um materielles Polizeirecht.

Polizeiliche Datenverarbeitung setzt voraus, daß Gefahren abgewendet oder Straftaten verfolgt bzw. verhütet werden sollen. Hotelgäste und Krankenhauspatienten können jedoch nicht schlechthin als Gefahrenquellen oder (potentielle) Straftäter angesehen werden. Vielmehr ist zu berücksichtigen, daß es sich im Regelfall um Bürger handelt, die ein Recht darauf haben, von polizeilichen Ermittlungen unbehelligt zu bleiben.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder und die Datenschutzkommission Rheinland-Pfalz ist darüber hinaus der Auffassung, daß den Bürgern in allen Meldegesetzen ein Widerspruchsrecht gegen die Weitergabe ihrer Daten an politische Parteien und Wählergruppen zum Zwecke der Wahlwerbung eingeräuml werden muß.

Gegenstimme Bayern mit Ausnahme des letzten Absatzes

1.11 Beschluß der 40. Konferenz am 4./5. Oktober 1990 zur Erarbeitung von Krebsregistergesetzen in Bund oder Ländern

1. Die Datenschutzbeauftragten haben schon in ihren Entschließungen vom 14. Dezember 1981 und 27. April 1982 zur Schaffung gesetzlicher Grundlagen für die Errichtung und Führung bevölkerungsbezogener epidemiologischer Krebsregister Stellung genommen. Wenn sich der Gesetzgeber zugunsten solcher Register, deren Nutzen auch unter Medizinern nicht unumstritten ist, entscheiden sollte, entspricht es dem gesetzlichen Auftrag der Datenschutzbeauftragten darauf zu achten, daß die Errichtung und Führung solcher Register in einer Weise geschieht, die auf das Persönlichkeitsrecht der Krebskranken in größtmöglichem Umfang Rücksicht nimmt.

2. Würde den Ärzten die Befugnis eingeräumt, ihre Krebskranken in jedem Fall ohne deren Einwilligung mit Namen an ein solches Register zu melden, würde dies einen äußerst schwerwiegenden Eingriff in deren durch Artikel 1 i. V. m. Artikel 2 Abs. 1 GG geschütztes Persönlichkeitsrecht darstellen, eine weitere Durchbrechung der ärztlichen Schweigepflicht zur Folge haben und damit das Arzt-/Patientenverhältnis erheblich belasten. Die Krebskranken würden ohne ihre Einwilligung zentral in einem Register gespeichert werden und zwar so, daß die registerführende Stelle feststellen kann, welche Personen an Krebs erkrankt und zum Register gemeldet worden sind.

Die Datenschutzbeauftragten sind deshalb der Auffassung, daß die Einrichtung eines Krebsregisters auf einer solchen Grundlage (Melderechtsmodell) nicht in Betracht kommt. Sie sind nach wie vor der Meinung, daß das Krebsregister nur mit Einwilligung der Patienten oder auf anonymer Basis geführt werden können. Für beides gibt es bereits Modelle (Einwilligungsmodell und dezentrales Verschlüsselungsmodell). Die Datenschutzbeauftragten sehen in diesen Modellen gangbare Wege zur Führung bevölkerungsbezogener Krebsregister, die auch noch fortentwickelt werden können.

Sollten weitere Modelle, die das Persönlichkeitsrecht der Krebskranken in gleicher Weise wahren, weiterentwickelt werden, sind die Datenschutzbeauftragten selbstverständlich bereit, auch sie in Erwägung zu ziehen.

2. Entschließungen der Internationalen Konferenz der Datenschutzbeauftragten

2.1 Entschließung der 12. Internationalen Konferenz am 19. September 1990 über Datenschutz und die Europäische Gemeinschaft

Im Hinblick auf die von der 11. Internationalen Konferenz der Datenschutzbeauftragten am 30. August 1989 verabschiedete Berliner Entschließung und insbesondere im Hinblick auf das Zusatzkommuniqué der Datenschutzbeauftragten der Mitgliedstaaten der Europäischen Gemeinschaften;

in Kenntnis der Tatsache, daß die Kommission der Europäischen Gemeinschaften eine Reihe von Entwurfsvorschlägen für Richtlinien hinsichtlich der automatischen Verarbeitung personenbezogener Daten und die Sicherheit von Informationssystemen verabschiedet hat, und zwar u. a.:

- einen Entwurfsvorschlag für eine Richtlinie des Rates zur Harmonisierung bestimmter Gesetzes-, Durchführungs- und Verwaltungsbestimmungen der Mitgliedstaaten zum Schutze des Einzelnen hinsichtlich der automatischen Verarbeitung personenbezogener Daten;
- einen Entwurfsvorschlag für eine Richtlinie des Rates zum Schutze personenbezogener Daten und der Privatsphäre im Zusammenhang mit öffentlichen digitalen Telekommunikationsnetzen und insbesondere im Zusammenhang mit dem „Integrated Services Digital Network" (ISDN - Dienste integrierendes Digitales Netz) und den Mobilfunknetzen;

In Anerkenntnis der Tatsachen, daß die Entwürfe für diese Rechtsinstrumente von der Kommission der Europäischen Gemeinschaften ohne vorherig Konsultierung der Datenschutzbeauftragten der Mitgliedstaaten erarbeitet wurden;

haben die Datenschutzbeauftragten (der Mitgliedstaaten der Europäischen Gemeinschaften), die am 19. September 1990 anläßlich der 12. Internationalen Konferenz der Datenschutzbeauftragten zusammentraten,

nach Anhörung des Vortrages und der Erläuterungen des/der Vertreter/s der Kommission der Europäischen Gemeinschaften beschlossen,

- die Richtlinienentwürfe ihrerseits zu prüfen und nach dem gegenseitigen Austausch ihrer Prüfungsergebnisse noch vor Ende des Jahres 1990 erneut zusammenzutreten, um sich auf eine gemeinsame Haltung zu diesen Vorschlägen zu einigen;
- diese gemeinsame Haltung in geeigneter Weise ihrer jweiligen Regierung zur Kenntnis zu bringen;
- diese gemeinsame Haltung gemeinsam der Kommission und dem Rat der Europäischen Gemeinschaften sowie dem Europäischen Parlament zur Kenntnis zu bringen, so daß sie bei der künftigen Prüfung der Richtlinienentwürfe Berücksichtigung finden kann;
- angesichts der zunehmenden Bedeutung europäischer Fragen die Möglichkeit zu prüfen, einmal jährlich zu einer Konferenz zusammenzutreten, um insbesondere datenschutzrelevante Fragen innerhalb der Europäischen Gemeinschaften zu erörtern.

2.2 Beschluß der 12. Internationalen Konferenz am 19. September 1990 zu Problemen öffentlicher Telekommunikationsnetze und des Kabelfernsehens

Nachdem die XII. Internationale Konferenz der Datenschutzbeauftragten in ihrer Entschließung vom 31. August 1989 allgemeine Grundsätze zu dienste-integrierenden digitalen Netzen (ISDN) aufgestellt hat, begrüßt sie den zweiten Bericht der Arbeitsgruppe „Telekommunikation und Medien", der zeigt, daß diese Grundsätze konkretisiert und auf der technischen Ebene garantiert werden sollten. Diese Grundsätze sind auf jede Form der Telekommunikation einschließlich analoger Formen und bestimmter Formen massenmedialer Kommunikation (insbesondere Kabelfernsehen) anzuwenden. Öffentliche und private Netzbetreiber sollten diese Prinzipien ebenso verwirklichen wie Anbieter von Telekommunikationsdiensten.

I.

Teilnehmerverzeichnisse

Verzeichnisse von Teilnehmern an Telekommunikationsdiensten sind inzwischen weltweit die wichtigsten öffentlich verfügbaren personenbezogenen Dateien. Die Konferenz stellt mit Sorge fest, wie schwierig es ist, die Nutzung dieser Daten weltweit zu kontrollieren. Die Risiken nehmen durch den Verkauf der Teilnehmerverzeichnisse auf elektronischen Datenträgern zu.

Personenbezogene Daten, die von Netzbetreibern erhoben und gespeichert werden, müssen dem Zweck entsprechen, dem Betroffenen einen Telekommunikationsdienst zur Verfügung zu stellen und ihm den Zugang zum Netz zu ermöglichen; die Daten müssen für diesen Zweck erheblich sein und dürfen nicht darüber hinausgehen.

Ein Teilnehmerverzeichnis sollte nur solche personenbezogenen Daten enthalten, die unbedingt zur hinreichend sicheren Identifikation bestimmter Teilnehmer erforderlich sind. Die Teilnehmer haben auch das Recht, einen Hinweis auf ihr Geschlecht (und auf ihren Wohnort)*) auszuschließen. Andererseits schließt dies die Veröffentlichung zusätzlicher Daten auf Wunsch des Teilnehmers nicht aus.

Teilnehmer haben das Recht, gebührenfrei und ohne Begründung den Eintrag ihrer Daten in ein Teilnehmerverzeichnis auszuschließen.

Bei der Erhebung von Bestandsdaten sollte der Netzbetreiber den betroffenen vollständig darüber aufklären, ob er zur Aufnahme seiner Daten in ein Teilnehmerverzeichnis unabhängig von der Form der Veröffentlichung verpflichtet ist oder nicht.

Bestandsdaten, die einen Mitbenutzer des Endgerätes betreffen, dürfen nur mit dessen Zustimmung in ein Teilnehmerverzeichnis aufgenommen werden.

Die Weitergabe von Bestandsdaten durch einen Netzbetreiber an Dritte zu Werbezwecken darf nur mit der freiwilligen und informierten Zustimmung des Betroffenen erfolgen, es sei denn, dieser hat nach innerstaatlichem Recht die Möglichkeit, der Weitergabe zu widersprechen.

Bestandsdaten von Teilnehmern, die einen Eintrag in das Teilnehmerverzeichnis ausgeschlossen oder sich entschieden haben, ihren Namen nicht für Werbezwecke nutzen zu lassen, sollten in keinem Fall an Dritte weitergegeben werden.

Besondere Aufmerksamkeit muß der höchsten räumlichen Ebene gewidmet werden, auf der dem Verzeichnis Teilnehmerdaten entnommen werden können.

Die Konferenz betrachtet mit Sorge die wachsenden Gefahren der telefonischen Direktwerbung und wird diese Probleme eingehender untersuchen.

II.

Anzeige der vom Anrufer benutzten Rufnummer

Die Einführung einer Einrichtung, die die Anzeige der Nummer des vom Anrufer benutzten Anschlusses am Endgerät des angerufenen Teilnehmers vor der Herstellung der Verbindung ermöglicht, wirft ernste Fragen des Schutzes der Privatsphäre auf.

Es ist wichtig, den Schutz der Privatsphäre des einzelnen Teilnehmers - der anrufenden und der angerufenen Person - mit den Erfordernissen der Kommunikationsfreiheit in Einklang zu bringen. Dies wird durch die Beachtung der folgenden Grundsätze erreicht:

Der Anrufer muß die Möglichkeit haben, durch eine einfache technische Vorrichtung im Einzelfall zu entscheiden, ob er seine Rufnummer anzeigen lassen will oder nicht, auf die Gefahr hin, daß sein Anruf von der angerufenen Person nicht entgegengenommen wird.

Dieses Verfahren zur Unterdrückung der Rufnummernanzeige muß für den Teilnehmer gebührenfrei sein.

Bei der Anwendung dieser Grundsätze sollen die folgenden Maßnahmen getroffen werden:

Teilnehmer müssen das Recht haben, gebührenfrei in das Teilnehmerverzeichnis einen Hinweis darauf aufnehmen zu lassen, daß sie kein Verfahren zur Anzeige der vom Anrufer benutzten Rufnummer anwenden.

Es ist notwendig, die Offenbarung übermittelter Informationen über den Anrufer an Dritte einzuschränken.

*) bezüglich des Klammerzusatzes bestehen unterschiedliche Auffassungen

Ausnahmsweise darf die Unterdrückung der Rufnummernanzeige entsprechend dem innerstaatlichen Recht außer Kraft gesetzt werden, wenn Personen über Notruf die Feuerwehr oder den Notarzt anrufen.

Der Netzbetreiber kann die Unterdrückung der Rufnummernanzeige auch außer Kraft setzen, um auf Antrag der angerufenen Person den Urheber belästigender Anrufe festzustellen.

Diese Grundsätze sollen bei der Abwicklung internationaler Telefongespräche in gleicher Weise beachtet werden.

III.

Mobilfunk

Netzbetreiber, die ein Mobilfunknetz betreiben und anbieten, sollten Teilnehmer über die Sicherheitsrisiken informieren, die normalerweise - insbesondere bei fehlender Verschlüsselung der übermittelten Nachrichten - mit der Benutzung eines Mobilfunknetzes verbunden sind. Der Betreiber sollte dem Teilnehmer vor allem empfehlen, das Mobilfunknetz nicht zur Übermittlung vertraulicher Nachrichten zu benutzen, solange Probleme der Datensicherheit bestehen.

Netzbetreiber sollten verpflichtet sein, den Teilnehmern am Mobilfunknetz wirksame Verschlüsselungsverfahren anzubieten.

Wirksame technische Vorkehrungen sollen getroffen werden, um den unbefugten Netzzugang über mobile Endgeräte zu verhindern.

Die Speicherung von Verbindungsdaten muß strikt auf den kurzen Zeitraum des Verbindungsaufbaus zwischen Teilnehmer und Netz beschränkt werden. Das Tarifsystem soll so gestaltet werden, daß die Orte, an denen Mobiltelefone benutzt worden sind, nicht Teil der Abrechnungsdaten sind. Besondere Beachtung verdient die Frage, inwieweit die Speicherung der vollständigen Rufnummer der angerufenen Person für Abrechnungszwecke notwendig ist.

IV.

Gebührenabrechnung

Inwieweit die Speicherung der vollständigen Nummer des angerufenen Teilnehmers für Zwecke der Gebührenabrechnung im allgemeinen erforderlich ist, sollte noch näher untersucht werden.

V.

Kabelfernsehen

Die Speicherung individueller Zuschauerprofile durch Kabelfernsehgesellschaften, die einzeln abrufbare („pay per view") Programme anbieten, ist ein Eingriff in die Privatsphäre des Kunden.

Deshalb sollten Kabelfernsehgesellschaften „pay per view"-Programme nur dann anbieten, wenn die Kunden eine praktikable und wirtschaftliche Möglichkeit (z. B. im voraus bezahlte Karten oder Decoder) haben, die Programme zu empfangen, ohne daß zuschauerbezogene Information gespeichert werden.

Messungen der Sehbeteiligung und Tantiemen dürfen nicht auf der Grundlage zuschauerbezogener Daten berechnet werden.

Die Konferenz befürchtet, daß in naher Zukunft im Bereich des Kabelfernsehens zahlreiche Datenschutzprobleme entstehen werden und wird die Entwicklung deshalb eingehend überwachen.