Abgeordnetenhaus von Berlin Drucksache 10/1883

10. Wahlperiode 15. 12. 87

Mitteilungen des Präsidenten

- Nr. 221 -

Druckschluß: 19. November 1987

Ausgegeben am 15. Dezember 1987

Der Präsident
Peter Rebsch

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

Vorlage zur Kenntnisnahme

Bericht des Berliner Datenschutzbeauftragten zum 31. Dezember 1987

Inhaltsverzeichnis

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

[2] § 3 Abs. 3 Gesetz zum Staatsvertrag über Bildschirmtext, GVBl. 33, 871 und § 55 Abs. 1 Kabelpilotprojektgesetz, GVBl. 84, 965.
Die Bestimmungen lauten gleichermaßen: „Der Berliner Datenschutzbeauftragte berichtet dem Abgeordnetenhaus von Berlin über von ihm festgestellte Mängel und über seine Vorschläge zu ihrer Behebung und zur Verbesserung des Datenschutzes".

6. Nachträge zu Feststellungen aus den Vorjahren

Landeseinwohneramt
(Jahresbericht 1986, Ziff. 2.1)

Ausländerwesen
(Jahresbericht 1986, Ziff. 2.1)

Kostenübernahme für Krankenhausbehandlungen
(Jahresbericht 1986, Ziff. 2.3)

Nebentätigkeit von Hochschullehrern
(Jahresbericht 1986, Ziff. 2.3)

Anonyme Anzeige wegen Rauschgiftschmuggels
(Jahresbericht 1986, Ziff. 4.2)

Urlaubsreise nach Indien
(Jahresbericht 1986, Ziff. 4.2)

Aussonderung von Altakten
(Jahresbericht 1986, Ziff. 4.2)

Rückmeldeverfahren bei der Strafverfolgung
(Jahresbericht 1986, Ziff. 4.2)

Jubiläen
(Jahresbericht 1986, Ziff. 4.3)

AV-Schülerunterlagen
(Jahresbericht 1986, Ziff. 4.4)

Aktenführung in Sozial- und Jugendverwaltungen
(Jahresbericht 1986, Ziff. 4.5)

Altlasten-Suchkonzept
(Jahresbericht 1986, Ziff. 4.6)

Rückverteilungen von Lohnsteuerkarten
(Jahresberichte 1980, Ziff. 2.6; 1981, Ziff. 2.3; 1986, Ziff. 5)

7. Zusammenarbeit mit anderen Stellen

Konferenz der Datenschutzbeauftragten

Abgeordnetenhaus

Aufsichtsbehörde nach dem Bundesdatenschutzgesetz

Meldungen zum Dateienregister

Anlagen

1. Datenschutz und Neue Medien
   Beschluß der Internationalen Konferenz der Datenschutzbeauftragten 1987
2. Anforderungen an datenschutzrechtliche Regelungen des Bundes aus der Sicht der Länder
3. Empfehlungen zum Datenschutz bei der Automatisierung des Zahlungsverkehrs
4. Beschluß der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 4./5. Mai 1987 zur Neukonzeption des Ausländerregisters
5. Europarat
   Empfehlung Nr. R (83) 10 des Ministerkomitees an die Mitgliedstaaten zum Schutz personenbezogener Daten für Zwecke der wissenschaftlichen Forschung und Statistik
6. Vorläufige Verwaltungsvorschriften über die Führung von Personalakten der Dienstkräfte des Landes Berlin - Teilregelung - vom 3. Dezember 1986
7. Entwurf von Ausführungsvorschriften über den Schulpsychologischen Dienst an den öffentlichen Schulen des Landes Berlin - Auszug -

Stichwortregister
für alle seit 1979 veröffentlichten Jahresberichte

1. Zur Situation

Die Furcht vor der Zunahme staatlicher Überwachung

Die Furcht vor einer ungerechtfertigten Zunahme staatlicher Überwachung muß ernstgenommen werden. Denn sie kann bereits das Verhalten der Menschen, wie die Ausübung der Grundrechte, in einer Weise bestimmen, die nicht den Vorstellungen des Grundgesetzes entspricht. Allerdings zeigt die öffentliche Diskussion, daß die Behauptung, die staatliche Überwachung nehme zu, jeweils gründlich geprüft werden muß.

So stand mit der *Volkszählung 87* ein Projekt im Blickpunkt der Öffentlichkeit, das - bei aller möglichen Kritik im Grundsätzlichen und in Einzelfragen - seinem Inhalt nach mit Sicherheit kein Instrument der Überwachung ist. Parolen, die dies suggerierten, sind geeignet, das deutlich gestiegene Datenschutzbewußtsein der Bürger irrezuleiten. Sie instrumentalisieren den Datenschutz - und das damit verbundene öffentliche Interesse - für andere Zwecke. Nichtsdestoweniger stand die Volkszählung im Mittelpunkt meiner eingehenden Datenschutzkontrolle. Über die Ergebnisse wird im nächsten Abschnitt anhand der Fakten ausführlich berichtet. Dies erscheint besonders deswegen erforderlich, weil nicht nur von Volkszählungsgegnern, sondern auch von seiten des Bundesinnenministers Sachverhalte bewertet werden, die aufgrund des Verfahrensstandes noch gar nicht feststehen.

Die Zunahme staatlicher Kontrolle wird dagegen durch den neuen *maschinenlesbaren Ausweis* prinzipiell ermöglicht, der seit April 1987 auch für Berliner ausgegeben wird. Soweit das Projekt öffentlich diskutiert worden ist, geschah dies häufig unter falschem Vorzeichen: Angesichts der absehbaren technischen Entwicklung kann die Diskussion nicht mehr an der Maschinenlesbarkeit an sich ansetzen. Vielmehr müssen die technischen Infrastrukturen kritisch hinterfragt werden, die dieses Potential für administrative Zwecke nutzbar machen. Es kommt daher darauf an, ob mit der Anschaffung und dem Einsatz von Lesegeräten die Kontrolldichte ungerechtfertigt erhöht wird und ob die gesetzlichen Vorschriften ausreichen, dies zu verhindern.

Dafür, daß die Kontrolldichte in Berlin nicht wesentlich erhöht wird, steht nach wie vor die Erklärung des Innensenators vor dem Abgeordnetenhaus. Vorschriften über die Benutzung der gelesenen Ausweisdaten für Fahndungszwecke fehlen weitgehend. Dies ist allerdings nicht problematisch, wenn daraus der - einzig zulässige - Schluß gezogen wird: Soweit keine ausreichenden Rechtsvorschriften vorliegen, können keine Lesegeräte aufgestellt werden. Dies gilt nicht nur für maschinenlesbare Personalausweise, sondern auch für den *maschinenlesbaren Paß*, der ab 1988 eingeführt werden soll.

Aktuell ist ferner die Frage des Umgangs mit den Daten von *AIDS*-infizierten und -erkrankten Bürgern. So ist bei einer ganzen Reihe von Vorstellungen - auch der Bayerischen Staatsregierung - im Einzelfall umstritten, ob sie noch vom geltenden Recht gedeckt werden[1]. Insgesamt bewertet würden sie - selbst wenn sie im einzelnen allesamt zulässig wären - jedenfalls ein Klima der Überwachung schaffen, das weder dem Bild des Grundgesetzes von unserer offenen Gesellschaft noch der moralischen Verpflichtung zur persönlichen Zuwendung entspricht.

Der Wunsch nach umfassender personenbezogener Registrierung erscheint vielmehr als Reflex der Furcht vor einer bisher (noch) unheilbaren Krankheit, ähnlich wie der maschinenlesbare Ausweis - und der maschinenlesbare Paß, der ab 1988 ausgegeben wird, - wohl vor allem Reflexe der Furcht vor Terrorismus sind. Die Gefahr derartiger Reflexe liegt darin, daß sie als Problemlösung selbst angeboten werden. Datenschutzrelevant sind diese Vorgehensweisen, wenn die Verdatung an die Stelle der Problemlösung tritt, diese aber am Ende ausbleibt und die Datensammlung keinen Nutzen stiftet. Die sich abzeichnende „Berliner Linie" in der Frage der AIDS-Bekämpfung kann von mir unter diesen Gesichtspunkten nur begrüßt werden.

Genährt wird die Furcht vor Überwachung nicht zuletzt durch die sich aus dem wissenschaftlichen Fortschritt ergebende Zunahme der Überwachungsmöglichkeiten. Der von der Enquete-

[1] Vgl. BVerfG 1 BvR 842/87 in: Europäische Grundrechte Zeitschrift (EuGRZ) 1987, S. 353 f., das diese Frage ausdrücklich offenläßt.

Kommission „Chancen und Risiken der *Gen-Technologie*" dem Deutschen Bundestag vorgelegte Bericht läßt auf einem Spezialgebiet das Gefahrenpotential erkennen. So steht zu erwarten, daß in Zukunft in zunehmendem Maße genetische Daten anfallen, die höchstsensible Informationen über die genetische Konstitution des Einzelnen enthalten können (z. B. über Erbanlagen für Krankheiten oder besondere Empfindlichkeiten gegenüber speziellen Stoffen). Es muß daher sorgfältig geprüft werden, ob überhaupt und unter welchen Umständen genetische Register angelegt, „genetische Fingerabdrücke" zur Aufklärung von Verbrechen verwendet werden können und wann eine „Genomanalyse" zulässig oder verboten ist. Es wird für jede dieser Methoden in Einzelfällen Gründe geben, sich der neuen Techniken zu bedienen. Das verfassungsrechtliche Ziel, dem einzelnen Bürger einen hinlänglichen Freiraum zu verschaffen, gebietet jedoch, darüber nachzudenken, ob und in welchem Umfang man von bestimmten Möglichkeiten Gebrauch machen kann. Die Verpflichtung des Gesetzgebers, diese Möglichkeiten zu beschränken - ich denke z. B. an das Verbot einer Genomanalyse als Voraussetzung für die Einstellung von Arbeitnehmern - erscheint offenkundig. Konkrete Vorschläge werden von einer Arbeitsgruppe Gentechnologie der Datenschutzbeauftragten vorbereitet.

Unmittelbarer erscheinen allerdings die Gefahren einer anderen technischen Entwicklung, der Datenverarbeitung über *Netze*. So waren bereits in der Vergangenheit bestimmte Formen der Fernwartung durch Hersteller problematisch. Vor allem mußte ich bereits vor Jahren nachdrücklich darauf dringen, daß nicht Mitarbeiter von zu Hause über Leitungen auf die Datenverarbeitungsanlagen der öffentlichen Verwaltung zugreifen können. In mehreren Fällen mußte ich sogar die sofortige Abkoppelung entsprechender Geräte verlangen, was auch geschah.

Die gerade abgeschlossene Überprüfung der Datenverarbeitung der Berliner Krankenhausbetriebe hat ergeben, daß auch dort die Netzgestaltung ein beachtliches Risiko darstellt. So waren unbefugte Zugriffe auf Berliner Gesundheitsdaten über das internationale Forschungsnetz möglich.

In der vernetzten Datenverarbeitung liegt ein Schwerpunkt für reale Gefahren, der angesichts der stürmisch vorangetriebenen Vernetzung noch ernster genommen werden muß. Die Kontrollen des Berliner Datenschutzbeauftragten werden sich daher in Zukunft auch auf diesen Bereich konzentrieren.

Allerdings zeigt der folgende Bericht, daß nicht der Mißbrauch staatlicher Macht, sondern individuelle Fehler, Vertrauensseligkeit und der Mißbrauch durch einzelne Mitarbeiter Quellen der festgestellten Mängel sind. Aufgabe des Datenschutzes ist es, diese Schwachstellen soweit als möglich aufzudecken und für ihre Beseitigung zu sorgen.

Rechtsentwicklung

Vor dem Ende der Legislaturperiode wurden auf Bundesebene noch zwei Gesetze verabschiedet, die auf unterschiedliche Weise für die Zukunft große datenschutzrechtliche Bedeutung haben: Am 22. Januar 1987 wurde das neue *Bundesstatistikgesetz* verkündet, in dem die statistische Geheimhaltung eine ausführliche neue, die Belange des Datenschutzes in besonderem Maße berücksichtigende Regelung erfahren hat. Das rechtzeitige Inkrafttreten vor der Volkszählung verschaffte dieser zwar den allgemeinen statistikrechtlichen Rahmen, das Gesetz enthält aber seinerseits Bestimmungen, die hinter dem Volkszählungsgesetz zurückbleiben und damit erhebliche Unsicherheit über die Reichweite des Datenschutzes bei der Volkszählung auslösten. Sie konnten nur durch eine Anweisung des Bundesinnenministeriums beseitigt werden, nach der den datenschutzfreundlicheren Bestimmungen des Volkszählungsgesetzes trotz dessen früheren Zeitpunktes der Vorrang eingeräumt werden sollte.

Eine Woche später wurde ein *Änderungsgesetz zum Straßenverkehrsgesetz* verkündet, mit dem die Vorschriften über das Verkehrszentralregister sowie die Fahrzeugregister grundsätzlich neu gestaltet wurden. Erhebung, Speicherung und Übermittlung personenbezogener Daten über Halter und deren Fahrzeuge sind nunmehr weitgehend normenklar geregelt; eine ergänzende Fahrzeugregisterverordnung, deren Verabschiedung sich allerdings verzögert hat, enthält ergänzende Bestimmungen insbesondere über die Protokollierung der Abrufe. Die anderen im sogenannten „Sicherheitspaket" enthaltenen, aber nicht verabschiedeten Gesetzentwürfe (Zusammenarbeitsgesetz, Bundesverfassungsschutzgesetz, MAD-Gesetz und Bundesdatenschutzgesetz) fielen der Diskontinuität zum Opfer und sind bislang nicht wieder in den Bundestag eingebracht worden.

Die Vielfalt der erforderlichen Gesetzesvorhaben auf Bundesebene ergibt sich aus einer Aufstellung[1], die ich der Konferenz der Datenschutzbeauftragten vorgelegt habe.

Landesrechtlich bedeutsam war insbesondere die Verkündung einer alliierten Rechtsvorschrift (BK/O (87) 1 vom 10. März 1987), mit der die bestehenden Vorschriften über den *Berliner Behelfsmäßigen Personalausweis* ergänzt wurden und die Rechtsgrundlage für die Einführung des maschinenlesbaren Personalausweises geschaffen wurde. Aufgrund dieser Vorschrift erließ der Senat eine Verordnung zur Durchführung der BK/O (46) 61, in der die datenschutzrechtlichen Vorgaben des Bundespersonalausweisgesetzes übernommen wurden. Der Landesgesetzgeber selbst verabschiedete keine Gesetze mit erheblichen datenschutzrechtlichen Gehalten. Auf untergesetzlicher Ebene traten im Dezember 1986 die *Vorläufigen Verwaltungsvorschriften über die Führung von Personalakten* der Dienstkräfte - Teilregelung - in Kraft, mit denen die Personalaktenführung für die öffentlichen Bediensteten des Landes Berlin erstmals einheitlich geregelt wurde, wenn auch wesenliche materielle Bestimmungen noch folgen müssen. Neben der hierzu erforderlichen *Ergänzung des Beamtenrechts* stehen weiterhin wichtige Gesetzgebungsvorhaben aus, deren Behandlung ich bereits früher für vordringlich erklärt hatte: In erster Linie zu nennen sind das *Landesstatistikgesetz*, sowie datenschutzrechtlich erforderliche Ergänzungen des *Landeskrankenhausgesetzes* und des *Schulgesetzes*, nicht zuletzt die *Novellierung des Allgemeinen Sicherheits- und Ordnungsgesetzes (ASOG)*. Gerade angesichts der Bedeutung des ASOG kann es nicht länger hingenommen werden - nicht zuletzt auch im Interesse der Beamten, die selbst unter Unklarheiten in der täglichen Arbeit leiden -, daß in Berlin bisher keine neue Regelung - wenigstens als Referentenentwurf - vorgelegt worden ist, obwohl feststeht, daß die geltende Regelung wesentlichen verfassungsrechtlichen Geboten nicht entspricht. Auch bei Anerkennung des Bestrebens, die Entwicklung auf Bundesebene einzubeziehen, und der gerade für diese schwierige Materie erforderlichen gründlichen Vorbereitung, ist die Zeit bisher nur ungenügend genutzt worden. Dies muß sich ändern.

Weiter fortgeschritten ist die Diskussion um die *Archivgesetzgebung*. Nachdem das Bundesarchivgesetz erneut beraten worden ist, hat auch das Abgeordnetenhaus in der Sitzung vom 12. November 1987 aufgrund eines Initiativantrags der AL-Fraktion über ein Landesarchivgesetz[2] die Problematik behandelt. Übereinstimmend wurde die Dringlichkeit eines Landesarchivgesetzes festgestellt.

In der *Rechtsprechung des Bundesverfassungsgerichts* ist es noch nicht zu der erwarteten Fortentwicklung der Grundsätze zum informationellen Selbstbestimmungsrecht gekommen. Zwar gab es eine Fülle von *Verfassungsbeschwerden* auch gegen die *Volkszählung 1987*, bislang hat das Bundesverfassungsgericht jedoch noch keine Beschwerde zur Entscheidung angenommen, da es die Überprüfung der rechtmäßigen Durchführung der Volkszählung als Aufgabe der Datenschutzbeauftragten oder Verwaltungsgerichte betrachtet. Auch die erwähnte Verfassungsbeschwerde, deren Ziel legislative Maßnahmen zur *AIDS-Bekämpfung*, insbesondere zur Einführung einer Meldepflicht war, wurde nicht angenommen.

Unter den anderen Bundesgerichten mußte sich vor allem das *Bundesarbeitsgericht* mit datenschutzrechtlichen Fragen befassen. In einer grundsätzlichen Entscheidung zu *Personalinformationssystemen* bekräftigte es die Geltung des Verhältnismäßigkeitsgrundsatzes auch bei der Beurteilung des zulässigen Umfanges der Speicherung von Personaldaten durch private Arbeitgeber und bestätigte damit die von den Datenschutzbeauftragten vertretene Auffassung, daß bei der Auslegung privatrechtlicher Vorschriften auch das informationelle Selbstbestimmungsrecht be-

[1] Anlage 2
[2] Drucksache 10/837

rücksichtigt werden muß. Dem entspreche es, wenn in die Privatsphäre des Arbeitnehmers nicht tiefer eingedrungen werden dürfe, als es der Zweck des Arbeitsverhältnisses unbedingt erfordert. In einer anderen Entscheidung hatte das Gericht seine eigene Rechtsprechung zur Zulässigkeit der *Erfassung* personenbezogener Daten über *Telefongespräche* zu präzisieren. War zuvor nur die Zulässigkeit der Speicherung personenbezogener Daten bei Privatgesprächen bezweifelt worden, steht es nunmehr fest, daß bei besonderen Ausgestaltungen des Arbeitsverhältnisses auch die Speicherung von Daten über dienstliche Gespräche unzulässig sein kann. In diesem Fall handelte es sich um die Speicherung von Daten über Gespräche, die ein Berufspsychologe als Berater in Ehe-, Erziehungs- und Jugendfragen geführt hat. Der Arbeitgeber dürfe die Arbeit des Klägers nicht soweit kontrollieren und überwachen, daß ihm dadurch ein vom Betroffenen zu wahrendes Geheimnis einer dritten Person bekannt wird.

Weiter hat das Bundesarbeitsgericht über die Frage der Aufbewahrung von *Gesundheitsdaten* in *Personalakten* entschieden. Danach bedürfen sensible Daten, zu denen insbesondere Gesundheitsdaten gehören, des verstärkten Schutzes. Es ist daher nicht mit Art. 1 und 2 GG vereinbar, wenn derjenige, der irgendeinen Vorgang in der Personalakte abheftet, Gesundheitsdaten einsehen könnte. Der Arbeitgeber hat vielmehr je nach Datenart für ein System abgestufter Zugangsmöglichkeiten zu sorgen. Die Verletzung des Persönlichkeitsrechts tritt bereits ein, wenn der Arbeitgeber entsprechende Schutzmaßnahmen unterläßt und nicht erst dann, wenn Unbefugte Kenntnis nehmen.

Einen datenschutzrechtlichen Aspekt weist ein Urteil des *Bundesverwaltungsgerichts* auf, mit dem die Anrechnung der allein mit zusätzlichen eigenen Mitteln finanzierten Leistungen einer privaten Krankenversicherung auf die einem Beamten zustehende *Beihilfe* rechtswidrig ist. Bei einer Übertragung dieses zunächst das nordrhein-westfälische Landesrecht betreffenden Entscheidung wäre in Berlin die Erhebung von Angaben über die private Krankenversicherung, die seit der letzten Änderung der Beihilfevorschriften auch in Berlin zu einer Reihe datenschutzrechtlicher Beschwerden geführt hat, nicht mehr zulässig.

Auch eine Reihe anderer Gerichte befaßte sich mit datenschutzrechtlichen Fragen. Von großem Interesse sind Urteile der *Oberverwaltungsgerichte Berlin und Bremen,* nach denen die Verfassungsschutzbehörde nicht zu einer pauschalen *Auskunftsverweigerung* berechtigt ist. Zu dieser Frage hatte ich im Zusammenhang mit einem Vorlagebeschluß zum Bundesverfassungsgericht im Vorjahr eine Stellungnahme abgegeben, die eine nach den verschiedenen Aufgabenbereichen des Verfassungsschutzes differenzierte Praxis verlangt. Das *OVG Berlin* hat in einem - allerdings nicht rechtskräftigen - Urteil entschieden, daß auch Feststellungen und Belehrungen, die von der Dienstbehörde wertfrei und ohne Schuldvorwurf erfolgen, dann nicht in die *Personalakte,* sondern in eine - innerhalb einer bestimmten Frist zu tilgenden - Unterakte zu nehmen sind, wenn der Gesamtvorgang unwiderlegbar als Maßregelung charakterisiert werden kann; eine ähnliche Auffassung hatte ich im Zusammenhang mit sogenannten „Sachverhaltsfeststellungen" vertreten.

2. Volkszählung 1987 - eine Zwischenbilanz

2.1 Rechtliche Vorgaben

Verfassungsmäßigkeit des Volkszählungsgesetzes

Das Volkszählungsgesetz 1987, die zu seiner Durchführung in Berlin erlassene Rechtsverordnung und die Ausführungsvorschriften zum Volkszählungsgesetz entsprechen den Vorgaben, die das Bundesverfassungsgericht in seinem Urteil zum Volkszählungsgesetz 1983 gemacht hat.

Das Bundesverfassungsgericht hat es im September 1987 in einer Reihe von Beschlüssen abgelehnt, Verfassungsbeschwerden gegen das Volkszählungsgesetz 1987 zur Entscheidung anzunehmen, weil sie keine Aussicht auf Erfolg hätten[1]. Dabei hat es erstmals zu erkennen gegeben, daß es die auch in der Öffentlichkeit erhobenen verfassungsrechtlichen Bedenken gegen das Volkszählungsgesetz für unbegründet hält. Besondere Bedeutung messe ich dem erneuten Hinweis des Bundesverfassungsgerichts bei, daß es Aufgabe der unabhängigen Datenschutzbeauftragten und - auf Anrufung durch den Betroffenen hin - der Verwaltungsgerichte ist, dem Bürger im Einzelfall Rechtsschutz gegen unzulässige Maßnahmen bei der Durchführung der Volkszählung zu gewähren.

Die zitierten Entscheidungen enthalten auch eine Reihe von Hinweisen zur grundrechtssichernden Funktion bestimmter Detailregelungen bei der Erhebung und Aufbereitung der Volkszählungsdaten, die für meine Kontrolltätigkeit Bedeutung haben. So betont das Bundesverfassungsgericht die Bedeutung interner organisatorischer Maßnahmen in den Statistikämtern zur Gewährleistung der Datensicherheit, zur Trennung und Löschung der Hilfsmerkmale sowie zur Vernichtung der Erhebungsunterlagen zum frühestmöglichen Zeitpunkt. Zwar sind diese Entscheidungen im Verfahren der Vorprüfung von Verfassungsbeschwerden ergangen und nicht mit Entscheidungen eines Senats des Bundesverfassungsgerichts gleichzusetzen; dennoch geben sie Anhaltspunkte dafür, welche Rechtsauffassung das Gericht bei einer Entscheidung in der Sache vertreten würde.

Mehrere Bürger äußerten die Sorge, daß der Datenschutz bei der Volkszählung durch das Zugriffsrecht der *alliierten Behörden* gefährdet sei. Nach Ziff. VIII der Erklärung der Alliierten Kommandantur über Berlin vom 5. Mai 1955 haben die alliierten Behörden zur Erfüllung ihrer aufgrund dieser Erklärung erwachsenen Verpflichtungen das Recht, die von ihnen für notwendig erachteten Auskünfte und Statistiken anzufordern und zu erlangen. Ich habe hierzu die Auffassung vertreten, daß dieser besatzungsrechtliche Auskunftsanspruch keinen Einfluß auf die Rechtmäßigkeit der Volkszählung in Berlin nach innerstaatlichem Recht hat. Zudem haben die alliierten Behörden versichert, sie würden auf Einzeldaten aus der Volkszählung 1987 nicht zugreifen. Dies leuchtet auch aus praktischen Gründen ein, weil die Volkszählungsdaten stichtagsbezogen erhoben worden sind und daher schnell veralten. Falls alliierte Behörden zur Wahrung ihrer Sicherheitsbelange (z. B. Einstellung von Wachpersonal am Flughafen Tegel) Informationen benötigen, sind sie auf aktuellere und vor allem weitergehende Informationen angewiesen, als sie bei der Volkszählung erhoben worden sind. Inzwischen kam das *Oberverwaltungsgericht Berlin* zum gleichen Ergebnis[1].

Erhebungsunterlagen

Auf Unverständnis stieß es bei Bürgern, daß der *Bogen für die Gebäudevorerhebung* neben den Erhebungsmerkmalen auch die von den Grundsteuerstellen übermittelten Adreßdaten der Gebäudeeigentümer enthielt. Ich habe gegen die Gestaltung des Gebäudevorerhebungsbogens keine rechtlichen Einwände erhoben, da dieser nicht maschinenlesbar ist und unmittelbar nach Abschluß der Eingangskontrollen im Statistischen Landesamt - also früher als die übrigen Erhebungsunterlagen - vernichtet wird. Diese Auffassung ist vom Bundesverfassungsgericht bestätigt worden. Ich hätte es gleichwohl begrüßt, wenn der Erhebungsbogen für die Gebäudezählung ebenso gestaltet worden wäre wie die Erhebungsunterlagen für die Haupterhebung, um dem Grundsatz der Trennbarkeit von Name und Anschrift einerseits und Erhebungsmerkmalen andererseits konsequent Rechnung zu tragen.

Zahlreiche Beschwerden richteten sich gegen die *Frage 12* („Bitte Name und Anschrift Ihrer Arbeitsstätte oder Schule/Hochschule angeben") des *Personenbogens.* Das Volkszählungsgesetz unterscheidet zwischen dem Namen der Arbeits- oder Ausbildungsstätte, der lediglich Hilfsmerkmal ist und nicht elektronisch gespeichert werden darf, und der vollständigen Anschrift, die das Gesetz als Erhebungsmerkmal einstuft. Bezüglich des Hilfsmerkmals „Name der Arbeits- oder Ausbildungsstätte" hat das Bundesverfassungsgericht im September 1987 indirekt Kritik an der Gestaltung des Personenbogens geübt. Das Gericht hat insbesondere Bedenken gegen den Verzicht auf eine mög-

[1] BVerfG 1 BvR 970/87, Neue Juristische Wochenschrift 1987, S. 2805; 1 BvR 782/87; 1 BvR 936/87; 1 BvR 1063/87; 1 BvR 1122/87; 1 BvR 1148/87

[1] Beschluß vom 16. Oktober 1987 (OVG 8 S 366. 87)

lichst frühzeitige Abtrennung des Hilfsmerkmales „Name der Arbeits- oder Ausbildungsstätte" jedenfalls in den Fällen geltendgemacht, in denen - bei selbständig Tätigen - der Name des Auskunftspflichtigen in dem seiner Beschäftigungsstelle enthalten ist. Dabei hat das Gericht hervorgehoben, daß die Gestaltung des Personenbogens den verfassungsrechtlichen Trennungsanforderungen zu folgen hat.

Neben dem Namen, der nicht automatisiert gespeichert werden darf, wird auch die Anschrift der Arbeits- und Ausbildungsstätte erhoben. In den Fällen, in denen Auskunftspflichtige auf ihrem Wohngrundstück unter ihrem Namen einer Erwerbstätigkeit nachgehen, ergibt sich im Zusammenhang mit der Antwort auf die *Frage 14* („Zeit für Hinweg zur Arbeit entfällt, da auf gleichem Grundstück"), daß die Anschrift der Arbeitsstätte zugleich die Wohnadresse des Auskunftspflichtigen ist. Ein Verbot der Übernahme auf Datenträger enthält das Volkszählungsgesetz zwar für den Namen, nicht aber für die Anschrift der Arbeitsstätte. Wenn die Arbeitsstättenanschrift auch bei solchen Personen, die keinen Weg zur Arbeitsstätte zurückzulegen haben (Nicht-Pendler) automatisiert gespeichert würde, so liefe dies den Vorkehrungen gegen eine leichte Deanonymisierung direkt zuwider, die das Bundesverfassungsgericht auch für den internen Bereich der amtlichen Statistik gefordert hat. Das Volkszählungsgesetz 1987 sieht in der Anschrift der Arbeitsstätte ein Erhebungsmerkmal, in der Wohnanschrift dagegen ein Hilfsmerkmal. Wenn beide zusammenfallen, führt eine verfassungskonforme Auslegung des Gesetzes zu dem Ergebnis, daß die Anschrift der Arbeitsstätte von Nicht-Pendlern nur als Hilfsmerkmal behandelt und deshalb nicht gespeichert wird. Dementsprechend ist im Signierfeld des Personenbogens nur die Verschlüsselung der Arbeitsstättenadressen von Pendlern vorgesehen. Es wäre konsequent gewesen, bei der Gestaltung des Personenbogens bereits die Frage nach der Anschrift der Arbeitsstätte oder Schule/Hochschule auf Pendler zu beschränken. Dies gilt umso mehr, als nur Pendler Verkehrsströme verursachen, die mit Hilfe der Fragen 12 und 14 statistisch dargestellt werden sollen.

Während das Gesetz nur die Erhebung der Hauptfachrichtung des zeitlich *letzten* Ausbildungsabschlusses zuläßt, beharrte das Statistische Bundesamt auf seinem Standpunkt, daß - wie in *Frage 10 b)* des Personenbogens geschehen - die Fachrichtung des *höchsten* Abschlusses erfragt werden durfte. Eine rechtmäßige Durchführung der Volkszählung läßt sich in diesem Punkt nur dadurch sicherstellen, daß auf eine Verfolgung von Auskunftspflichtigen, die insoweit fehlerhaft oder überhaupt nicht geantwortet haben, verzichtet wird. Dies hat mir das Statistische Landesamt zugesichert.

Auch die Erläuterungen zu einzelnen Fragen im Haushaltsmantelbogen waren teilweise irreführend. So soll auf die *Frage 17* des Personenbogens möglichst die genaue Bezeichnung der gegenwärtig ausgeübten Tätigkeit angegeben werden. Unter anderem war dazu im *Haushaltsmantelbogen* das Beispiel „Postsekretär (nicht Beamter)" genannt. Richtig ist, daß in Frage 17 eine differenziertere Tätigkeitsbeschreibung verlangt wird als z. B. in Frage 15 („Sind Sie z. Z. tätig als . . .?"), wo eine mögliche Antwort „Beamter/Beamtin" lautet. Dagegen hat die tatsächlich ausgeübte Tätigkeit nichts mit der Dienstbezeichnung des Beamten zu tun, der sie daher auf dem Personenbogen nicht anzugeben braucht. Ich habe das Statistische Landesamt gebeten, die örtlichen Erhebungsstellen darauf hinzuweisen und selbst bei Nacherhebungen entsprechend zu verfahren.

Bei der Frage, *wann* die Auskunftspflicht erfüllt ist, unterscheidet das Volkszählungsgesetz zwischen der mündlichen Beantwortung gegenüber dem Zähler, der Übergabe ausgefüllter Erhebungsbogen an den Zähler sowie der Abgabe beim Volkszählungsamt einerseits und der *postalischen Rücksendung* andererseits. Mit der Beantwortung gegenüber dem Zähler oder der Abgabe bei der örtlichen Erhebungsstelle erlischt die Auskunftspflicht. Soweit also dem Zähler Erhebungsunterlagen abhandenkommen, sind die betroffenen Auskunftspflichtigen nicht zur erneuten Ausfüllung der Erhebungsunterlagen verpflichtet. Sie können darum nur auf freiwilliger Basis gebeten werden. Demgegenüber trägt der Bürger, der seine Erhebungsunterlagen per Post zurückschickt, das Risiko des Verlustes bei der Beförderung auf dem Postweg. Daß dieses Risiko nicht zu vernachlässigen ist, zeigten mir zahlreiche Fehlzustellungen durch die Deutsche Bundespost. Der Bürger ist also zum erneuten Ausfüllen der Bogen verpflichtet, wenn das Amt für Volkszählung ihm erklärt, es habe seinen Bogen nicht erhalten oder sie seien nicht auffindbar. Diese gesetzliche Regelung stieß bei vielen Bürgern auf Unverständnis. Durch sie wird die Wahrnehmung des Rechts auf postalische Rücksendung in unzumutbarer Weise erschwert.

Zur *Vernichtung der Erhebungsbogen* hat das Bundesverfassungsgericht die Pflicht der Statistikämter betont, für jede der Erhebungsunterlagen den jeweils frühestmöglichen Zeitpunkt zu ermitteln und die Vernichtung zu diesem Zeitpunkt vorzunehmen. Eine Aufbewahrung aller Erhebungsunterlagen bis zur Feststellung der amtlichen Bevölkerungszahl wäre dagegen rechtswidrig. Die Erhebungsunterlagen sollten deshalb sukzessiv (z. B. bezirksweise) zum jeweils frühestmöglichen Zeitpunkt vernichtet werden.

Ergebniskontrolle

Im November fand in Berlin in 25 Zählbezirken die *Wiederholungsbefragung zur Volkszählung 1987* statt, die das Gesetz zur Prüfung der Zuverlässigkeit der Ergebnisse vorsieht. Dabei wurden ein Haushaltsmantelbogen und ein Personenbogen mit einem eingeschränkten Fragenkatalog verwandt. Ursprünglich hatten das Statistische Bundesamt und das Statistische Landesamt die Absicht, die vollständigen Antwortdatensätze eines Auskunftspflichtigen in der Haupterhebung und in der Wiederholungsbefragung auf individueller Ebene miteinander zu verknüpfen. Dies sollte jedoch erst nach Abschluß der Aufbereitung der gesamten Daten aus der Haupterhebung, also nicht vor Ende 1988, geschehen.

Hiergegen haben mehrere Datenschutzbeauftragte Einwände erhoben. Diese stützten sich insbesondere auf die Formulierung im Volkszählungsgesetz, wonach nur die Zuverlässigkeit der „Ergebnisse", nicht aber von einzelnen Antworten, in der Wiederholungsbefragung geprüft werden dürfe. Auch sei es nicht hinnehmbar, daß die bei der Wiederholungsbefragung erhobenen Daten bis zum Abschluß der Aufbereitung der Haupterhebung unausgewertet vorgehalten würden. Demgegenüber hat die amtliche Statistik betont, eine Überprüfung der Zuverlässigkeit der Ergebnisse sei ohne einen Vergleich auf Individualdatenbasis nicht möglich.

Es ist schließlich Übereinstimmung dahingehend erzielt worden, daß eine Verknüpfung der Datensätze einer Person, die die Erhebungsbogen sowohl bei der Haupterhebung als auch bei der Wiederholungsbefragung ausgefüllt hat, nur unter bestimmten Voraussetzungen zulässig ist. Die Auswertung der Wiederholungsbefragung muß unverzüglich nach deren Abschluß, also vor Abschluß der Auswertung der Haupterhebung stattfinden. Es wird ein anonymisierter Datensatz aus den Antworten auf die gleichlautenden Fragen in der Haupt- und der Wiederholungsbefragung sowie vier weiteren Antworten auf dem Personenbogen der Haupterhebung erstellt. Sobald diese Verknüpfung erfolgt ist, sind alle Daten, mit deren Hilfe ein Personenbezug hergestellt werden könnte, zu löschen. Als Regionalangaben dürfen im Datensatz der Wiederholungsbefragung nur das Bundesland, die Gemeindegrößenklasse und der Gemeindetyp gespeichert werden.

Wesentlich ist die Zusicherung gegenüber dem Befragten, daß ihm bei Abweichungen zwischen den Antworten in der Wiederholungsbefragung und der Haupterhebung keine Sanktionen drohen.

Zur Kontrolle der Zuverlässigkeit der Volkszählungsergebnisse war von den Statistikbehörden ursprünglich auch ein *individueller Abgleich* zwischen den Antworten im parallelen *Mikrozensus 1987* und in der Volkszählung vorgesehen worden. Ich habe in Übereinstimmung mit dem Bundesbeauftragten für den Datenschutz die Auffassung vertreten, daß das Reidentifizierungsverbot im Volkszählungsgesetz einem solchen Individualdatenabgleich entgegensteht. Das Statistische Landesamt kann allenfalls einen Vergleich der Mikrozensus- und Volkszählungsergebnisse ohne Personenbezug durchführen.

Durchsetzung der Auskunftspflicht

Besonders aufmerksam verfolge ich den Umgang der Ämter für Volkszählung mit den Daten derjenigen Personen, die auch nach Erlaß eines *förmlichen Heranziehungsbescheides* keine Volkszählungsbogen ausgefüllt haben. Diese Daten werden mit den Erhebungsunterlagen der abgeschlossenen Zählbezirke dem Statistischen Landesamt übergeben. Sie sind deshalb besonders sensibel, weil die Betroffenen vorschnell mit „Verweigerern" gleichgestellt werden können, obwohl die Gründe für die Nichtbeantwortung ungeklärt sind. Hier wirken sich z. B. Fehler des Melderegisters aus. So kann es sich unter Umständen um Daten verstorbener oder verzogener Bürger handeln, wenn die Zähler und Mitarbeiter der Erhebungsstelle dies nicht vor Abschluß des Zählbezirks festgestellt haben. Aber auch soweit Daten von Personen enthalten sind, die tatsächlich ihrer Auskunftspflicht nicht genügen wollen, muß mit diesen Daten so verfahren werden, daß das informationelle Selbstbestimmungsrecht der Betroffenen gewahrt bleibt. Der Datenschutz bei der Volkszählung ist nicht auf Personen beschränkt, die ihrer Auskunftspflicht nachgekommen sind.

Die Frage, welche Daten aus *Ordnungswidrigkeitenanzeigen* wegen des Aufrufs zum Boykott der Volkszählung dem Polizeilichen Staatsschutz zur Erstellung eines Lagebildes übermittelt werden dürfen, wird unter 5.3 behandelt.

Um die strikte Trennung zwischen Statistik und Verwaltungsvollzug auch in dieser Phase aufrechtzuerhalten, hat mir der Senator für Inneres zugesichert, daß das Statistische Landesamt bei der Einleitung von Bußgeldverfahren gegen Auskunftspflichtige, die nach dem Stichtag umgezogen sind, von Melderegisteranfragen absehen wird. Dies muß auch für die von den Bezirken eingeleiteten Zwangsgeldverfahren gelten.

Bisher ist noch offen, ob das Statistische Landesamt überhaupt *Bußgeldverfahren* wegen Auskunftsverweigerung bei der Volkszählung einleiten wird. Gegenwärtig betreiben auf Anweisung des Senators für Inneres nur die bezirklichen Volkszählungsämter Zwangsgeldverfahren.

2.2 Organisation der Volkszählung in Berlin

Abschottung

Vor Beginn der Erhebung habe ich die örtlichen Erhebungsstellen, die *Ämter für Volkszählung* in den Bezirken, aufgesucht und Hinweise zur Verbesserung des Datenschutzes bei der konkreten Organisation des jeweiligen Amtes gegeben. Inzwischen habe ich jedes Volkszählungsamt von Amts wegen mindestens viermal, davon nach dem Stichtag zweimal unangekündigt, überprüft. In einem Fall ist auf meine Empfehlung hin ein Amt für Volkszählung in einem anderen Gebäude untergebracht worden, weil in den zunächst bezogenen Räumlichkeiten die Abschottung nicht hinreichend gewährleistet war.

Insgesamt habe ich festgestellt, daß mit erheblichem finanziellem Aufwand ein hoher Standard an räumlicher, organisatorischer und personeller Abschottung erreicht worden war. Ich halte dies deshalb für bedeutsam, weil hier Maßstäbe gesetzt worden sind, die nicht auf die Volkszählung beschränkt bleiben dürfen. Zwar hat der Gesetzgeber im Anschluß an die Rechtsprechung des Bundesverfassungsgerichts gerade für die Volkszählung strikte Anforderungen formuliert, der Grundsatz der Zweckbindung personenbezogener Angaben gilt jedoch nicht nur im Verhältnis zwischen Statistik und Verwaltungsvollzug, sondern auch innerhalb des Verwaltungsvollzuges. Es gibt eine ganze Reihe von Bereichen öffentlicher Verwaltung, in denen die Zweckentfremdung zwangsweise erhobener Daten zu sehr viel gravierenderen Eingriffen in das informationelle Selbstbestimmungsrecht des Bürgers führen kann als bei der Volkszählung. Soweit aus diesem Grund Abschottungsmaßnahmen erforderlich sind, wird nach den - insoweit positiven - Erfahrungen bei den bezirklichen Ämtern für Volkszählung der Einwand der Undurchführbarkeit in Zukunft nicht mehr verfangen.

PC-Einsatz

Für die Kontrolle des Rücklaufs der Erhebungsbogen für das Mahn- und Aufforderungsverfahren sowie für das Zwangsgeldverfahren und zur Vorbereitung eines Bußgeldverfahrens nach dem Bundesstatistikgesetz haben die Ämter für Volkszählung der Bezirke *Einplatz-Personalcomputer (PC)* eingesetzt. Bereits im letzten Jahresbericht hatte ich die Voraussetzungen genannt, unter denen ich keine Einwände gegen den Einsatz solcher Rechner erheben würde:

- sorgfältige Beachtung aller Vorschriften über die Datenverarbeitung sowie meiner Grundsätze für organisatorische und technische Maßnahmen zum Datenschutz beim Einsatz von Personalcomputern[1];
- Aufklärung des Bürgers über die Datenverarbeitung bei den örtlichen Erhebungsstellen;
- keine Speicherung von Daten, die im Rahmen der Volkszählung beim Bürger erhoben wurden;
- ausschließlich dezentrale Datenverarbeitung der Daten der Auskunftspflichtigen bei der Rücklaufkontrolle.

Das Statistische Landesamt hat sich bemüht, meine Zweifel auszuräumen, daß die zur Verfügung stehende Zeit für eine sorgfältige Vorbereitung des PC-Einsatzes ausreicht. Die beiden letztgenannten Voraussetzungen sind ohne Einschränkung erfüllt worden; die Bürger wurden sehr früh durch die Presse über die Absicht des Statistischen Landesamtes informiert. Vom Statistischen Landesamt wurde eine Unterlage erstellt, mit der jeder Bürger sich sehr detailliert über den PC-Einsatz informieren konnte.

Die technisch-organisatorischen Anforderungen sind in die „Richtlinien für die Tätigkeit an den Personalcomputern in den Ämtern für Volkszählung *(PC-Richtlinien)*" des Senators für Inneres eingeflossen[2]. Sie betrafen im wesentlichen die

- Festlegung der Anwendungsbereiche für die Personalcomputer;
- Datensicherung und Datenschutz, dabei insbesondere Festlegung der internen Verantwortungsbereiche für die Anwendung der PC's, Verwendung eines Sicherheitssystems für die Speicher-, Benutzer- und Zugriffskontrolle, Umgang mit beweglichen Datenträgern, Anfertigung von Sicherungskopien, Sicherstellung der Eingabekontrolle;
- Durchführung der Datenverarbeitung, dabei insbesondere Vorgänge bei der Rücklaufkontrolle, Umgang mit den Daten von Bürgern nach vermerktem Rücklauf, Löschung der Zähler- und Bürgerdaten.

Strittig war vor allem die Fortsetzung der Speicherung der aus dem Melderegister stammenden Daten für die Rücklaufkontrolle nach dem Eingeben des ordnungsgemäßen Rücklaufs des ausgefüllten Fragebogens in einer sogenannten *„Hintergrunddatei"*, zunächst so genannt, weil die Daten mit der Markierung des ordnungsgemäßen Rücklaufs nur noch besonders privilegierten Mitarbeitern zugänglich sein sollten. Der Senator für Inneres und das Statistische Landesamt hielten dies für erforderlich, um Doppelabgeber erkennen zu können und um bei irrtümlichen Eintragungen die Daten der Bürger, die noch nicht abgegeben haben, wieder korrigieren zu können. Meine Bedenken beruhten auf der Tatsache, daß bei Zusammenführung aller „Hintergrunddateien" zumindest für wenige, aber wichtige Merkmale ein aktualisierter und korrigierter Einwohnerdatenbestand entstehen würde, der den verfassungswidrigen Abgleich mit dem als fehlerhaft erkannten bestehenden Melderegister geradezu herausfordern würde. Meine Bedenken wurden mit dem Kompromiß ausgeräumt, daß mit der Abschlußbearbeitung eines Zählbezirks in der Erhebungsstelle gleichzeitig mit dem Ausdruck der Restliste für die Durchführung des Bußgeldverfahrens im Statistischen Landesamt die Hintergrunddatei für diesen Zählbezirk physisch gelöscht wird.

Um die PC's auch zur Durchführung des *Zwangsgeldverfahrens* nach Abschluß der einzelnen Zählbezirke einsetzen zu können, hat der Senator für Inneres die PC-Richtlinien geändert. Vor der

[1] Vgl. meine Broschüre „Isolierte Rechner, Personalcomputer - Grundsätze zum Datenschutz"

[2] PC-Richtlinien vom 23. April 1987, veröffentlicht im Amtsblatt von Berlin vom 8. Mai 1987, S. 649, geändert durch Verwaltungsvorschriften vom 26. Mai 1987 (Amtsblatt vom 5. Juni 1987, S. 767) sowie vom 11. November 1987 (Amtsblatt vom 20. November 1987, S. 1670).

Löschung der vollständigen Personendatei des abgeschlossenen Zählbezirks werden die für das Zwangsgeld- und Widerspruchsverfahren erforderlichen Daten der noch auskunftspflichtigen Personen in einer neuen Datei auf dem Rücklaufkontroll-PC gespeichert. Diese Datensätze werden nach Abschluß der Arbeiten am PC unverzüglich - spätestens am 30. Juni 1988 - gelöscht. Beim Einsatz der PC's im parallelen Zwangsgeld- und Widerspruchsverfahren ist sicherzustellen, daß Mitarbeiter des Statistischen Landesamtes, die zur technischen Unterstützung der Widerspruchsbearbeitung tätig werden können, nur auf Daten des Widerspruchsverfahrens und nicht des Zwangsgeldverfahrens zugreifen können. Das Zwangsgeldverfahren liegt in der ausschließlichen Zuständigkeit der bezirklichen Erhebungsstellen.

Großrechnereinsatz

Ursprünglich bestand die Absicht, die zentrale Verarbeitung der bei der Volkszählung erhobenen Daten beim Landesamt für Elektronische Datenverarbeitung (LED) durchzuführen. Dies wäre, wie im letzten Jahresbericht ausgeführt, unter den geplanten Bedingungen möglich gewesen.

Dennoch hat sich der Senator für Inneres für die Beschaffung eines der Verarbeitung der Volkszählungsdaten gewidmeten, von anderen Rechnern in der Verwaltung isolierten Systems in einem neuen, vom Statistischen Landesamt betriebenen *Rechenzentrum* entschieden. Dieses soll zur Akzeptanz beitragen. Überdies können die bei der ursprünglichen Lösung befürchteten Kapazitätsengpässe vermieden werden. Trotz dieser rigorosen und demonstrativen Abschottungsmaßnahmen muß beachtet werden, daß das Landesamt für Elektronische Datenverarbeitung und damit das „Vier-Augen-Prinzip", also die korrigierende Wirkung einer zweiten Instanz, ausgeschaltet wurde, und mit dem Statistischen Landesamt eine Behörde ein Großrechenzentrum zu betreiben begann, welche noch keine hinreichenden Erfahrungen aufweisen konnte.

Bei einer ersten Besichtigung habe ich dann auch festgestellt, daß bei der *baulichen Konzeption* des Rechenzentrums Grundregeln für die Abgangskontrolle unbeachtet blieben, was nach Aussagen des Statistischen Landesamtes mit organisatorischen Maßnahmen bei den Produktionsabläufen im Rechenzentrum ausgeglichen werden soll.

Andererseits bietet die Neueinrichtung des Rechenzentrums des Statistischen Landesamtes die Möglichkeit, die technischen und organisatorischen Rahmenbedingungen für die Verarbeitung von statistischen Daten von Grund auf neu zu überdenken. Es bestehen keine Meinungsverschiedenheiten darüber, daß die aus Erhebungen wie der Volkszählung oder den Mikrozensen gewonnenen Einzelangaben für die Primärstatistiken und die aus den Verwaltungsregistern gewonnenen Daten der Sekundärstatistiken (Mikrodaten) personenbezogen sind und somit neben dem Statistikgeheimnis auch dem Datenschutz unterliegen. Dies bedeutet, daß das Statistische Landesamt Mikrodaten oder auch nicht ausreichend aggregierte Mikrodaten nicht nur nicht nach außen geben darf, sondern auch nach innen eine *differenzierte Zugriffskontrolle* einsetzen muß. Daraus folgt im einzelnen:

- Mitarbeiter des Statistischen Landesamtes sollen nur im Rahmen ihres Auftrages zur Durchführung einer bestimmten statistischen Auswertung Zugriff auf Mikrodatenbestände haben. Dieser Zugriff darf nur durch den Abruf von Programmen erfolgen, die mit diesen Daten arbeiten. Eine unmittelbare Darstellung der Mikrodaten auf dem Bildschirm oder durch Ausdruck ist für die statistische Auswertung auf validierten Datenbeständen unnötig, daher unzulässig und durch technische Abschottungen zu verhindern.
- Der so beschränkte Zugriff auf Mikrodaten ist automatisch so zu protokollieren, daß nachvollziehbar ist, wer wann von welchem Terminal aus unter Anwendung welcher Programme, Transaktionen oder Kommandos auf welche Mikrodatenbestände zugegriffen hat.
- Der zur Validierung, zur Vervollständigung oder Korrektur erforderliche Direktzugriff auf Mikrodaten ist organisatorisch, personell und zeitlich von der Verwendung der Daten zu statistischen Zwecken zu trennen.

Diese Anforderungen setzen voraus, daß die eingesetzte fortschrittliche Datenschutzsoftware mit der notwendigen Flexibilität administriert, der dabei angebotene Protokollierungsumfang den Anforderungen angepaßt und eine zusätzliche Zugriffsdifferenzierung auf der Datenbankebene eingerichtet wird.

Hintergrund dieser strengen und keineswegs auf die Volkszählungsdaten beschränkten Anforderungen ist auch, daß im Vorfeld der Volkszählung öffentlich Zweifel an der vollständigen *Anonymität* der Volkszählungsdaten geäußert wurden, was allerdings keinen Fachmann überraschte und vom Bundesverfassungsgericht auch so nicht verlangt wurde. Die von einem Hamburger Hochschullehrer öffentlich befürchtete Deanonymisierung von Mikrodaten aus der Volkszählung unter Anwendung von relationalen Datenbanksystemen ist zwar rechtswidrig, aber keineswegs technisch ausgeschlossen, zumal - entgegen der Aussagen eines vom Statistischen Bundesamtes verbreiteten Gutachtens eines Münchener Hochschullehrers - die Mikrodaten zumindest beim Berliner Statistischen Landesamt sehr wohl mit einer relationalen Datenbank verwaltet werden.

Es ist daher Voraussetzung für das Vertrauen in die amtliche Statistik, die ihre Rolle als statistische Dienstleistung für öffentliche und private Zwecke erweitern will, daß der Einsatz modernster Informationstechnik vom Einsatz wirkungsvoller - auch interner - Abschottungsmaßnahmen flankiert wird.

2.3 Durchführung

Gebäudevorerhebung

Bereits im Vorfeld der *Gebäudevorerhebung* mußte ich gegenüber dem Senator für Finanzen einen Verstoß gegen das Volkszählungsgesetz und das Steuergeheimnis beanstanden. Obwohl seit dem Inkrafttreten des Volkszählungsgesetzes 1987 vom 8. November 1985 bekannt war, daß die Oberfinanzdirektion dem Statistischen Landesamt ausschließlich Vor- und Familiennamen oder Bezeichnung sowie Straße, Hausnummer der Eigentümer und Verwalter der zu erhebenden Gebäude und Unterkünfte mitteilen durfte, übermittelte die Oberfinanzdirektion pauschal darüber hinaus auch *Namen und Anschriften von Steuerbevollmächtigten* der Gebäudeeigentümer, ohne im Einzelfall zu prüfen, ob die Steuerbevollmächtigten - was nur z. T. der Fall war - gleichzeitig Gebäudeverwalter waren. Dabei wurde ungeprüft ein Verfahren der Datenübermittlung aus den Grundsteuerstellen angewandt, das bereits bei der Volkszählung 1983 praktiziert worden war. Nach dem Volkszählungsurteil des Bundesverfassungsgerichts von 1983 konnte und kann keine öffentliche Stelle, die mit der Vorbereitung und Durchführung der Volkszählung 1987 befaßt ist, Organisationsformen und Verfahren der Datenverarbeitung übernehmen, die bereits für die Volkszählung 1983 vorgesehen waren. Ich habe es deshalb gegenüber dem Senator für Finanzen als besonders mißlich und der Akzeptanz der Volkszählung abträglich bezeichnet, daß schon die erste Datenübermittlung im Rahmen der Volkszählung 1987 mit einem derart gravierenden Mangel behaftet war.

Zählerbenennung

Eine vergleichbare Datenübermittlung, die den gesetzlich zugelassenen Datenumfang überschritt, mußte ich im Zuge der Zählerbenennung bei einem Bezirksamt beanstanden. Dieses hatte dem Statistischen Landesamt eine *vollständige Liste* mit allen gegenwärtigen und teilweise sogar ehemaligen Mitarbeitern übermittelt. Dieses Vorgehen war mit dem Volkszählungsgesetz nicht vereinbar, das zum einen nur die Benennung gegenwärtiger Bediensteter zuläßt und zum anderen von der Dienstbehörde eine Auswahlentscheidung verlangt, wenn - wie dies in Berlin der Fall war - die überörtliche Erhebungsstelle die Benennung einer bestimmten Quote von Bediensteten verlangt.

Nicht mit dem Volkszählungsgesetz im Einklang stand auch das Vorgehen einer Hochschule, die dem Statistischen Landesamt einen Privatdozenten für die Zählertätigkeit benannt hatte, obwohl dieser nicht in einem Beamtenverhältnis, sondern in einem korporationsrechtlichen Verhältnis zu dieser Hochschule stand und hauptberuflich bei einem privaten Forschungsinstitut arbeitete.

Da sich nicht genügend öffentliche Bedienstete freiwillig meldeten, mußten die örtlichen Erhebungsstellen in größerem Umfang Verpflichtungen zur Übernahme des Zähleramtes vornehmen. In diesem Zusammenhang stellte sich aus datenschutzrechtlicher Sicht die Frage, ob Informationen über Rechtsbehelfe öffentlicher Bediensteter gegen ihre Verpflichtung oder über deren Verhalten als Zähler an ihre Dienstbehörde weitergegeben werden dürfen. Ich teile die Auffassung des Senators für Inneres, daß die gesetzliche Pflicht zur Übernahme der Zählertätigkeit keine spezifische Dienstpflicht, sondern eine allgemeine Bürgerpflicht ist. Solange das Verhalten eines zur Zählertätigkeit verpflichteten öffentlichen Bediensteten nicht disziplinarrechtlich zu ahnden ist, dürfen deshalb keine Informationen über Widersprüche eines öffentlichen Bediensteten gegen seine Verpflichtung an die Dienstbehörde weitergegeben oder zur *Personalakte* genommen werden.

Zählereinsatz

Das Volkszählungsgesetz verpflichtet jeden Zähler, sich gegenüber den Auskunftspflichtigen auszuweisen. Bundeseinheitlich wurde hierfür ein *Zählerausweis* an die Zähler verteilt, der neben dem Namen auch die Anschrift des Zählers enthielt und nur im Zusammenhang mit dem amtlichen Personalausweis gültig war. Da es bereits vor dem Stichtag zu Drohungen und gewalttätigen Übergriffen gegenüber Zählern gekommen war, wandten sich viele Zähler an mich mit der Frage, ob sie zur Offenbarung ihrer Anschrift auf dem Zählerausweis verpflichtet seien. Zwar war die Pflicht zur Bekanntgabe der Zähleradresse gesetzlich nicht vorgesehen, sie sollte jedoch dem auskunftspflichtigen Bürger die Überprüfung ermöglichen, ob der Zähler in seiner Nachbarschaft wohnte und damit nicht hätte eingesetzt werden dürfen. Das Statistische Landesamt hat auf meinen Vorschlag hin ein praktikables und datenschutzgerechtes Verfahren bei denjenigen Zählern gewählt, die Repressalien befürchteten.

Der Grundsatz, daß ein Zähler nicht in unmittelbarer Nähe seiner Wohnung *(Nachbarschaft)* eingesetzt werden darf, hat nach der Rechtsprechung des Bundesverfassungsgerichts bei amtlichen Erhebungen mit Auskunftspflicht eine grundrechtssichernde Funktion. Der Begriff „Nachbarschaft" wurde in Berlin durch die Ausführungsvorschriften zum Volkszählungsgesetz 1987 dahingehend konkretisiert, daß ein Zähler nicht in dem Wohnblock, zu dem seine Wohnung gehört, oder in den an diesen unmittelbar angrenzenden Wohnblöcken eingesetzt werden darf. Darin habe ich eine für die Großstadtsituation vertretbare Präzisierung des Nachbarschaftsbegriffs gesehen. Es war auch nicht auf Mängel dieser Regelung zurückzuführen, daß sich zahlreiche Bürger während der Haupterhebung an mich wandten, weil sie der Meinung waren, sie sollten von einem Zähler aus ihrer Nachbarschaft gezählt werden. Ein Großteil dieser Beschwerden war unbegründet und beruhte auf unzureichender Information des Bürgers über den Inhalt der Berliner Nachbarschaftsregelung. In den übrigen Fällen hätten die Zähler in bestimmten Wohnblöcken allerdings nicht eingesetzt werden dürfen. Auf meinen Hinweis wurden die betreffenden Zähler ausgetauscht, soweit diese ihre Zählertätigkeit nicht schon abgeschlossen hatten. Nur in einem Fall lehnte ein Amt für Volkszählung den Austausch des in der Nachbarschaft wohnenden Zählers ab und verwies den Bürger auf die Rückgabemöglichkeit per Post. Dies war ein datenschutzrechtlicher Mangel, weil das Verbot des Zählereinsatzes in der Nachbarschaft nach der Rechtsprechung des Bundesverfassungsgerichts neben, und nicht an Stelle der brieflichen Beantwortungsmöglichkeit steht.

Bei einer anderen örtlichen Erhebungsstelle habe ich beanstandet, daß das Verbot des Zählereinsatzes in der Nachbarschaft in mehreren Fällen nicht beachtet worden ist. Dies war zum Teil darauf zurückzuführen, daß Zählerkoffer, die im Anschluß an die Zählerschulungen ausgegeben wurden, nicht abgeholt worden waren und vom Volkszählungsamt umgehend an Ersatzzähler ausgegeben wurden, ohne daß in allen Fällen sorgfältig geprüft worden wäre, ob der Einsatz des Ersatzzählers im Zählbezirk zulässig war. Zum Teil wurden Zähler in ihrer Nachbarschaft eingesetzt, weil der Begriff der „Nachbarschaft" fehlerhaft ausgelegt wurde.

In mehreren Fällen beschwerten sich Auskunftspflichtige darüber, daß die Zähler es abgelehnt hätten, ihnen offizielle *Rückantwortumschläge* auszuhändigen. Teils wurde dies mit der höheren Entschädigung für solche Erhebungsbögen begründet, die den Zählern direkt ausgehändigt werden, teils waren zunächst zu wenig Rückantwortumschläge gedruckt worden, weil die Zahl der Bürger unterschätzt wurde, die ihre Bögen per Post zurückschikken wollten.

Das Bundesverfassungsgericht hat dem Wahlrecht des Auskunftspflichtigen bei der Volkszählung zwischen einer offenen Beantwortung der Fragen gegenüber dem Zähler einerseits und der schriftlichen Beantwortung und Rücksendung der Erhebungsunterlagen per Post grundrechtssichernde Bedeutung beigemessen. Dies hätte den Zählern bei den Schulungen stärker verdeutlicht werden müssen. Ich begrüße es, daß die Deutsche Bundespost sich bereiterklärt hat, auch normale DIN-A 4-Umschläge, die an die Ämter für Volkszählung gerichtet wurden, portofrei zu befördern. Über diese Möglichkeit hätten Zähler und Mitarbeiter der Erhebungsstellen die Auskunftspflichtigen gerade dann informieren müssen, wenn zu wenig offizielle Rückantwortumschläge vorhanden waren.

Dem Recht auf *postalische Rücksendung* der Erhebungsbögen entspricht es nicht, wenn der Bundesminister des Innern und Vertreter der amtlichen Statistik Presseberichten zufolge die angeblich inhaltlich schlechte Qualität der ausgefüllten Erhebungsbogen auf die Wahrnehmung dieses Rechtes zurückführen, obwohl zuverlässige Aussagen über die Qualität frühestens nach Abschluß der Wiederholungsbefragung gemacht werden können. Wenn viele Bürger nicht in der Lage waren, einzelne Fragen richtig zu beantworten, spricht dies eher gegen die Verständlichkeit der Erhebungsbogen und der beigefügten schriftlichen Erläuterungen. So setzt eine korrekte Beantwortung der Frage 16 des Personenbogens („Zu welchem Wirtschaftszweig gehört der Betrieb, in dem Sie tätig sind?") die Kenntnis der statistischen Kategorienbildung bezüglich der Wirtschaftszweige voraus. Diese wurde weder den Auskunftspflichtigen noch den Zählern hinreichend erläutert.

Rücklaufkontrolle

Vereinzelt hobe ich auch während der Rücklaufkontrolle bei der Haupterhebung Verstöße beanstandet.

So hatte ein Zähler der Mitarbeiterin einer Erhebungsstelle Informationen über den angeblich verwahrlosten Zustand der Wohnung einer auskunftspflichtigen Person gegeben. Die Mitarbeiterin der Erhebungsstelle gab diesen Hinweis an das Bau- und Wohnungsaufsichtsamt desselben Bezirks weiter, dem dieser Umstand allerdings bereits bekannt war. Aus keiner anderen örtlichen Erhebungsstelle ist mir bisher ein vergleichbar schwerer Verstoß gegen die gesetzliche Verpflichtung der Zähler und Erhebungsstellenmitarbeiter zur Verschwiegenheit bekannt geworden.

Wiederholt haben sich Bürger darüber beschwert, sie hätten ihre Erhebungsunterlagen bereits ausgefüllt dem Volkszählungsamt übermittelt und seien trotzdem erinnert oder gemahnt worden. Die Abwälzung der *Übermittlungsgefahr* bei der Rücksendung der Erhebungsunterlagen auf dem Postweg habe ich bereits an anderer Stelle kritisiert. Die Erinnerung und Mahnung solcher Bürger, die bereits geantwortet hatten, waren zum Teil auf Fehlzustellungen durch die Bundespost, aber auch auf Mängel im Melderegister zurückzuführen. In einem Fall versäumte es das Volkszählungsamt, auf den Hinweis des Auskunftspflichtigen die Personendatei im PC zu korrigieren, so daß das Erinnerungs- und Mahnverfahren zunächst weiterlief, bis sich der Bürger beschwerte.

Welche *praktischen Probleme* die Ämter für Volkszählung mit der Geheimhaltung statistischer Einzelangaben selbst bei der Versendung neuer Erhebungsunterlagen im Erinnerungs- und Mahnverfahren und bei der Versendung der Aufforderungsbescheide hatten, wurde in folgenden Fällen deutlich:

Ein Bürger beschwerte sich darüber, daß er im Rahmen der Arbeitsstättenzählung insgesamt dreimal - zuletzt verbunden mit dem Aufforderungsbescheid - Arbeitsstättenbogen zugeschickt bekam, die er alle ausgefüllt an das Volkszählungsamt zurück-

geschickt habe. In dem Brief des Volkszählungsamtes, der den Aufforderungsbescheid und den dritten Arbeitsstättenbogen enthielt, lag auch ein *ausgefülltes Ergänzungsblatt* zum Arbeitsstättenbogen eines anderen Unternehmens. Meine Überprüfungen beim zuständigen Amt für Volkszählung ergaben, daß der Sachbearbeiter zumindest in vier Fällen leere Arbeitsstättenbogen versandt hatte, ohne zu bemerken, daß in diese Bogen jeweils einzelne ausgefüllte Ergänzungsblätter eingelegt waren, die zu dem Arbeitsstättenbogen der Hauptniederlassung eines Unternehmens mit zahlreichen Zweigniederlassungen gehörten. Dies war ein Verstoß gegen das Statistikgeheimnis. Das Amt für Volkszählung wurde darauf hingewiesen, daß mehrfach ausgefüllte Erhebungsunterlagen entsprechend einer Anweisung des Statistischen Landesamtes zur Vermeidung einer Doppelspeicherung in der Erhebungsstelle zu vernichten sind, falls sie noch aufgefunden werden sollten.

Auch in anderen Fällen haben Bürger von Volkszählungsämtern versehentlich Erhebungsunterlagen erhalten, die von anderen Auskunftspflichtigen bereits ausgefüllt worden waren. Grund dafür war, daß die Erhebungsstellen teilweise von den Zählern zurückgebrachte, überwiegend unbenutzte Erhebungsbögen neu versandt haben. Diese datenschutzrechtlichen Mängel hätten sich vermeiden lassen, wenn man von vornherein ausschließlich neue, auch keinem Zähler ausgehändigte Erhebungsunterlagen versandt hätte.

Bei der Überprüfung der *Vollständigkeit von Angaben* in den Erhebungsunterlagen stellt sich die Frage, ob die örtliche Erhebungsstelle fehlende Angaben eigenständig ergänzen oder widersprüchliche Angaben korrigieren darf. Die einzigen Daten, die die Erhebungsstelle selbständig in die Personenbogen eintragen darf, sind die Stammdaten aus dem Melderegister, die im Wege der Ersatzvornahme übernommen werden dürfen, wenn eine Auskunft vom Bürger innerhalb von sechs Wochen nach dem Zählungsstichtag nicht zu erreichen ist. Im übrigen fehlt für eine Ergänzung von Angaben durch die Erhebungsstelle eine gesetzliche Grundlage. Sie darf deshalb erst nach Rückfrage bei den Auskunftspflichtigen oder von diesen selbst vorgenommen werden. Allerdings sehe ich keine Veranlassung, eine selbständige Ergänzung der Erhebungsbogen in den Fällen zu beanstanden, in denen nur eine Antwort sinnvoll ist (z. B. Familienstand eines zweijährigen Kindes).

Anstaltszählung

Besondere datenschutzrechtliche Probleme warf die Durchführung der *Volkszählung in Gemeinschafts- und Anstaltsunterkünften* auf. Dabei war zu berücksichtigen, daß das Bundesverfassungsgericht die 1983 noch vorgesehene Frage nach der Eigenschaft des Auskunftspflichtigen als Anstaltsinsasse oder Angehöriger des Anstaltspersonals für verfassungswidrig erklärt hatte.

Der Personenbogen bei der Volkszählung 1987 enthielt diese Frage nicht mehr. Darüber hinaus hat das Statistische Landesamt ein differenziertes Verfahren zur Durchführung der Zählung in Anstalts- und Gemeinschaftsunterkünften entwickelt, mit dem sichergestellt werden konnte, daß Bewohner von Anstalten, die der Gefahr der sozialen Abstempelung ausgesetzt waren (z. B. psychiatrische Krankenhäuser, Wohnheime für Asylbewerber, Frauenhäuser, Strafvollzugsanstalten), ihre Identität weder dem Zähler noch der Erhebungsstelle gegenüber offenbaren mußten.

Während die Bewohner von Anstalten im sogenannten nichtsensiblen Bereich (z. B. Seniorenwohnheime) die vollständigen Erhebungsunterlagen auszufüllen hatten, erhielten die Bewohner der sensiblen Anstalten lediglich einen Personenbogen und einen Rücksendeumschlag mit geschwärztem Absenderfeld. Diese Unterlagen übergab der Zähler dem Anstaltsleiter in der erforderlichen Zahl, der sie an die Anstaltsbewohner weitergab. Der Zähler nahm in seine Adressenliste lediglich die Heftnummern der Erhebungsbögen auf, die in der betreffenden Anstalt zu verteilen waren, so daß das Volkszählungsamt nach Erhalt der entsprechenden Bogen feststellen konnte, daß aus dem Bereich dieser Anstalt geantwortet worden war. Die Bewohner dieser Anstalten waren weder verpflichtet, ihren Namen noch ihre Anschrift anzugeben. Durch den Verzicht auf die Erhebung der Hilfsmerkmale hatten die Volkszählungsämter keine Möglichkeit, einzelne Bewohner dieser Anstalten zu mahnen oder bei Auskunftsverweigerung Sanktionen gegen sie zu verhängen, so daß hier die Volkszählung faktisch auf freiwilliger Basis stattgefunden hat. Dies begrüße ich.

In einer unangemeldeten Überprüfung der Volkszählung in der *Karl-Bonhoeffer-Nervenklinik* habe ich eine vorbildliche Durchführung durch Anstaltsleitung und Zähler festgestellt. Die sorgfältige Auswahl und besondere Schulung der Zähler für die Anstaltszählung und die Benennung einer besonderen Kontaktperson für Probleme der Anstaltszählung in jedem Amt für Volkszählung haben mit dazu beigetragen, daß ich zu diesem Fragenkreis nur wenige Eingaben erhalten habe. Ein Problem bei der praktischen Durchführung bestand in der *persönlichen Auskunftserteilung* durch den Heimbewohner. Sowohl in sensiblen wie nichtsensiblen Anstalten sollten die Betroffenen selbst die Erhebungsunterlagen ausfüllen. Nur wenn diese wegen einer Behinderung oder wegen Minderjährigkeit selbst nicht Auskunft geben konnten, setzte die Auskunftspflicht des Anstaltsleiters ein. Dieser oder die von ihm beauftragte Person durfte dafür nur auf allgemeine Verwaltungsdaten zurückgreifen, die ihm bekannt waren. Nicht zulässig waren eigene Nachforschungen oder ein Rückgriff auf medizinische Akten. Mir ist kein Fall bekannt geworden, in dem dies mißachtet wurde.

Allerdings habe ich in einem Amt für Volkszählung einen datenschutzrechtlichen Mangel bei der Durchführung der Anstaltszählung festgestellt. Dort hatte der Zähler, der in allen Anstalten des Bezirks eingesetzt wurde, in jeder dieser Einrichtungen (unabhängig von ihrer Einordnung als sensible oder nichtsensible Anstalten) die Erhebungsunterlagen entweder dem Leiter der Anstalt übergeben oder sie mit diesem bzw. seinem Beauftragten für die Volkszählung anhand der *Verwaltungskarteien* ausgefüllt. Demgegenüber hätte der Zähler sich im Rahmen des in der jeweiligen Anstalt Möglichen selbst davon überzeugen müssen, welcher Anstaltsbewohner aufgrund von Behinderung oder Minderjährigkeit nicht selbst Auskunft geben konnte. Dabei bin ich mir dessen bewußt, daß die Umsetzung dieser gesetzlichen Regelung in der Praxis gerade in Heimen für behinderte und alte Menschen teilweise auf Schwierigkeiten gestoßen ist. Das Amt für Volkszählung, bei dem ich diesen Mangel festgestellt hatte, hat die Zählung in den betreffenden Anstalten ordnungsgemäß wiederholt.

Ich habe die *Einhaltung der PC-Richtlinien* in allen Ämtern für Volkszählung überprüft. Dabei habe ich festgestellt, daß die Ausführung der PC-Richtlinien keine grundsätzlichen Schwierigkeiten machte. Auffällig war jedoch, daß trotz der eindeutigen Bestimmungen zur Datenträgerverwaltung bei den meisten Ämtern hier Defizite festzustellen waren. Der sorgfältige Umgang mit den Sicherungskassetten und den Programmdisketten bedeutet, daß jederzeit ohne besonderen Aufwand Vollzähligkeit und Authentizität der Datenträger überprüfbar sein müssen. In einigen Ämtern habe ich festgestellt, daß die Authentizität der Programmdisketten nicht überprüfbar war, da die notwendigen unverfälschbaren Kennzeichnungen fehlten, bei anderen fehlte der geforderte schriftliche Nachweis der Datenträger als Voraussetzung für die Vollzähligkeitskontrolle. In einem Amt für Volkszählung mußte ich die Häufung von Leichtfertigkeiten im Umgang mit den beweglichen Datenträgern beanstanden.

Vorläufige Bewertung

Insgesamt sehe ich meine bereits im Jahresbericht 1984 getroffene skeptische Aussage bestätigt, daß eine grundlegende Neukonzeption zur Volkszählung insbesondere unter starker Reduzierung der Erhebungsmerkmale dem Urteil des Bundesverfassungsgerichts von 1983 eher gerecht geworden wäre als die tatsächlich erfolgte Nachbesserung. Ich hoffe, daß die amtliche Statistik nicht zuletzt aufgrund ihrer Erfahrungen bei der diesjährigen Volkszählung ihrer rechtlichen Verpflichtung zur Entwicklung einer Erhebungsmethode nachkommt, die den einzelnen Bürger weniger stark belastet.

In diesem Zusammenhang erscheint es mir bemerkenswert, daß der Entwurf für eine Richtlinie des Rates der *Europäischen Gemeinschaften* über die gleichzeitige Durchführung der allgemeinen Volkszählungen[1] es ausdrücklich solchen Mitgliedstaa-

[1] KOM (86) 775 endg.; Ratsdok. 4219/87

ten, die nicht in der Lage sind, im Frühjahr 1991 eine Vollerhebung durchzuführen, ermöglicht, statistisch vergleichbare Angaben auf der Grundlage alternativer Verfahren wie Verwendung von Registern oder Stichprobenerhebungen in tabellarischer Form der EG-Kommission zu übermitteln. Die Bundesregierung hat bei den Beratungen über diesen Richtlinienentwurf erklärt, daß sie die gemeinschaftsrechtliche Pflicht zur Übermittlung statistischer Daten im Jahre 1991 auf der Grundlage der Volkszählung 1987 erfüllen wird. Auch für die weitere Zukunft scheint es mir wichtig, daß die Vereinheitlichung der Statistik auf europäischer Ebene nicht zur Durchführung von Vollerhebungen zwingt. Die amtliche Statistik in der Bundesrepublik ist deshalb gemeinschaftsrechtlich nicht daran gehindert, auf Vollerhebungen mit Auskunftspflicht in Zukunft zu verzichten.

3. Vernetzung

3.1 Die Autobahnen der Informationsgesellschaft

Die Vernetzung von Datenverarbeitungsanlagen ist ein Charakteristikum der Informationsgesellschaft, einer Gesellschaftsform, in der Bereitstellung und Verarbeitung von Informationen zum konstituierenden Merkmal in Staat, Wirtschaft und Privatleben werden. Erst die Vernetzung ermöglicht den ortsunabhängigen Zugriff auf vorhandene Datenbestände und deren unmittelbare Nutzung im eigenen System. Die zunehmende Abhängigkeit gesellschaftlicher Abläufe von diesen Prozessen erzeugt vielfältige Anfälligkeiten: Systemausfälle führen zu Störungen, fehlerhafte Konzepte beeinflussen die Funktionsfähigkeit gesellschaftlicher Institutionen. Insbesondere ist die Gesellschaft durch bewußte, die vorgegebenen Regeln mißachtende Eingriffe „verwundbar". Die Vernetzung erhöht auch das Potential von Eingriffen. So können selbst legale Möglichkeiten in erheblich höherem Maße als bisher ausgeschöpft werden. Die Technologiefolgenforschung kennzeichnet dies mit dem plastischen Begriff der *Verletzlichkeit der Gesellschaft.* Die Furcht vor dem Überwachungsstaat, die gerade im Zusammenhang mit der Volkszählung - wenn auch dort zu Unrecht - häufig artikuliert wurde, hat hier eine ihrer Wurzeln. Trotz der Geläufigkeit des Begriffes „Netz" in der aktuellen gesellschaftspolitischen Diskussion ist seine Bedeutung unklar.

Die *Begriffe* „Netz", „Netzwerk", „Datennetz" werden im Zusammenhang mit der automatisierten Datenverarbeitung in vielfältiger, häufig irritierender Weise verwendet. Allen Netzen ist gemeinsam, daß Daten von einem Punkt zum anderen übertragen werden können, sei es nun von Rechner zu Rechner, von Datenendgerät zum Rechner und zurück, sei es über eine Entfernung von wenigen Metern, sei es weltumspannend. Sobald Personalcomputer miteinander verbunden werden, damit sie Datenkommunikation miteinander betreiben können, wird ebenso von einem Netz gesprochen wie beim weltweit operierenden Datenaustausch für den internationalen Zahlungsverkehr (SWIFT-Netz) oder dem genauso weitgemaschten Datennetz für die Forschung.

Die *Vielschichtigkeit* und Mehrdeutigkeit des Netzbegriffs zeigt folgendes Beispiel: Auf physischer Ebene stellt die Deutsche Bundespost in dem Integrierten Datennetz (IDN) den Anwendern eine Infrastruktur für die Übertragung digitaler Daten zur Verfügung. Auf IDN werden Datenübertragungsdienste mit unterschiedlicher Vermittlungstechnik betrieben, insbesondere DATEX-P und DATEX-L. Mit DATEX-L wird unter anderem der Textübertragungsdienst Teletex betrieben, der auch allgemein als Netz bezeichnet wird, wobei hier die Besonderheit der Spezialisierung auf eine besondere Datenart, nämlich auf Text, liegt. Das Teletex-Netz z. B. ist wiederum Träger des zwischen den Ämtern für Volkszählung und dem Statistischen Landesamt aufgebauten sternförmigen Netzes für den Austausch oder die zentrale Vorgabe von Textbausteinen.

Unbeschadet der dargestellten Ebenen und der Mehrdeutigkeit des Netzbegriffs können die wichtigsten Datenschutzprobleme der Netze benannt werden.

Hacking

Wo auf Rechner durch selbsttätige Einrichtungen über ein Datennetz zugegriffen werden kann, muß sichergestellt werden, daß nur Berechtigte zugreifen können. Unberechtigte können auf Rechner zugreifen, wenn ihnen der Zugang an das Netz über ein angeschlossenes Terminal ermöglicht wird und sie sich als berechtigte Benutzer dem System gegenüber ausweisen können[1].

Die erste Voraussetzung kann bei geschlossenen Netzen erfüllt werden, wenn der Unbefugte *physisch Zugang* zu einer Datenstation am Netz erhält, was durch wirksame Zugangskontrollen zu verhindern ist. Anders ist es bei offenen Netzen, in denen über Wählverbindungen der Zugang zum Rechner eröffnet wird. Hier könnte prinzipiell - sofern nicht Sicherungsmaßnahmen greifen - von jedem Anschluß des Wählnetzes mittels einer angeschlossenen Datenstation die Verbindung zum Rechner hergestellt werden.

Die zweite Voraussetzung, nämlich sich dem System gegenüber *als befugt ausgeben* zu können, ist nach aller Erfahrung kein entscheidendes Hindernis für den Zugriff auf ADV-Anwendungen in offenen Netzen. Zwar werden ausgeklügelte Paßwortverfahren mit beliebigen Änderungsmöglichkeiten und tiefer Zugriffsdifferenzierung angeboten, aber ihre Wirksamkeit hängt vor allem von der organisatorischen Vorbereitung und der Bereitschaft der Benutzer, ihre Paßwörter wirklich geheimzuhalten, ab. Die in der jüngsten Vergangenheit bekannt gewordenen Hacking-Fälle finden meist ihre Ursache in der leichtfertigen Verwendung und Auswahl der Paßwörter.

Es gibt eine Bandbreite von *Gegenmaßnahmen,* die den Hacker-Zugriff auf Rechner in Netzen verhindern sollen:

- Einsatz von *Benutzerkontrollverfahren,* die sicherer sind als das herkömmliche Paßwortverfahren, wie z. B. Ausweisleseverfahren (in der Regel aber nur in geschlossenen Netzen eingesetzt), Chipkarten-Verfahren, Prädialogverfahren, die den Paßwortschutz verstärken, automatische Rückruftechniken, möglichst mit Protokollierung, Prüfung von Terminalkennungen, die automatisch abgesandt werden (vergleichbar mit dem Bildschirmtext-Zugang), eventuell auch so zukunftsweisende - aber noch nicht existierende - Verfahren wie Fingerabdruck-, Augenhintergrund-, Stimm- oder Schriftanalyse zur Authentifizierung des Benutzers.
- Beschränkung des Zugriffs der Benutzer und damit auch der Mißbrauchsmöglichkeiten Unbefugter auf bestimmte Anwendungsverfahren durch die Einrichtung solcher Verfahren als *Teilhabersysteme,* bei denen der Benutzer sich nur für diese Verfahren identifizieren muß, aber zum weiteren Durchgriff auf die Programm- bzw. Betriebssystemebene keine Möglichkeit erhält, das System zu täuschen. Dieses Verfahren ist natürlich nur sinnvoll, wenn der Zugriff auf die Programm- oder Betriebssystemebene für die Aufgabenerfüllung der befugten Benutzer nicht erforderlich ist. Im Gegensatz zu den Teilhabersystemen stehen die Teilnehmersysteme, bei denen die befugten Teilnehmer eben diesen Durchgriff auf die Programm- bzw. Betriebssystemebene erhalten können. Die Mißbrauchsmöglichkeiten im Teilnehmerstatus sind daher wesentlich größer.
- Einsatz der sogenannten *Speicherverschlüsselung,* womit zwar nicht der unbefugte Zugriff auf die Daten in einem System verhindert wird, jedoch der Mißbrauch dieser Daten. Dabei wird natürlich vorausgesetzt, daß die Hacker nicht die Gelegenheit erhalten, die Daten zu entschlüsseln.

Zusammengefaßt kann gesagt werden, daß Hacking kein unvermeidbares Risiko moderner Datenverarbeitung ist. Es beruht stets auf einer unzureichenden Ausstattung mit Sicherheitskomponenten oder dem unzureichenden Umgang damit, wenn nicht gar - wie kürzlich zu lesen war - gravierende Betriebssystemmängel die Ursache sind.

[1] Unter Hacking werden unberechtigte Zugriffe sowohl durch Außenstehende als auch durch interne Mitarbeiter verstanden.

Mitschneiden des Datenverkehrs

Wo Daten über Leitungen übertragen werden, muß verhindert werden, daß Daten auf dem Übertragungsweg, also auf der Leitung, in Vermittlungspunkten und Netzabschlüssen unbefugt mitgeschnitten („abgehört") werden können.

Ein *Angriff auf Übertragungswege* ist insbesondere bei der elektrischen Übertragungsform (im Gegensatz zur optischen Übertragungsform) technisch leicht möglich, ohne daß Sender und Empfänger dieses sofort erkennen können. Voraussetzungen sind jedoch erstens der physische Zugang zu diesen Datenleitungen oder zu den Vermittlungspunkten und Netzabschlüssen und zweitens die Fähigkeit, den Datenstrom so zu interpretieren, daß die Daten für einen Mißbrauch verwendbar sind.

Die erste Voraussetzung kann zumindest für die Leitungen bei den meisten Netzen leicht erfüllt werden, da der Zugang zu einer Übertragungsstrecke bei größeren Entfernungen nicht vollständig abgesichert werden kann. Die Erfüllung der zweiten Voraussetzung hängt davon ab, ob die Daten unverschlüsselt oder verschlüsselt übertragen werden. Bei verschlüsselter Übertragung setzt der sinnvolle Datenmitschnitt die Möglichkeit zur Entschlüsselung voraus, was bei modernen kryptographischen Verschlüsselungsverfahren als nicht wahrscheinlich angesehen werden kann. Bei der unverschlüsselten Übertragung hängt es davon ab, mit welchen Übertragungsformaten und -prozeduren das jeweilige Netzwerk arbeitet. Multiplex-Verfahren, Datenverdichtung, paketweise Übertragung sind Methoden zur Optimierung und Flexibilisierung der Datenübertragungsverfahren, die auch die Interpretation der mitgeschnittenen Datenströme erschweren, jedoch zumindest Zufallsfunde nicht generell ausschließen. Die unverschlüsselten Datenströme können durch Datenanalysatoren mitgelesen werden.

Beispiele für Netze

Diese Analyse der wichtigsten Risiken auf Netzen ist Maßstab zur Bewertung der Datensicherung auf den Netzen, die öffentliche Stellen des Landes Berlin einsetzen oder einsetzen wollen.

In der Diskussion befindet sich derzeit das *ISDN* (Integrated Services Digital Network), für das in diesem Jahr Betriebsversuche der Deutschen Bundespost begonnen haben. Dabei handelt es sich um ein neues Telekommunikationsnetz, in dem sowohl Daten als auch Sprache in digitaler Form übertragen werden. Es ist daher geeignet, die Datenübertragungsdienste und die bisher auf dem Fernsprechnetz abgewickelten Dienste (Fernsprechen, Bildschirmtext, Telefax) zu integrieren. Dabei profitieren alle von wesentlich höheren Bandbreiten und damit höheren Datenübertragungsraten. Wie auch das Verwaltungsnetz ist das ISDN lediglich eine unabhängig von ihren Anwendungen zu betrachtende Infrastruktur. Probleme des Zugangs an angeschlossene Rechner werden durch das ISDN, welches natürlich ein offenes Netz ist, nicht gelöst; dies bleibt Sache der Dienste und der Anwender der Dienste. Das gleiche gilt für die Verschlüsselung der Daten bei der Übertragung über das ISDN. Die Datenschutzbeauftragten haben gefordert, daß die Deutsche Bundespost im Rahmen von ISDN einen Datenverschlüsselungsdienst als Dienstleistung mit anbieten sollte, um damit für diese wichtige Sicherungsmaßnahme auf dem Datennetz Anreiz zu bieten.

Das neue *Berliner Verwaltungsnetz* wird in Kürze in Betrieb gehen. Es soll nach Maßgabe der von der Netzadministration zugelassenen Übertragungswege (Standleitungen) den Datenverkehr zwischen verschiedenen Rechnern des Landesamtes für Elektronische Datenverarbeitung integriert übernehmen und dabei die bisher bestehenden herstellerspezifischen Netze auf der reinen Übertragungsebene aus ökonomischen Gründen ersetzen, weil damit die bestehenden HfD-Standleitungen besser ausgelastet werden. Das Netz ist geschlossen, der Benutzer kann daher nur von vorgegebenen Terminals aus mit den Rechnern kommunizieren, die von der zentralen Netzadministration her dem jeweiligen Verfahren auf diesem Rechner zugeordnet werden. Die Übertragung erfolgt in verdichteter Form, die Verschlüsselung des Datenverkehrs ist möglich, aber Sache des Anwendungsverfahrens, nicht des Netzes.

Im *Forschungsbereich* ist weltweit ein Netz aufgebaut worden, auf dem Wissenschaftler in mannigfaltiger Weise Daten austauschen. Auch die Berliner wissenschaftlichen Rechenzentren, die ihrerseits in das Berliner Forschungsnetz BERNET eingebunden sind, sind Bestandteil dieses Kommunikationsverbundes. Dazu gehört das Dialogsystem Süd der Freien Universität Berlin, welches auch andere Hochschulen und Schulen mit ADV-Kapazitäten zu Forschungs- und Ausbildungszwecken versorgt. Außerdem gehört der CDC-Großrechner der Freien Universität dazu, der im Frühjahr Opfer eines Hacker-Angriffs geworden ist, welcher in der Öffentlichkeit Aufmerksamkeit erregte. Bei Rechnernetzen, die zu Zwecken der Forschung und Ausbildung, etwa in der Programmierung eingesetzt werden, geht es darum, möglichst vielen Benutzern in möglichst flexibler Weise DV-Kapazität bereitzustellen und die Möglichkeiten des Netzes und von Datenbanken anzubieten. Dies alles setzt voraus, daß das Netz offen ist und die angeschlossenen Rechner im Teilnehmermodus benutzbar sind. Dies bedeutet, daß solche Systeme außerordentlich anfällig für Hacker sind. Muß dies schon in einem gewissen Umfang hingenommen werden, trifft diejenigen, die das System nutzen, die Verantwortung für die von ihnen gespeicherten oder übertragenen vertraulichen Daten. Insbesondere müssen die Risiken bekannt gemacht werden. Aus der Sicht des Datenschutzes bedeutet es ferner, daß die Speicherung personenbezogener Daten im Rahmen eines solchen Netzes grundsätzlich unterbleiben sollte.

Zwei weitere Beispiele sollen im folgenden näher behandelt werden:

3.2 Automatisierter Zahlungsverkehr

Traditionell gehören die Kreditinstitute zu den ersten Organisationen, die neue Entwicklungen der Informationstechnik erschließen. Das anfallende Massengeschäft war frühzeitig Gegenstand der Rationalisierung durch Computer. Die Automatisierung der Dienstleistungen im Geldsektor ist fast jedem etwa durch die Geldausgabeautomaten gegenwärtig und neuerdings kann man - zumindest in Berlin und München - das im durch Datenfernverarbeitung unterstützten bargeldlosen POS (Point Of Sale)-Zahlungsverfahren beim Einkauf in bestimmten Geschäften üben.

Zusammen mit diesen eingeführten oder in der Erprobung befindlichen Verfahren im automatisierten Zahlungsverkehr sprechen viele weitere anspruchsvolle Anwendungen dafür, daß das *„Electronic Banking"* in Zukunft die Branche prägen wird:

- *Automatisierte Bankendienste* wie Geldausgabeautomaten, Kontoauszugsdrucker, Selbstbedienung bei der Kontenführung, Expertensysteme für die Beratung in verschiedenen Geldangelegenheiten, Cash-Management-Systeme für die wirtschaftlich optimale Liquiditätsplanung von Unternehmen, Informationssysteme zu Kunden-, in der Regel Firmenmerkmalen;
- *POS-Zahlungsverfahren* für die bargeld- und schecklose Zahlung im Einzelhandel;
- *Home-Banking* über Bildschirmtext;
- Internationaler und nationaler *Datenverkehr* zwischen den Kreditinstituten.

Es ist dabei von folgenden *Entwicklungstendenzen* auszugehen:

- Die automatisierten Bankendienste verstärken sich sowohl hinsichtlich der Dichte als auch der Anwendungsbreite. Standardisierbare Vorgänge im Verhältnis zum Kunden werden aus Wirtschaftlichkeitsgründen seitens der Kreditinstitute zunehmend maschinell abgewickelt.
- POS wird in Kürze aus dem Erprobungsstadium heraustreten und bundesweit angeboten werden. Es steht zu erwarten, daß neben den ec-Karten auch Kundenkreditkarten verschiedener Anbieter in das Verfahren einbezogen werden.
- Home-Banking wird nicht nur über Bildschirmtext möglich sein, sondern auch im Rahmen anderer Datenfernübertragungsverfahren, etwa von einem Personalcomputer aus, durchgeführt werden können. Dies ergibt sich aus der

Tendenz, die ursprünglich zwischen den Girozentralen, zwischenzeitlich zwischen beliebigen Kreditinstituten untereinander und auch mit Großkunden aufgebauten Datenfernübertragungsverfahren für den nationalen Zahlungsverkehr für die Datenkommunikation mit beliebigen ADV-Systemen zu öffnen, sofern bestimmte Mindeststandards für die Kompatibilität mit dem System der Bank und für die Autoritätssicherung eingehalten werden.

Diese strukturellen Neuerungen durch den Einsatz modernster Informationstechnik im Kreditwesen bedürfen selbstverständlich auch der intensiven Beobachtung aus der Sicht des Datenschutzes. Aus diesem Grunde beschäftigt sich die Konferenz der Datenschutzbeauftragten mit dem Ziel, konkrete technische, organisatorische und rechtliche Anforderungen an die Automatisierung im Kreditwesen aus der Sicht des Datenschutzes zu formulieren. Ein erstes Ergebnis ist als Anlage abgedruckt.

Mit der Ausweitung der automatisierten Bankendienste und des Home-Banking geht zunehmend mehr *Verantwortlichkeit* für die ordnungsgemäße Abwicklung seiner Bankgeschäfte vom Kreditinstitut auf den Kunden über. Sollten also durch Mißbrauch oder Nachahmung der ihm in die Hand gegebenen Identifizierungsmittel (in der Regel Eurocheque-Karte und persönliche Identifikationsnummer [PIN]) Schäden entstehen, so hätte er aufgrund der gegebenen Geschäftsbedingungen nachzuweisen, daß er keine Ursache für die mißbräuchliche Verwendung seiner Identifikationsmittel gegeben hat. Dieser Nachweis wäre gleichbedeutend mit dem Nachweis von Sicherheitsmängeln im System oder in der Systemkonzeption, was dem einzelnen Kunden mit Sicherheit unmöglich wäre. Meines Erachtens müssen hieraus Konsequenzen für die Allgemeinen Geschäftsbedingungen für die Kontoführung gezogen werden.

Hinzu kommt, daß der *sichere Umgang mit PIN und ec-Karte* zunehmend risikobehaftet ist:

- Es werden immer mehr Mißbrauchsfälle bei Geldausgabeautomaten bekannt.
- Die Geheimhaltung der PIN fällt um so schwerer, je häufiger sie benutzt werden muß und je unüberschaubarer die Verhältnisse sind, unter denen sie benutzt wird. So ist etwa im Ausverkaufstrubel an einer POS-Kasse, bei der die PIN-Eingabetastatur nicht besonders gegen fremde Einsicht geschützt ist, die PIN kaum gegenüber Interessierten geheimzuhalten. Das gleiche gilt für offen stehende Geldausgabeautomaten oder für solche, die zwar in geschlossenen Kabinen stehen, während PIN-Eingabetastaturen jedoch so angebracht sind, daß sie bei normaler Körperhaltung des Benutzers von außen beobachtet werden können.
- Das Problem wird dadurch verschärft, daß von der Technik her eine einfache und flexible Änderung der PIN durch den Kunden selbst nicht möglich ist.
- Bei der herkömmlichen Technik entsteht keine Dokumentation der vom Kunden mit automatisierter Authentifikation veranlaßten Banktransaktionen, die er gegenüber dem Kreditinstitut zum Nachweis der von ihm tatsächlich veranlaßten Geschäftsvorgänge benutzen könnte.

Neben den Identifikationsrisiken und der unbefriedigenden Beweislastverteilung gibt es weitere Ansatzpunkte für datenschutzrechtliche Betrachtungen:

- Bei Verfahren, die sich der Datenfernverarbeitung bedienen, wie z. B. POS oder der nationale (ONGUM) oder internationale (SWIFT) Austausch von Zahlungsverkehrsdaten, sind neben den Institutionen, die dem Kunden aufgrund seiner eigenen Disposition bekannt sind, zusätzliche Institutionen wie z. B. *Clearing-* oder *Autorisierungszentralen* (Netzzentralen oder -knoten) beteiligt, von denen der Kunde nichts weiß. Die datenschutzrechtlich bedeutsame Einhaltung dieser Institutionen als eigene speichernde Stellen oder als Auftragnehmer von Datenverarbeitung gelingt häufig nicht präzise, insbesondere dann nicht, wenn sie im Ausland liegen und damit strittig ist, welches Datenschutzrecht im einzelnen anzuwenden ist. Da der Kunde über diese beteiligten Institutionen nicht unterrichtet wird, kann er weder seine Einwilligung zur Einschaltung dieser Institutionen bekunden, noch kann er seine aus den Datenschutzgesetzen folgenden Rechte (etwa auf Auskunft) anwenden, die er gegenüber diesen Instanzen geltend machen muß.
- Ist bereits durch die Verwendung von Schecks beim Einkauf die traditionelle *Anonymität des Kaufvorgangs* bei der Barzahlung aufgehoben worden, so verstärkt sich dieser Trend gravierend bei der Benutzung von POS-Kassen. Über den Zahlungsvorgang werden automatisiert alle Daten erhoben, die für die ordnungsgemäße Verbuchung und für den späteren Nachweis des Zahlungsvorgangs erforderlich sind. Bei intensiver Nutzung können daraus personenbezogene Verhaltens- bzw. Bewegungsprofile abgeleitet werden. Es wird daher stark darauf zu achten sein, daß das geplante bundesweite POS-Verfahren so organisiert wird, daß eine zentrale Dokumentation der Zahlungsvorgänge überflüssig wird - etwa dadurch, daß, wie von der Sparkassenorganisation erwogen, die Deckung direkt beim Konto des Kunden geprüft wird.
- Im Rahmen des POS-Versuchs in Berlin wurden auch Kassen erprobt, bei denen differenzierte Meldungen über eine *Ablehnung* nicht beim Kunden, sondern beim Kassierer anfallen. Gegen dieses Verfahren bestehen Bedenken, da der Kassierer lediglich erfahren muß, ob es zu einer POS-Verbuchung kommt oder nicht.
- Bei POS besteht das Problem, wie der Kunde sicher sein kann, ob die POS-Kassen oder die Datenfernübertragungs-Schnittstellen im Bereich des besuchten Handels- oder Dienstleistungsunternehmens nicht dahingehend manipuliert worden sind, daß die Vertraulichkeit des Dialogs zwischen Kunden und System (so etwa die der PIN) gebrochen wird. Wie dieses sichergestellt werden kann, bleibt vorerst noch offen. Zumindest bei den POS-Versuchen ist die Vertraulichkeit auf den Datenübertragungswegen durch Transportverschlüsselung gewährleistet.
- Zum internationalen Zahlungsverkehr mittels SWIFT ist festzustellen, daß er zwar als technisch sicher einzustufen ist, jedoch eine befriedigende datenschutzrechtliche Betrachtung an den relativ ungeklärten Rechtsverhältnissen beim grenzüberschreitenden Datenverkehr scheitert. So ist z. B. zu beachten, daß der Firmensitz von SWIFT in Belgien liegt, wo es noch keine Datenschutzgesetzgebung gibt.

3.3 Datenverarbeitung in den Berliner Krankenhäusern - Grenzen der Vernetzung

Bereits seit Jahren wird angestrebt, die automatisierte Datenverarbeitung in den öffentlichen Berliner Krankenhäusern einheitlich zu betreiben. Das datenschutzrechtliche Interesse konzentriert sich dabei zunächst auf die Verfahren zur Patienten- und Personalverwaltung.

Die Entwicklung eines hierfür geeigneten, modernen On-line-Verfahrens sowie die Durchführung der Datenverarbeitung in den Krankenhausbetrieben des Landes Berlin findet in Kooperation mit der Gesellschaft für Systemforschung und Dienstleistungen im Gesundheitswesen mbH Berlin (GSD) statt. Dabei handelt es sich um ein privatrechtlich organisiertes Unternehmen, dessen einzige Gesellschafterin derzeit das Land Berlin ist.

Aufgabe der GSD ist die Forschung und Entwicklung auf dem Gebiet der Krankenhausdatenverarbeitung, Entwicklung und Pflege einheitlicher ADV-Verfahren für die Krankenhausbetriebe sowie die Beschaffung und der Betrieb von Datenverarbeitungsanlagen für die Krankenhäuser.

Die GSD entwickelte ein vom damaligen Senator für Gesundheit und Umweltschutz erstelltes Batch-Verfahren zum kaufmännischen Krankenhausrechnungswesen (KRW-1) bis zur Betriebsreife weiter und setzt dies seit 1983 in städtischen Krankenhausbetrieben ein. Da dieses Verfahren den gewachsenen Leistungsanforderungen nicht mehr entsprach, wurde die GSD beauftragt, ein modernes Dialogverfahren (krw-2) zu entwickeln. Das krw-2 wird seit 1985 in einigen Berliner Krankenhäusern für die Patienten- und Personalstammdaten-Verwaltung eingesetzt. Nach Vorstellungen der „Konferenz der Krankenhausbetriebe" soll dieses Verfahren bis 1990 sämtliche Leistungsansprüche im Datenver-

arbeitungssektor der Materialwirtschaft, Finanzbuchhaltung sowie der Patienten- und Personalverwaltung abdecken. Der Berliner Senat plant, dieses einheitliche Software-Angebot dann in allen Berliner Krankenhäusern einzusetzen.

Das krw-2-Verfahren sowie das dafür aufgebaute Rechnernetz waren Gegenstand einer eingehenden datenschutzrechtlichen Überprüfung. Das ältere Verfahren KRW-1 wurde bedarfsweise mit einbezogen. Neben dem zentralen Rechenzentrum der GSD habe ich das Max-Bürger-Krankenhaus, die Karl-Bonhoeffer-Nervenklinik, die Krankenhausbetriebe Spandau und Neukölln und das Universitätsklinikum Steglitz ausgewählt, da diese Stellen jeweils unterschiedliche Rollen im Datenverarbeitungsnetz des Berliner Gesundheitswesens spielen.

KRW-1

Das KRW-1-Verfahren wird im zentralen Rechenzentrum der GSD abgewickelt. Die Daten werden in den beteiligten Krankenhausbetrieben mit Hilfe von Datensammelsystemen erfaßt und mittels Datenträgeraustausch an die GSD-Zentrale geliefert.

Meine Prüfung hat folgendes ergeben:

In keinem Fall wird der vom eingesetzten paßwortgesteuerten Zugriffskontrollsystem angebotene Sicherheitsstandard hinreichend genutzt, da zu kurze und damit leicht erratbare oder erprobbare Paßworte verwendet werden. Eine ausreichende *Datenträgerverwaltung* habe ich nur im Klinikum Steglitz vorgefunden. Im übrigen wurden Mängel der Datenträgerverwaltung, insbesondere hinsichtlich der Abgangskontrolle, festgestellt. In einem Krankenhaus ergaben sich darüber hinaus schwerwiegende Mängel, insbesondere hinsichtlich der Zugangskontrolle sowie der Sicherung der Datenträger vor unbefugter Verwendung oder Entnahme.

In einem Krankenhaus wurde ich auf ein Problem bei dem Modul *„Personalausfallzeiten"* der Personalverwaltung mit KRW-1 aufmerksam gemacht. Der Zugriff auf diese sensiblen Personaldaten kann vom verwendeten System nicht auf diejenigen Mitarbeiter beschränkt werden, die sie für ihre Arbeit benötigen. Wer die Personalausfallzeiten der ihm zugeordneten Mitarbeiter zur Kenntnis nehmen kann, kann dies auch für beliebige andere Mitarbeiter tun. Die Einführung einer Zugriffsdifferenzierung ist mit dem veralteten technischen System nur mit unverhältnismäßigem Aufwand möglich. In Anbetracht der Absicht, das Verfahren auf krw-2 umzustellen, habe ich übergangsweise den weiteren Einsatz dieses Moduls unter folgenden Voraussetzungen hingenommen: Mißbräuchliche Aufrufe ziehen dienstrechtliche Konsequenzen nach sich; dies wird durch geeignete Belehrungen bekräftigt; die GSD hält ihre Terminzusage ein, ein Personalausfallzeitenverfahren mit erforderlichen Zugriffsdifferenzierungen bis zum Januar 1988 auf krw-2 bereitzustellen.

krw-2

Das neue Dialogverfahren im Krankenhausrechnungswesen (krw-2) läuft auf GSD-eigenen Rechnern in verschiedenen Krankenhäusern. Mit Ausnahme des Universitätsklinikums Rudolf-Virchow und des Universitätsklinikums Steglitz betreibt die GSD auch die Rechenzentren in diesen Krankenhausbetrieben. Diese *Rechenzentren* sind sternförmig mit dem zentralen Rechenzentrum der GSD verbunden. Darüber hinaus nutzen kleinere Krankenhausbetriebe die Rechenzentren größerer Krankenhausbetriebe über Datenfernverarbeitung mit. Eine Trennung der Dateien der unterschiedlichen Krankenhausbetriebe ist dabei gewährleistet. Beim Universitätsklinikum Steglitz habe ich einen Netzübergang zu einem kompatiblen klinikumseigenen Rechner festgestellt, der seinerseits mit dem Berliner Forschungsnetz verbunden war.

Die Überprüfung hat insbesondere zu folgenden Feststellungen geführt:

- Die bestehenden *Kooperationsverträge* zwischen der GSD und den Krankenhausbetrieben stellen die *datenschutzrechtlichen Verantwortlichkeiten* nicht klar, sie definieren insbesondere nicht die Kompetenzverteilung zwischen Auftraggebern und Auftragnehmern bei der Datenverarbeitung im Auftrag.

  Bezeichnend für die unklare Regelung ist, daß mir bei Kontrollbesuchen entgegengehalten wurde, die datenschutzrechtliche Verantwortung für die eigenen Daten sehe man nicht bei sich, sondern bei der GSD, und deshalb habe man keine Veranlassung, sich besonders um den Schutz der eigenen Daten zu kümmern. Andererseits verweist die GSD entsprechend der Rechtslage auf die datenschutzrechtliche Verantwortung der speichernden Stellen.

- Die Verträge lassen den gesetzlich vorgesehen *Weisungsstrang* vom Auftraggeber zum Auftragnehmer nicht erkennen. So verweisen die Krankenhäuser darauf, daß sie trotz ihrer Verantwortung faktisch nicht bestimmen können, was mit ihren Daten geschieht, wie diese vor unbefugter Offenbarung geschützt werden oder wer auf sie zugreifen darf.

- Zum Zeitpunkt der Prüfung waren für das krw-2-Verfahren die *Verfahrens- und Programmdokumentation* sowie die für die ordnungsgemäße Verwendung der Systeme erforderlichen Benutzer- und Betriebshandbücher von der GSD ordnungsgemäß erstellt worden. Andererseits lagen von keinem Krankenhausbetrieb *Abnahmeprotokolle und Freigabebestätigungen* für die Verarbeitungsprogramme vor. Dies bedeutet, daß kein Krankenhausbetrieb der programmierenden Stelle GSD bestätigt hatte, daß die Verarbeitungsprogramme den Anforderungen der anwendenden Stellen in den Krankenhäusern entsprechen. Dennoch werden sie seit langem ohne Kontrolle ordnungsgemäßer Anwendung im Echtbetrieb eingesetzt. Damit ist gegen § 16 Satz 2 Nr. 2 Berliner Datenschutzgesetz verstoßen worden. Sowohl von der GSD als auch von den Krankenhausbetrieben wurde mir zugesagt, daß für alle Programme Abnahmeprotokolle durch den jeweiligen Fachbereichsleiter des Krankenhauses erstellt werden.

  Jedoch hat zumindest ein Krankenhausbetrieb eine formelle Freigabe mit dem Hinweis verweigert, daß die Programme der GSD seinen Anforderungen und Wünschen nicht voll entsprechen.

- Viele Datenendeinrichtungen im krw-2-Verfahren sind *prädialogfähig*. Sie erlauben somit den Zugang auf die Programm- oder Betriebssystemebene des Gesamtverfahrens, sowie Zugriff auf beliebige Programme und Datenbestände im Netz, sofern die Paßwörter bekannt sind. Für eine solche Freizügigkeit beim Zugang zu Programmen und der ärztlichen Schweigepflicht unterliegenden Daten gibt es weder ein praktisches Erfordernis noch eine Rechtsgrundlage.

- Ferner läßt das Datenfernübertragungs-Konzept für das krw-2-Verfahren die *Übermittlung ganzer Dateien* zwischen beliebigen Rechenzentren mittels File-Transfer zu. Es sind keine praktischen Gründe oder sonstigen Erfordernisse erkennbar, die etwa die Übertragung personenbezogener Daten von einem Rechenzentrum an ein anderes notwendig machen, zumal das gegenseitige Einspringen der Rechner im Notfall (back-up) gar nicht vorgesehen ist.

- Der beim Universitätsklinikum Steglitz bestehende *Netzübergang an das Forschungsnetz* (Dialogsystem Süd) erlaubte sachkundigen Benutzern, die über ein entsprechendes Paßwort verfügen, den Zugriff auf Daten und Programme im GSD-Netz von Terminals des Dialogsystems Süd aus. Damit war es möglich, von beliebigen Punkten des weltweiten Forschungsnetzes unter Verwendung einfacher Codes und bei entsprechendem Sachverstand auf personenbezogene Daten zuzugreifen, die der ärztlichen Schweigepflicht unterliegen.

Technischer Hintergrund der untragbaren Risiken für die Vertraulichkeit der gespeicherten Daten ist neben der fehlenden Regionalisierung des GSD-Netzes auch die Tatsache, daß das krw-2-Verfahren mit unterschiedlichen Anwendungsbereichen als *Teilnehmersystem* betrieben wird. Somit wird der Durchgriff auf die Betriebssystem- und Programmierebene in weiten Bereichen des Netzes ermöglicht. Dies bedeutet starke Flexibilität der Benutzer bei der Anwendung des Systems, für die jedoch in fast allen Fällen kein nachweisbarer Bedarf besteht und die die Manipulation des Systems zu mißbräuchlichen Zwecken ermöglicht. Dies ist bei Teilhabersystemen, bei denen der Benutzer nur auf das Anwendungsverfahren geführt wird, ausgeschlossen.

Verarbeitung medizinischer Daten im Auftrag

Sowohl KRW-1 als auch krw-2 werfen ein grundsätzliches Problem auf, das bereits früher Gegenstand datenschutzrechtlicher Erörterungen im Krankenhauswesen war[1]: Bei KRW-1 liefern die beteiligten Krankenhausbetriebe Datenträger an die GSD-Zentrale, die dort im Auftrag verarbeitet und an die Krankenhäuser zurückgegeben werden. Bei krw-2 habe ich festgestellt, daß Mitarbeiter der GSD eine Zugriffsberechtigung auf personenbezogene Daten der Krankenhäuser haben. Gemeinsam ist den Verfahren, daß medizinische Daten aus den Krankenhausbetrieben Mitarbeitern der GSD offenbart werden.

Obwohl diese Situation von den Beteiligten für selbstverständlich gehalten wird, bestehen gegen die Offenbarung medizinischer Daten von den Krankenhäusern an Mitarbeiter der GSD erhebliche datenschutzrechtliche Bedenken.

Die *Datenschutzgesetze* behindern die Verarbeitung im Auftrag nicht, da sie mangels Vorliegen einer Übermittlung an die Zulässigkeit der Weitergabe von Daten an Auftragnehmer keine materiellen Anforderungen stellen. Da die Vorschriften des *Landeskrankenhausgesetzes* sowie der *ärztlichen Berufsordnung* demgegenüber aber auf den weiteren Begriff der Offenbarung abstellen, ist zu prüfen, ob die Kenntnisnahme durch einen Auftragnehmer mit den Bestimmungen über die ärztliche Schweigepflicht vereinbar ist.

Mangels einer besonderen Regelung steht nach dem Landeskrankenhausgesetz nur eine relevante Offenbarungsbefugnis „zur Durchführung des Behandlungsvertrages einschließlich einer Nachbehandlung, soweit nicht der Patient etwas anderes bestimmt hat" zur Verfügung (§ 26 Abs. 3 Ziff. 2). Die Berufsordnung der Ärztekammer Berlin enthält ebenfalls keine explizite Befugnis zur Offenbarung medizinischer Daten an Auftragnehmer, unterstellt aber, daß eine Offenbarung an Mitarbeiter, die „an der ärztlichen Tätigkeit teilnehmen", zulässig ist (§ 2 Abs. 3). Dem entspricht die Bestimmung in § 203 StGB, nach der den Schweigepflichtigen „ihre berufsmäßig tätigen Gehilfen" gleichgestellt sind, so daß diese zwar ebenso wie der Arzt an die Schweigepflicht gebunden sind, ihnen gegenüber aber im erforderlichen Umfange Daten offenbart werden dürfen. Damit stellt sich die grundsätzliche Frage, ob bei Verfahren der vorliegenden Art noch von berufsmäßig tätigen Gehilfen gesprochen werden kann. Dies ist aus der Sicht des Datenschutzes zu verneinen.

Die *Konferenz der Datenschutzbeauftragten* des Bundes und der Länder hat in einer Entschließung vom 14. März 1986 gefordert, daß die Verarbeitung medizinischer Daten außerhalb des eigenen Krankenhauses allenfalls bei einem anderen Krankenhaus zugelassen werden dürfe, da durch eine Auftragsdatenverarbeitung das Arztgeheimnis durchbrochen werde. Es bestünde die Gefahr einer Grundrechtsbeeinträchtigung durch Verknüpfung von medizinischen Daten und solchen aus anderen Bereichen sowie durch überregionale Konzentration medizinischer Daten.

Bei der Prüfung des Klinikums Steglitz im Jahr 1983 bin ich ebenfalls davon ausgegangen, daß die Einbeziehung der Mitarbeiter externer Rechenzentren in den Kreis der ärztlichen Gehilfen eine nicht akzeptable Ausweitung dieses Begriffs darstellen würde. Für die Verfahren, bei denen sich das Klinikum Steglitz der Datenverarbeitung im Auftrag bediente, habe ich deshalb eine konsequente Anonymisierung der Daten gefordert[2].

Damit ist eine auftragsweise Verarbeitung medizinischer Daten nur dann zulässig, wenn ein Krankenhaus für ein anderes Dienstleistungen erbringt. Nur in diesem Fall ist die funktionale und personelle Nähe des Auftragnehmers zum Auftraggeber so groß, daß der Kreis der ärztlichen Berufsgehilfen klar genug abgegrenzt werden kann.

Insoweit war das KRW-1-Verfahren von vornherein datenschutzrechtlich problematisch. Beim krw-2-Verfahren war die Möglichkeit des Zugriffs der GSD-Mitarbeiter auf die personenbezogenen Daten in den Krankenhäusern zu beanstanden.

[1] Vgl. Jahresbericht 1983, Ziff. 2.8
[2] Vgl. Jahresbericht 1986, Ziff. 2.8

Privatisierung

Ein weiteres Problem wirft schließlich die Ankündigung des Senators für Gesundheit und Soziales auf, die vom Land Berlin gehaltenen Anteile an der GSD zu veräußern und damit auf den öffentlichen Einfluß auf die GSD zu verzichten. Die GSD hat sich zwar über den gesetzlichen Rahmen hinaus der Geltung des Berliner Datenschutzgesetzes unterworfen. Durch die Privatisierung darf sich an der Prüfungskompetenz des Berliner Datenschutzbeauftragten nichts ändern.

Darüber hinaus darf der Staat jedoch bei derart sensiblen Verfahren auf seinen formellen Einfluß auf die Ausgestaltung des Systems nicht verzichten. Auch dann, wenn personenbezogene Daten nicht offenbart werden, hat der Auftragnehmer, der Hard- und Software gestaltet, einen erheblichen Einfluß auf die Informationsverarbeitungsprozesse. Die damit verbundenen Risiken, die die gesamte Datenverarbeitung betreffen, gehen weit über das Risiko einzelner Datenzugriffe hinaus. Dies wird Gegenstand weiterer Erörterungen mit den verantwortlichen Stellen sein müssen. Jedenfalls müssen vor einer Privatisierung die festgestellten Mängel beseitigt werden.

4. Beobachtung der Neuen Medien

Die folgende Darstellung der Entwicklung der Neuen Medien zeigt deutlich, daß – entgegen in der Vergangenheit vielfach erhobenen Behauptungen – die Verwirklichung datenschutzgerechter Technik bei Bildschirmtext, beim TEMEX-Dienst und selbst bei Abrufdiensten möglich ist und durchgesetzt werden kann.

4.1 Bildschirmtext

Änderungen des Dienstes

Auch in diesem Jahr wurden bei Bildschirmtext neue Funktionen eingeführt. Die wichtigsten für den Datenschutz bedeutsamen Erweiterungen sind:

- *Vereinfachter Dialog:* Erst mit dem Bestätigen von Dateneingaben mit „19" wurden bisher Dialogseiten an den Adressaten abgesendet. Die Eingabe der Ziffernfolge kann jetzt unter folgenden Bedingungen entfallen: Die betreffende Dialogseite darf keine personenbezogenen Daten enthalten und nicht mit einer Anbietervergütung belegt sein. Beim Ausfüllen des letzten Dialogfeldes werden die Eingaben nunmehr sofort an den Empfänger übermittelt.
- *Mitteilungsrückgabe:* Alle nicht gelesenen Mitteilungen werden automatisch nach 30 Tagen an den Absender zurückgeschickt. Bei ihm werden diese Mitteilungen mit einem „Z" gekennzeichnet.
- *Individuelle Abrufsperre:* Mit dieser Sperre können Anbieter bestimmte Btx-Teilnehmer vom Abruf ihrer Btx-Seiten ausschließen. Durch Listeneinträge können sowohl vollständige Btx-Nummern als auch Btx-Nummerngruppen vom Abruf ausgeschlossen werden.
- *Kennwörter:* Für die verschiedenen Nutzungsbereiche (z. B. Zugang, Benutzerverwaltung, Eingabe von Seiten) können unterschiedliche Kennwörter und damit unterschiedliche Berechtigungen vergeben werden. Sie werden vom Teilnehmer oder Mitbenutzer selbst festgelegt und können jederzeit geändert werden. Die Kennwörter müssen zwischen vier und acht Stellen lang sein.

Weitere der Benutzerfreundlichkeit dienende Änderungen sind:

- *Kurzer Suchweg:* Durch Eingabe von *Anbietername # können im bundesweiten und in allen regionalen Anbieter-Verzeichnissen aufgeführte Anbieter gesucht werden.
- *Kurzwahl:* Jeder Teilnehmer kann bis zu zehn persönliche Kurzwahlen für Btx-Seiten festlegen. Hierfür müssen die Seitennummer und die Bereichskennzahl angegeben werden.

- *Vergütungsschwelle:* Sie verhindert den Abruf vergütungspflichtiger Seiten, wenn dadurch ein bestimmter, vom Teilnehmer individuell festgelegter Betrag überschritten wird. Die Vergütungsschwelle kann jederzeit höher oder tiefer gelegt werden.
- *Briefkastenverwaltung:* Nicht nur bei der Anwahl von Btx werden neue Mitteilungen genannt, auch während einer Btx-Verbindung besteht die Möglichkeit, mit *88 # in den elektronischen Briefkasten zu sehen. Diese Seite zeigt jetzt auf einen Blick neben dem Namen des Absenders und dem Absendedatum mit Uhrzeit auch die Teilnehmer-/Mitbenutzernummer. Werbemitteilungen sind jetzt mit „W" gekennzeichnet. Aus der Auflistung kann die Btx-Post entweder gelesen oder ungelesen gespeichert bzw. direkt gelöscht werden.

Nunmehr werden die vollen Btx-Gebührensätze (bis jetzt nur zur Hälfte) berechnet. Wie schon seit der Gebühreneinführung zu beobachten war, ist die Zusendung von Werbemitteilungen weiter stark zurückgegangen. Ich gehe davon aus, daß das Problem der unerwünschten Zusendung von Werbung durch Btx damit gelöst ist.

Der Wirkbetrieb des *Elektronischen Telefonbuches* hat begonnen. Es soll durch Verbesserungen des Suchverfahrens und durch Sondersuchen nach Namensteilen, nach ähnlicher Schreibweise und im Nahbereich des Zielortes die gewünschte Rufnummer anzeigen. Der Befürchtung, mit dem Elektronischen Telefonbuch könne ein bundesweites Adreßregister entstehen, wird dadurch entgegengewirkt, daß der Wohnort eines Teilnehmers bei der Suche bekannt sein muß.

Anbieterprüfungen

Erneut habe ich Eingaben und Hinweise über Btx erhalten, die Verstöße gegen den Btx-Staatsvertrag betrafen. Dabei wurde vor allem die Möglichkeit der individuellen *Farbgestaltung* beim Aufbau von Text und Hintergrund zu *Manipulationen* ausgenutzt. Von einem Anbieter wurden bei Antwortseiten personenbezogene Daten verdeckt abgefragt, indem diese Daten in der gleichen Farbe wie die Hintergrundfarbe abgesetzt wurden. Dieser Text wird erst beim Drücken der Attribute-Taste (Schwarzweißabbildung) sichtbar.

In einem anderen Fall wurde der gleiche Farbtrick angewandt, jedoch wurde hierbei - auf den ersten Blick unbemerkt - die Einwilligung zur weiteren Verwendung der personenbezogenen Daten eingeholt. Dies geschah, ohne daß vor bzw. nach dem Aufruf dieser Seite die Zustimmung des Teilnehmers abverlangt wurde.

Ich habe die Beschwerden an die zuständige Aufsichtsbehörde weitergeleitet. Alle beanstandeten Seiten wurden korrigiert bzw. gelöscht.

Beim *Verkehrsamt* wurde im Oktober 1987 mit der Erprobung eines Btx-Reservierungssystems begonnen, das eine Hotelreservierung durch Btx-Teilnehmer - vornehmlich auch für Berlin-Besucher von öffentlichen Btx-Geräten aus - ermöglichen soll. Das Verfahren, das von einem Software-Unternehmen in Zusammenarbeit mit einem Hersteller entwickelt wurde, ist über einen externen Rechner an das Btx-System angebunden. Bei der bis mindestens Januar 1988 laufenden Erprobung werden Hotels, Hotelpensionen und Pensionen aufgeschlüsselt nach Kategorien, Preisen und Stadtbezirken ins System aufgenommen, die dann direkt gebucht werden können.

Dabei werden die Namen der Teilnehmer ins System übernommen; sodann wird vom Verkehrsamt ein Schreiben ausgedruckt und an die gewählten Unterkünfte weitergeleitet. Die Namen werden dann unverzüglich gelöscht. Damit entspricht das Verfahren Art. 9 Btx-Staatsvertrag.

Der *Polizeipräsident in Berlin* hat sich frühzeitig an Bildschirmtext beteiligt. Dabei spielt die Fahndung mit Hilfe des Systems eine besondere Rolle. Hierzu war zu klären, ob und aufgrund welcher Rechtsgrundlage die Veröffentlichung von Personalien und Fotografien gesuchter Personen zulässig ist. Der Btx-Staatsvertrag verweist hier auf die allgemeinen datenschutzrechtlichen Zulassungsvoraussetzungen, wegen der Subsidiarität der Datenschutzgesetze somit auf die strafprozessualen und polizeirechtlichen Befugnisnormen. Diese finden sich für Steckbriefe in § 131 StPO, wenn diese Vorschrift auch die nötige Normenklarheit insbesondere bezüglich des zulässigen Inhalts eines Steckbriefes vermissen läßt. Für die Veröffentlichung von Fahndungsfotos enthält § 24 Kunsturhebergesetz eine spezielle Befugnisnorm. Gegen dieses Btx-Angebot des Polizeipräsidenten bestehen damit keine datenschutzrechtlichen Bedenken.

Mit Risiken für die Persönlichkeitsrechte verbunden sind Angebote, in die die Teilnehmer beliebige Nachrichten für andere Teilnehmer einstellen können. Die Problematik dieser *Pinnwände* beleuchtet folgender Fall: Unter einer verdeckten Absenderangabe stellte ein Unbekannter (möglicherweise ein Schüler) einen Text ein, in dem eine Frau (Lehrerin) unter Angabe ihrer Telefonnummer obszöne Angebote macht. Daraufhin kam es zu erheblichen Belästigungen dieser Frau. Fraglich ist, wie in solchen Fällen der Urheber festzustellen ist.

Unter den Datenschutzbeauftragten besteht Einigkeit, daß die Post für diese Zwecke Daten nicht speichern bzw. auswerten darf. Vielmehr wird es als Aufgabe des Pinnwand-Anbieters angesehen, möglicherweise durch die Erhebung von Daten der Teilnehmer zumindest den Urheber schadensersatzrelevanter Texte ermitteln zu können. Die Erhebung wäre insoweit für die Abwicklung des Pinnwand-Angebots erforderlich (Art. 9 Btx-Staatsvertrag) und damit datenschutzrechtlich zulässig.

4.2 Kabelpilotprojekt

Da weiterhin im Rahmen des Kabelpilotprojektes nur einfache *Verteildienste* angeboten werden, bei denen eine Verarbeitung personenbezogener Daten nicht erforderlich ist, entstanden datenschutzrechtliche Probleme auch im Berichtsjahr nicht. Die Erweiterung des Kabelpilotprojektgesetzes auf terrestrische Frequenzen birgt wegen des Verteilcharakters ebenfalls keine datenschutzrechtlichen Probleme.

Die nächste Stufe des Kabelpilotprojekts, nämlich die Einführung von *Verteildiensten auf Abruf* (insbesondere Pay-TV), konnte auch in diesem Jahr nicht realisiert werden. Ursache für den zumindest vorläufigen Verzicht auf Pay-TV sind nicht Probleme der technischen Realisierbarkeit, sondern ein mangelndes Interesse von Anbietern. Damit entgeht dem Berliner Projekt allerdings die Chance, ein besonders geeignetes *datenschutzfreundliches Abrechnungssystem* zu erproben: Unterdessen wurde von einer Herstellergruppe ein Angebot unterbreitet, das den Anforderungen des Datenschutzes auf eine nutzungsneutrale Abrechnung in besonderem Maße entspricht. Dem Teilnehmer wird dabei ein Kontingent von Nutzungseinheiten verkauft, das in seinem Entschlüsselungsgerät gespeichert ist und sich entsprechend der Nutzung verbraucht. Wenn das Kontingent erschöpft ist, kann gegen Bezahlung ein neues Kontingent bestellt werden. Auf diese Weise entsteht keine individuelle Nutzungsdokumentation; es wird nicht festgehalten, wer was wann sehen will oder gesehen hat. Bestrebungen, dieses System zumindest in einem beschränkten kommerziellen Umfang zu nutzen, würden von mir begrüßt werden: Diese Technikgestaltung zeigt, daß bei hinreichenden Bemühungen die Anforderungen des Datenschutzes entgegen anders lautenden Behauptungen sehr wohl in technische Verfahren umgesetzt werden können.

Eine andere Entwicklungslinie von Abrufdiensten wird von mir mit Aufmerksamkeit verfolgt: In Zusammenarbeit mit der posteigenen Firma DETEKOM, die in Berlin ein Versuchsprojekt zur Erprobung der Breitbandkommunikation mit Glasfasertechnik betreibt (BERKOM), hat die Projektgesellschaft Kabelkommunikation Berlin (PK Berlin) bei der Internationalen Funkausstellung 1987 ein *Breitband-Dialogsystem* erprobt. Dieses System erlaubt, anders als bei Pay-TV, das nur das Verfolgen laufender Sendungen gestattet, den individuellen Abruf stehender und bewegter Bilder über Breitband. Die Präsentation bereitete einen Feldversuch vor, bei dem über zwölf öffentlich zugängliche Terminals ein Stadtinformationssystem abgerufen werden soll. Es beteiligen sich dabei mit unterschiedlichen Programmangeboten das Senatspresseamt, das Verkehrsamt Berlin, der Museumspädagogische Dienst, die Technologietransfergruppe der TU Berlin sowie der Senator für Schulwesen, Berufsausbildung und Sport.

Das Breitbanddialogsystem funktioniert im Textbereich wie Bildschirmtext, benötigt jedoch einen besonderen Rechner, der das Zusammenwirken zwischen Benutzeranforderungen und Bildplattenspieler für Bilder und Filme steuert. Vorläufig ist auch dieses System anonym. Teilnehmer werden nicht registriert, da bei ihnen keine Gebühren erhoben werden und personenbezogene Daten daher nicht gespeichert werden müssen.

4.3 Andere Telekommunikationsdienste

Fernwirkdienste

Unter Begleitung von publizistischer Begleitmusik wie „das Telefon wird zum Alleskönner" oder „elektronischer Zauberer vertreibt Einbrecher" wurde im Juli 1987 von der Bundespost offiziell der Betriebsversuch *TEMEX* begonnen. Die gesetzlichen Rahmenbedingungen in § 53 Kabelpilotprojektgesetz (KPPG), die besonders hohe datenschutzrechtliche Anforderungen stellen, können sich nun in der Praxis bewähren.

Die Berliner Wasserwerke spielen als Projektteilnehmer eine Schlüsselrolle bei der Erprobung eines von mir geforderten datenschutzgerechten elektronischen Meß- und Zählgerätes. Die Berliner Wasserwerke testen seit diesem Herbst einen *Wasserzähler* mit einer „intelligenten" elektronischen Kapsel. Er wird über das Telefonnetz zu vertraglich zuvor festgelegten Zeitpunkten die jeweiligen Verbrauchswerte übermitteln. Der von zwei deutschen Herstellern entwickelte Wasserzähler ist mit einer Langzeitbatterie ausgerüstet, die eine Daueranzeige gewährleistet. Die LCD-Anzeige ist so ausgelegt, daß eine Ziffernfolge sowie die Fließrichtung und der Ladezustand der Batterie angezeigt werden können. Durch Betätigung eines unter dem Deckglas angebrachten elektronischen Schalters, der mit einem kleinen Magneten aktiviert wird, zeigt die Ziffernfolge innerhalb von ca. 7,5 Sekunden die nachstehenden Funktionen an:

1. Funktionskontrolle; Anzeige aller vorhandenen Segmente des Displays
2. Löschen der Anzeige
3. Anzeige des Zählerstandes bei der letzten elektronischen Auslesung
4. Anzeige der Anzahl der Zugriffe (datenschutzrechtlich relevante Zahl)
5. Anzeige des Durchflusses.

Diese Daten sind dem Kunden jederzeit zugänglich. Bei der Fernübertragung wird dem Datenpaket noch die Identifikationsnummer des Wasserzählers hinzugefügt.

Bei jedem elektronischen Fernmeßvorgang, bei dem die Verbrauchswerte an die erhebende Stelle übermittelt werden, wird die oben unter Ziff. 4 als Zugriffszahl bezeichnete Anzeige um eine Stelle erhöht. Somit wird jede Datenübermittlung gezählt. Der Kunde hat damit jederzeit die Möglichkeit, eine Kontrolle über die Ablesehäufigkeit und den Ablesezeitpunkt durchzuführen. Er kann außerdem den Zählerstand zum Zeitpunkt der letzten elektronischen Ablesung zur Anzeige bringen. Der Zählerstand der letzten Ablesung, die Zugriffszahl und zusätzlich das Datum und die Uhrzeit werden in die dem Kunden zugestellte Rechnung aufgenommen. Der Kunde kann somit die Richtigkeit der Rechnung prüfen. Da allen Kunden vom Wasserversorgungsunternehmen vorab die Häufigkeit und der ungefähre Zeitpunkt der Fernablesung *(Ablesefenster)* mitgeteilt wird, kann die Richtigkeit dieses Verfahrens auch zwischenzeitlich jederzeit überprüft werden. Zwar ist eine auf die Sekunde genaue Fernablesung nicht vorgesehen und kann von der Post technisch auch nicht realisiert werden, angesichts der durch die Höhe der Zugriffszahl fixierten Anzahl der Ablesevorgänge ist eine mißbräuchliche Ablesung aber jederzeit feststellbar und kann vertragsrechtlich sanktioniert werden. Die datenschutzrechtlichen Sicherheitsvorkehrungen erscheinen unter diesen Bedingungen so hoch, daß sie im jetzigen Zeitpunkt vorbehaltlich weiterer durch den Betriebsversuch zu gewinnender Erkenntnisse als positiv bewertet werden können.

Weitere Versuche sind aus den Bereichen des Bank- und Kreditwesens, der Automatenaufsteller, des Bewachungsgewerbes und der Alarmanlagenbetriebe zu erwarten.

Sprachspeicherdienst

Die bisherigen Telekommunikationsdienste waren durch eine relativ klare Trennung zwischen analoger (Übermittlung von Sprache und Bildern) und diskreter Datenübermittlung (Schriftzeichen) gekennzeichnet. Die Abspeicherung von Informationen zum Abruf durch den Adressaten *(Mail-Box)* war bisher nur mit schriftlichen Mitteilungen möglich. Die neuen technischen Entwicklungen des Telekommunikationsnetzes und die damit verbundene Digitalisierung ermöglichen künftig, auch analoge Nachrichten zu hinterlegen. Die Post bietet für sprachliche Informationen inzwischen einen derartigen Dienst an *(Voice-Box)*. Diese Entwicklung zeigt, daß die traditionelle Trennung einzelner Formen der Kommunikation künftig aufgehoben wird zugunsten verschiedener Mischformen. Für das Datenschutzrecht bedeutet dies, daß die starke Betonung von Daten im Sinne einzelner Zeichen hinter einer Betrachtung zurücktreten muß, die auch Sprache und Bilddarstellung einschließt.

4.4 Telekommunikationsordnung

Zum 1. Januar 1988 tritt die Telekommunikationsordnung (TKO) in Kraft, die die bisherigen Benutzungsordnungen im Bereich des Fernmeldewesens ersetzt. Die ursprüngliche, am 5. November 1986 verkündete Fassung war von den Datenschutzbeauftragten in einer Reihe von Punkten kritisiert worden[1]; es fehlten ferner Regelungen insbesondere zu Fernwirkdiensten (TEMEX-Dienst) und Breitbandverteildiensten.

Noch vor Inkrafttreten der Telekommunikationsordnung wurde am 15. Juni 1987 eine Verordnung zur Veränderung der Telekommunikationsordnung verkündet, in der die Telekommunikationsordnung ergänzt wurde.

Von den Forderungen der Datenschutzbeauftragten wurde insbesondere diejenige nach einer Regelung der Verarbeitung von Daten über Vergleichszählung und Feststellen ankommender Wählverbindungen (*Fangschaltung*) aufgegriffen (§ 453). Die ausführliche Regelung enthält nunmehr normenklare Bestimmungen zum Verfahren und dem Datenumfang bei diesen besonderen Betriebsformen.

Breitbandverteildienste und TEMEX-Dienste werden ebenfalls geregelt. Allerdings greift die besondere Vorschrift über den Datenschutz im TEMEX-Dienst (§ 458) die Vorgabe des KPPG (Erkennbarkeit, Abschaltbarkeit) nicht auf, sondern verpflichtet den Fernwirkanbieter lediglich, in eigener datenschutzrechtlicher Verantwortung die Kunden insbesondere über die Voraussetzungen, den Umfang und den Zeitpunkt der Informationsübermittlung zu unterrichten.

Geht man davon aus, daß dem Bundesgesetzgeber bei der Ausgestaltung der Telekommunikationsdienste auf Seiten der Teilnehmer jedenfalls aus der fernmelderechtlichen Kompetenz keine Zuständigkeit zusteht, ist diese Beschränkung konsequent. Sie belegt aber, daß die Länder nach Inkrafttreten der TKO nunmehr auch den *nutzungsrechtlichen Rahmen* der künftigen TKO gesetzlich regeln müssen. Eine solche Rahmenregelung könnte ähnlich wie der in diesem Jahr ebenfalls verabschiedete Rundfunkstaatsvertrag, der Regelungen zum Jugend- und Ehrschutz, nicht aber zum Datenschutz enthält, in Form eines Staatsvertrages geschaffen werden. Ziel müßten möglichst einheitliche Regelungen zur (datenschutzfreundlichen) Nutzung der über den reinen Datentransport hinausgehenden Dienste (Mehrwertdienste) sein. Der von mir geleitete Arbeitskreis Medien der Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat erste Initiativen zur Entwicklung eines entsprechenden Vorschlages unternommen.

4.5 Internationale Aspekte

Arbeitskreis Medien der Internationalen Konferenz der Datenschutzbeauftragten

Anläßlich der Funkausstellung 1987 erarbeitete der Arbeitskreis Medien der Internationalen Konferenz der Datenschutzbeauftragten einen Beschlußvorschlag, der auf der Plenumssit-

[1] Vgl. Jahresbericht 1986, Ziff. 3.4

zung der Internationalen Konferenz in Quebec Ende September angenommen wurde[1] und der im Hinblick auf die aktuellen Entwicklungen auf dem Gebiet der internationalen Telekommunikation Maßnahmen zur internationalen Regelung des Datenschutzes verlangt.

Medienforum Berlin 1987

Ebenfalls im Zusammenhang mit der Funkausstellung gestaltete ich im Rahmen des Medienforums 1987 den Kongreßteil „Datenschutz und Medienrecht". Hierzu konnten prominente Referenten aus dem In- und Ausland gewonnen werden, die über die neuesten Entwicklungen auf dem Gebiet des Datenschutzes und der Datensicherung bei neuen Netzen und neuen Diensten berichteten. So wurden beispielsweise die entsprechenden Aktivitäten der Europäischen Gemeinschaften dargestellt, Methoden der Verschlüsselung in Telekommunikationsnetzen erörtert und die neuesten Entwicklungen bei dem Datenschutz in der Bankautomation in den USA vorgestellt.

Die Mitglieder des Arbeitskreises Medien der Internationalen Konferenz der Datenschutzbeauftragten nahmen im Rahmen ihrer Sitzung an dieser Veranstaltung teil. Bei einem Empfang des Präsidenten des Abgeordnetenhauses sowie aus einem Grußwort des Senators für Kulturelle Angelegenheiten wurde das große Interesse auch politischer Verantwortungsträger Berlins an einer datenschutzgerechten Ausgestaltung der Telekommunikationsdienste erkennbar.

5. Weitere Fragen aus der Kontroll- und Beratungspraxis

5.1 Finanzwesen

Steuerverwaltung

Jedermann weiß aus eigener Erfahrung, daß im Besteuerungsverfahren eine Vielzahl von Daten erhoben wird, die einen Einblick in die berufliche Stellung und die persönliche Lebensführung vermitteln. Der Gesetzgeber hat die Finanzbehörden in der Abgabenordnung (AO) mit weitgehenden Befugnissen bei der Datenerhebung ausgestattet, um durch exakte Kenntnis der finanziellen Situation des Steuerbürgers eine gleichmäßige und gerechte Besteuerung durchführen zu können. Zum Ausgleich der umfangreichen Mitwirkungs- und Offenbarungspflichten, die das Steuerrecht dem Bürger auferlegt, haben die Finanzbehörden das Steuergeheimnis zu wahren. Nach § 30 AO dürfen in einem Steuerverfahren oder in einem gerichtlichen Verfahren in Steuersachen bekannt gewordene Verhältnisse grundsätzlich nicht unbefugt offenbart oder verwertet werden. Die Ausnahmen von dieser Regel sind in § 30 AO ausdrücklich und abschließend aufgezählt. Daß die Wahrung des Steuergeheimnisses nicht nur bei der Aktenführung der Finanzbehörden in Steuersachen gilt, hat der Gesetzgeber durch die Einfügung des § 30 Abs. 6 AO im Zuge des *Steuerbereinigungsgesetzes 1986* deutlich gemacht: Für automatisierte Verfahren gelten die Vorschriften des Steuergeheimnisses ebenso. Der Bundesminister für Finanzen kann durch Rechtsverordnung bestimmen, welche Maßnahmen gegen den unbefugten Abruf von Daten zu treffen sind. Insbesondere kann er nähere Regelungen treffen über die Art der Daten, deren Abruf zulässig ist und über den Kreis der Zugriffsberechtigten.

In diesem Jahr wurde der Entwurf einer *Steuerdatenabrufverordnung* vorgelegt. Bei der Diskussion wird darauf zu achten sein, einer Datenstreuung, die mit automatisierten Abrufverfahren verbunden ist, durch restriktive Regelungen vorzubeugen.

Zur vollständigen Erfassung von Steuerquellen haben seit jeher andere Behörden den Finanzämtern aufgrund von Verwaltungserlassen und Vereinbarungen *Kontrollmitteilungen* über bestimmte, steuerlich relevante Sachverhalte gegeben, so z. B. über Nebentätigkeiten und Vergabe von Subventionen. Es bestand Einigkeit darüber, daß derartige Mitteilungen nicht ohne gesetzliche Grundlage erfolgen dürfen, damit der Betroffene dem Gesetz entnehmen kann, in welchen Fällen Meldungen an das Finanzamt gemacht werden. Ebenfalls durch das Steuerbereinigungsgesetz 1986 ist mit § 93 a AO eine Ermächtigungsgrundlage für den Erlaß von Rechtsverordnungen über „Allgemeine Mitteilungspflichten" der Behörden gegenüber Finanzverwaltungen in das Steuerrecht eingebracht worden.

Diese Vorschrift bringt Rechtsklarheit im Bereich der Kontrollmitteilungen und ist aus Gründen des Persönlichkeitsschutzes zu begrüßen. Die Einzelheiten des Mitteilungsverfahrens sollen in einer *Kontrollmitteilungsverordnung* enthalten sein, die derzeit noch erarbeitet wird. Darin sind auch die vorherige Unterrichtung des Betroffenen, die aus Gründen der Transparenz bei jeder Mitteilung erfolgen sollte, und Ausnahmen von der Mitteilungspflicht zu regeln. Dann könnte bei Bagatellsummen auf die Mitteilung verzichtet werden. Wegen der Einzelheiten müssen die Erörterungen zur Kontrollmitteilungsverordnung, die zwischen den Finanzverwaltungen und den Datenschutzbeauftragten derzeit stattfinden, abgewartet werden.

Auch die Eingaben betreffen meist die Frage, ob bestimmte *Datenerhebungen im Besteuerungsverfahren* zulässig sind. Die Befugnisse der Finanzbehörden sind, wie dargestellt, umfangreich, jedoch nicht schrankenlos. So können die Finanzbehörden eine Auskunft nur verlangen, wenn sie zur Sachverhaltsaufklärung geeignet und notwendig ist, die Beantwortung für den Betroffenen möglich und seine Inanspruchnahme erforderlich, verhältnismäßig und zumutbar ist. Ob diese Voraussetzungen vorliegen, ist in manchen Fällen zweifelhaft: So haben sich mehrere Bürger darüber beschwert, daß ihr Finanzamt bei der Absetzung von Kosten für besuchsweise Aufnahmen von Bürgern aus der DDR oder Ost-Berlin *Ablichtungen der Pässe* der Besucher zum Nachweis für deren Anwesenheit verlangt hat. Tatsächlich sind auch andere Nachweise anzuerkennen; der Finanzsenator hat die Finanzämter hierauf nochmals hingewiesen.

In einem weiteren Beispielsfall hatte der Petent an einer *Bildungsreise* teilgenommen und die Aufwendungen als Werbungskosten geltendgemacht. Das Finanzamt bestritt den beruflichen Anlaß der Reise und verlangte eine Teilnehmerliste. Bevor hier die Daten einer Vielzahl von an dem Steuerverfahren unbeteiligten Personen erfragt werden, hätte eine Bestätigung des Veranstalters und ein Einblick in das Programm genügt, um dem Finanzamt ausreichende Erkenntnisse für die steuerliche Bewertung zu vermitteln.

Von großer Bedeutung für den Bürger ist bei der Datenerhebung die Aufklärung über die Rechtsgrundlage. Auch hier sind Verbesserungen angezeigt[1].

Zu beanstanden war weiter die Übermittlung der Daten von Steuerbevollmächtigten im Rahmen der Volkszählung[2].

Zur Unterstützung der Besteuerung beabsichtigt der Senator für Finanzen, eine *neue technische Infrastruktur* für die Durchführung seiner *ADV-Verfahren* (Berliner Verfahren) einzuführen. Dies wird derzeit in einigen Finanzämtern erprobt. Dabei werden die Finanzämter unter Verwendung intelligenter Terminals (PC's) über zwischengeschaltete Knotenrechner auf das zentrale Rechenzentrum der Oberfinanzdirektion zugreifen.

Der Einsatz eines solchen Netzes führt zu neuen Risiken[3], denen erhöhte Sicherungen gegenüberstehen müssen. Ich habe im Vorfeld mit Vertretern des Senators für Finanzen und der Oberfinanzdirektion Gespräche über die erforderlichen Maßnahmen geführt. Insbesondere wurde dabei das technische Sicherungskonzept eingehend erörtert. Die Realisierung wird 1988 überprüft werden.

Haushaltswesen

Das Verfahren „Automatisiertes Haushaltswesen (AHW)", das seit Mitte der sechziger Jahre existiert, wird nach dem Scheitern eines Entwicklungsverbundes mit anderen Bundesländern nun vom Senator für Finanzen neu konzipiert. Danach sollen die

[1] Vgl. Anlage 1

[1] Vgl. 5.7
[2] Vgl. 2.3
[3] Vgl. 3.1

Sachbearbeiter mit intelligenten Terminals am Arbeitsplatz, die mit einer zentralen ADV-Anlage verbunden sind, die erforderlichen Daten direkt eingeben oder abrufen können. Das Spektrum der Anwender reicht von den Haushaltsämtern in den Bezirken über die Haushaltsabteilungen und -referate beim Senator für Finanzen bis hin zu den Wirtschaftsstellen. Datenschutzrechtliches Hauptproblem ist der geplante On-line-Zugriff auf die personenbezogenen Daten in den Personenkonten.

Grundsätzlich wird darauf zu achten sein, daß der On-line-Zugriff der beteiligten Stellen sich auf jene Daten beschränkt, die sie in eigener Zuständigkeit benötigen. Dies ist durch technische Zugriffskontrollmaßnahmen zu gewährleisten.

5.2 Gesundheit und Soziales

AIDS

Im Mittelpunkt der gesundheitspolitischen Diskussion steht nach wie vor die Immunschwächekrankheit *AIDS*. Einen breiten Raum nehmen dabei Fragen ein, die von datenschutzrechtlicher Brisanz sind. Dies ergibt sich nicht nur daraus, daß medizinische Daten in jedem Fall einer strengen Geheimhaltungspflicht unterliegen, sondern auch daraus, daß AIDS gerade ein Eindringen in Bereiche der Intimsphäre erforderlich macht, die bisher dem staatlichen Interesse weitgehend entzogen schienen.

Am heftigsten erörtert wird die Frage, ob entsprechend den Bestimmungen des Bundesseuchengesetzes und des Geschlechtskrankheitengesetzes eine *Meldepflicht* für alle Erkrankten und Infizierten eingeführt werden soll. Dabei ist deutlich zwischen einer personenbezogenen Meldepflicht, die in vollem Umfang datenschutzrechtlichen Kriterien standhalten muß, und anonymisierten Verfahren zu unterscheiden, bei denen datenschutzrechtliche Überlegungen nur hinsichtlich des Grades der Anonymisierung sowie des damit verbundenen Risikos der Reindividualisierung angestellt werden müssen.

Entgegen Tendenzen in einem anderen Bundesland und radikalen Stimmen in der öffentlichen Diskussion hat der Senator für Gesundheit und Soziales wiederholt betont, daß er die Einführung einer personenbezogenen Meldepflicht für ein ungeeignetes Mittel zur Bekämpfung der Krankheit hält. Dies ist zu begrüßen: Ohne gesetzliche Grundlage wäre wegen der Bedeutung der Maßnahme eine derartige Meldepflicht ohnehin rechtswidrig. Aber auch eine gesetzliche Regelung würde einer verfassungsrechtlichen Prüfung nicht standhalten. Eine umfassende Meldepflicht für alle Ärzte und Labors würde einen massiven Eingriff in das Grundrecht auf informationelle Selbstbestimmung der Betroffenen darstellen. Selbst wenn man von einem hohen Allgemeininteresse an der Registrierung aller Betroffenen ausgeht, müßte eine gesetzliche Regelung am Verhältnismäßigkeitsgrundsatz gemessen werden, d. h. die Maßnahme müßte geeignet sein, den geringstmöglichen Eingriff darstellen und in einem angemessenen Verhältnis zum angestrebten Zweck stehen. Eine personenbezogene Meldepflicht würde bereits an der Geeignetheit scheitern: Die überwiegende Mehrheit der Experten geht davon aus, daß eine Meldepflicht lediglich die Bereitschaft der Betroffenen zu freiwilligen Maßnahmen vermindern würde; Erfahrungen in Schweden, wo eine Meldepflicht eingeführt wurde, bestätigen dies. Somit würde gerade das Gegenteil dessen erreicht, was bezweckt wird. Zur Beobachtung der Ausbreitung der Krankheit sind anonyme Verfahren mit erheblich geringeren Eingriffen für die Betroffenen verbunden. Die Risiken für die Betroffenen, die mit einer Meldepflicht verbunden wären, insbesondere die stets schwebende Gefahr der Isolierung, werden auch angesichts fehlender Therapiemöglichkeiten durch den Verwendungszweck nicht gedeckt.

Anders verhält es sich mit *anonymen Meldungen*. Bereits seit Jahren melden Ärzte und Labors auf freiwilliger Basis an verschiedene Forschungsinstitutionen die ihnen bekannten Fälle. So sammelt das Landesinstitut für Tropenmedizin Berlin entsprechende Erkenntnisse. Das Bundesgesundheitsamt führt ein Register, das ebenfalls epidemiologische Erkenntnisse ermöglichen soll. Der für diese Erhebungen verwendete Fallberichtsbogen war zunächst nicht hinreichend anonymisiert. Inzwischen wird eine verbesserte Fassung verwendet, an der allerdings ebenfalls noch Kritik geübt wird. Die Verordnung über die Berichtspflicht für positive HIV-Bestätigungstests vom 9. September 1987[1] begründet darüber hinaus für einen kurzen Zeitraum eine Meldepflicht für die positiven Ergebnisse von HIV-Tests, mit denen das Humane Immunschwäche-Virus (HIV) nachgewiesen wird. Dabei sind die Daten über das bei der freiwilligen Meldung verwendete Maß hinaus anonymisiert.

Von den regelmäßigen Meldungen zu unterscheiden ist die Frage, unter welchen Voraussetzungen personenbezogene Daten Betroffener im Einzelfall weitergegeben werden dürfen. Zugrundezulegen sind dabei in erster Linie die *Offenbarungsregelungen* der ärztlichen Berufsordnung sowie im Krankenhausbereich des § 26 Landeskrankenhausgesetz. Soweit nicht der Behandlungszusammenhang oder die ausdrückliche Einwilligung des Betroffenen die Weitergabe rechtfertigt, kann nur eine *Güterabwägung des Arztes* zwischen Rechten der Betroffenen und höheren Rechtsgütern (§ 2 Abs. 4 Berufsordnung der Ärztekammer) oder die Erforderlichkeit für die Abwehr von Gefahren für Leib oder Leben des Patienten oder eines Dritten (§ 26 Abs. 3 Ziff. 3 Landeskrankenhausgesetz) die Weitergabe rechtfertigen, Dabei ist dem informationellen Selbstbestimmungsrecht auch im Einzelfall großes Gewicht einzuräumen.

Ein Beispiel für die Problematik war Gegenstand eines Rundschreibens des Senators für Gesundheit und Soziales[2]: Bei einer stationären Krankenhausbehandlung wurde bei einer Prostituierten AIDS diagnostiziert. Die Frau gab bei der Entlassung zu verstehen, daß sie ihre Tätigkeit weiter ausüben wollte. Fraglich war, ob das Krankenhaus die zuständigen Ordnungsbehörden benachrichtigen darf. Der Senator für Gesundheit und Soziales stützte dies zunächst auf die allgemeine polizeiliche Generalklausel in § 14 Allgemeines Sicherheits- und Ordnungsgesetz (ASOG). Ich habe darauf hingewiesen, daß diese Vorschrift keine geeignete Befugnisnorm ist, da sie zwar der Gesundheitsbehörde als Ordnungsbehörde, nicht aber den Krankenhäusern Befugnisse einräumt. Auch die Berufung auf § 34 Strafgesetzbuch, nach dem tatbestandsmäßig vorliegende Straftaten (Verletzung der ärztlichen Schweigepflicht) gerechtfertigt sind, wenn durch die Handlung die Verletzung erheblicher Rechtsgüter abgewendet werden kann, kann keine Befugnis für die Übermittlung verschaffen, sondern allenfalls den Arzt straffrei stellen. Es muß vielmehr dabei bleiben, daß im Vordergrund nicht polizeirechtliche Erwägungen stehen, sondern ausschließlich der Arzt unter Berücksichtigung der Persönlichkeitsrechte der Betroffenen eine Entscheidung trifft, die den besonderen Gefährdungen Dritter Rechnung trägt.

Die Verarbeitung personenbezogener Daten der Betroffenen setzt mit der Datenerhebung ein, bei AIDS mit der Durchführung eines *HIV-Tests*. Die Erforderlichkeit eines derartigen Tests ist zwar zunächst ein medizinisches Problem. Wegen der weitgehenden Folgen für die Verarbeitung der erhobenen Daten wiegt aber der datenschutzrechtliche Aspekt ebenso schwer. Für die Verarbeitung der beim Test gewonnenen Daten ist ebenso die Einwilligung der Betroffenen zu fordern wie für die Blutabnahme selbst. Eine Untersuchung gegen den Willen oder ohne Wissen des Betroffenen ist nur aufgrund einer eindeutigen Rechtsgrundlage zulässig. Das gleiche muß dann gelten, wenn die Gewährung subjektiver Rechte oder auch die Ausübung von Ermessensentscheidungen von der Einwilligung in die Untersuchung abhängig gemacht wird. Die diesbezüglichen Diskussionen in verschiedenen Verwaltungsbereichen dauern an (z. B. im Strafvollzug, im Asylverfahren, bei der Einstellung öffentlicher Bediensteter, in der Drogenbehandlung, beim Abschluß von Versicherungsverträgen).

Zu welchen diskriminierenden Folgen eine Kombination von Mängeln führen kann, zeigt folgender Fall: Ohne Wissen eines Krankenhauspatienten wurde ein HIV-Test vorgenommen. Das (negative) Ergebnis des Tests wurde im Krankenblatt am Bett offen ausgehängt, so daß jeder Besucher erfuhr, daß ein derartiger Test durchgeführt wurde. Abgesehen davon, daß der offene Aushang derartiger Krankenblätter von mir mehrfach beanstandet worden ist, bestand hier der zusätzliche Mangel, daß der Eindruck entstand, aufgrund bestimmter Tatsachen sei ein HIV-Test erforderlich gewesen.

[1] BGBl. I, S. 2141
[2] SenGesSoz - II C 1 - 540 212 vom 4. August 1986

Einsicht in medizinische Unterlagen

Die Einsicht in medizinische Unterlagen ist bisher noch immer nicht befriedigend geregelt. Dies zeigen die folgenden Eingaben:

In einem Fall wurde versucht, bei der Krankenkasse Einsicht in die vom Arzt angegebenen Diagnosen zu nehmen, nachdem der Arzt selbst die Einsicht verweigert hatte. Die Akteneinsicht wurde für erforderlich gehalten, um einen Nachweis über fehlerhafte Diagnosen durch den Arzt zu führen. Da davon auszugehen ist, daß die Daten der Versicherten bei der *Krankenkasse* dateimäßig gespeichert werden, kann ein Auskunftsanspruch auf § 13 Abs. 1 Bundesdatenschutzgesetz gestützt werden. Zu prüfen war daher, ob die Daten im überwiegenden Interesse eines Dritten (vgl. § 13 Abs. 2 Ziff. 2 Bundesdatenschutzgesetz) geheimgehalten werden müssen. Ich habe darauf hingewiesen, daß eine Krankenkasse nicht verpflichtet ist, das Therapieprivileg zu berücksichtigen, wenn die Berufung darauf durch den Arzt offensichtlich rechtsmißbräuchlich ist. Auf keinen Fall darf das Therapieprivileg dazu genutzt werden, Mängel in der Behandlung zu verdecken. Da die Diagnose zu den objektiven Beurteilungselementen der Krankenunterlagen gehört, muß in der Regel Einsicht gewährt werden.

In einer interessanten Variante begehrte der *Rechtsnachfolger* eines Patienten Akteneinsicht gegenüber dem Rechtsnachfolger des verstorbenen Arztes, der selbst nicht Arzt war. Aus den gleichen Rechtsgründen muß die Einsicht nach § 26 Abs. 1 Bundesdatenschutzgesetz gewährt werden, solange sich nicht aus der Aktenlage ergibt, daß subjektive Beurteilungen des behandelnden Arztes geheimgehalten werden müssen. Ein Therapieprivileg ist als berechtigtes Drittinteresse abzulehnen, wenn sowohl der Patient als auch der Arzt schon verstorben sind. Daß der Rechtsnachfolger eines Verstorbenen zumindest in entsprechender Anwendung datenschutzrechtliche Ansprüche geltend machen kann, ist jedenfalls bei vermögensrechtlichen Angelegenheiten anerkannt.

Suizid-Daten

Aufgrund einer Kleinen Anfrage[1] wurde die Problematik der Datenweitergabe bei Selbstmordversuchen von den Berliner Krankenhäusern an die Polizei aktuell. Ich habe dazu folgende Auffassung vertreten: Gemäß §§ 5 und 6 Abs. 2 Bestattungsgesetz beendet der Arzt die Leichenschau, wenn er Anhaltspunkte dafür entdeckt, daß der Patient nicht eines natürlichen Todes gestorben ist, und benachrichtigt sofort die Polizeibehörde. Offenbarungspflichten aus §§ 159, 161 Strafprozeßordnung (StPO) bestehen nicht, weil Ärzte oder Krankenhäuser in § 169 StPO nicht benannt sind bzw. keine Behörden i. S. des § 161 StPO sind. Auch aus § 11 Abs. 2 Landeskrankenhausgesetz ergibt sich keine Offenbarungsbefugnis, da diese Vorschrift lediglich die rechtzeitige Verständigung von Angehörigen ermöglichen soll.

Wenn ein Patient den Suizidversuch überlebt, dürfen ohne seine Einwilligung keine Behandlungsdaten an andere Behörden übermittelt werden, es sei denn, daß eine Rechtsvorschrift dies ausdrücklich zuläßt. Gerade bei suizidgefährdeten Patienten ist das Vertrauensverhältnis zum Arzt von existenzieller Bedeutung für eine weitere therapeutische Betreuung, die nach § 3 Abs. 3 Gesetz über psychisch Kranke (PsychKG) nur auf freiwilliger Basis geleistet werden kann. Sollten allerdings bei der Einlieferung des Patienten Kosten entstanden sein, so ist der Eingelieferte gem. § 12 Abs. 2 Allgemeines Sicherheits- und Ordnungsgesetz (ASOG) dem Kostenträger zum Ersatz verpflichtet. Name und Anschrift der eingelieferten Person können ausschließlich zu diesem Zweck offenbart werden, denn die hilfeleistende Stelle darf nicht deshalb schlechter gestellt werden, weil sie auf die Feststellung der Identität oder anderer erkennungsdienstlicher Maßnahmen zunächst verzichtet hat, um das Leben des Betroffenen zu retten. Der Betroffene sollte allerdings die Möglichkeit erhalten, die Kosten selbst zu tragen, um dadurch die Datenweitergabe zu vermeiden.

[1] Nr. 2102 in Mitteilungen des Präsidenten Nr. 107, Drs. 10/956 vom 26. September 1986

5.3 Inneres

Amtliche Statistik

Die *freiwilligen Mikrozensus-Testerhebungen* geben Aufschluß über den Stand der statistischen Methodenentwicklung und ihrer praktischen Anwendung. Schon der Vergleich zwischen den Testerhebungen 1985 und 1986 zeigt eine interessante Entwicklung. Während bei der Testerhebung 1985 die Antwortquote in Berlin bei 39,8 % (im Bundesgebiet: 49,6 %) lag, stieg sie 1986 in Berlin auf 63,9 % (im Bundesgebiet: 65 %). Das Statistische Landesamt führt diese Steigerung unter anderem darauf zurück, daß bei der Erhebung 1985 Befragte, die bei der ersten Kontaktaufnahme gegenüber dem Interviewer jede Beteiligung abgelehnt hatten, nicht mehr angeschrieben oder erneut um ihre Beteiligung gebeten wurden. Demgegenüber hat das Statistische Landesamt 1986 in solchen Fällen den Befragten den Zweck der Testerhebung schriftlich nochmals ausführlich erläutert und sie argumentativ zur Mitwirkung zu bewegen gesucht. Dagegen hat die alternative Verwendung von amtlichen und nichtamtlich wirkenden Formularen 1986 nicht zu signifikanten Unterschieden im Antwortverhalten geführt.

Die Steigerung der Antwortquote um mehr als 15 % zwischen 1985 und 1986 zeigt, daß sich durch die Veränderung der Organisation und einer Intensivierung der Interviewerschulung durchaus ein verbessertes Antwortverhalten bei freiwilligen Erhebungen erreichen läßt. Es bleibt abzuwarten, ob die letzte nach dem Mikrozensusgesetz vorgesehene freiwiliige Testerhebung, die Ende Oktober/Anfang November 1987 stattfand, zu einer weiteren Erhöhung geführt hat. Bei dieser Erhebung wurde ein Teil der Befragten zunächst nur angeschrieben und lediglich bei ausbleibender Reaktion vom Interviewer aufgesucht. Außerdem wurden erneut unterschiedlich gestaltete Erhebungsunterlagen getestet.

Es ist vorschnell, wenn der Vorsitzende der Deutschen Statistischen Gesellschaft nach dem Ergebnis der Testerhebungen 1985 und 1986 den Schluß zieht, ein Verzicht auf die Auskunftspflicht beim Mikrozensus oder bei der Volkszählung sei ausgeschlossen. Die amtliche Statistik muß ihre verfassungsrechtliche Pflicht zur Prüfung eines Verzichts auf die Auskunftspflicht ernstnehmen.

Auch der Einfluß, den die Auskunftspflicht oder Freiwilligkeit der Teilnahme auf die Qualität der erhobenen Daten haben, sollte verstärkt untersucht werden. Nach den Erfahrungen bei der Volkszählung 1987 spricht vieles dafür, daß aufgrund der Auskunftspflicht nicht nur ein bestimmter Prozentsatz der Befragten die Antwort verweigert hat, sondern daß auch die Qualität der gegebenen Antworten negativ beeinflußt wurde.

Im Gegensatz zum neugefaßten Bundesstatistikgesetz konnte das ebenfalls erforderliche *Landesstatistikgesetz* vor dem Stichtag der Volkszählung 1987 nicht mehr dem Parlament vorgelegt werden. Dies soll nach Auskunft des Senators für Inneres Anfang 1988 geschehen. Bei der Erstellung des Entwurfs bin ich frühzeitig beteiligt worden.

Das Landesstatistikgesetz wird zum großen Teil dem Bundesstatistikgesetz entsprechende Regelungen für Landesstatistiken enthalten. Zusätzlich zu diesen Regelungen sind gesetzliche Grundlagen für die Nutzung personenbezogener Daten aus dem Verwaltungsvollzug für statistische Zwecke und für den Betrieb eines *statistischen Informationssystems (STATIS)* zur vielfältigen Verknüpfung personenbezogener Daten aus unterschiedlichen Quellen erforderlich.

Bei der Regelung mußte vor allem die Forderung des Bundesverfassungsgerichts nach einer Trennung von Statistik und Verwaltungsvollzug berücksichtigt werden. Während Daten, die im Verwaltungsvollzug erhoben werden, einer strikten Zweckbindung unterliegen und nach Erreichung dieses Zwecks zu löschen sind, dienen die für die amtliche Statistik unmittelbar erhobenen Daten (Primärstatistik) verschiedenen, nicht vorhersehbaren Zwecken.

Würde die amtliche Statistik auf diese Weise jederzeit und unbeschränkt auf alle in der Vollzugsverwaltung vorhandenen personenbezogenen Daten für statistische Zwecke zugreifen können, wüßte der Bürger nicht mehr, wer was wann bei welcher Gelegenheit über ihn weiß. Daher muß das Landesstatistikgesetz

eine Rechtsverordnung nach dem Vorbild der Durchführungsverordnung zum Meldegesetz vorsehen, in der festgelegt wird, welche Daten aus welchen Bereichen der Vollzugsverwaltung zu welchem Verwendungszweck an das Statistische Landesamt übermittelt werden dürfen. Der Senator für Inneres hat meine Formulierungsvorschläge im Entwurf für ein Landesstatistikgesetz bisher weitgehend berücksichtigt.

Personaldaten

Im Bereich der Personaldaten stellte das Inkrafttreten einer Teilregelung der Vorläufigen Vorschriften zur Führung von Personalakten den wichtigsten Schritt dar[1], wenngleich wesentliche Regelungen noch folgen müssen[2]. Zu klären waren erneut eine Reihe von Einzelfällen, die zeigen, daß nur eine sorgfältige Abwägung der Interessen der Behörden und der Betroffenen zu datenschutzgerechten Ergebnissen führt.

Ein Bezirksamt wandte sich an mich mit der Frage, ob es verpflichtet sei, der *Kriminalpolizei* Einsicht in eine bestimmte Personalakte im Rahmen eines Ermittlungsverfahrens zu gewähren.

Personaldaten sind - auch soweit sie in Personalakten enthalten sind - nach der Rechtsprechung des Bundesverwaltungsgerichts ihrem Wesen nach geheimzuhalten. Ihre Offenbarung ist nur zulässig, wenn sie zur Wahrung berechtigter Interessen der übermittelnden Stelle oder eines Dritten oder der Allgemeinheit erforderlich ist und dadurch schutzwürdige Belange des Betroffenen nicht beeinträchtigt werden. Das Interesse der Allgemeinheit muß präzisiert und im Hinblick auf die jeweils gewünschten personenbezogenen Daten begründet werden. Der bloße Hinweis auf die öffentliche Sicherheit und Ordnung reicht in diesem Zusammenhang nicht aus. Eine Beeinträchtigung schutzwürdiger Belange liegt dann vor, wenn der Betroffene seine Daten der speichernden Stelle zu ganz bestimmten Zwecken überläßt, der Informationsempfänger die Angaben aber zur Erreichung ganz anderer Ziele verwenden will.

Bei Anlegung dieser Grundsätze ist eine Beeinträchtigung schutzwürdiger Belange bei der Offenbarung von Personaldaten gegenüber der Kriminalpolizei regelmäßig anzunehmen. Die Strafprozeßordnung enthält bisher keine bereichsspezifische Regelung dieser Frage. Bei einer entsprechenden Anfrage der Kriminalpolizei sollte die personalaktenführende Stelle deshalb klären, ob Einwände dagegen bestehen, daß die Einwilligung des Betroffenen eingeholt wird. Will die Kriminalpolizei zunächst ohne Wissen des Betroffenen ermitteln, so muß sie darlegen, daß das Ermittlungsverfahren einen Bezug zum Dienstverhältnis hat, und sie muß darüber hinaus präzisieren, an welchen Informationen, die möglicherweise in der Personalakte enthalten sind, sie interessiert ist. Nur so kann sichergestellt werden, daß eine Datenoffenbarung sich im Rahmen des Erforderlichen hält. Ist die Kriminalpolizei auch hierzu nicht bereit oder in der Lage, so muß sie auf den Weg der Beschlagnahme verwiesen werden.

Die personalaktenführende Stelle hat neben der Prüfung der Erforderlichkeit auch dafür zu sorgen, daß keine Daten offenbart werden, die einem besonderen Berufs- oder Amtsgeheimnis unterliegen und in der Personalakte enthalten sind (Steuerdaten, z. B. die Lohnsteuerkarte; Sozialdaten, z. B. Kindergeldakten). Für diese gelten besondere Offenbarungsbefugnisse.

Umgekehrt muß sichergestellt sein, daß die Kriminalpolizei bei ihrer Bitte um Akteneinsicht nur so viel Informationen an die Dienstbehörde weitergibt, wie zur Überprüfung der Erforderlichkeit der Einsicht notwendig ist. Insbesondere dürfen die Mitteilungen in Strafsachen (MiStra) nicht umgangen werden, nach denen die Dienstbehörde erst dann von einem Ermittlungsverfahren gegen einen Bediensteten erfahren darf, wenn ein mitteilungsbedürftiger Umstand (Haftbefehl, Klageerhebung, Verurteilung oder Ausgang des Verfahrens) vorliegt. Ebensowenig ist es zulässig, daß Hinweise auf die Akteneinsicht durch Beamte der Kriminalpolizei oder Beschlagnahmebeschlüsse zur Personalakte geheftet werden. Sie sind vielmehr zu personenbezogenen Sachakten in der personalaktenführenden Stelle zu nehmen.

Verständlich ist das Bedürfnis von *Personalräten*, den Mitarbeitern ihres Zuständigkeitsbereiches rechtzeitig zu Geburtstagen zu gratulieren, bei Jubiläen auch mit kleineren Präsenten ihrer besonderen Verbundenheit Ausdruck zu verleihen. Zu erörtern war die Frage, ob die Dienststelle verpflichtet ist, dem Personalrat die notwendigen Daten ohne Einwilligung der Betroffenen zur Verfügung zu stellen. Dabei muß berücksichtigt werden, daß einzelne Mitarbeiterinnen und Mitarbeiter ein Interesse daran haben, ihr Alter nicht allgemein bekannt zu machen. Da sich aus dem Personalvertretungsgesetz keine Befugnis zur Datenweitergabe ergibt, habe ich empfohlen, daß der Personalrat eine eigene Datenerhebung mit Rückmeldekarten vornimmt, so daß die Bediensteten mit der Rücksendung an den Personalrat ihre Zustimmung zum vorgesehenen Verwendungszweck verbinden würden.

Aus dem gleichen Grund ist auch das Geburtsdatum auf Dienstausweisen regelmäßig nicht erforderlich. Der Senator für Inneres hat daher den Dienststellen der Hauptverwaltung empfohlen, auf das Geburtsdatum zu verzichten[1].

Bedenken waren aufgetaucht, inwieweit Besoldungs- bzw. Gehalts- und Lohnstellen berechtigt sein können, Mitteilungen über *Gehalts- und Lohnpfändungen* in die Personalhauptakten zu geben.

Dabei ist zunächst festzustellen, daß diese Stellen Teil der personalaktenführenden Stellen sind und selbst Akten führen, die Teil der jeweiligen Personalakten sind (Beiakten), d. h. mit der Aufnahme der Mitteilung in die Beiakte wird sie Bestandteil der Personalakte. Dies ist zulässig, weil die Pfändung das Dienst- bzw. Arbeitsverhältnis betrifft. Dennoch ist zu prüfen, ob die Mitteilung auch zur Personalhauptakte genommen werden darf.

Auch hier sollten die Grundsätze der Verhältnismäßigkeit und damit des geringstmöglichen Eingriffes für Betroffene beachtet werden, da jede unmittelbar in der Personalakte geführte negative Information den Betroffenen unangemessen belasten könnte. Bei einer Bewerbung kann eine Information über Gehaltspfändungen in der Personalhauptakte dazu führen, daß die ausschreibende Stelle bei ihrer Entscheidung an der objektiven Beurteilung der fachlichen Eignung des Betroffenen gehindert wird. Das Bundesverwaltungsgericht hat allerdings entschieden, daß Pfändungsdaten dem Fachvorgesetzten nur im Ausnahmefall zur Verfügung gestellt werden dürfen[2].

Ich würde es daher begrüßen, wenn Gehaltspfändungen in die Personalhauptakte nur von einer bestimmten Höhe oder Häufigkeit an und selbst dann nur in den Fällen aufgenommen werden, für die regelmäßig auch dienstrechtliche Konsequenzen vorgesehen sind.

Schon in früheren Jahresberichten[3] hatte ich über das Problem der *amtsärztlichen Begutachtung* von Beamten berichtet. Ich hatte bemängelt, daß der Verhältnismäßigkeitsgrundsatz verletzt werde, wenn die amtsärztlichen Gutachten vollständig mit allen Befunden und Diagnosen der vorgesetzten Dienststelle zugänglich gemacht werden. Die jahrelangen Erörterungen dieses Problems haben nun endlich dazu geführt, daß durch die Vorlage einer Novelle zum Landesbeamtengesetz die Voraussetzungen für eine informationsrechtliche Klärung des Ablaufs geschaffen worden sind. Der Gesetzentwurf geht davon aus, daß ein Beamter nicht gezwungen werden kann, sich einer ärztlichen Untersuchung zu unterziehen. Da er jedoch gegenüber dem Dienstherrn die Pflicht hat, sich kooperativ zu verhalten, kann aus der Weigerung, sich der Begutachtung zu unterziehen, eine entsprechende dienstrechtliche Schlußfolgerung gezogen werden. Dies soll gesetzlich festgeschrieben werden.

Ich habe darüber hinaus empfohlen, auch für die Fälle, in denen der Beamte bereit ist, sich einer ärztlichen Begutachtung zu unterziehen, eine gesetzliche Regelung darüber zu treffen, in welchem Umfang medizinische Daten an die vorgesetzte Dienststelle übermittelt werden können. Der Amtsarzt sollte zwar verpflichtet werden, eine Niederschrift über die Begutachtung für interne Zwecke anzufertigen und das Ergebnis mit dem Betroffenen zu erörtern, übermitteln sollte der Arzt jedoch nur die Tatsache

[1] Vgl. Anlage 6
[2] Vgl. Jahresbericht 1984, Ziff. 4.3; Jahresbericht 1986, Ziff. 4.3

[1] Rundschreiben SenInn - AV A 24 - 0553/I vom 6. März 1987
[2] BVerwG 2 C 51/84 = NJW 9/87, 1214 f
[3] Vgl. Jahresbericht 1984, Ziff. 2.3; Jahresbericht 1985, Ziff. 5

der weiteren dienstlichen Verwendbarkeit oder Nichtverwendbarkeit sowie die maßgebliche Behinderung. Verweigert der Betroffene sein Einverständnis, ist er so zu behandeln, als hätte er die Begutachtung insgesamt verweigert. Ich habe in dem Zusammenhang noch einmal darauf hingewiesen, daß Ferngutachten oder diagnostische Feststellungen nach Aktenlage unzulässig sein sollten.

Von mehreren Bezirksämtern sind mir Überlegungen zum Einsatz eines *PC* in der *Personalwirtschaftsstelle* bekannt. In meinem letzten Jahresbericht habe ich bereits auf die grundsätzliche Zulässigkeit der Speicherung von Daten, mit denen die Dienstbehörde oder der Arbeitgeber gesetzliche und vertragliche Verpflichtungen gegenüber Mitarbeitern erfüllen, sowie von Daten, die für die innerbetriebliche Organisation der Arbeitsabläufe erforderlich sind, hingewiesen[1].

Die Personalwirtschaftsstelle führt die Unterlagen über die Planung und Bewirtschaftung der Stellen für die Beschäftigten der Bezirksverwaltung. Hierzu gehört die Führung der Stellenplan-Sichtkartei, von vielfältigen Listen und weiteren sonstigen Karteien und die Bewirtschaftung der Personalmittel. Fortschreibung der Stellenkartei, Aufstellen von Listen und die damit anfallenden Sortierarbeiten werden bis jetzt manuell durchgeführt. Durch den Einsatz der Datenverarbeitung sollen die vielfältigen Doppelnotierungen von Daten möglichst ausgeschlossen, Wiederholungsarbeiten und häufig langwierige Sucharbeiten vermieden werden.

Ist die Zulässigkeit der Speicherung geklärt, muß für das einzelne Verfahren festgestellt werden, wie groß das Sicherheitsbedürfnis aus rechtlichen und tatsächlichen Gründen ist. Je nach Sensibilität der gespeicherten Daten sind geeignete technisch-organisatorische Maßnahmen zum Datenschutz erforderlich. Die laufende technische Entwicklung zeigt, daß die organisatorischen Rahmenbedingungen für das Arbeiten mit dem PC ständig mehr technisch-organisatorische Maßnahmen zum Datenschutz zulassen. Nur wenn die Risiken im Einzelfall mit abgestimmten Maßnahmen auf ein Mindestmaß reduziert werden, ist eine Speicherung von Personaldaten auf einem PC zulässig.

Bereits 1985 habe ich das Bezirksamt Neukölln bei der Einführung eines PC-Verfahrens zur Personalbewirtschaftung beraten und verschiedene Hinweise zu Fragen des Datenschutzes gegeben. Mit dem Vorwand, es handele sich dabei nur um eine Erprobung, lehnte das Bezirksamt seinerzeit die Durchführung datenschutzrechtlich gebotener Maßnahmen ab. Eine Überprüfung des Verfahrens ergab nun, daß das Bezirksamt seither sehr wohl einen Wirkbetrieb des Personalwirtschaftsverfahrens durchgeführt hat, ohne daß die erforderliche Meldung zum Dateienregister erfolgte. Die Überprüfung ergab ferner, daß die Datenträgerverwaltung so nachlässig betrieben wird, daß weder eine Gewähr für die Vollständigkeit der Datenträger noch für die ordnungsgemäße Anwendung der System- und Anwendungsprogramme gegeben werden kann. Auch für die Arbeiten am System fehlten jegliche Unterlagen und Protokolle, die das Verfahren revisionsfähig machen könnten. Meiner schon 1985 abgegebenen Empfehlung, individuelle Paßwörter zu vergeben und zu verwenden, ist man im Ergebnis nicht gefolgt.

Das genannte Beispiel zeigt, daß unbekümmertes Drauflosorganisieren mit Personalcomputern die ordnungsgemäße, nachprüfbare und damit rechtssichere Abwicklung von Verwaltungsverfahren in Frage stellt.

Öffentliche Sicherheit

Hauptproblem im Bereich der öffentlichen Sicherheit und Ordnung ist nach wie vor das Fehlen polizeirechtlicher Bestimmungen, die der Vollzugspolizei und den allgemeinen Ordnungsbehörden eine hinreichende Befugnis für die Verarbeitung der benötigten Daten verschaffen. Die von mir seit Jahren angemahnte Novellierung des *Allgemeinen Sicherheits- und Ordnungsgesetzes (ASOG)* wurde in Berlin auch in diesem Jahr nicht in Angriff genommen. Vielmehr berief sich der Senator für Inneres auf einen Beschluß der Innenministerkonferenz, nach dem vor einer endgültigen Beschlußfassung über einen Musterentwurf, den ein Arbeitskreis erarbeitet hatte, erst eine Abstimmung mit den Justizverwaltungen über die künftige Ausgestaltung der Strafprozeßordnung herbeigeführt werden sollte. Obwohl im Ergebnis sicherlich eine Harmonisierung zwischen präventivem und repressivem Recht erforderlich ist, wäre der Berliner Gesetzgeber nicht gehindert, bereits jetzt eine Linie für die künftige Ausgestaltung des Polizeirechts zu finden. Denn es sind Entscheidungen erforderlich, die von den Vorgaben der Strafprozeßordnung unabhängig sind. Hierzu zählen z. B. die Frage, ob im Hinblick auf die Datenverarbeitung eine Differenzierung der Befugnisse für Vollzugspolizei und Ordnungsbehörden erforderlich ist oder wie die rechtlichen Vorgaben für die zulässigen Formen der automatischen Datenverarbeitung für die Berliner Polizei aussehen sollen. Eine gewisse Bewegung erhoffe ich mir von einem Beschluß des Abgeordnetenhauses, der den Senat auffordert, bis zum 1. April 1988 einen ersten Entwurf für ein novelliertes Polizeirecht vorzulegen.

Vor welch schwierige Situation die derzeitige Rechtslage die Sicherheitsbehörden stellt, zeigt die datenschutzrechtliche Bewertung von Maßnahmen, die die Polizei im Rahmen von *Sicherheitsüberprüfungen* anläßlich der *Staatsbesuche* zur 750-Jahr-Feier für erforderlich hielt und über die ich bereits im Vorfeld unterrichtet wurde. An bestimmten Stellen der Fahrtroute, die für den Staatsgast als besonders gefährlich eingestuft wurden, sollten in angrenzenden Gebäuden Anwohner und Mitarbeiter von Gewerbebetrieben überprüft werden. Hierzu waren personenbezogene Daten über diesen Personenkreis zu erheben, mit den der Polizei zur Verfügung stehenden Datensammlungen zu vergleichen, während der Dauer der Staatsbesuche aufzubewahren und schließlich unverzüglich zu vernichten. Das bestehende ASOG enthält neben der völlig unbestimmten polizeilichen Generalklausel keine hinreichend normenklare Befugnisnorm für die Verarbeitung von Daten dieser Personen, die weder als Störer noch als Tatverdächtige in Erscheinung getreten sind. Der Musterentwurf für ein einheitliches Polizeigesetz enthält hierzu folgende Regelungen: „Bei Anlässen, die erfahrungsgemäß eine besondere Gefährdungslage hervorrufen, kann die Polizei zur Vorbereitung und Durchführung ihres Einsatzes personenbezogene Daten erheben, soweit dies erforderlich ist." Zur Bewertung der Maßnahmen habe ich die in dieser Regelung zum Ausdruck kommende Abwägung zur Auslegung der §§ 9 ff. Berliner Datenschutzgesetz herangezogen, die auf die Erforderlichkeit zur Aufgabenerfüllung verweisen und derzeit die einzigen relevanten Vorschriften darstellen.

Der *Übergangsbonus*, der bei derartigen Fallkonstellationen den Sicherheitsbehörden von Gerichten und anderen Kontrollinstanzen eingeräumt wird, kann allerdings weder in materieller noch in zeitlicher Hinsicht überstrapaziert werden. Auf ihn können nur unerläßliche Maßnahmen gestützt werden und dies nur solange, wie der Gesetzgeber bei zielstrebigem Vorgehen für die Schaffung der Rechtsgrundlagen benötigt. Sieht man diesen Zeitpunkt spätestens als dann verstrichen an, wenn die auf Bekanntwerden der Problematik folgende Legislaturperiode zu Ende geht, ist der Berliner Gesetzgeber gehalten, im Laufe des Jahres 1988 ein neues Polizeirecht zu schaffen.

Der Antwort des Senators für Inneres auf eine mündliche Anfrage im Abgeordnetenhaus[1] entnahm ich, daß die Landespolizeidirektion angeordnet hatte, alle im Zusammenhang mit der *Volkszählung* gefertigten *Ordnungswidrigkeitenanzeigen und Strafanzeigen* dem *Polizeilichen Staatsschutz* zuzuleiten, um aufgrund der zahlenmäßigen Erfassung der Ereignisse ein zutreffendes Lagebild zu erhalten. Die Ordnungswidrigkeitenanzeigen würden danach unmittelbar an die zuständige Verwaltungsbehörde, z. B. das Statistische Landesamt, weitergeleitet. Später präzisierte der Senator für Inneres seine Antwort dahingehend, daß nur Anzeigen wegen öffentlicher Aufrufe zum Boykott der Volkszählung 1987 über den Polizeilichen Staatsschutz geleitet werden sollten. Für beide Verfahrensvarianten fehlt die erforderliche Rechtsgrundlage. Der Polizeibeamte, der Ordnungswidrigkeiten feststellt, ist nach dem Ordnungswidrigkeitengesetz verpflichtet, seine Vorgänge unverzüglich der Verwaltungsbehörde, in den Fällen des Zusammenhangs mit einer Straftat der Staatsanwaltschaft zu übersenden. Für die Verfolgung der Ordnungswidrig-

[1] Vgl. Jahresbericht 1986, Ziff. 4.3

[1] Nr. 15 in Mitteilungen des Präsidenten Nr. 156, Drs. 10/1445 vom 2. April 1987

keiten „Auskunftsverweigerung" und „Boykottaufruf" bei der Volkszählung ist ausschließlich das Statistische Landesamt zuständige Verwaltungsbehörde. Für die Verweigerung der Übernahme des Zähleramtes und den Aufruf hierzu sind die bezirklichen Ämter für Volkszählung zuständig. Aufgrund meiner Intervention hat der Polizeipräsident die Polizeiabschnitte angewiesen, die Ordnungswidrigkeitenanzeigen im Zusammenhang mit der Volkszählung direkt dem Statistischen Landesamt bzw. den Ämtern für Volkszählung zuzuleiten. Dem Polizeilichen Staatsschutz werden seitdem nur noch Angaben über Tatort, Tatzeit und Tatart zur Erstellung eines Lagebildes mitgeteilt.

Unabhängig davon ist der Polizeiliche Staatsschutz zuständig für die Bearbeitung von *Strafanzeigen* im Zusammenhang mit der Volkszählung, die ihm deshalb vollständig zugeleitet werden. Ich habe in diesem Zusammenhang die Speicherung und Verarbeitung personenbezogener Angaben beim Polizeipräsidenten überprüft. Von den zu diesem Zeitpunkt gespeicherten Datensätzen betrafen zwei Drittel ausschließlich Sachbeschädigungen in Form von Beschmieren oder Abreißen von offiziellen Volkszählungsplakaten bzw. Besprühen von Fassaden mit Boykottparolen, die übrigen Datensätze schwere Formen der Kriminalität (z. B. schwerer Landfriedensbruch, Widerstand gegen Vollstreckungsbeamte). Alle Datensätze waren sowohl im Informationssystem Verbrechensbekämpfung (ISVB) als auch in der *„Arbeitsdatei PIOS - Innere Sicherheit" (APIS)* gespeichert. Die Datei APIS wird beim Bundeskriminalamt als Verbunddatei mit Direktverbindungen zu den Landeskriminalämtern geführt.

Sowohl der Bundesbeauftragte für den Datenschutz als auch der Bayerische Landesbeauftrate für den Datenschutz haben Bedenken gegen die *undifferenzierte Speicherung aller Straftaten zum bundesweiten Abruf* erhoben, sofern wegen der Angriffsrichtung, des Motivs des Täters oder dessen Verbindung zu einer Organisation der Verdacht besteht, daß mit der Tat ein gegen die freiheitliche demokratische Grundordnung gerichtetes Ziel verfolgt wird. Auch ich halte es für problematisch, daß ein technisches Instrumentarium wie APIS, das speziell zur Bekämpfung des Terrorismus entwickelt worden ist, auf die - politisch motivierte - Kleinkriminalität erstreckt wird.

Die Eingabe personenbezogener Daten in APIS stellt eine Übermittlung dieser Daten an das Bundeskriminalamt sowie alle zuständigen Landespolizeibehörden der anderen Länder dar und ist deshalb nur im erforderlichen Umfang zulässig. Für Daten zu Farbschmierereien und vergleichbarer Kleinkriminalität ist die Erforderlichkeit der Übermittlung nicht ersichtlich, weil diese Straftaten häufig keine überörtliche, sondern nur örtliche Bedeutung haben. Von daher wäre aus meiner Sicht eine Beschränkung der Speicherung solcher Straftaten auf das ISVB sachgerecht. In jedem Fall bin ich mit dem Bayerischen Landesbeauftragten für den Datenschutz der Auffassung, daß bei einer weiteren Speicherung der Kleinkriminalität im APIS eine Abschottung zwischen Straftaten von überörtlicher und örtlicher Bedeutung geboten ist. Eine Speicherung personenbezogener Daten bei politisch motivierter Kleinkriminalität in APIS zum undifferenzierten Abruf durch alle Landeskriminalämter und das Bundeskriminalamt ist unverhältnismäßig, insbesondere auch ungeeignet zur polizeilichen Aufgabenerfüllung, da die abrufende Stelle durch die zunehmende Menge der Informationen mehr Zeit braucht, um die für sie erforderlichen Informationen zu erkennen.

Zahlreiche Ermittlungsverfahren wurden wegen Sachbeschädigung durch *Herausschneiden von Heftnummern* aus den Erhebungsunterlagen eingeleitet. Die personenbezogenen Angaben der Beschuldigten wurden in APIS gespeichert. Zu der Frage, ob in dem Herausschneiden von Heftnummern eine strafbare Sachbeschädigung zu sehen ist, gibt es jedoch bisher keine einheitliche Rechtsprechung der Strafgerichte. Während das Kammergericht offenbar in diesem Verhalten eine Straftat sieht, haben westdeutsche Landgerichte zum Teil gegenteilige Auffassungen vertreten. Dies führt dazu, daß bestimmte Landeskriminalämter bei einem entsprechenden Abruf von personenbezogenen Datensätzen aus APIS, die in Berlin eingegeben wurden, erst aufgrund der Sachverhaltsbeschreibung feststellen können, daß es sich nach der Auffassung des für sie zuständigen Gerichts nicht um einen Straftäter handelt. Dieses Beispiel macht deutlich, daß durch die undifferenzierte Speicherung politisch motivierter Kleinkriminalität in APIS diese Datei für den Polizeilichen Staatsschutz an Aussagekraft ständig verliert. Die Stelle, die Auskünfte aus APIS abruft, muß stets eine eigene Bewertung des jeweiligen Sachverhalts daraufhin vornehmen, ob der Betroffene in einem bestimmten Bereich strafbarer Handlungen in Erscheinung getreten ist. Diese Bewertung wird umso zeitaufwendiger, je größer die Menge der konkret nicht benötigten Informationen wird. Gerade die Speicherung der nur örtlich bedeutsamen Kleinkriminalität erhöht den Anteil nicht erforderlicher Daten in APIS wesentlich.

Der Leiter der *Amtsanwaltschaft* hatte angeordnet, daß Einsprüche gegen *Bußgeldbescheide* aus Anlaß der *Volkszählung* 1987 dann der Abteilung I der Staatsanwaltschaft bei dem Landgericht Berlin vorzulegen seien, wenn sich aus dem Bußgeldvorgang Anhaltspunkte für eine vom Betroffenen neben der Ordnungswidrigkeit begangene Straftat ergeben oder wenn gegen den Betroffenen bereits ein strafrechtliches Ermittlungsverfahren bei der Staatsanwaltschaft anhängig ist. Dieses Verfahren entspricht den Zuständigkeitsvorschriften im Ordnungswidrigkeitengesetz. Auch trifft die in den Medien geäußerte Befürchtung nicht zu, damit erhalte die Staatsanwaltschaft Zugriff auf die sogenannte Restliste beim Statistischen Landesamt bzw. bei den Ämtern für Volkszählung. Bereits die Amtsanwaltschaft erhält nämlich nur Kenntnis von denjenigen Bußgeldverfahren, in denen der Betroffene Einspruch eingelegt hat.

Erörterungsbedürftig bleiben nach wie vor Probleme im Zusammenhang mit der *automatisierten Datenverarbeitung.*

Zwischenzeitlich wurden weitere Mängel behoben, die bei der Überprüfung des *Informationssystems Verbrechensbekämpfung (ISVB)* im Jahre 1985 festgestellt worden waren. So wird inzwischen ein Gerät eingesetzt, mit dem die im INPOL-Verbund nach Westdeutschland übermittelten personenbezogenen Daten verschlüsselt werden. In einem Rundschreiben über die Befugnis von Datenabfragen aus dem ISVB und anderen der Polizei zugänglichen Datensystemen wurde die Bedeutung der Zugriffsberechtigungen in großer Klarheit hervorgehoben. Die Ausstattung des internen Datenschutzbeauftragten der Polizei wurde verstärkt. Nicht vollzogen wurde dagegen die von mir empfohlene formale Beschreibung des Zusammenwirkens von ADV-und Anwenderbereich, in der ich eine wichtige Garantie für die Ordnungsmäßigkeit der Datenverarbeitung sehe.

Ungelöst bleibt ferner die Frage, ob und unter welchen Voraussetzungen in den polizeilichen Informationssystemen *personengebundene Hinweise* enthalten sein dürfen, d. h. Eintragungen, die jedem Zugriffsberechtigten beim Aufruf des Namens der Betroffenen angezeigt werden. Es handelt sich hier in der Mehrzahl um Merkmale, die geeignet sind, den Betroffenen psychisch oder sozial abzustempeln (z. B. suizidgefährdet, Prostitution, häufig wechselnder Aufenthaltsort), ohne daß sie in jedem Fall für die Strafverfolgung von Bedeutung sind. Als Zweck für die Speicherung wird vielmehr die Gefahrenabwehr für die abrufenden Beamten, aber auch für die Betroffenen genannt. Das Beispiel der Suizidgefährdung zeigt, daß auch diese Begründung nicht ausreicht.

Zu keinem Ergebnis kam bisher der Arbeitskreis II der Innenministerkonferenz, der mit einer Prüfung der Zulässigkeit personengebundener Hinweise beauftragt worden war.

Auch der Unterausschuß Datenschutz des Ausschusses für Inneres, Sicherheit und Ordnung des Abgeordnetenhauses hat sich mit der Frage befaßt. Ich werde der dort geäußerten Empfehlung nachkommen und Umfang und Erforderlichkeit der Speicherung personengebundener Hinweise im ISVB gesondert prüfen.

Besonders umstritten war im vergangenen Jahr die Frage, ob ein Hinweis auf AIDS in die Systeme eingestellt werden darf. Der Polizeipräsident folgt hier einer Empfehlung der Innenministerkonferenz, nach der dafür der *personengebundene Hinweis ANST* (Ansteckungsgefahr) verwendet werden soll. Eine unmittelbare Eintragung der Krankheit oder eines Verhaltenshinweises („Vorsicht Blutkontakte") ist nur bei Fahndungsausschreibungen möglich. Die Erforderlichkeit der Maßnahme wird von den Datenschutzbeauftragten des Bundes und der Länder in Frage gestellt: Die Tatsache, daß weltweit praktisch kein Fall der Ansteckung

eines Polizeibeamten durch einen Infizierten bekannt geworden ist, läßt die Verhältnismäßigkeit des Eingriffs in das informationelle Selbstbestimmungsrecht, der mit einem derartigen personengebundenen Hinweis verbunden ist, fraglich erscheinen.

Auch im Bereich des Polizeipräsidenten nimmt der Umfang des Einsatzes von *Personalcomputern* zu. Der Polizeipräsident hat hierzu eine PC-Anweisung erlassen, die die Anwendung der Kleincomputer im verantwortbaren Rahmen halten soll. Diesen Anwendungen wird bei datenschutzrechtlichen Kontrollen große Aufmerksamkeit zu widmen sein.

Daß auch die Alltagsarbeit der Polizei an unvermuteten Stellen Datenschutzprobleme aufwerfen kann, zeigt folgendes Beispiel:

In mehreren Eingaben trugen Petenten die Vermutung vor, daß von der *Kriminalpolizeilichen Beratungsstelle* Namen und Anschriften an Dritte weitergegeben würden, weil Spezialfirmen für Sicherungsapparaturen an sie herangetreten waren, nachdem sie sich nach einem Einbruch hatten beraten lassen. Ich hatte mich daher vor Ort sachkundig gemacht und konnte feststellen, daß eine Übermittlung personenbezogener Daten an Dritte durch die Polizei nicht stattfindet. Über das jeweilige Beratungsgespräch mit betroffenen Bürgern wird ein Protokoll geführt, das mit einer Empfehlung für die einzubauenden Maßnahmen abgeschlossen wird. Dabei werden keine firmenbezogenen Produkte, sondern geeignete Systeme empfohlen mit allgemeinen Hinweisen auf in Frage kommende Hersteller. Eine Durchschrift wird dann den beratenen Bürgern ausgehändigt.

Der Einfachheit halber hatten die Betroffenen später selbst dieses Protokoll den aufgesuchten Firmen für Sicherungssysteme vorgelegt und dabei nicht bedacht, daß jene dadurch in der Lage waren, die ebenfalls notierten personenbezogenen Daten herauszuschreiben.

Gleichwohl ist der Polizeipräsident in Berlin meiner Bitte nachgekommen und fügt jetzt am Schluß eines jeden Protokolls als erläuternden Zusatz an, daß eine Durchschrift des Protokolls bei der Kriminalpolizeilichen Beratungsstelle ein Jahr lang für eventuelle Rückfragen hinterlegt und dann vernichtet wird, und daß eine Weitergabe personenbezogener Daten an Dritte ohne Zustimmung der Betroffenen ausgeschlossen ist.

5.4 Justiz

Strafverfolgung

Wie erwähnt, hat die Innenministerkonferenz die Weiterführung der Bemühungen um eine Novellierung des Polizeirechts von einer Anpassung der *Strafprozeßordnung* an die Anforderungen des Volkszählungsurteils abhängig gemacht. Bislang liegen erste Entwürfe für datenschutzrechtlich relevante Teilbereiche, so beispielsweise hinsichtlich der Fahndungsmaßnahmen und der Hilfsmittel bei der Fahndung sowie zur Akteneinsicht, vor. Ein ergänzender Entwurf betrifft die zentrale Frage der Befugnis zur Speicherung personenbezogener Daten, die für die Strafverfolgung erforderlich sind.

Die vorliegenden Arbeitsentwürfe zur Neuregelung von einzelnen Bereichen der Strafprozeßordnung bergen die Gefahr in sich, daß isolierte Regelungen zu bestimmten Einzelkomplexen geschaffen werden. Erforderlich ist darüber hinaus ein übergreifendes Konzept, d. h. eine Harmonisierung des Strafverfahrensrechts im umfassenden Sinne, das die Tätigkeit der Polizei und der Staatsanwaltschaft, das Strafverfahren bei den Gerichten und die Strafvollstreckung umfassen muß. Der Umfang der Datenerhebung, die Verantwortlichkeit für die Datenverarbeitung und die Zulässigkeit der Übermittlungen müssen sich normenklar und am Gebot der Verhältnismäßigkeit orientiert aus dem Gesetz ergeben.

In diesem Zusammenhang muß ich feststellen, daß der Senator für Justiz mir die Abgabe von Stellungnahmen zu Gesetzentwürfen erschwert, indem er Gesetzentwürfe häufig erst auf ausdrückliche Anforderung übersendet und sich in einzelnen Fällen darauf beruft, für die Weiterleitung von Bundesgesetz-Entwürfen nicht zuständig zu sein. Dem ist entgegenzuhalten, daß meine Beratungsaufgabe auch die Abgabe von Stellungnahmen zu Gesetzentwürfen umfaßt. Da der Justizsenator - ebenso wie andere Landesjustizbehörden - bei der Bundesgesetzgebung beteiligt wird, ist konsequenterweise auch der Berliner Datenschutzbeauftragte einzubeziehen. Eine rechtzeitige Unterrichtung bürgt dafür, daß datenschutzrechtliche Aspekte im Gesetzgebungsverfahren angemessen berücksichtigt werden und verhindert schwierige Nachbesserungen. Hier ist eine größere Kooperationsbereitschaft zwingend erforderlich.

Entscheidungen der Gerichte, aber auch prozeßvorbereitende Maßnahmen (z. B. Anklageerhebung durch die Staatsanwaltschaft) lösen häufig die Pflicht aus, andere Behörden oder Personen hierüber zu unterrichten. Da diese *Mitteilungspflichten* bisher nur in Verwaltungsvorschriften bundeseinheitlich geregelt sind, hatten die Datenschutzbeauftragten seit langem das Fehlen einer gesetzlichen Grundlage bemängelt. Auch die Justizminister und -senatoren sind inzwischen zu der Auffassung gelangt, daß die Schaffung einer gesetzlichen Grundlage für diese Mitteilungen erforderlich sei.

Nunmehr sind vom Bundesminister der Justiz verschiedene Regelungsmodelle vorgelegt worden. So ist geprüft worden, ob die Mitteilungen in die jeweiligen Gesetze (ZPO, StPO, GVG) eingefügt werden sollten oder ob eine vollständige und abschließende Regelung in einem besonderen Gesetz geschaffen werden sollte. Bisher liegt ein Entwurf eines *Justizmitteilungsgesetzes* vor, demzufolge allgemeine Vorschriften über die Mitteilungspflichten in das GVG und das JGG eingefügt werden, wobei im übrigen auf die einzelnen Prozeßordnungen verwiesen wird.

Der Entwurf ist ein erster konkreter Schritt auf dem Weg zu einer nach dem Volkszählungsurteil unumgänglich gewordenen gesetzlichen Verankerung des Mitteilungswesens im Justizbereich. Er beschränkt sich jedoch auf Mitteilungen an solche Stellen, die Aufgaben außerhalb des zugrundeliegenden Verfahrens wahrzunehmen haben. Für Mitteilungen an Verfahrensbeteiligte oder auf Ersuchen wird auf die einzelnen Prozeßordnungen verwiesen. Dort müßten dann die entsprechenden gesetzlichen Grundlagen noch ergänzt werden.

Bedenklich ist allerdings die geringe Regelungsdichte des Entwurfs. Häufig werden generalklauselartige Regelungen verwendet, die Anlaß und Umfang der vorgesehenen Datenverarbeitung nicht hinreichend deutlich machen und die Umgehungsmöglichkeiten bieten.

Grundbuchwesen

Gemäß § 55 Grundbuchordnung (GBO) soll jede Eintragung im Grundbuch dem Antragsteller und dem eingetragenen Eigentümer sowie allen aus dem Grundbuch ersichtlichen Personen bekanntgemacht werden, zu deren Gunsten die Eintragung erfolgt ist, oder deren Recht durch sie betroffen wird. Die Eintragung eines Eigentümers ist auch denen bekanntzugeben, für die eine Hypothek, Grundschuld, Rentenschuld, Reallast oder ein Recht an einem solchen Recht im Grundbuch eingetragen ist. Aufgrund dieser Regelung wird z. B. bei einer Umschreibung eines alten Grundbuchblattes auf ein neues Blatt der wegeberechtigte Nachbar über die Umschreibung unterrichtet. Da jeweils ein vollständiger Grundbuchauszug übersandt wird, der auch Angaben zu den Belastungen enthält, erhalten alle Beteiligten Kenntnis über die finanzielle Situation des Grundstückseigentümers.

Die Unterrichtung über die Belastungen verletzt die schutzwürdigen Belange der Betroffenen. Für die anderen Beteiligten reicht eine Unterrichtung über solche Eintragungen, die ihre Rechte betreffen.

Der Senator für Justiz hat vorgetragen, daß eine umfassende Unterrichtung der Beteiligten erforderlich sei. Dies beruhe unter anderem darauf, daß gemäß § 879 BGB die Rangfolge der verschiedenen Rechte, die im Grundbuch eingetragen sind, auch vom jeweiligen Eintragungsdatum abhängen. Darüber hinaus stehe es nach § 12 GBO jedem, der ein berechtigtes Interesse nachweise, frei, ins Grundbuch Einsicht zu nehmen, so daß die entsprechenden Informationen ohnehin erreichbar seien.

Auch diese Argumentation berücksichtigt nicht, daß die Höhe der Darlehensschulden des Grundstückseigentümers die Rechte anderer Beteiligter nicht beeinträchtigen kann und eine entsprechende Unterrichtung überflüssig ist. § 12 GBO erlaubt eine Ein-

sichtnahme im berechtigten Einzelfall, kann jedoch nicht Grundlage eines umfassenden Unterrichtungsverfahrens sein.

Derzeit wird im Bundesministerium der Justiz an einer Novellierung der Grundbuchordnung gearbeitet, die auch datenschutzrechtliche Belange berücksichtigen soll.

Für die Zwischenzeit empfehle ich, bei Grundbucheintragungen die Unterrichtung auf jene Teile zu beschränken, die Rechte der Beteiligten betreffen können. Mit der Unterrichtung könnte ein Hinweis auf die Möglichkeit einer weitergehenden Einsichtnahme ins Grundbuch verbunden sein. Dieses Einsichtsrecht können dann solche Beteiligten wahrnehmen, die ein berechtigtes Interesse daran haben.

Automatisiertes Mahnverfahren

Nach Baden-Württemberg hat auch Berlin das „Automatisierte Mahnverfahren" eingeführt. Nunmehr werden die jährlich rund 250 000 Mahnverfahren zentral beim Amtsgericht Wedding bearbeitet. Damit soll vor allem eine schnellere Abwicklung erreicht werden. Allerdings ist mit den gesetzlichen Voraussetzungen für das Mahnverfahren eine deutliche Verschlechterung der Rechtsstellung des betroffenen rechtsunerfahrenen Bürgers verbunden, der mangels eigener Prüfung durch die Gerichte der Willkür einschlägiger Firmen ausgesetzt wird.

Das automatisierte Mahnverfahren stellt eine nahezu direkte Umsetzung des konventionellen Verfahrens dar. Im wesentlichen werden die Mahnanträge schriftlich gestellt und nach der Datenerfassung der Datenverarbeitung zugeführt. Für sogenannte Großgläubiger (Banken, Versandhäuser) besteht jedoch auch die Möglichkeit, Anträge auf maschinell lesbaren Datenträgern einzureichen. Dabei deckt sich der Informationsgehalt der gelieferten Anträge mit dem der entsprechenden Vordrucke.

Der Senator für Justiz hat mich bei der Planung des DV-Systems beteiligt. Ich habe gegen die Einführung des Verfahrens keine grundsätzlichen Bedenken geltendgemacht, da die Möglichkeit der Automatisierung von Mahnverfahren bereits in den §§ 688 ff. ZPO ausdrücklich vorgesehen ist. Die vom Senator für Justiz geplanten Maßnahmen zum Schutz personenbezogener Daten und zur Datensicherung sind zu begrüßen.

Der Senator für Justiz weigert sich allerdings, das Verfahren durch Anmeldung zum Dateienregister für den Bürger und die Datenschutzkontrolle transparent zu machen. Er vertritt den Standpunkt, daß es sich bei dem Mahnverfahren um eine Tätigkeit handele, die gemäß § 21 Abs. 1 Berliner Datenschutzgesetz meiner Zuständigkeit entzogen sei.

Dem ist nicht zu folgen. Die Beschränkung der Kontrollkompetenz des Datenschutzbeauftragten soll die Unabhängigkeit der richterlichen Entscheidung sichern, d. h. es soll kein Eingriff in die Spruchtätigkeit stattfinden. Dies ist bei der Einrichtung eines ADV-Verfahrens auch nicht der Fall: Wie bei anderen Sachmitteln auch, wird hier den Gerichten von den Justizverwaltungen ein vom Inhalt der Rechtsprechung unabhängiges Organisationsmittel zur Verfügung gestellt, dessen Angemessenheit auch unter Datenschutzgesichtspunkten geprüft werden muß. Es handelt sich daher um einen meldepflichtigen Sachverhalt. Das Dateienregister ist vor allem eine vertrauensbildende Maßnahme gegenüber dem Bürger, dem Gelegenheit gegeben wird, sich selbst über Art und Umfang der Staatstätigkeit zu informieren.

Alle Vorhaben, in denen meine Beteiligung erschwert oder verhindert wurde, verschlechtern letztlich die Position des Bürgers gegenüber dem Staat.

5.5 Schulwesen, Berufsausbildung und Sport

Schulrecht

Bereits in meinem letzten Jahresbericht[1]) hatte ich auf die Notwendigkeit hingewiesen, die Erhebung und Verarbeitung von Schülerdaten durch eine *Ergänzung des Schulgesetzes* bereichsspezifisch zu regeln. Hierzu habe ich der Schulverwaltung meine Vorstellungen erläutert. Insbesondere sollte die Erhebung, Verarbeitung und Nutzung schüler- und elternbezogener Daten im gesamten Bereich des Schulwesens, also durch Schulen, Bezirksämter und den Schulsenator auf eine normenklare gesetzliche Grundlage gestellt werden, die sich am Grundsatz der Verhältnismäßigkeit zu orientieren hat. Auch wenn Detailprobleme durch Rechtsverordnung geregelt werden können, halte ich eine generelle Regelung über die Art der personenbezogenen Daten, die erhoben und verarbeitet werden dürfen, für notwendig.

Zunehmend wird aus Schulen die Frage an mich gerichtet, ob die *automatisierte Verarbeitung von Leistungsdaten*, insbesondere Zensuren, zulässig ist. Ich habe erhebliche Zweifel, ob die Erfüllung des schulischen Auftrags davon abhängt, daß diese sensiblen Daten in allen Schulstufen automatisiert verarbeitet werden. In jedem Fall bedarf es hierzu einer Grundsatzentscheidung des Gesetzgebers. Bevor diese gefallen ist, halte ich eine automatisierte Verarbeitung von Leistungsdaten nur zu Zwecken der Textverarbeitung (z. B. Ausdruck von Zeugnissen) für zulässig.

Gesetzlich sollte auch klargestellt werden, daß bestimmte personenbezogene Informationen in keinem Fall automatisiert verarbeitet werden dürfen. Hierzu zählen nach meiner Auffassung Daten, die dem ärztlichen Berufsgeheimnis unterliegen (z. B. „gesundheitliche Rücksichten"), aber auch besondere pädagogische, soziale und therapeutische Maßnahmen, Informationen über Behinderungen und über die Ergebnisse der schulärztlichen Untersuchungen sowie Verhaltensdaten. Derartige Informationen sollten ausschließlich in konventionellen Datensammlungen (Akten, Schülerunterlagen) enthalten sein.

Auch die Erhebung und Verarbeitung personenbezogener Daten durch den *Schulärztlichen und Schulpsychologischen Dienst* sollten im Schulgesetz verankert werden. Auf untergesetzlicher Ebene wurden bereits Fortschritte mit der Regelung des Einsichtsrechts und der Aktenführung in einem Entwurf zu Ausführungsvorschriften über den Schulpsychologischen Dienst erzielt[1]).

Das *Akteneinsichtsrecht* und die Festlegung von *Aufbewahrungs- und Löschungsfristen* gehören ebenfalls zu den grundsätzlichen Problemen, die im Schulgesetz geregelt werden sollten.

Erforderlich ist schließlich eine bereichsspezifische Regelung über *wissenschaftliche Forschungsvorhaben in der Schule.* Dabei sollte von dem Grundsatz ausgegangen werden, daß personenbezogene Daten nur mit schriftlicher Einwilligung der Erziehungsberechtigten oder des volljährigen bzw. einsichtsfähigen minderjährigen Schülers erhoben werden dürfen, nachdem die Betroffenen über das Ziel und den wesentlichen Inhalt des Forschungsvorhabens aufgeklärt und auf die Freiwilligkeit der Teilnahme hingewiesen worden sind.

Ich habe darum gebeten, mir einen Novellierungsentwurf zur Stellungnahme zuzuleiten. Die Schulverwaltung teilt meine Auffassung, daß eine spezielle gesetzliche Grundlage für die Datenverarbeitung in der Schule erforderlich ist. Sie will jedoch zunächst abwarten, ob und in welchem Umfang ebenfalls notwendige Ergänzungen des Verwaltungsverfahrensgesetzes besondere Regelungen im Schulgesetz überflüssig machen. Das halte ich für falsch.

Auch in anderen Bereichen der Gesetzgebung, wie z. B. beim Landesstatistikgesetz, beim Berliner Hochschulgesetz und beim Landesarchivgesetz, ist mir von den Fachverwaltungen entgegengehalten worden, die laufenden Gesetzgebungsverfahren auf Bundesebene in diesen Spezialbereichen müßten abgewartet werden, bevor der Landesgesetzgeber tätig werden könne. Die Novellierung des Schulgesetzes kann mit diesem Argument jedoch nicht aufgeschoben werden. In den genannten drei Bereichen (Statistik, Hochschulstatistik und Archivwesen) hat der Bund eigene Gesetzgebungskompetenzen für bereichsspezifische Regelungen. Dies ist im Schulwesen nicht der Fall. Das Bundesverfassungsgericht hat Eingriffe in das informationelle Selbstbestimmungsrecht des Bürgers nur im überwiegenden Allgemeininteresse auf der Grundlage bereichsspezifischer Regelungen für zulässig gehalten. Das Verwaltungsverfahrensrecht, das in Berlin auch im Bildungsbereich gilt, enthält solche bereichsspezifischen Regelungen nicht, sondern hat nur subsidiären Charakter. Der Landesgesetzgeber sollte deshalb die besonderen Daten-

[1]) Vgl. Jahresbericht 1986, Ziff. 4.4

[1]) Vgl. Anlage 7

schutzprobleme der Schule unabhängig vom Verwaltungsverfahrensrecht legislatorisch in Angriff nehmen, zumal ungewiß ist, wann der Entwurf für eine Änderung des Verwaltungsverfahrensgesetzes des Bundes, der der Diskontinuität anheimgefallen ist, von den Koalitionsparteien erneut im Bundestag eingebracht werden wird. Auch der Schulsenator kann sich nach dem Volkszählungsurteil des Bundesverfassungsgerichts nicht auf einen unbefristeten Übergangsbonus berufen. Ich habe ihn deshalb gebeten, mir mitzuteilen, wann mit der Vorlage eines entsprechenden Gesetzentwurfs in Berlin zu rechnen ist. Seine Antwort hierauf steht noch aus.

Einzelfälle

Ein Vater hatte sich bei mir darüber beschwert, daß das über seine Tochter an einer Schule für Lernbehinderte erstellte *sonderpädagogische Gutachten* vom leitenden Schulaufsichtsbeamten allen Schulen, die diese Schülerin vorher besucht hatte, mit der Bitte zugeleitet worden war, diese Schullaufbahn in der Gesamtkonferenz zu erörtern. Dieses Vorgehen war dadurch ausgelöst worden, daß die Sonderpädagogin, die das Gutachten verfaßt hatte, den früher beteiligten Grund- und Hauptschullehrern vorgeworfen hatte, daß sie die Schülerin sehr viel früher der Sonderschule hätten zuweisen müssen.

Ich habe dieses Vorgehen als unverhältnismäßigen Eingriff in das informationelle Selbstbestimmungsrecht der Schülerin und ihrer Eltern beanstandet. Die Übermittlung von derart sensiblen Informationen, wie sie bei der Erstellung von sonderpädagogischen Gutachten anfallen, darf auch vor der bereichsspezifischen Regelung dieser Frage im Schulgesetz nur im Rahmen des Verhältnismäßigkeitsprinzips erfolgen. Nach den Ausführungsvorschriften über die Führung schriftlicher Unterlagen über Schüler unterliegen die bei der sonderpädagogischen Tätigkeit anfallenden Daten strenger Vertraulichkeit und dürfen ohne Einwilligung der Erziehungsberechtigten nur unter bestimmten engen Voraussetzungen an bestimmte Adressaten weitergegeben werden.

Das sonderpädagogische Gutachten enthielt personenbezogene Informationen sowohl über die betroffene Schülerin als auch über ihre Eltern und Geschwister. So wurde der Vater der Schülerin als gewalttätig geschildert. Neben einer Darstellung der negativen familiären Situation und ihrer Auswirkungen auf die Schullaufbahn enthielt das Gutachten auch unterdurchschnittliche Testergebnisse der Schülerin. Es ist davon auszugehen, daß an den Gesamtkonferenzen, auf denen das Gutachten nach der Anordnung des Schulaufsichtsbeamten erörtert werden sollte, auch Lehrer teilgenommen haben, die die Schülerin zu keinem Zeitpunkt unterrichtet haben. Auch den Lehrern, die sie unterrichtet haben, dürften die in dem Gutachten enthaltenen Informationen zumindest teilweise nicht bekannt gewesen sein. Der Schulaufsichtsbeamte hätte durchaus die Möglichkeit gehabt, Konsequenzen aus dem Gutachten in der Weise zu ziehen, daß das informationelle Selbstbestimmungsrecht der Schülerin, ihrer Eltern und Geschwister nicht in unverhältnismäßiger Weise beeinträchtigt worden wäre. So hätte er die wesentlichen Ergebnisse des Gutachtens mit den ehemaligen Klassenlehrern der Schülerin erörtern können. Auch eine Diskussion des Vorwurfs der Gutachterin in nicht personenbezogener Form auf den Gesamtkonferenzen aller früheren Schulen wäre nicht zu beanstanden gewesen.

Mehrere Elternvertreter haben sich bei mir darüber beschwert, daß sie von Kreisverbänden oder Fraktionen einer Partei in Bezirksverordnetenversammlungen zu Informationsveranstaltungen mit der Senatorin für Schulwesen, Berufsausbildung und Sport eingeladen wurden. In einem Fall habe ich festgestellt, daß eine Fraktion Adressen der Elternvertreter von der Abteilung Volksbildung eines Bezirksamtes erhalten hat und die an die Elternvertreter adressierten Einladungsschreiben im Büro des Kreisverbandes frankieren ließ. Dies habe ich beanstandet, da die *Übermittlung der Adressen von Elternvertretern an politische Parteien* ohne Einwilligung der Betroffenen unzulässig ist.

In seiner Stellungnahme zu meiner Beanstandung wandte das Bezirksamt ein, die Fraktion habe lediglich die Frankiermaschine des Kreisverbandes „mitbenutzt"; Adressen seien dem Kreisverband nicht mitgeteilt worden. Dies hat jedoch keinen Einfluß auf die datenschutzrechtliche Beurteilung, denn selbst bei einer Mitbenutzung der Frankiermaschine war nicht ausgeschlossen, daß Mitarbeiter der politischen Partei Kenntnis von Namen und Anschriften von Elternvertretern erhielten. Entscheidend ist aus meiner Sicht der Umstand, daß jeder Empfänger der Einladungen, die mit dem Stempel der politischen Partei versehen waren, den Eindruck gewinnen mußte, daß dieser Partei personenbezogene Angaben unter Verletzung datenschutzrechtlicher Vorschriften übermittelt worden waren. Dieser Eindruck hätte nur vermieden werden können, indem die Einladungsschreiben von der einladenden Fraktion kuvertiert, aber ohne Adressen zum Frankieren gegeben und die Adressen erst anschließend von der Abteilung Volksbildung eingesetzt worden wären. Über dieses Verfahren hätten die Adressaten im Einladungsschreiben auch aufgeklärt werden müssen.

Die Schulverwaltung teilt meine Auffassung und ist darüber hinaus mit mir der Ansicht, daß auch eine Übermittlung der Adressen von Elternvertretern an einzelne Fraktionen in Bezirksverordnetenversammlungen nicht erforderlich und damit unzulässig ist. Demgegenüber ist eine Weitergabe der Adressen von Elternvertretern zur Erfüllung ihrer Aufgaben an die von ihnen vertretenen Eltern nicht zu beanstanden.

5.6 Wissenschaft und Forschung

Die Zahl der Forschungsvorhaben, deren datenschutzgerechte Durchführung ich zu beurteilen habe, nimmt ständig zu. Dabei bewähren sich die von mir entwickelten datenschutzrechtlichen Kriterien[1]. Forschungsvorhaben werden zwar zumeist von Hochschulinstituten, aber auch von privaten Forschungseinrichtungen durchgeführt, die von öffentlichen Stellen beauftragt sind.

Forschung an den Hochschulen

Ein Hochschulinstitut plant eine *Rechtstatsachenstudie „Gemeinsames Sorgerecht geschiedener Eltern"*, für das es Einsicht in Akten zu abgeschlossenen Scheidungsverfahren bei den Familiengerichten nehmen will. Dieses Vorhaben wirft datenschutzrechtliche Probleme auf, weil die entsprechenden Vorschriften der Zivilprozeßordnung und des Gesetzes über die freiwillige Gerichtsbarkeit nur solchen Personen Akteneinsichtsrechte einräumen, die ein „berechtigtes" oder „rechtliches" Interesse glaubhaft machen. Ob ein öffentlich-rechtliches Forschungsinteresse insoweit ausreicht, ist umstritten. Die Datenschutzbeauftragten sind jedoch der Auffassung, daß dies jedenfalls bei Ehescheidungsakten, deren Weitergabe das Bundesverfassungsgericht nicht einmal an Behörden zugelassen hat[2], nicht der Fall ist. Eine wissenschaftliche Auswertung von Ehescheidungsakten durch Dritte ist deshalb nach geltendem Recht nur nach vorheriger Einwilligung der Betroffenen zulässig. Ich bin jedoch der Auffassung, daß die Zivilprozeßordnung und das Gesetz über die freiwillige Gerichtsbarkeit in der Weise geändert werden sollten, daß unter bestimmten engen Voraussetzungen für Zwecke der sogenannten Ressortforschung unter möglichst weitgehender Wahrung des Persönlichkeitsrechts der Betroffenen eine wissenschaftliche Auswertung von Ehescheidungsakten auch ohne deren Einwilligung ermöglicht wird, wenn der Forschungszweck nicht auf andere Weise erreichbar ist. Nur so läßt sich praktische Konkordanz zwischen dem informationellen Selbstbestimmungsrecht der Verfahrensbeteiligten einerseits und dem Grundrecht der Forschungsfreiheit andererseits herstellen.

Ein weiteres Forschungsprojekt befaßt sich mit dem *Einsatz des Einzelrichters in Zivilsachen*. Im Auftrag des Bundesministeriums der Justiz und des nordrhein-westfälischen Justizministeriums wurden mit Zustimmung einzelner Landesjustizverwaltungen Akten von Zivilkammern analysiert, um festzustellen, unter welchen Voraussetzungen und mit welchen Folgen die Landgerichtskammern Rechtsstreitigkeiten auf den Einzelrichter übertragen. Auf diese Weise soll unter anderem festgestellt werden, ob die Übertragung auf den Einzelrichter den gewünschten Effekt einer Entlastung der Kollegialgerichte und der Beschleunigung der Zivilprozesse hat. Damit die Forscher feststellen können, ob die von ihnen ausgewerteten Gerichtsakten eine repräsentative Stichprobe bilden, sollten die Statistikämter der beteiligten Länder aus der Zählkartenerhebung in Zivilsachen Einzelangaben

[1] Vgl. meine 1987 in 2. Auflage erschienene Informationsschrift: Forschung und Planung, Checkliste zum Datenschutz

[2] BVerfGE 34, S. 209

zur Identifizierung von Kammern der untersuchten Landgerichte und Aktenzeichen übermitteln. Bei der Zählkartenerhebung in Zivilsachen handelt es sich um eine Geschäftsstatistik, die die Statistischen Landesämter im Auftrag der Landesjustizverwaltungen auf der Grundlage eines Beschlusses der Justizministerkonferenz führen. Die Landesjustizverwaltungen bleiben deshalb im datenschutzrechtlichen Sinne speichernde Stellen für die Daten aus der Zählkartenerhebung in Zivilsachen. Die Statistischen Landesämter haben sich als Auftragnehmer an die Weisungen der Landesjustizverwaltungen zu halten. Die statistikrechtlichen Vorschriften über die Weitergabe von Einzelangaben aus gesetzlichen Statistiken, die von den Statistikämtern in eigener Verantwortung geführt werden, sind auf die Geschäftsstatistik nicht anzuwenden. Vielmehr haben die Justizverwaltungen des Bundes und der beteiligten Länder durch geeignete Vereinbarungen mit den Wissenschaftlern sicherzustellen, daß die aus den Akten erhobenen Einzelangaben nur für den jeweiligen Forschungszweck verwendet und nach Abschluß der Auswertungen vernichtet werden. Dies ist in diesem Fall geschehen, auch wenn die getroffene Vereinbarung, von der ich erst nach Beginn des Projekts erfahren habe, in einzelnen Punkten präzisierungsbedürftig gewesen wäre. Ich halte dieses Verfahren auch bei der gegenwärtigen Fassung der Zivilprozeßordnung bei solchen Projekten für zulässig, die zur sogenannten Rechtsstabforschung zählen, bei denen also ausschließlich personenbezogene Angaben von Richtern oder anderen Justizbediensteten erhoben werden, um Erkenntnisse über ihre dienstliche Tätigkeit zu sammeln. Diese Informationen unterliegen zwar wie die Daten der verfahrensbeteiligten Bürger dem Datenschutz, Mitglieder des Rechtsstabes haben jedoch die Verwendung der sie betreffenden dienstlichen Daten für wissenschaftliche Zwecke eher hinzunehmen als Verfahrensbeteiligte z. B. in Ehescheidungsverfahren, die dem Gericht häufig Daten aus ihrer Intimsphäre offenbaren müssen.

Bei einer Neufassung der Prozeßordnungen sollte der Gesetzgeber deshalb die Einsicht in Gerichtsakten für Forschungszwecke differenziert danach regeln, ob Gegenstand der wissenschaftlichen Analyse das erkennende Gericht und seine Entscheidungen oder die Bürger sind, die das Gericht angerufen haben.

Aufgrund einer Eingabe bin ich auf das Vorhaben eines Hochschulinstituts aufmerksam gemacht worden, auf Band aufgezeichnete *Protokolle von Interviews* und deren Abschriften, die im Rahmen bestimmter Forschungsvorhaben und Diplomarbeiten im Fach Psychologie entstanden sind, für spätere wissenschaftliche Auswertungen *zu archivieren*. Grundsätzlich ist eine Einwilligung in die Datenerhebung für Zwecke der wissenschaftlichen Forschung nur dann wirksam, wenn sie sich auf ein bestimmtes Forschungsvorhaben bezieht. Bei Anlegung dieses strikten Maßstabs würden jedoch Sekundäranalysen, die demselben Forschungszweck wie die Ausgangsuntersuchung dienen, unmöglich gemacht. In Abstimmung mit mir hat das Hochschulinstitut daher eine Interviewvereinbarung entwickelt, die die Freiwilligkeit der Teilnahme am Interview unterstreicht und dem Befragten alternative Möglichkeiten der Einwilligung in eine befristete Aufbewahrung des Interviewprotokolls oder eine ständige Archivierung eröffnet. Nach Ende der Bandaufnahme können auf Wunsch des Interviewten einzelne Abschnitte des Gesprächs gelöscht werden. Die Nutzung des Archivs mit den Interviewprotokollen ist auf Mitarbeiter und Studierende des Instituts für Psychologie beschränkt. Das schriftliche Protokoll kann vollständig oder in größeren Auszügen im Forschungsbericht benutzt werden, wenn dessen Text dem Interviewten vorgelegt worden ist und dieser sein Einverständnis schriftlich erklärt hat. Der Interviewte kann sein Einverständnis zur Teilnahme an dem Interview und zur weiteren wissenschaftlichen Auswertung innerhalb von 14 Tagen ganz oder teilweise widerrufen. Damit ist nach meiner Auffassung eine datenschutzgerechte Lösung gefunden worden, die auch den grundrechtlich geschützten Belangen der Forschung Rechnung trägt.

Erstmals habe ich zur inhaltlichen Ausgestaltung von Lehrveranstaltungen an der Hochschule, insbesondere zum *Schutz der Persönlichkeitsrechte von Studenten bei sozialpsychologischen Experimenten* Stellung genommen.

Nach Angaben eines Petenten waren bei einem Seminar zur *Selbst- und Fremdwahrnehmung* an einem Universitätsinstitut Studienanfänger aus einem Nebenraum mit einer Videokamera von anderen Studenten höherer Semester gefilmt worden. Die Erstsemester waren vorab lediglich über die Tatsache informiert worden, daß eine Videoaufzeichnung für Zwecke der wissenschaftlichen Auswertung stattfinde. An jeder der drei Kleingruppen des Seminars nahm eine Person teil, die sich regelmäßig als homosexuell und darüber hinaus in den drei Gruppen entweder als mit AIDS infiziert, nicht infiziert oder ohne Bezugnahme auf AIDS vorstellte. Dadurch sollten bei den Studienanfängern als *„naiven Versuchspersonen"* Reaktionen hervorgerufen werden, mit deren Hilfe Hypothesen über verstärkte Vorurteile gegenüber Homosexuellen aufgrund der öffentlichen Diskussion zum Thema „AIDS" wissenschaftlich überprüft werden sollten. Die Studienanfänger wurden erst einen Tag nach dem Seminar brieflich über die tatsächliche Versuchsanordnung aufgeklärt.

Ich habe das Institut darauf hingewiesen, daß die grundgesetzlich garantierte Forschungsfreiheit ihre Grenze am Persönlichkeitsrecht des Einzelnen findet, wie es unter anderem durch das Recht am eigenen Bild nach dem Kunsturhebergesetz konkretisiert wird. Dies gilt auch für solche Versuchsanordnungen, die wesentlich auf „naive Versuchspersonen" angewiesen sind. Abgesehen davon, daß diese Versuchsanordnungen auch unter Psychologen nicht unumstritten sind, läßt sich das Erfordernis der „naiven Versuchsperson" nicht mit der datenschutzrechtlich gebotenen informierten Einwilligung vereinbaren. Zumindest ist in derartigen Situationen eine rückhaltlose Aufklärung der getäuschten Versuchsperson unmittelbar im Anschluß an den Versuch erforderlich, auf deren Grundlage die Versuchsperson entscheiden kann, ob sie nachträglich einer Dokumentation ihres Verhaltens auf Tonband oder Videokassette zustimmt oder Löschung verlangt.

Das Hochschulinstitut hat mir mitgeteilt, daß die kritisierten Videoaufzeichnungen ausnahmslos unter Zeugen gelöscht worden sind.

Zu diesem Problem habe ich eine Stellungnahme gegenüber dem Vorstand der Deutschen Gesellschaft für Psychologie abgegeben. Ich begrüße dessen Beschluß, den Belangen des Datenschutzes innerhalb der psychologischen Forschung besondere Aufmerksamkeit zu widmen. Die Gesellschaft will zu diesem Zweck eine Informationsbroschüre erstellen, die als Handanweisung Psychologen in Wissenschaft und Forschung praxisrelevante Vorschläge machen soll, wie Forschungsvorhaben in diesem Bereich datenschutzgerecht durchgeführt werden können.

Auch gegenüber dem Wissenschaftsrat, der sich erneut mit dem Verhältnis von Datenschutz und Forschung befaßt, habe ich Stellung genommen.

Elektronischer Lotse

Im Auftrag des Bundesministers für Forschung und Technologie und des Senators für Wissenschaft und Forschung wird ein *Großversuch zur Erprobung eines „Leit- und Informationssystems Berlin"* vorbereitet. 500 Fahrzeuge von privaten und gewerblichen Verkehrsteilnehmern sowie Mietwagen und Taxen sollen mit einem Bordcomputer („elektronischer Lotse") von der Größe eines Autoradios ausgestattet werden, der über ein Infrarotsignal Informationen über Standort, Geschwindigkeit und Fahrziel meldet, die von Infrarot-Baken an 200 ausgewählten Verkehrsknotenpunkten im gesamten Stadtgebiet empfangen und an die Verkehrsleitzentrale der Polizei weitergegeben werden. Dieses System der individuellen und dynamischen Verkehrsbeeinflussung soll den Versuchsteilnehmern und – bei erfolgreichem Verlauf des Versuchs – später allen Verkehrsteilnehmern z. B. Umleitungsempfehlungen bei Staus geben. Um die Akzeptanz und Wirtschaftlichkeit des Verkehrsleitsystems gegebenenfalls durch mehrstufige Befragungen feststellen zu können, werden im Rahmen des Feldversuchs auch fahrzeugbezogene Kennziffern an die Verkehrsleitzentrale übertragen. Dies ist nur nach vorheriger umfassender Aufklärung und ausdrücklicher Einwilligung der Versuchsteilnehmer zulässig.

Verläuft der Feldversuch erfolgreich und wird das Leit- und Informationssystem generell eingeführt, so werden keine personen- oder fahrzeugbezogenen Angaben mehr an den zentralen Rechner übermittelt.

Ich habe dem privaten Forschungsinstitut, das den Feldversuch durchführt, detaillierte Empfehlungen zur Formulierung der Versuchsteilnehmerverträge gegeben, die die Freiwilligkeit der Teilnahme z. B. auch für Angehörige des öffentlichen Dienstes und Mietwagenbenutzer sicherstellen sollen. Diese Empfehlungen sind berücksichtigt worden.

5.7 Organisation und Geschäftsordnung

Wahrung der Vertraulichkeit

Das Problem, die Vertraulichkeit in Diensträumen mit starkem Publikumsverkehr zu wahren, ist noch immer Gegenstand zahlreicher Beschwerden und Hinweise. Zunehmend bemühen sich die Behörden, durch bauliche und organisatorische Veränderungen die Situation zu verbessern. Hervorzuheben sind die Anstrengungen der Sozialleistungsträger und des Landeseinwohneramtes. Oft scheitern bereits die Bemühungen, mit geringem Aufwand datenschutzfreundlichere Lösungen herbeizuführen, daran, daß notwendige Haushaltsmittel nicht zur Verfügung gestellt werden.

Aktenunterbringung

Die Aufbewahrung von Akten und Karteien mit Personenbezug weist nach wie vor erhebliche Mängel auf. Da die Bezirksverwaltungen mehr als die Hauptverwaltungen bürgerbezogene Vorgänge zu bearbeiten haben, tritt das Problem der Aufbewahrung von Akten und Karteien vor allem dort auf.

Bei meinen Bezirksüberprüfungen, zuletzt in Tiergarten und Spandau, habe ich erneut Mängel in dieser Hinsicht feststellen müssen, ebenso bei anlaßbezogenen Prüfungen bei anderen Stellen. Insbesondere ist es unbefriedigend, daß die unzureichende Unterbringung von Akten und Karteien vor allem dort auffällt, wo es mit dem Sozialgeheimnis nach § 35 SGB I ein besonderes Amtsgeheimnis zu wahren gilt.

Häufig wird mir entgegengehalten, daß die Beschaffung geeigneter Büromöbel oder sicherer Schließsysteme so viel Geld verschlingen würde, daß man bestenfalls allmählich eine Verbesserung herbeiführen könne.

Wenn allerdings vorhandene Schließsysteme nicht genutzt werden, wenn - wie in einem Bezirksamt festgestellt - bei modernen, mit Sicherheitsschloß ausgestatteten Schränken die Türen ausgebaut werden, um bequemen Zugang an hochsensible Akten zu erhalten oder wenn offene Regalschränke mit Sozialakten in dem Wartebereich für Bürger aufgestellt werden, dann sind nicht finanzielle Engpässe, sondern Gleichgültigkeit bei Sachbearbeitern und ihren Vorgesetzten ursächlich.

Vordrucke

Der Bürger hat Anspruch darauf, zu erfahren, für welche Zwecke und auf welcher Rechtsgrundlage Daten von ihm erhoben werden. Über die Regelung des § 9 Abs. 2 BlnDSG hinaus entspricht dies einem allgemeinen verfassungsrechtlichen Grundgedanken.

Der Senator für Inneres hat inzwischen für seinen Geschäftsbereich die in meinem letzten Jahresbericht[1] zur Vordruckgestaltung enthaltenen Vorschläge aufgegriffen und in einem Rundschreiben veröffentlicht[2].

Jedoch auch in anderen Bereichen sind Vordrucke verbesserungsbedürftig. So wird zwar bei mehreren Vordrucken zur Lohn- bzw. Einkommensteuer die Rechtsgrundlage benannt. In anderen Formularen, so z. B. bei der „Anlage N", dem häufig benutzten Formular zur Angabe der Einkünfte aus nichtselbständiger Arbeit, fehlen allerdings die entsprechenden Angaben noch. Ich habe dem Senator für Finanzen empfohlen, die notwendigen Ergänzungen und Erläuterungen anzufügen, und hoffe, daß damit eine Verbesserung der Aufklärung der Bürger über den Umfang ihrer Mitwirkungspflicht bei der Datenerhebung erreicht wird.

Zur *Aufnahme einer Gewerbetätigkeit* ist nur in wenigen, in der Gewerbeordnung genannten Fällen eine Erlaubnis des bezirklichen Wirtschaftsamtes erforderlich. Hierzu hat der Betroffene selbst ein Führungszeugnis beizubringen. Bei der Mehrzahl der Gewerbetätigkeiten ist dagegen nur eine Anzeige beim Wirtschaftsamt ohne Beibringung eines Führungszeugnisses notwendig. Um „schwarze Schafe" möglichst schnell erkennen zu können, wird in diesen Fällen sogleich nach der Anzeige geprüft, ob eine Gewerbeuntersagung ausgesprochen werden muß. Zu diesem Zweck wird auch bei nur anzeigepflichtigen Gewerben ein *Führungszeugnis für Behörden* vom Bundeszentralregister eingeholt. Der Betroffene wurde bisher darauf nicht hingewiesen. Wenn das Führungszeugnis ohne Eintrag war, erhielt er normalerweise auch keine Kenntnis davon, weil in diesen Fällen das Wirtschaftsamt keinen Anlaß hatte, weitere Maßnahmen zu ergreifen. Überrascht waren allerdings jene Bürger, deren Führungszeugnis eine Eintragung enthielt und bei denen unverzüglich überprüft wurde, ob das Gewerbe zu untersagen ist.

Grundsätzlich sollen Informationen zunächst beim Betroffenen selbst eingeholt werden. Davon geht auch das Bundeszentralregistergesetz aus (§ 31 BZRG). Die Praxis der Gewerbeämter führt dagegen dazu, daß bei nur anzeigepflichtigen Gewerbetätigkeiten ohne Kenntnis der Betroffenen die gleichen Daten erhoben werden wie bei genehmigungspflichtigen. Um dies zu vermeiden, sollte dem Betroffenen die Wahl gelassen werden, ob er ein Führungszeugnis selbst beibringen will oder ob er mit der Einholung durch die Behörde einverstanden ist. Der Senator für Wirtschaft und Arbeit hat demgegenüber darauf hingewiesen, daß bei den nur anzeigepflichtigen Gewerben eine Mitwirkung des Antragstellers durch Beibringung eines kostenpflichtigen Führungszeugnisses nicht zumutbar sei. Der widersprüchliche Zustand kann endgültig nur durch eine Änderung der einschlägigen Bundesgesetze abgestellt werden.

Inwieweit fehlerhafte Vorgaben in Vordrucken unerlaubte Datenübermittlungen zwischen Behörden bewirken können, ohne daß dies den Beteiligten bewußt wird, zeigt folgender Fall:

Bisher hat der Polizeipräsident in Berlin vollständige Durchschriften von *Verkehrsunfallanzeigen* zur statistischen Auswertung an das Statistische Landesamt Berlin übersandt. Begründet wurde dies mit dem Gesetz zur Durchführung einer Straßenverkehrsunfallstatistik. § 2 des Gesetzes regelt abschließend, welche Informationen die Polizeidienststellen den Statistischen Landesämtern übermitteln dürfen. Die regelmäßige Übersendung der vollständigen Verkehrsunfall-Anzeigen geht über diesen gesetzlichen Rahmen weit hinaus. Wenn lediglich ein geringer Sachschaden entstanden ist, dürfen danach lediglich der Ort des Unfalls, die beteiligten Verkehrsteilnehmer und Verkehrsmittel sowie die Höhe des entstandenen Sachschadens übermittelt werden. Auf jeden Fall dürfen die Daten nur anonym weitergegeben werden. Auf meine Beanstandung werden künftig die Verkehrsunfall-Vordrucksätze so gestaltet, daß eine rechtmäßige Datenübermittlung gewährleistet ist.

Postverkehr

Das Verfahren des *Postaustausches* zwischen Berliner Behörden unter Beteiligung der Hauptverteilungsstelle beim Landesverwaltungsamt Berlin sowie die Beteiligung verschiedener Bundesbehörden an diesem Verfahren war von mir in den vergangenen Jahren geprüft worden[1].

Einzelne Verwaltungen haben inzwischen ihre Mitarbeiter durch eigene Rundschreiben auf die Problematik beim Postversand hingewiesen. Der Senator für Inneres hat in seinem Geschäftsbereich den Mitarbeitern mitgeteilt, daß sämtliche Schriftstücke und Akten mit personenbezogenen Daten ausnahmslos verschlossen zu versenden sind[2]. Darüber hinaus hat er in einem Rundschreiben auf die Geheimhaltungspflichten beim Dienstpostaustausch in der Berliner Verwaltung hingewiesen[3].

In November 1986 habe ich - wiederum stichprobenartig - eine Nachprüfung in der Hauptverteilungsstelle des Landesverwaltungsamtes durchgeführt.

[1] Jahresbericht 1986, Ziff. 4.5

[2] Rundschreiben V Nr. 53 vom 23. Juni 1987

[1] Vgl. Jahresbericht 1985, Ziff. 2.4

[2] Schreiben vom 25. Juni 1985 - AV A 2 -

[3] Dienstblatt I Nr. 15 vom 11. September 1987

Als Ergebnis ist zwar insgesamt eine Verbesserung bei der Versendung von Schriftstücken und Akten festzustellen. Die einzelnen Mitarbeiter sind offensichtlich aufmerksamer für datenschutzrechtliche Fragen auch beim Postversand geworden. Gleichwohl habe ich wiederum eine Vielzahl von offen versandten Akten und Schriftstücken mit sensiblen personenbezogenen Daten, die zum Teil besonderen Geheimhaltungsvorschriften unterliegen (z. B. Arztgeheimnis, Sozialgeheimnis), vorgefunden.

Dabei waren beispielsweise Ausländer-, Nachlaß-, Pflegschafts-, komplette Sozialhilfe-, Erziehungsgeld-, Jugendamts-, Ermittlungs- und Prozeßakten sowie Schriftstücke im Zusammenhang mit Zwangsvollstreckungen, der Aufnahme in eine Nervenklinik, Vormundschaftsangelegenheiten, Mitteilungen über nichteheliche Elternschaft, Vaterschaftsanerkenntnisse sowie unzählige Erste-Hilfe-Bögen, die formularmäßig Angaben über den Patienten, den Unfallhergang, die Vorgeschichte, den Befund, Diagnose und Therapie enthalten, offen versandt worden.

Das Spektrum der betroffenen Behörden reichte quer durch die Berliner Verwaltung. Die Mängel wurden erneut bei den betroffenen Verwaltungen beanstandet. Ich habe unabhängig davon auch die von der Stichprobenuntersuchung nicht betroffenen Verwaltungen vom Ergebnis meiner Prüfung unterrichtet. Die Berliner Verwaltung muß endlich geeignete technisch-organisatorische Maßnahmen treffen, um die Mängel beim Fachaustauschverkehr künftig abzustellen.

Wie wichtig genaue Identitätsprüfungen von Adressaten sein können, um *Fehlzustellungen* zu Lasten betroffener Bürger zu vermeiden, zeigt folgender Fall:

Ein Doktor der Politologie hatte mir einen an ihn gerichteten Arztbrief eines Gesundheitsamtes übergeben. Darin wurde er gebeten, Angaben über Geschlechtskrankheiten einer Patientin zu machen, die bei ihm in Behandlung sei.

Die Überprüfung hat ergeben, daß die Patientin gegenüber einer Polizeistreife angegeben hatte, daß sie gesundheitlich durch einen Arzt überwacht wird, dessen Name fast identisch mit dem des Politologen war. Eine genaue Anschrift konnte sie dabei jedoch nicht angeben. Mit den vorhandenen Hinweisen hatte dann das Gesundheitsamt versucht, den Arzt zu ermitteln. Hierzu wurde telefonisch eine Melderegisterauskunft eingeholt. Dabei kam es zu der Verwechselung, da ein geringfügiger Unterschied in der Schreibweise nicht berücksichtigt wurde. Daraufhin wurde der Politologe angeschrieben, da das Gesundheitsamt annahm, daß dieser der gesuchte Arzt sei. Danach wurden nicht nur die schutzwürdigen Belange der Patientin erheblich beeinträchtigt, sondern auch der Adressat kam gegenüber seiner Familie in Erklärungszwang.

Das Gesundheitsamt hat daraufhin ein spezielles Adreßbuch für Ärzte beschafft, um zukünftig Verwechselungen zu vermeiden.

6. Nachträge zu Feststellungen aus den Vorjahren

Landeseinwohneramt
(Jahresbericht 1986, Ziff. 2.1)

Verschiedene Aufgaben der Polizei machen es erforderlich, auch außerhalb der Dienstzeiten auf die Datenbestände des Landeseinwohneramtes (z. B. Führerscheinkartei, Ausländerakten) zuzugreifen. Durch einen Dauerdienst im Landeseinwohneramt wird nunmehr sichergestellt, daß die Daten nur im erforderlichen Umfang herausgegeben werden.

Ausländerwesen
(Jahresbericht 1986, Ziff. 2.1)

Die ursprüngliche Absicht, ein automatisiertes Verfahren zur Bearbeitung von Asylanträgen einzuführen, wurde zugunsten einer Lösung fallengelassen, bei der die gesamte Ausländerverwaltung in die Automation einbezogen wird. Meine Empfehlungen zur Verbesserung des Datenschutzes wurden durchweg aufgegriffen.

Kostenübernahme für Krankenhausbehandlungen
(Jahresbericht 1986, Ziff. 2.3)

Ein Entwurf für Vereinbarungen der Landesverbände der Krankenkassen mit den Krankenhäusern und deren Vereinigungen über die allgemeinen Bedingungen der Abwicklung von Kosten nach § 372 Reichsversicherungsordnung wurde von der Krankenhausgesellschaft vorgelegt. An den Beratungen bin ich beteiligt.

Nebentätigkeit von Hochschullehrern
(Jahresbericht 1986, Ziff. 2.3)

Der Senator für Finanzen hat sich meiner Auffassung angeschlossen, daß in der Landeshaushaltsordnung die Aufgaben des Rechnungshofes zu präzisieren sind, und wird entsprechende Änderungsvorschläge entwickeln.

Anonyme Anzeige wegen Rauschgiftschmuggels
(Jahresbericht 1986, Ziff. 4.2)

Die personenbezogenen Daten der Petentin wurden in allen Verbunddateien sowie im ISVB gelöscht. Über die Grundsätze zur Behandlung personenbezogener Daten bei anonymen Anzeigen wird noch verhandelt.

Urlaubsreise nach Indien
(Jahresbericht 1986, Ziff. 4.2)

Der Fall konnte aufgeklärt werden: Die Petentin war mit einer vor Jahren international zur Festnahme ausgeschriebenen Terroristin mit einem ähnlichen Namen verwechselt worden. Hinzu kam, daß die Fahndungsausschreibung in Indien nicht gelöscht worden war, obwohl die Täterin seit Jahren inhaftiert ist. Die indischen Behörden teilten mit, in derartigen Fällen sei eine Klärung innerhalb weniger Tage „absolut undenkbar". Der Petentin sind von deutschen Behörden die Reisekosten erstattet worden. So begrüßenswert die Regelung des Einzelfalles erscheint, so unbefriedigend bleibt die Tatsache, daß die Vorkehrungen gegen eine Wiederholung entsprechender Fälle nach wie vor nicht ausreichen. Es müssen bei Weitergabe von Daten an das Ausland klare Vereinbarungen getroffen werden[1].

Aussonderung von Altakten
(Jahresbericht 1986, Ziff. 4.2)

Die Arbeitsgruppe, die bis zum Jahre 1991 die Aussonderung von Altakten im Kriminalaktenbestand abschließen soll, ist personell verstärkt worden. Anzustreben ist, daß auch nach diesem Zeitpunkt die aktuelle Bearbeitung der Vorgänge möglich sein wird.

Rückmeldeverfahren bei der Strafverfolgung
(Jahresbericht 1986, Ziff. 4.2)

Seit 1982 hatte ich darauf gedrängt, daß die Ausgänge von strafrechtlichen Ermittlungsverfahren an den Polizeipräsidenten zurückgemeldet werden sollten. Bisher war aus dem Informationssystem Verbrechensbekämpfung nicht zu entnehmen, ob ein eingeleitetes Verfahren letztlich mit der Einstellung, einem Freispruch oder einer Verurteilung endete. Das konnte zu Mißverständnissen beim Abruf der Daten führen. Nunmehr hat der Senator für Justiz ein Konzept für die automatische Übermittlung von Verfahrensausgängen vorgelegt. Die Rückmeldungen erfolgen sowohl durch die Staatsanwaltschaft als auch – bei Eröffnung des Hauptverfahrens – durch die Strafgerichte Berlins. Damit ist sichergestellt, daß künftig im Informationssystem Verbrechensbekämpfung der jeweilige Verfahrensausgang enthalten ist.

Jubiläen
(Jahresbericht 1986, Ziff. 4.3)

In einer gemeinsamen Sitzung der AV-Leiter der Hauptverwaltungen ist meine Empfehlung aufgenommen worden, die Betroffenen rechtzeitig zu fragen, ob sie die in die Dankansprache aufzunehmenden Daten selbst vorgeben wollen oder ob sie mit der Verwendung der Personalakte einverstanden sind.

[1] Vgl. dazu Anlage 2

AV-Schülerunterlagen
(Jahresbericht 1986, Ziff. 4.4)

Die Schulverwaltung hat die Ausführungsvorschriften über die Führung schriftlicher Unterlagen über Schüler vom 9. Juli 1986 durch Verwaltungsvorschriften vom 25. März 1987 an die Erfordernisse der Praxis angepaßt. Nach einer einjährigen Übergangszeit wurden zum Beginn des Schuljahres 1987/88 auch geänderte Klassenbücher und Klassenlisten an den Berliner Schulen eingeführt, die den AV-Schülerunterlagen entsprechen.

Aktenführung in Sozial- und Jugendverwaltungen
(Jahresbericht 1986, Ziff. 4.5)

Die Arbeitsgruppe, die für die Sozialverwaltung eine Bestandsaufnahme der Probleme vornehmen sollte, hat ihre Arbeit abgeschlossen und einen Bericht verfaßt, der bei mir abgefordert werden kann. Eine entsprechende Arbeitsgruppe für die Jugendverwaltung soll ebenfalls eingerichtet werden.

Altlasten-Suchkonzept
(Jahresbericht 1986, Ziff. 4.6)

Nach § 15 Abs. 3 Satz 2 des geänderten Vermessungsgesetzes Berlin dürfen Hinweise auf öffentlich-rechtliche Festsetzungen, öffentlich-rechtliche Verfahren und amtliche Feststellungen in das Liegenschaftskataster aufgenommen werden. Damit ist ein erster Schritt in Richtung auf die erforderliche normenklare Regelung des Datenbestandes im Liegenschaftskataster getan.

Zusätzlich ist eine spezielle Regelung des Einsichtsrechts in das Liegenschaftskataster erforderlich, soweit diese Einsicht sich auch auf die Hinweise zum Vorliegen von Altlasten erstrecken soll. Bis zu dieser gesetzlichen Regelung dürfen Private nur dann Einsicht in die Hinweise auf Altlasten auf einem bestimmten Grundstück nehmen, wenn der Grundstückseigentümer zuvor eingewilligt hat. Demgegenüber dürfen Behörden auf diese Information zugreifen, soweit dies zur Erfüllung ihrer gesetzlich geregelten Aufgaben erforderlich ist.

Rückverteilung von Lohnsteuerkarten
(Jahresberichte 1980, Ziff. 2.6; 1981, Ziff. 2.3; 1986, Ziff. 5)

Bei einer Umfrage bei Abrechnungsstellen der Berliner Verwaltung zeigte sich, daß inzwischen fast alle Lohn- und Gehaltsstellen die Lohnsteuerkarten einzeln kuvertieren und verschlossen den jeweiligen Büroleitungen übersenden, die diese dann an die Beschäftigten weiterleiten.

7. Zusammenarbeit mit anderen Stellen

Konferenz der Datenschutzbeauftragten

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat in drei Sitzungen unter Vorsitz des Landesbeauftragten für den Datenschutz des Landes Nordrhein-Westfalen beraten:

30. Konferenz am 23. Februar 1987
- Abstimmung über die Prüfung der Volkszählung in Bund und Ländern

31. Konferenz am 4./5. Mai 1987
- Beschluß über die Rückmeldung des Ausgangs von Strafverfahren durch die Justiz an die Polizei
- Beschluß über ZEVIS
- Beschluß zur Neukonzeption des Ausländerzentralregisters[1]

32. Konferenz am 7. Dezember 1987
- Beschluß zu HIV-Hinweisen in polizeilichen Informationssystemen

Der Konferenzvorsitz wird mit dem Jahreswechsel turnusgemäß auf die Datenschutzkommission Rheinland-Pfalz übergehen.

Abgeordnetenhaus

Die vielfältige und gute Zusammenarbeit mit dem Abgeordnetenhaus fand ihren Ausdruck in Aussprachen im Plenum, in Erörterungen von Datenschutzproblemen in den Ausschüssen sowie in Gesprächen mit Fraktionen und einzelnen Abgeordneten.

Hervorzuheben ist, daß sich das Plenum in einer eingehenden Debatte mit den Problemen der *Volkszählung* gründlich auseinandergesetzt hat. Darüber hinaus sind einzelne Fragenkomplexe der Volkszählung eingehend in den Ausschüssen behandelt worden. So z. B. anläßlich der Entscheidung über die Beschaffung der Personalcomputer im Unterausschuß automatisierte Datenverarbeitung des Hauptausschusses. Die Frage der Ausgestaltung der Anstaltszählung war Gegenstand mehrerer Beratungen im Rechtsausschuß. In beiden Ausschüssen hatte ich die Gelegenheit zu einer ausführlichen Stellungnahme, die auch berücksichtigt wurde. Erörtert wurde ferner die Problematik einer Sammlung von Ordnungswidrigkeitenanzeigen durch den Staatsschutz zur Erstellung eines Lagebildes.

Der *Unterausschuß Datenschutz* des Ausschusses für Inneres, Sicherheit und Ordnung hat in fünf Sitzungen Themen aus meinen Jahresberichten, aber auch datenschutzrelevante Fragen der Abgeordneten intensiv beraten. Gegenstand waren insbesondere ein Antrag zur Regelung der Forschung mit Entnazifizierungsakten, die Verordnung zur Durchführung des Meldegesetzes, Regelung, Organisation und Durchführung der Volkszählung, die Umsetzung des Volkszählungsurteils in landesrechtliche Vorschriften, die automatisierte Datenverarbeitung der Polizei (hier insbesondere die personengebundenen Hinweise), der Datenschutz in der Gesundheits- sowie in der Schulverwaltung.

Aufsichtsbehörde nach dem Bundesdatenschutzgesetz

Im Rahmen der guten Zusammenarbeit mit der *Aufsichtsbehörde für den Datenschutz* beim Senator für Inneres wurden Fragen des Datenschutzes im Bereich der Volkszählung, beim internen Dienstpostaustausch (Postverteilung, Fachpostaustausch), bei der Übermittlung von Daten im Zusammenhang mit AIDS, bei den Neuen Medien sowie die gesetzliche Regelung der Statistik behandelt.

Meldungen zum Dateienregister

Das von mir zu führende *Dateienregister* enthält nunmehr 1598 (Stand: 1. September 1987) Dateien (Vorjahr: 1454) von 333 (303) speichernden Stellen. Das Dateienregister gibt damit einen recht guten Überblick über die automatisierte Datenverarbeitung in der Berliner Verwaltung. Die Zunahme ist auch ein Zeichen für die ständig fortschreitende Automation in der Berliner Verwaltung. Zum besseren Überblick für den Bürger habe ich einen Auszug erstellt, der wegen der zahlreichen Änderungen neu herausgegeben wird.

Berlin, 14. Dezember 1987

Der Berliner Datenschutzbeauftragte

Dr. Kerkau

[1] Vgl. Anlage 4

Anlage 1

Datenschutz und Neue Medien
Beschluß der Internationalen Konferenz der Datenschutzbeauftragten 1987

1. Die Internationale Konferenz der Datenschutzbeauftragten beobachtet seit Jahren die Entwicklung der Neuen Medien und die damit verbundenen Probleme des Datenschutzes. Sie hat mit ihren Entschließungen vom 18. Oktober 1983 in Stockholm und vom 26. September 1985 in Luxemburg Forderungen zur Verbesserung des Datenschutzes erhoben.

2. Der Stand der Massenmedien und Telekommunikation im Jahre 1987 ist durch folgende Merkmale gekennzeichnet:
   - Die verschiedenen für die Telekommunikation genutzten analogen und digitalen Einzelnetze streben nach einer Vereinheitlichung der technischen Normen; zunehmend entstehen einheitliche nationale Infrastrukturen für die Telekommunikationsnetze.
   - Dienste für die Verbreitung von Massenmedien und für andere Telekommunikationsformen verschiedenster Art werden auf diesen Netzen national und international angeboten.

3. Die Internationale Konferenz der Datenschutzbeauftragten ist besorgt über die Sammlung einer zunehmend größeren Anzahl von personenbezogenen Daten durch Massenmedien und Telekommunikationsdienste. Die Risiken sind offensichtlich, die in einer derartigen Kumulation von Daten und deren möglichem Gebrauch zu Zwecken liegen, die nicht mit den Zwecken übereinstimmen, für die sie erhoben wurden. Soweit keine anonymen Nutzungsformen eingeführt werden, ermöglicht die über die ursprünglichen Kommunikationszwecke hinausgehende Verarbeitung derartiger Informationen den Aufbau von Daten über die Lebensführung und Interessen von Einzelindividuen und Familien. Eine solche Entwicklung wird als keineswegs wünschenswert angesehen.

   Die Informationen konzentrieren sich letztlich bei wenigen öffentlichen und privaten Netzbetreibern und Kommunikationsanbietern (Post, Teleports, internationale Serviceunternehmen). Die Risiken des Mißbrauchs, der Sabotage und Spionage sowie der Manipulation bürden diesen Institutionen eine erhebliche Verantwortung auf, ohne daß in den meisten Ländern die nationalen Gesetze hinreichende rechtliche Regelungen hierfür vorsehen.

4. Die Internationale Konferenz der Datenschutzbeauftragten fordert deshalb nachdrücklich die Entwicklung von Regelungswerken auf nationaler und internationaler Ebene. Für die erforderlichen technischen und organisatorischen Maßnahmen zur Datensicherung sind internationale Normen anzustreben. Die Zusammenarbeit der nationalen Kontrollinstanzen ist zu verbessern.

Anlage 2

Anforderungen an datenschutzrechtliche Regelungen des Bundes aus der Sicht der Länder

Gesetz	Änderungswünsche	Entwurfslage	Stellungnahmen der DSBen	Koalitions-vereinbarung
Bundesdaten-schutzgesetz	Anpassung an VZ-Urteil	EBTDrs. 10/4737 (verfallen)	Erklärung d. Konf. v. 4. 11. 83 Entschließung d. Konf. v. 9. 4. 86	ja
Strafprozeß-ordnung	Regelung der Informationseingriffe	-	Stellungnahme d. Konf. v. 24./25. 11. 86	ja
Justizmitteilungs-gesetz	Verringerung des Kreises der Adressaten	EBMJ v. 8. 9. 86	Stellungnahme d. AK Justiz der DSB vom 15./16. 12. 86	ja
Strafvollzugs-gesetz	Regelung des Umgangs mit Gefangenendaten	Arbeitsentwurf BMJ v. 31. 3. 87	bisher nein	ja
Jugendstrafvoll-zugsgesetz	Regelung des Umgangs mit Gefangenendaten	Arbeitsentwurf BMJ v. 1. 6. 84	bisher nein	nein
Untersuchungs-haftvollzugsgesetz	Regelung des Umgangs mit Gefangenendaten	Arbeitsentwurf v. 24. 2. 86	bisher nein	nein
Häftlings-überwachung	Schaffung einer Befugnisnorm	-	-	ja
Strafverfolgungs-statistik	Schaffung einer Befugnisnorm	-	-	ja
Bundesverfas-sungsschutzG	Anpassung an VZ-Urteil	BTDrs. 10/4737 (verfallen)	Entschließung d. Konf. v. 18. 4. 86 Entschließung d. Konf. zu „Sicherheitsgesetzen“ v. 27. 1. 86	ja
BND-Gesetz	Rechtsgrundlage	BRDrs. 66/86, § 15 (verfallen)	Beschluß d. AK Sicherheit der DSB v. 21. 1. 86	nein
BKA-Gesetz	Anpassung an VZ-Urteil	-	bisher nein	ja
BGS-Gesetz	Anpassung an VZ-Urteil	-	nein	ja
Sicherheits-überprüfungsG	Rechtsgrundlagen	Kerntechn. Anlage: BMI-Entwurf Stand: 8. 7. 86	BfD gegenüber BMI vom 11. 11. 86	ja
Bundeszentral-registerG	Beseitigung von Defiziten (z. B. § 12)	-	-	ja
AusländerG	Anpassung an VZ-Urteil Normenklarheit	-	-	ja
Ausländerzentral-registerG	Rechtsgrundlage	-	Beschl. Konf. v. 4./5. 5. 87	ja
Waffengesetz	Normenklarheit bei Überwachung	BTDrs. 10/1748 (verfallen)	BfD gegenüber BMI v. 30. 4. 87	ja
Melderechts-rahmenG	Hotelmeldepflicht Krankenhäuser	-	BlnDSB gegenüber Abge-ordnetenhaus v. 4. 7. 86	nein
Straßenverkehrs-gesetz	Datenflüsse bei Fahrerlaubnissen	-	-	nein
Gewerbeordnung	Verarbeitung von Daten d. Gewerbetreibenden	BRatDrs. 440/83	-	nein
GaststättenG	Verarbeitung von Daten d. Gewerbetreibenden	-	-	nein
Personen-beförderungsG	Verarbeitung von Daten	-	-	nein

Gesetz	Änderungswünsche	Entwurfslage	Stellungnahmen der DSBen	Koalitions-vereinbarung
KreditwesenG	Bankgeheimnis, Kundendaten	-	-	nein
Versicherungs-vertragsG	Versichertendaten	-	-	nein
Statistikgesetz	Fortführung der Bereinigung und Anpassung an das VZ-Urteil	HochSchulStatG Referentenentwurf Dezember 85	Entschließung v. 27./28. 3. 84	nein
Abgabenordnung	weitere Anpassung an VZ-Urteil	-	-	nein
Sozialgesetz-buch X	weitere Anpassung an VZ-Urteil	-	-	nein
Gesetz über So-zialversiche-rungsnummer	Rechtsgrundlage	Entwurf BMA v. 1. 12. 86	BlnDSB August 87 BayLfD 3. 2. 86 BfD 4. 2. 86 NdS 12. 2. 86	nein
„Datenhilfe"-Abkommen	Int. Vereinbarung über grenz-überschreitenden Datenschutz	-	-	nein
Arbeitnehmer-datenschutz	Umgang mit Personaldaten	-	Entschließung d. Konf. v. 27. 3. 84	nein
Beamtenrechts-rahmenG	Umgang mit Personaldaten	-	Entschließung d. Konf. v. 27. 3. 84	nein
BundesbeamtenG	Umgang mit Personaldaten	-	Entschließung d. Konf. v. 27. 3. 84	nein
Hochschul-rahmenG	Umgang mit Studentendaten	-	-	nein
ParteienG	Umgang mit Mitgliedsdaten	-	-	nein
Bundesrechts-anwaltsordnung	Umgang mit Personaldaten	BTDrs. 10/3854 (verfallen)	Schreiben BfD an BT-Rechtsausschuß v. 24. 1. 86	nein
Kammerrecht	Umgang mit Mitgliedsdaten	-	-	nein
BGB	Entmündigungs-, Vormund-schafts-, Pflegschaftsrecht	Entwurf ist geplant	-	ja
Prozeßkosten-hilfeG	Umfang der Datenverarbeitung	-	-	nein
ZPO	Akteneinsicht, -vorlage, Schuldver-zeichnis	Schuldverzeichnis: Entwurf BMJ 1. 8. 85	-	ja
FGG, AGG, SGG, VwGO	Akteneinsicht, -vorlage	-	-	nein
PersonenstandsG	Anpassung an VZ-Urteil	-	-	ja
Embryonen-schutzG	pers.bez. Daten im Zusammen-hang mit Gentechnologie	-	-	ja
BundesarchivG		Entwurf v. 26. 3. 85 BTDrs. 10/3072 (erneuert eingebracht)	Beschluß d. Konf. v. 27. 4. 82	ja
Presserechts-rahmenG	Datenschutz bei der Bericht-erstattung und im Archiv	Entwurf v. 25. 7. 74	-	
Telekommu-nikationsO	Nachbesserung der Defizite	VO v. 5. 11. 86 ÄndVO v. 15. 6. 87	Beschluß v. 21. 2. 86	nein

Anlage 3

Unter Mitwirkung von Berlin, Bremen, Hamburg und Nordrhein-Westfalen erarbeitete erste Empfehlungen zum Datenschutz bei der Automatisierung des Zahlungsverkehrs

Es ist davon auszugehen, daß der Bürger nicht in der Lage ist, die Sicherheit eines automatisierten Verfahrens zu beurteilen. Besonders groß sind seine Unsicherheit gegenüber einem so komplexen System wie dem zur Automatisierung des Zahlungsverkehrs und seine Ungewißheit über die mit dem Einsatz dieses Systems verbundene mögliche Gefährdung. Systeme des automatisierten Zahlungsverkehrs kommen weltweit zunehmend zum Einsatz. Beispiele dafür sind Geldausgabeautomaten, Btx-Kontoführung, POS-Kassen.

Im folgenden wird auf einige heute bereits erkennbare Gefährdungen für den Bürger hingewiesen. Es werden jeweils Maßnahmen empfohlen und Hinweise gegeben, um diese Gefährdungen nach Möglichkeit zu reduzieren. Die Wirksamkeit, Durchführbarkeit und Angemessenheit der empfohlenen Maßnahmen bedürfen noch eingehender Erörterung.

1. Fehlen einer Nachweismöglichkeit für den Bürger bei maschinell authentifizierter Transaktion

   Der Glaube an die Zuverlässigkeit automatisierter Systeme wird dann besonders bedenklich, wenn dieser Glaube negative Auswirkungen von existenzieller Bedeutung für den Betroffenen haben kann. Ein Bürger, der eine Buchung bei einer Transaktion reklamiert, die maschinell authentifiziert wurde, setzt sich möglicherweise dem schwerwiegenden Vorwurf aus, selbst eine kriminelle Handlung begangen zu haben. Dieser Vorwurf ist immer dann von dem Betroffenen selbst nicht widerlegbar, wenn der reklamierten Transaktion kein von ihm selbst unterschriebener Beleg zugrunde liegt. Die besondere Gefahr für den Bürger besteht daher immer dann, wenn Transaktionen ausschließlich auf der Basis maschineller Authentifizierung erfolgen. In einem solchen Fall wird kein Beleg archiviert, der zur Prüfung der Echtheit des Belegs einschließlich der Unterschrift einer neutralen Stelle übergeben werden könnte. Archiviert wird günstigstenfalls das, was einer Datenverarbeitungsanlage zur Authentifizierung zur Kenntnis gebracht wurde.

   Der Bürger hat im Ernstfall keine Möglichkeit, seine Aussage durch Unterlagen zu stützen. Der Nachweis der Gegenseite beruht wesentlich auf der Aussage, das automatisierte System sei sicher. Diese Aussage wird ein Außenstehender nur sehr selten widerlegen können. Gegen den Bürger wird damit eine Aussage als Beweis genutzt, deren Wahrheitsgehalt praktisch nur die Gegenseite beurteilen kann.

   Empfehlungen:

   - Der Bürger sollte über eine als Beweismittel verwendbare Zusammenstellung aller von ihm veranlaßten Transaktionen verfügen. Damit sollte nicht nur der Inhalt jeder einzelnen Transaktion, sondern auch die Lückenlosigkeit dieser Aufzeichnungen nachgewiesen werden können. Bei einem Einspruch wäre der Bürger dann in der Lage nachzuweisen, daß eine bestimmte Transaktion nicht oder nicht so von ihm veranlaßt wurde.
   - Im Streitfall ist die Beweislage für den Bürger besonders ungünstig, wenn für Beweiszwecke nur maschinell authentifizierte Nachrichten archiviert werden können. Grundlage des Beweises der Gegenseite ist dann die Behauptung, das automatisierte System sei sicher und arbeite fehlerfrei.

     Der Bürger oder eine für ihn tätige Stelle sollte in diesem Fall die Sicherheit und Zuverlässigkeit des Systems überprüfen können. Dazu ist es wichtig zu wissen, ob und in welchem Umfang bisher Fehler und Mißbrauchshandlungen oder -versuche bekannt geworden sind. Es sollte daher überlegt werden, ob für datenverarbeitende Systeme, bei denen wesentliche Transaktionen auf der Basis maschineller Authentifizierung erfolgen, eine Melde- oder Aufzeichnungspflicht wichtiger Ereignisse, die die Datensicherheit betreffen, vorgeschrieben werden kann.
   - Die Maßnahmen zur Datensicherung sollten so geartet sein, daß sie offengelegt werden können. Die Schutzwirkung verwendeter Verfahren sollte nicht wesentlich auf der Vertraulichkeit der getroffenen Sicherungsmaßnahmen beruhen. Vertraulich müssen selbstverständlich die verwendeten Schlüssel sein. Falls die verwendeten Verfahren unter Berufung auf deren notwendige Vertraulichkeit der unabhängigen und umfassenden Prüfung nicht zugänglich gemacht werden, besteht die Gefahr, daß eine hinreichende Datensicherheit unterstellt wird, ohne wirklich vorhanden zu sein.
   - Es müssen die Folgen für den Fall überlegt werden, daß ein geheimer Schlüssel wie zum Beispiel der Poolschlüssel oder der Institutsschlüssel zur Berechnung der PIN Dritten bekannt wird.

2. Durchsetzbarkeit von Datenschutzrechten

   Das Geflecht der diversen an einem automatisierten Zahlungsvorgang (zum Beispiel POS) beteiligten Stellen birgt die erhebliche Gefahr in sich, daß der Kunde als Träger des informationellen Selbstbestimmungsrechts nicht mehr nachvollziehen kann, welche Stelle aus welchem Grund welche Daten über ihn erhält, verarbeitet oder speichert. Bei POS wird an die Stelle des anonymen Kaufs ein Vorgang gesetzt, bei dem die Daten des Kunden im Rahmen eines komplexen ADV-Verfahrens übermittelt, verarbeitet und gespeichert werden.

   Die datenschutzrechtliche Einordnung von Autorisierungszentralen ist wie die anderer Clearingstellen im Bereich des Kreditwesens nicht eindeutig. Es bleibt unklar, wie das Verantwortungsgeflecht „Kunde", „Handelsunternehmen", „Kreditinstitut", „Clearingstelle" bzw. „Autorisierungszentrale" den datenschutzrechtlichen Termini „speichernde Stelle", „Auftragsdatenverarbeitung", „Auftragnehmer", „Auftraggeber" zugeordnet werden kann.

   Durch diese Unklarheit wird die datenschutzrechtliche Verantwortung dem Kunden gegenüber verwischt. Es besteht Unsicherheit über den Adressaten datenschutzrechtlicher Ansprüche (§ 4 BDSG), sofern dem Kunden die beteiligten Institutionen überhaupt bekannt werden.

   Empfehlungen:

   - Es ist darauf zu achten, daß der Kunde die Möglichkeit erhält, die seine personenbezogenen Daten betreffenden ADV-Prozesse zu übersehen, so daß die Nutzung des Systems mit einer impliziten aber qualifizierten Einwilligung in das Verfahren verbunden werden kann. Mit der Aufklärung über die in dem jeweiligen Verfahren stattfindenden datenschutzrechtlich relevanten Phasen der automatisierten Datenverarbeitung wird dem Kunden auch die Möglichkeit gelassen, seine aus den Datenschutzgesetzen folgenden Rechte gezielt wahrzunehmen.
   - Die rechtliche Einordnung von Autorisierungszentralen läßt sich möglicherweise nur durch klare Anpassungen der Nutzungs- und Zusammenarbeitsverträge an die Rechtskonstruktion der Datenschutzgesetze erreichen. Es könnte auch über die Sinnhaftigkeit des in den bestehenden Datenschutzgesetzen definierten Begriffs der Auftragsdatenverarbeitung diskutiert werden.

3. Rechtliche Überprüfung der AGB sowie der Bedingungen für die Abwicklung des automatisierten Zahlungsverkehrs

   Ein Kontoinhaber dürfte kaum eine reelle Chance haben nachzuweisen, daß er keine Ursache für die mißbräuchliche Verwendung seiner Identifikationsmerkmale gegeben hat. Es ist zweifelhaft, ob eine Bank selbst dann überhaupt haftet, wenn dem Kunden der Nachweis gelingen sollte, daß ein Dritter die Codes technisch ausgeforscht hat; denn trifft dafür die Bank ein Verschulden? Es sei die Frage erlaubt,

warum Banken das Restrisiko dem Kunden auferlegen, wenn sie von der Richtigkeit ihrer Aussage überzeugt sind, ihr Sicherungssystem sei absolut sicher.

Empfehlung:

Die für die Kontoführung geltenden Geschäftsbedingungen sollten unter Zugrundelegung der jeweiligen technisch-organisatorischen Bedingungen einer juristischen Prüfung im Hinblick auf das Gesetz zur Regelung des Rechts der Allgemeinen Geschäftsbedingungen (AGB-Gesetz, insbesondere §§ 3, 9 Abs. 2 Nr. 1 und 2, 11 Nr. 15 Alternative a) unterzogen werden. Möglicherweise führt das Prüfungsergebnis zu Konsequenzen für die AGB der Banken.

4. Gefahr für die Anonymität von Transaktionen

In einem automatisierten Zahlungssystem ist die maschinelle Authentifizierung häufig mit einer Zusatzinformation verbunden. Ein maschineller Scheck wird etwa in einem bestimmten Geschäft unterschrieben. Der unterschriebene Scheck enthält zwar keinerlei Aussage darüber, bei welcher Gelegenheit er unterschrieben wurde. Es ist aber damit zu rechnen, daß dem Scheck eine Information über seine Herkunft zugefügt wird, mit der er bei seiner weiteren automatisierten Bearbeitung verbunden bleibt. Durch das Archivieren der Schecks mit Herkunftsangabe in einer maschinell auswertbaren Form entsteht bei der Bank eine Art Verhaltensprofil des einzelnen Kunden. Soweit bei dem Zahlungssystem zusätzliche Stellen in den Datenfluß einbezogen werden (zum Beispiel Autorisierungszentralen bei POS, Clearingstellen) entstehen noch zusätzliche Risiken durch institutsübergreifende zentrale Aufzeichnungen der Zahlungsvorgänge.

Empfehlungen:

- Um das Erstellen von Verhaltensprofilen unmöglich zu machen, sollte das Gesamtverfahren so gestaltet werden, daß vom archivierten maschinellen Scheck durch automatisierte Auswertung nicht unmittelbar auf den Erstempfänger des Schecks geschlossen werden kann. Möglicherweise könnte auch die maschinenlesbare Archivierung derartiger Schecks bei der Bank untersagt werden.
- Die dokumentierten Daten sollten auf das für die Durchführung des Verfahrens erforderliche Maß eingeschränkt und das Gesamtverfahren so gestaltet werden, daß möglichst wenig Daten erforderlich werden. Die dann zu speichernden Daten über die Zahlungsvorgänge sollten so früh wie möglich gelöscht werden oder - sofern aus gesetzlichen Gründen eine längere Speicherungsdauer notwendig ist - auf Datenträger übertragen werden, die eine maschinelle Auswertung nicht zulassen.
- Im Hinblick auf das bundesweite POS-Verfahren sollten vorrangig Autorisierungsverfahren eingerichtet werden, die eine zentrale Dokumentation der Zahlungsvorgänge überflüssig machen.

5. Preisgabe differenzierter Negativmeldungen an den POS-Kassierer

Für den Zahlungsvorgang sind differenzierte Meldungen an den Händler nicht erforderlich, da für diesen lediglich wichtig ist, ob diese Zahlungsweise gewählt werden kann. Im Falle der Negativmeldung erfolgt eine gewisse Differenzierung im Antwortcode, die Rückschlüsse darauf zuläßt, ob von Kunden nicht zu vertretende technische Probleme an ec-Karte, ec-Kasse, Datenfernverkehr oder Rechner der Autorisierungsstelle vorliegen, ob die Karte ungültig ist oder ob das Kreditinstitut den Kunden um Rücksprache bittet. Diese Differenzierung geht heute bei bestimmten POS-Kassen an den Kassierer, bei anderen ausschließlich an den Kunden und wird damit begründet, daß der Kunde nähere Auskunft fordert, wenn ein Zahlungsversuch zurückgewiesen wird.

Empfehlung:

- Der Kassierer sollte lediglich den Hinweis erhalten, ob eine Zahlung im POS-Verfahren möglich ist oder nicht; der Kunde dagegen wird über den näheren Grund der Abweisung unterrichtet.

6. Gefahren für die Vertraulichkeit des Dialogs

Der Kunde hat keine Möglichkeit zu überprüfen, ob nicht Manipulationen an den Endgeräten (zum Beispiel POS-Kassen, Geldautomaten) oder an den DFÜ-Schnittstellen vorgenommen worden sind, die zur Offenbarung, gegebenenfalls auch Aufzeichnung der PIN oder für den Kunden bestimmter Nachrichten führen können. Die Vertraulichkeit der Eingabe der PIN durch den Kunden sowie gegebenenfalls der Rückmeldungen an den Kunden über ein Display hängt wesentlich von der verwendeten Technik und von baulichen und organisatorischen Gegebenheiten an den Endgeräten ab. Eigene Beobachtungen haben gezeigt, daß die verwendeten Tastaturen mit Display auch dann nicht immer zuverlässig vor unbefugter und unbemerkter Beobachtung geschützt sind, wenn Abdeckungen verwendet werden.

Bei Btx-Konten darf davon ausgegangen werden, daß der Bürger, der die Einrichtung eines Kontos erwägt, nicht beurteilen kann, ob das Sicherungskonzept seiner Bank ausreicht, um eine richtige Verarbeitung seiner per Btx erteilten Aufträge zu gewährleisten und jeden unbefugten Zugriff auf seine Konten abzuwehren. Die Banken rechnen Verfügungen, die durch ihre Programme für die Btx-Kontenführung ausgeführt wurden, in jedem Fall dem Kontoinhaber zu. Aus der Sicht von Fachleuten muß diese absolute Sicherheit in Frage gestellt werden.

Empfehlungen:

- Die Sicherheit vor Manipulationen an Endgeräten, die zur Offenbarung von Daten aus der Interaktion führen können, kann nur technische Sicherungen an den Endgeräten bzw. der DFÜ-Schnittstelle erfolgen. Dies kann durch wirksamen Verschluß und Verplombung nebst Plombenüberwachung erfolgen. Wer dies etwa bei POS durchführen soll, muß zunächst offen bleiben.
- Die Vertraulichkeit der Eingabe der PIN und gegebenenfalls der Rückmeldungen des Systems an den Kunden kann nur durch eine geeignete Gestaltung der Endgeräte und ihrer Umgebung erreicht werden, die es dem Kunden ermöglicht, seine Aktivitäten vertraulich zu halten.
- Bei der Datenübertragung können durch Transportverschlüsselung wesentliche Risiken der unbefugten Kenntnisnahme des Datenverkehrs gemindert werden. Dabei wird vorausgesetzt, daß die Verschlüsselung in einem besonders vor Manipulationen geschützten Bereich der Endgeräte erfolgt.
- Bei Btx sollte das bestehende Sicherungskonzept laut „Abkommen über Bildschirmtext" noch stärker darauf ausgerichtet werden, Gefährdungen für das Vermögen der Kunden auszuschließen oder zu begrenzen. Dies könnte unter anderem durch verstärkte Nutzung der TAN, intensivere Überwachung von Fehlversuchen bei PIN- und TAN-Eingabe sowie zeitlich befristete Sperren - zum Beispiel während Urlaubsreisen - erreicht werden.

Die beschriebenen Risiken erlangen besonderes Gewicht, wenn ein sozialer oder wirtschaftlicher Druck zur Nutzung von Systemen zur Automatisierung des Zahlungsverkehrs erzeugt wird. So muß mit der Möglichkeit gerechnet werden, daß der einzelne Bürger nur noch in beschränktem Umfang frei ist zu entscheiden, ob er sich eines solchen Systems bedienen will. Der soziale Druck kann so groß werden, daß der einzelne in seiner Entscheidung nicht mehr frei ist. Bei der Btx-Kontenführung könnte zum Beispiel eine Gefahr für die freie Entscheidung entstehen, wenn die Banken aus Rationalisierungsgründen ihren Schalterservice abbauen und Druck auf die Kunden, von denen heute bekanntlich keiner auf ein Girokonto verzichten kann, zur Führung von Btx-Konten ausüben würden.

Um dieser Gefahr zu begegnen, ist zu fordern, daß die heutigen Zahlungsformen im nichtautomatisierten Zahlungsverkehr (zum Beispiel Barzahlung, Überweisung) erhalten bleiben und auf zumutbare und nicht diskriminierende Weise genutzt werden können.

Anlage 4

Beschluß
der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 4./5. Mai 1987 zur Neukonzeption des Ausländerzentralregisters

I.

Unter Federführung des Bundesministers des Innern wird zur Zeit das bestehende Ausländerzentralregister (AZR) beim Bundesverwaltungsamt mit dem Ziel einer Effizienzsteigerung überarbeitet.

Grundsätzlich ist die beabsichtigte Schaffung einer verfassungsrechtlich notwendigen gesetzlichen Regelung sowohl für die Datenverarbeitung beim Bundesverwaltungsamt als auch für die Kommunikation der Teilnehmer mit dem Ausländerzentralregister zu begrüßen. Schon jetzt stehen den Benutzern weit über 100 Millionen Daten von ca. 10 Millionen Ausländern zur Verfügung. Geplant ist, die Verwendbarkeit des Datenbestandes durch den potentiellen Teilnehmerkreis des AZR zu erhöhen.

Dient das AZR bis jetzt vorwiegend der Aufenthaltsermittlung von Ausländern und der Vorbereitung ausländerrechtlicher Entscheidungen, so sieht die geplante Regelung eine „stärkere Einbindung in das System zum Schutz der inneren Sicherheit" sowie eine verbesserte Nutzung zu statistischen Zwecken vor. So ist die Einstellung des polizeilichen INPOL-Fahndungsbestands in das AZR geplant.

Das Recht auf informationelle Selbstbestimmung steht auch den in der Bundesrepublik Deutschland und Berlin lebenden Angehörigen anderer Staaten zu. Eine Neuregelung muß daher vermeiden, daß besondere Vorschriften für diese Personengruppe zu einer allgemeinen Diskriminierung der Betroffenen als potentielle Rechtsbrecher führen.

II.

Von entscheidender Bedeutung für die datenschutzrechtliche Bewertung des Registers sind die Funktionen, die es erfüllen soll. Außer Frage steht seine Verwendung als Indexregister zum Zweck der Feststellung, ob eine - und wenn ja, welche - Ausländerbehörde Unterlagen über einen bestimmten Ausländer besitzt.

Damit soll das AZR den Zugang zu den eigentlichen Ausländer- und Meldedaten erleichtern; es kann und darf den Rückgriff auf die bei den örtlichen Behörden gesammelten Informationen nicht ersetzen. Allenfalls bei Eilentscheidungen sollten die im Register gespeicherten Daten unmittelbar für Maßnahmen der Verwaltung herangezogen werden. Keinesfalls darf das AZR zu einem bundesweiten zentralen Melderegister für Ausländer werden.

Für nichtöffentliche Stellen und Privatpersonen darf der Zugang zu den Daten des AZR nur in eng begrenzten Ausnahmefällen gewährt werden, die gesetzlich festzulegen sind.

III.

Das Urteil des Bundesverfassungsgerichts zur Volkszählung 1983 ist wesentlicher Anlaß für die gesetzliche Neuregelung. Aus Gründen der Normenklarheit, der Bestimmtheit und der Zweckbindung muß die Regelung das Ausmaß der vorgesehenen Datennutzung abschließend festlegen.

Das Register dient nicht dem Vollzug von Verwaltungsentscheidungen durch die Registerbehörde selbst. Wenn seine Hauptfunktion die Unterstützung der Tätigkeit der Ausländerbehörden und der Polizei ist - soweit diese Stellen ausländer- und allgemeinvollzugspolizeiliche Aufgaben erfüllen -, so muß der Gesetzgeber diesen Verwendungszusammenhang darstellen. Es ist zu begrüßen, daß nicht nur die Verwendung der Daten im Register selbst, sondern auch ihre Anlieferung und Weitergabe an andere Dienststellen gesetzlich geregelt werden sollen. Nur wenn die Datenverarbeitung klar und eindeutig festgelegt ist, kann der Betroffene den Eingriff in sein Recht auf informationelle Selbstbestimmung einschätzen. Allein ein Registergesetz genügt diesen Anforderungen nicht. Eine zeitlich parallele Novellierung des Ausländerrechts ist deshalb unabdingbar. Gleichzeitig muß auch der Datenaustausch zu Fahndungszwecken und zur Erfüllung anderer polizeilicher Aufgaben in der Strafprozeßordnung und in den Polizeigesetzen geregelt werden.

IV.

Für den in das AZR aufzunehmenden Datensatz sind die vom Register zu erfüllenden Funktionen maßgeblich.

Entsprechend der Indexfunktion gehören in das AZR solche Daten über einen Ausländer, die das Auffinden bestimmter, zu einer Person angelegter Unterlagen zur Vorbereitung vor allem ausländerrechtlicher Entscheidungen ermöglichen.

Darüber hinaus ist geplant, den Benutzern unmittelbar Daten zur Verfügung zu stellen, um verschiedene Informationsansprüche zu erfüllen. Dadurch sollen zum Teil die Empfänger die Möglichkeit erhalten, auf die Beiziehung von Akten vor Entscheidungen zu verzichten.

Besonders problematisch ist die Speicherung und Verwendung des Datums „Einreisebedenken". Unter diesem Datum werden belastende Vorgänge im Umfeld des Ausländers erfaßt, die noch keine ausländerrechtlichen Maßnahmen ausgelöst haben. Damit erhält der Datensatz eine neue Qualität: Gespeichert werden nicht mehr Informationen über in einem formalisierten und rechtsstaatlichen Verfahren ergangene Maßnahmen der Ausländerbehörde, sondern auch unpräzise Angaben über ein vermutetes (Fehl-) Verhalten des Ausländers selbst.

Der Mangel an Genauigkeit dieses Datums bedingt es, daß z. B. ein bei einer Grenzpolizeibehörde beantragter Ausnahmesichtvermerk nicht ohne Hinzuziehung der zugrundeliegenden Akte versagt werden kann. Die Voraussetzungen der Entstehung dieses Datums sowie seiner Verwendung bedürfen wegen des verfassungsrechtlichen Gebots der Normenklarheit einer Präzisierung. Dabei wird nicht verkannt, daß sich diese Regelung in denjenigen Fällen positiv auswirken wird, in denen in diesem Datenfeld keine Eintragung vorliegt, und dies dürfte die große Mehrheit sein. Wenn nämlich das Datum „Einreisebedenken" nicht belegt ist, besteht die Möglichkeit, etwa über einen Ausnahmesichtvermerk in einem beschleunigten Verfahren zu entscheiden, ohne daß auf die Ausgangsunterlagen zurückgegriffen werden muß.

Die geplante Aufnahme von Daten aus dem INPOL-Fahndungsbestand macht die Funktionserweiterung in den Polizeibereich hinein deutlich. Die Notwendigkeit der Aufzeichnung von Fahndungsnotierungen im AZR ist bisher angesichts möglicher Alternativen - z. B. eines regelmäßigen Datenabgleichs - nicht ausreichend dargelegt.

Die Speicherung von Suchvermerken kann hingenommen werden, wenn sie nur für die Verfolgung im Gesetz selbst festgelegter Zwecke erfolgt und - wie im Bericht des Bundesministers des Innern vorgesehen - zeitlich begrenzt zugelassen wird.

Bei den Daten, die ausschließlich für statistische und Planungszwecke erhoben werden sollen, ist sicherzustellen, daß ihre Verwendung getrennt von derjenigen anderer Daten des Ausländers erfolgt und die Angaben derart anonymisiert werden, daß die Verbindung zu den personenbezogenen Daten nicht mehr hergestellt werden kann.

V.

Die Kommunikation zwischen AZR und den verschiedenen Behörden oder Privatpersonen ist gesetzlich so zu regeln, daß sie den Anforderungen des Bundesverfassungsgerichts an den bereichspezifischen Datenschutz gerecht wird.

Eine gesetzliche Regelung ausschließlich des Teilnehmerkreises und des Datenumfangs wäre nicht ausreichend, solange nicht präzise festgelegt wird, für welche konkreten Zwecke die Behörden Daten abrufen dürfen, bzw. das AZR an sie übermitteln darf. Nur eine verwendungsorientierte Regelung macht den potentiellen Verwendungszusammenhang transparent und würde den Anforderungen des Bundesverfassungsgerichts genügen.

Eine Festlegung, daß den Benutzern nur solche Daten übermittelt werden, die sie zur Aufgabenerfüllung benötigen, würde nicht ausreichen; es bedarf gerade der Festlegung derjenigen Aufgaben, zu deren Erfüllung Datenübermittlungen vorgenommen

werden sollen. Auch eine Differenzierung nach Abfragearten, die jeweils verschiedene, stufenweise gestaffelte Datenmengen umfassen, wäre ungenügend, solange nicht feststeht, für welche Aufgaben welche Behörden die festgelegten Datenmengen abrufen können.

Der On-line-Zugriff auf die im AZR gespeicherten Daten stellt eine besonders intensive Form des Zugriffs auf personenbezogene Informationen dar. Er bedarf daher der besonderen Rechtfertigung, die in der Aufgabenstellung der beteiligten Behörden begründet sein muß.

Anlage 5

Europarat
Empfehlung Nr. R(83)10 des Ministerkomitees an die Mitgliedstaaten zum Schutz personenbezogener Daten für Zwecke der wissenschaftlichen Forschung und Statistik

Das Ministerkomitee, kraft Artikel 15 (b) der Satzung des Europarates,

in der Erwägung, daß das Ziel des Europarates darin besteht, eine größere Einheit unter seinen Mitgliedern herzustellen;

in dem Bewußtsein, daß es notwendig ist, den Persönlichkeitsbereich des einzelnen gegenüber der zunehmenden Anwendung der Datenverarbeitung in dem Bereich der wissenschaftlichen Forschung und der Statistik zu schützen;

in der Überzeugung, daß die Verwendung personenbezogener Daten oft eine notwendige Bedingung für den Fortschritt der Wissenschaft darstellt;

in Anbetracht der Bedeutung, die der wissenschaftlichen Forschung sowohl als Wert für sich wie als unerläßlicher Faktor für den Fortschritt in der Gesellschaft zukommt;

eingedenk der Ausnahmen, die zugunsten der Tätigkeiten auf dem Gebiet der wissenschaftlichen Forschung und der Statistik in dem Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten zugelassen sind;

in der Feststellung, daß Ausnahmen in diesem Sinn auch von mehreren Mitgliedstaaten in den bestehenden oder in Ausarbeitung befindlichen Datenschutzgesetzen vorgesehen sind;

unter Berücksichtigung der Erklärung der European Science Foundation über den Schutz des Persönlichkeitsbereichs und die Verwendung personenbezogener Daten für Forschungszwecke;

eingedenk der Erfordernisse des Forschungsbereichs;

in der Erwägung, daß ein Ausgleich zwischen den Erfordernissen der Forschung und Statistik einerseits und dem unerläßlichen Schutz des einzelnen andererseits, besonders bei der automatisierten Datenverarbeitung geschaffen werden muß;

in dem Bewußtsein, daß es notwendig ist, geeignete Verfahren festzulegen, um die Interessen der verschiedenen betroffenen Parteien in Einklang zu bringen;

EMPFIEHLT den Regierungen der Mitgliedstaaten,

- ihr innerstaatliches Recht und ihre innerstaatlichen Praktiken hinsichtlich der Verwendung personenbezogener Daten zu Zwecken der wissenschaftlichen Forschung und der Statistik an den Grundsätzen und Leitlinien zu orientieren, die in dem Anhang zu dieser Empfehlung aufgeführt sind;
- dafür zu sorgen, daß diese Empfehlung in den mit wissenschaftlicher Forschung und Statistik befaßten öffentlichen und privaten Kreisen weite Verbreitung findet.

Anhang zur Empfehlung Nr. R (83) 10

1. Anwendungsbereich und Begriffsbestimmungen

1.1 Die in diesem Anhang enthaltenen Grundsätze und Leitlinien gelten für die Verwendung personenbezogener Daten für Zwecke der wissenschaftlichen Forschung und der Statistik sowohl im öffentlichen als auch im privaten Bereich, unabhängig davon, ob diese Daten automatisch oder nach manuellen Methoden verarbeitet werden.

1.2 Im Sinne dieser Empfehlung:

bedeutet »personenbezogene Daten« jede Information über eine bestimmte oder bestimmbare natürliche Person. Eine natürliche Person gilt nicht als »bestimmbar«, wenn die Feststellung der Identität einen unverhältnismäßigen Aufwand an Zeit, Kosten und Arbeitskraft erfordert;

umfaßt »Forschung« auch die Sammlung und Verarbeitung personenbezogener Daten zu statistischen Zwecken;

1.3 Die Mitgliedstaaten können diese Grundsätze und Richtlinien auf Informationen über Personengruppen, Vereinigungen, Stiftungen, Gesellschaften, Körperschaften oder andere Stelle anwenden, die unmittelbar oder mittelbar aus natürlichen Personen bestehen, unabhängig davon, ob diese Stellen Rechtspersönlichkeit besitzen oder nicht.

2. Achtung des Persönlichkeitsbereichs

2.1 Die Achtung des Persönlichkeitsbereichs ist im Rahmen jedes Forschungsprojekts zu gewährleisten, das die Verwendung personenbezogener Daten erfordert.

2.2 Forschung soll soweit wie möglich anonymisierte Daten verwenden. Die wissenschaftlichen und fachlichen Organisationen sowie die öffentlichen Behörden sollen die Entwicklung von Techniken und Verfahren zur Wahrung der Anonymität fördern.

3. Einwilligung des Betroffenen

3.1 Jede Person, die Daten über sich mitteilt, soll ausreichend über die Art des Projekts, seine Ziele sowie über den Namen der Person oder der Stelle unterrichtet werden, für die die Forschungsarbeit durchgeführt wird.

3.2 Falls für den Betroffenen keine Verpflichtung besteht, die erbetenen Daten zur Verfügung zu stellen, soll er darüber unterrichtet werden, daß es ihm freisteht, mitzuarbeiten oder seine Mitwirkung abzulehnen. Der Betroffene soll das Recht haben, jederzeit seine Mitwirkung ohne Darlegung von Gründen abzubrechen.

3.3 Wenn in Anbetracht des verfolgten Ziels die in Absatz 3.1 erwähnte Information nicht ganz oder teilweise offenbart werden kann, bevor die Daten erfaßt sind, soll der Betroffene unmittelbar nach der Datenerfassung über diesen Inhalt vollständig unterrichtet werden, und es soll ihm freistehen, seine

Mitwirkung fortzusetzen oder abzubrechen, und im letzteren Fall soll er die Löschung der erfaßten Daten verlangen können.

3.4 Besondere Schutzmaßnahmen sollen im Hinblick auf die Personen getroffen werden, deren Daten erfaßt werden und die unfähig sind, ihre eigenen Interessen zu wahren, oder die nicht in der Lage sind, ihre Einwilligung frei zu erteilen.

4. Verwendung der Daten

4.1 Die für Forschungszwecke beschafften personenbezogenen Daten dürfen für keinen anderen Zweck als die Forschung verwendet werden.

Insbesondere dürfen sie nicht verwendet werden, um Entscheidungen oder Maßnahmen zu treffen, die den einzelnen unmittelbar angehen, außer im Rahmen der Forschung oder mit ausdrücklicher Einwilligung des Betroffenen.

4.2 Die personenbezogenen Daten, die im Rahmen eines bestimmten Forschungsprojekts und mit Einwilligung der Betroffenen erhoben wurden, dürfen nur mit Einwilligung des Betroffenen für ein anderes Forschungsprojekt benutzt werden, das sich in seiner Art und seinem Ziel wesentlich von diesem unterscheidet. Wenn es jedoch nicht möglich ist, diese Einwilligung wegen der inzwischen verstrichenen Zeit oder der großen Anzahl von Betroffenen zu erlangen, können die früher erhobenen Daten im Einklang mit Sicherheitsbestimmungen des innerstaatlichen Rechts verwendet werden.

4.3 Die öffentlichen und privaten Stellen sollen berechtigt sein, die personenbezogenen Daten, die sie für Verwaltungszwecke haben, für eigene Forschungszwecke zu verwenden. Wenn im Verlauf derartiger Forschungsarbeiten personenbezogene Daten in Dateien eingefügt werden, die bei dem betreffenden Verwaltungsorgan bereits geführt werden, oder wenn dessen Dateien verändert werden, sollen diese neuen Dateien nicht dem Verwaltungspersonal zur Verfügung gestellt werden, das mit Einzelfällen beschäftigt ist, es sei denn, mit Einwilligung des Betroffenen.

4.4 Die Bekanntgabe personenbezogener Daten durch öffentliche oder private Stellen zu Forschungszwecken darf nur mit Einwilligung des Betroffenen oder gemäß sonstigen Sicherheitsbestimmungen des innerstaatlichen Rechts erfolgen.

5. Erstellung von Stichproben

Der Zugang zu Einwohnermelderegistern sollte Forschern erleichtert werden, damit sie die für die Erhebungen erforderlichen Stichproben zusammenstellen können. Vorbehaltlich der von den nationalen Behörden in bestimmten Fällen vorgesehenen Einschränkungen können die Stichproben über Namen, Anschrift, Geburtsdatum, Geschlecht und Beruf Aufschluß geben.

6. Zugang des Betroffenen zu den Daten

6.1 Das Recht des einzelnen auf Zugang und Berichtigung der ihn betreffenden Daten darf eingeschränkt werden, wenn die Daten zu rein statistischen Zwecken oder anderen Forschungszwecken erhoben und gespeichert werden und die erstellten Statistiken oder Forschungsergebnisse den einzelnen nicht leicht identifizieren, und wenn es angemessene Sicherheitsmaßnahmen gibt, um seinen Persönlichkeitsbereich in jedem Stadium des Forschungsprojekts zu schützen, einschließlich der Speicherung der Daten für eine spätere Verwendung.

6.2 Diese Bestimmung findet keine Anwendung, wenn in Anbetracht der Art der Forschung die natürliche Person ein besonders schutzwürdiges Interesse nachweisen kann.

7. Sicherung der Daten

7.1 Die Forschungsprojekte sollen ausdrücklich technische und organisatorische Maßnahmen vorsehen, um die Sicherung und Vertraulichkeit der Daten zu gewährleisten.

8. Veröffentlichung der Daten

8.1 Die für Forschungszwecke verwendeten personenbezogenen Daten dürfen nur dann in personenbezogener Form veröffentlicht werden, wenn die Betroffenen ihre Einwilligung gegeben haben, und in Einklang mit sonstigen Sicherheitsbestimmungen des innerstaatlichen Rechts.

9. Aufbewahrung der Daten

Bei jedem Forschungsprojekt soll, soweit wie möglich, angegeben werden, ob die erfaßten personenbezogenen Daten nach Beendigung des Projekts gelöscht, anonymisiert oder aufbewahrt werden, und im letzteren Fall unter welchen Bedingungen.

9.2 Wenn die Einwilligung des Betroffenen für die Durchführung eines Forschungsprojekts erforderlich ist, sollte sie auch die Frage der eventuellen Aufbewahrung der erfaßten personenbezogenen Daten nach Beendigung des Programms umfassen. War es nicht möglich, um die Einwilligung zur Aufbewahrung zu bitten, dürfen die Daten unter der Bedingung aufgehoben werden, daß die Aufbewahrung entsprechend den Sicherheitsbestimmungen des innerstaatlichen Rechts erfolgt.

9.3 Bevor über die Löschung personenbezogener Daten entschieden wird, die von öffentlichen Behörden in Besitz gehalten werden, sollte die mögliche zukünftige Verwendung
9.1 solcher Daten für Forschungszwecke in Betracht gezogen werden, vorzugsweise nach Beratung mit für die Aufbewahrung öffentlicher Unterlagen zuständigen Institutionen.

9.4 Wenn nach Abschluß eines Projekts die verwendeten personenbezogenen Daten nicht gelöscht oder anonymisiert werden, wäre es angebracht, ihre Aufbewahrung in Institutionen zu fördern, die mit dieser Aufgabe betraut sind und in denen geeignete Sicherungsmaßnahmen ergriffen wurden.

10. Einrichtung von Kontrollgremien innerhalb des Forschungsbereichs

10.1 Die Einrichtung von Kontrollgremien innerhalb des Forschungsbereichs soll gefördert werden, um zur Entwicklung der in dieser Empfehlung enthaltenen Grundsätze und Leitlinien beizutragen.

Anlage 6

Vorläufige
Verwaltungsvorschriften
über die Führung von Personalakten der Dienstkräfte des Landes Berlin
- Teilregelung -

Vom 3. Dezember 1986

§ 1
Begriff und Inhalt

(1) Zu den Personalakten gehören alle Vorgänge, die die Dienstkräfte in ihrem Beamten- oder Arbeitsverhältnis betreffen. Sie sollen ein möglichst vollständiges, dem Geschehensablauf entsprechendes Bild der Persönlichkeit der Dienstkräfte und der Gestaltung der Beamten- oder Arbeitsverhältnisse geben.

(2) Nicht zu den Personalakten gehören Vorgänge, die besonderen, von der Person und dem Beamten- oder Arbeitsverhältnis sachlich zu trennenden Zwecken dienen. Diese Vorgänge sind in Sachakten einzuordnen, die insbesondere geführt werden über

1. Prüfungen,
2. Personalplanung,
3. Ausleseverfahren,
4. Stellenausschreibungen und darauf beruhende Bewerbungen, die nicht berücksichtigt worden sind,
5. Stellenbewertung,
6. Rechtsstreitigkeiten aus dem Beamten- oder Arbeitsverhältnis,
7. Sicherheitsüberprüfungen,
8. Kindergeld (siehe auch § 2 Abs. 3 Nr. 6),
9. Dienstausweise,
10. Dienstreisegenehmigungen,
11. Reisekostenabrechnungen, einschließlich Wegstreckenentschädigungen,
12. Flugkostenzuschüsse,
13. Umzugskosten,
14. Aussagegenehmigungen,
15. Prozeßvollmachten,
16. Beschwerden, die sich ausschließlich gegen die sachliche Entscheidung einer Dienstkraft richten.

Soweit erforderlich, sind Auszüge, Abschriften oder Kopien aus den Sachakten in die Personalakten zu nehmen. Das gilt insbesondere für die abschließenden Entscheidungen bei Prüfungen, Rechtsstreitigkeiten und Stellenbewertungen. Von Vorgängen, die sich auf mehrere Dienstkräfte beziehen (Sammelvorgänge), sind Auszüge nur zu den jeweiligen Personalakten zu nehmen, soweit sie die personellen und dienstlichen Verhältnisse der einzelnen Dienstkraft betreffen.

§ 2
Gliederung

(1) Die Personalakten gliedern sich in Haupt- und Beiakten. Die Hauptakte enthält Vorgänge über die Begründung, die Gestaltung und die Beendigung des Beamten- oder Arbeitsverhältnisses sowie alle anderen die Dienstkraft betreffenden Vorgänge, soweit sie nicht in Beiakten aufgenommen sind.

(2) Führungszeugnisse und Mitteilungen über unbeschränkte Auskünfte aus dem Zentralregister sind in verschlossenem Umschlag unnumeriert zu der Hauptakte zu nehmen, soweit sie nicht gesondert bei der obersten Dienstbehörde aufbewahrt werden. Bei der Entscheidung über die Einsichtnahme in diese Vorgänge, ihre Weiterleitung oder die Erteilung von Auskünften an andere Behörden sind die Vorschriften des Bundeszentralregistergesetzes zu beachten.

(3) Beiakten sind im Aktenvorblatt der Hauptakte, Beiakten nach Satz 2 Nr. 3 und Absatz 4 in einem Anhang zum Aktenvorblatt zu vermerken. Beiakten werden für folgende Vorgänge geführt:

1. Ausbildung innerhalb des öffentlichen Dienstes,
2. Beihilfen,
3. Disziplinarverfahren, Abmahnungen und Vorgänge, die zu einer verhaltensbedingten Kündigung führten - mit Ausnahme des Kündigungsschreibens selbst -,
4. Nebentätigkeiten,
5. Personalakten aus früheren Beamtenverhältnissen oder Arbeitsverhältnissen im öffentlichen Dienst,
6. Ortszuschlag, Sozialzuschlag, Anwärterverheiratetenzuschlag; diese Vorgänge können als Beiakte zusammen mit den Kindergeldvorgängen geführt werden (vgl. Anhang*),
7. Dienstunfälle,
8. Zurruhesetzungsverfahren, wenn in dem Verfahren die Dienstfähigkeit des Beamten festgestellt wurde - mit Ausnahme des Bescheides über die Einstellung des Verfahrens selbst -,
9. Abtretungen, Pfändungen, Regresse,
10. Vorgänge, die die Übersendung der Personalakten an andere Dienstbehörden bzw. Personalstellen im Zusammenhang mit einer Bewerbung betreffen.

(4) In eine weitere Beiakte aufzunehmen sind

1. Vorgänge, die bei der Würdigung von Eintragungen im Führungszeugnis oder in der Auskunft aus dem Zentralregister entstanden sind,
2. Vorgänge oder Vermerke über strafgerichtliche oder berufsgerichtliche Verurteilungen, staatsanwaltschaftliche Ermittlungsverfahren oder sonstige Entscheidungen in einem Straf- oder Ermittlungsverfahren sowie in einem Ordnungswidrigkeitenverfahren, es sei denn, daß
   a) Gegenstand ein außerdienstliches Verhalten ist und
   b) offensichtlich kein Bezug zum Beamten- oder Arbeitsverhältnis besteht.

§ 3
Aktenführung

(1) Für die ordnungsgemäße Führung der Personalakten ist die zuständige Dienstbehörde bzw. Personalstelle verantwortlich. Sie entscheidet im Zweifelsfall, ob ein bestimmtes Schriftstück in die Personalakte aufgenommen wird.

(2) Die Vorgänge müssen vollständig sein, sie sind zeitlich zu ordnen und fortlaufend zu numerieren.

(3) Keine Dienstkraft darf ihre Personalakte selbst führen.

(4) Die Führung geheimer Personalakten ist untersagt. Die Personalakten dürfen nicht mit geheimen Kennzeichen versehen werden.

(5) Personalakten dürfen nicht doppelt geführt werden.

(6) Personenstandsurkunden, Zeugnisse und sonstige Nachweise sind in der Regel als Abschriften, Kopien oder Auszüge in beglaubigter Form zu den Personalakten zu nehmen.

(7) Bei der Einstellung von Dienstkräften, die bereits früher im öffentlichen Dienst beschäftigt waren, sind nach Möglichkeit die früheren Personalakten heranzuziehen.

§ 4
Inkrafttreten

Diese Verwaltungsvorschriften treten mit sofortiger Wirkung in Kraft. Gleichzeitig treten entgegenstehende Vorschriften außer Kraft.

* nicht abgedruckt

Anlage 7

Entwurf von Ausführungsvorschriften über den Schulpsychologischen Dienst an den öffentlichen Schulen des Landes Berlin - Auszug -

III. Arbeitsweise

...

10. (1) Der Schulpsychologische Dienst wird tätig

a) in Fällen des § 21 Abs. 2 SchulG,

b) in sonstigen Fällen auf Ersuchen von Lehrern, Schulleitern, Schulärzten oder des Schulamtes,

c) auf Wunsch einzelner Erziehungsberechtigter oder Schüler.

(2) Vor einer Untersuchung gemäß Absatz 1 Buchstabe a sind die Erziehungsberechtigten bzw. der volljährige Schüler auf die Rechtsgrundlage der Maßnahme und auf die in Betracht kommende Entscheidung nach § 21 SchulG hinzuweisen. Für eine Untersuchung nach Absatz 1 Buchstaben b und c ist die Zustimmung der Erziehungsberechtigten oder des volljährigen Schülers einzuholen.

(3) Schüler der Mittel- und Oberstufe, die nicht volljährig sind, können sich auch ohne Einwilligung der Erziehungsberechtigten an den Schulpsychologischen Dienst wenden, um Rat einzuholen. Falls über eine Beratung hinaus weitere Maßnahmen erforderlich werden, ist das Einverständnis der Erziehungsberechtigten einzuholen, es sei denn, daß dadurch das Wohl des Schülers gefährdet wird.

(4) Für therapeutische Maßnahmen ist die Zustimmung der Erziehungsberechtigten oder des volljährigen Schülers einzuholen.

11. Die Dienstkräfte im Schulpsychologischen Dienst dürfen alle Gespräche, Untersuchungen und therapeutischen Maßnahmen ohne Anwesenheit Dritter vornehmen.

12. Unterrichtsbesuche von Dienstkräften im Schulpsychologischen Dienst dürfen nur mit Zustimmung von Lehrern durchgeführt werden; dem Lehrer sind die Gründe für den gewünschten Besuch zu erläutern. Stimmt der Lehrer nicht zu, so kann eine Entscheidung des Schulleiters oder danach des zuständigen Schulaufsichtsbeamten im Bezirk eingeholt werden.

IV. Behandlung vertraulicher Unterlagen und Informationen sowie Einsichtsrecht

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

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

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

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

(3) Schriftliche Berichte an die Schulen sind als besonders vertraulich zu kennzeichnen und zum Schülerbogen zu nehmen.

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

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

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

16. Akten des Schulpsychologischen Dienstes sind bis zum Ablauf von 3 Jahren nach Beendigung des Schulverhältnisses aufzubewahren. Danach sind diese als Vorgänge vertraulichen Inhalts zu vernichten.

...

Stichwortverzeichnis

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