22 Seiten

Abgeordnetenhaus von Berlin

Drucksache 9/ 248

9. Wahlperiode

29. 12. 81

Mitteilungen des Präsidenten

- Nr. 20 -

Inhaltsübersicht

Druckschluß: 4. Dezember 1981, 12.00 Uhr

Ausgegeben am 29. Dezember 1981

Der Präsident
Peter Rebsch

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

BERICHT DES BERLINER DATENSCHUTZBEAUFTRAGTEN zum 31. Dezember 1981

Inhaltsverzeichnis

[1] Nach § 26 Abs. 2 Berliner Datenschutzgesetz berichtet der Berliner Datenschutzbeauftragte dem Abgeordnetenhaus und dem Regierenden Bürgermeister jährlich.
Es liegen folgende Berichte vor:
- Bericht über die Aufnahme der Tätigkeit des Berliner Datenschutzbeauftragten vom Januar 1980, Mitteilungen des Präsidenten - Nr. 40 -, Drucksache 8/277 vom 22. Januar 1980 - vom Ausschuß für Inneres am 11. Juni 1980 beraten -.
- Bericht des Berliner Datenschutzbeauftragten zum 31. Dezember 1980 (Jahresbericht 1980) Mitteilungen des Präsidenten - Nr. 107 -, Drucksache 8/666 vom 28. Januar 1981.

1. Aufgaben des Berliner Datenschutzbeauftragten

1.1 Entwicklung der Informationsverarbeitung im öffentlichen Bereich

Im folgenden berichte ich über die Ergebnisse meiner Tätigkeit, über Anstände und Datenschutzdefizite der Berliner Verwaltung und unterbreite Vorschläge, um aufgetretene Probleme zu überwinden.

Der Anspruch jedes Bürgers, daß seine Rechte und schutzwürdigen Belange beim Umgang mit den ihn betreffenden Daten geachtet werden, soll damit verdeutlicht und fester verankert werden.

Die vorgelegten Ergebnisse, insbesondere auf den Gebieten des Gesundheitswesens, des Personalwesens und der öffentlichen Sicherheit und Ordnung zeigen jedes für sich bereits wie notwendig die Datenschutzkontrolle ist. Einzelne Fälle können jedoch nur richtig beurteilt werden, wenn man sie vor dem Hintergrund einer rasch fortschreitenden technischen Entwicklung der Datenverarbeitung sieht, wie sie in Berlin etwa in der Erprobung Neuer Medien allgemein erkennbar wurde. Dabei handelt es sich allerdings nur um einen Mosaikstein der zu erwartenden Gesamtentwicklung zu einer „Informationsgesellschaft". Folgende Antriebskräfte bestimmen diese Entwicklung:

Das Preis-/Leistungs-Verhältnis verbessert sich für Datenverarbeitungsprodukte stetig. Insbesondere gilt dies für überwiegend elektronische Geräte wie Zentraleinheiten und Arbeitsspeicher, die heute computergestützt entwickelt und in Massen gefertigt werden. Aber auch Geräte mit mechanischen Bestandteilen werden trotz stetiger Weiterentwicklung im Preis-/Leistungs-Verhältnis günstiger, da sie in größeren Produktionsserien hergestellt werden können.

Selbst für die Programme (Software), mit denen die Datenverarbeitungsanlagen betrieben werden, erscheint dieser Trend möglich: Die Standardisierung von Programmen und Programmierverfahren und der zunehmend angebotene Komfort bei den Programmiersprachen führen zu Rationalisierungseffekten bei der Software-Herstellung, die sich auf Kosten und Qualität der Software positiv auswirken.

Die Konsequenzen dieses Trends liegen in der zunehmenden Verbreitung von Datenverarbeitungs-Kapazitäten. Mit den bereits für wenige tausend Mark erhältlichen „Home-" oder „Personal-"Computern haben leistungsfähige Datenverarbeitungsgeräte bereits heute Einzug auch in kleinere Betriebe, ja im Einzelfall schon in Privathaushalte gehalten.

Mikroprozessoren, die letzten Endes nichts anderes sind als kleine Zentraleinheiten, sind heute nicht mehr als Steuerungszentralen verschiedenster technischer Geräte (z. B. Verkehrsmittel, Haushaltsmaschinen, Schreibmaschinen) wegzudenken. Deutlich wird dies etwa durch die Ausrüstung von Schreibmaschinen mit Speicherelementen. Entsprechende Geräte sind bereits im Landesbereich eingesetzt.

Die zunehmende und kaum kontrollierbare Verbreitung qualitativ hochstehender Datenverarbeitung führt dazu, daß Zahl und Umfang der Dateien zunehmen. Damit gewinnt die Frage nach dem Datenschutz zunehmend an Bedeutung. Verschärft wird die Situation dadurch, daß immer mehr Dateien auf sogenannten On-line-Speichern (zumeist Festplatten) gehalten werden. Insoweit können Daten jederzeit direkt (ohne Einschaltung einer Zwischeninstanz) abgerufen werden.

Die zweite beachtliche Entwicklung ist in der verstärkten Verknüpfung von Datenverarbeitungs- und Kommunikationstechnik zu sehen, die in dem Begriff „Informationstechnik" zum Ausdruck kommt. Sie führt zu einer qualitativ neuen Form der Datenverarbeitung, die sich rasch weiterentwickeln wird. Die Verbesserung der Datenübertragungsmöglichkeiten, die zunehmende Beherrschung von Rechnernetzen, der Aufbau einer passenden Infrastruktur[2] wird den Benutzer zunehmend unabhängig davon machen, in der räumlichen Nähe eines Rechenzentrums zu sein. Daten, die irgendwo im Netz gespeichert sind, sind an den Schnittstellen jederzeit greifbar, wenn nicht Maßnahmen zur Sicherung getroffen werden.

Der Trend kann dadurch gekennzeichnet werden, daß der Computer zum Benutzer kommt, und daß potentiell die gesamte Bevölkerung zum Benutzer wird.

Diese Trends, die für die absehbare Zukunft gelten können, und für die grundsätzliche innovative Entwicklungen nicht mehr gemacht werden müssen, treten heute bereits deutlich bei der Erprobung von Bildschirmtext in Erscheinung: Der Bürger kann über Telefon und Fernsehgerät bisher nicht erreichte Computerleistungen nutzen.

Zusammengefaßt ergibt sich:

Computerleistungen, die bisher vor allem Fachleuten zugänglich waren, werden schrittweise Allgemeingut. Diese sozial zu begrüßende Entwicklung birgt aber auch zusätzliche Gefahren, da immer mehr Daten gespeichert und zugänglich gemacht werden. Daher muß sie sehr sorgfältig beobachtet und in die richtigen Bahnen gelenkt werden. Hierfür wird es auch erforderlich werden, Schutzvorschriften im Rahmen rechtlicher Regelungen, z. B. bei den Neuen Medien, vorzusehen.

Die öffentliche Verwaltung trägt mit der Verantwortung für den Einsatz neuer Informationstechnologien auch die Mitverantwortung für die dem Einsatz vorausgehende und ihn begleitende Aufklärung der Bevölkerung. Gerade in einem Stadtstaat wie Berlin ergeben sich hierfür erhebliche Chancen, die in Zukunft verstärkt genutzt werden sollten, aber auch Gefahren, gegen die man gewappnet sein muß.

Die beachtlichen Perspektiven, die sich aus dem Fortschritt der Datenverarbeitung ergeben, dürfen jedoch nicht den Blick dafür verstellen, daß auch die manuellen Datensammlungen ihre Bedeutung nicht verlieren werden. Sie sind nicht zuletzt deshalb weiterhin stark zu beachten, weil technische Entwicklungen auch ihre Effektivität steigern.

Noch nehmen moderne Formen manueller Datenverarbeitung, z. B. Mikroverfilmung, trotz ihrer unbestreitbaren Vorteile einen geringen Platz in der Verwaltungspraxis ein. Im Hinblick darauf, daß solche Systeme den Vorteil der Aktualität automatischer Datenverarbeitungsanlagen mit dem Vorzug geringen technischen Aufwands kombinieren, wird die Bedeutung dieser Verwaltungsmittel jedoch noch anwachsen. Auch ist abzusehen, daß dieses Instrument als ein durch Menschen lesbares Ein- und Ausgabemedium für die automatische Datenverarbeitung eine besondere Bedeutung für die rationelle Datenhaltung erlangen kann.

Die Erschließung von Akten mit Hilfe der automatisierten Datenverarbeitung wird der klassischen Aktenhaltung eine neue Qualität geben, die datenschutzrechtlich gewürdigt werden muß.

Einzelne Verwaltungen neigen dazu, Anforderungen des Datenschutzes mit dem Argument zurückzuweisen, sie verarbeiteten die Daten in Verfahren, die nicht den Datenschutzgesetzen unterliegen. Da in automatischen Systemen kaum Daten verarbeitet werden, die nicht auch an anderer Stelle in Akten vorgehalten sind, könnte eine derart formale Betrachtung in der Konsequenz zum Leerlauf der Datenschutzregelungen führen.

Dieser Betrachtung treten nicht nur die Datenschutzbeauftragten, sondern neuerdings auch die Gerichte entgegen. So hat das Verwaltungsgericht Wiesbaden rechtskräftig entschieden, daß auch beim Bundeskriminalamt geführte Akten, die über Hinweise in automatischen Verfahren erschlossen werden, dem Datenschutzgesetz unterliegen[3].

Die zweifellos faszinierende technologische Entwicklung bei den Organisationsmitteln darf jedoch nicht dazu führen, daß die klassischen Formen der Datenhaltung, die Aktensammlungen und Karteien in ihrer Bedeutung für das staatliche Handeln unterschätzt werden.

In den Aktensammlungen sind nach traditionellem Verständnis sämtliche anfallenden Vorgänge aufzunehmen. Diesem Vollständigkeitsprinzip, das auch vor ausdrücklich falschen

[2] Kabelfernsehen, Glasfaserkabel – im Versuch wurde bereits eine Übertragungsrate von einem Gigabit = 5000 Schreibmaschinenseiten je Sekunde erreicht –

[3] Deutsches Verwaltungsblatt 1981, S. 790 VG Wiesbaden, Urteil vom 11. 11. 1980 - IV/1 F. 79/79 -

Akteninhalten nicht halt macht, entspricht die Tendenz, nach Möglichkeit die Transparenz des Akteninhaltes zu verhindern. Generelle Akteneinsicht, die ebenso wie die umfassende Auskunft über in automatischen Dateien gespeicherte Daten als „Magna Charta" des Datenschutzes zu betrachten ist, wird nur in Bereichen gewährt, in denen sich entsprechende Interessen hinreichend artikulieren konnten, so z.B. im Bereich der Personalakten. Allerdings wandelt sich hier ebenfalls das Verständnis. Insbesondere wird der Akteneinsicht durch die Rechtsprechung zunehmende Bedeutung beigemessen. Ein bemerkenswertes Urteil des Kammergerichts[4] schreibt das grundsätzliche Recht auf Akteneinsicht in Fortführung der Rechtsprechung des Bundesgerichtshofes selbst im Bereich psychiatrischer Unterlagen fest.

Ihren traditionellen Platz in der Verwaltungspraxis haben auch Karteien, wobei der Übergang von der Akte zur Kartei durchaus fließend sein kann. Beispiele sind hier auch die Aufnahme verstärkter und formatierter Vorblätter in Akten oder die gleichzeitig mit Hilfe von Matrizen vorgenommene Fertigung von Aktenstücken und Karteien. Auch bei Karteien gilt, daß die Vollständigkeit der Eintragungen, nicht aber deren Erforderlichkeit im Vordergrund steht. So finden sich auf Karteikarten häufig noch Eintragungen, die in automatischen Systemen, die auf Grund des Karteikarteneintrags erstellt wurden und parallel geführt werden, bereits gelöscht sind oder gar nicht erst aufgenommen sind.

Bei meiner Beratungs- und Kontrolltätigkeit habe ich mich bemüht, auf die einheitliche Handhabung des Datenschutzes im automatisierten und im nicht automatisierten Bereich zu drängen. Dieser Auffassung entsprechen u.a. Vorschriften, die bei der Regelung des Datenschutzes nicht mehr zwischen der Datenhaltung in Computern und Akten unterscheiden[5].

Es bleibt festzustellen, daß das Persönlichkeitsrecht des Bürgers sowohl durch die technologische Entwicklung als auch durch im wesentlichen technikunabhängige Datenhaltung betroffen werden kann.

Bei der bevorstehenden Diskussion um eine Novellierung des Bundesdatenschutzgesetzes sollte berücksichtigt werden, daß die Bürger vor allem die Beseitigung von Beeinträchtigungen ihres Persönlichkeitsrechts anstreben und für sie dabei die Ursache - z. B. falsche Datenhaltung im Computer oder in konventionellen „Vorgängen" - zweitrangig ist.

1.2 Tätigkeitsbereiche des Berliner Datenschutzbeauftragten

Anrufungen durch jedermann

Die Zahl der Eingaben hat gegenüber dem Vorjahr weiter zugenommen. Über die dabei aufgetretenen Fragen berichte ich unter 2. Die Anrufungen erstrecken sich nach der Häufigkeit geordnet insbesondere auf folgende Gebiete:

1. (1)[6] Öffentliche Sicherheit und Ordnung
2. (2) Sozial- und Gesundheitswesen
3. (-) Justiz
4. (4) Schulen, Hochschulen, Kultur
5. (3) Behandlung der Personaldaten von Mitarbeitern der öffentlichen Verwaltung

Gegenüber dem Vorjahr haben die Eingaben bemerkenswert zugenommen, die den Bereich der Justizverwaltung betreffen.

In ca. 50 % aller Eingaben haben sich Mängel herausgestellt.

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

Beratung und Kontrolle

Erwartungsgemäß waren von mir auch Beratungsaufgaben nach § 21 Abs. 1 letzter Satz des Berliner Datenschutzgesetzes gegenüber öffentlichen Stellen in steigendem Maße wahrzunehmen. Zu den Schwerpunkten gehörten

- die Konsequenzen des seit Anfang 1981 geltenden Sozialgesetzbuches Buch X, die zu vielfältigen rechtlichen und praktischen Fragen geführt haben,
- die Behandlung von Gesundheitsdaten.

Mit der Aufnahme systematischer Kontrollen von Datenverarbeitungsverfahren kann es notwendig werden, zahlreichen Einzelfällen nachzugehen. So fielen bei der stichprobenartigen Überprüfung einer einzigen sensitiven Datengruppe des automatisierten Einwohnerwesens allein 50 Fälle an, in denen die Unrichtigkeit von Daten festgestellt wurde und die Korrektur veranlaßt werden mußte. Auf diesen Fall wird unter 2.2 noch näher eingegangen.

Öffentlichkeitsarbeit

Die anhaltende, lebhafte Beteiligung der Öffentlichkeit am Datenschutz ist bemerkenswert. Soweit möglich, haben sich meine Mitarbeiter und ich auch in diesem Jahr an der öffentlichen Diskussion über Datenschutzfragen, u.a. durch Vorträge und Veröffentlichungen beteiligt. So hat im Frühjahr 1981 eine gut besuchte Podiumsveranstaltung über den Datenschutz im Gesundheitswesen stattgefunden, an der u.a. auch der Bundesbeauftragte teilnahm. Die Diskussion wurde im Mittwochsforum des SFB übertragen. Weiter konnte ich in der SFB-Expertenrunde datenschutzrechtliche Fragen beantworten. Insbesondere im Anschluß an diese Sendung haben sich noch zahlreiche Bürger an mich gewendet.

Für den öffentlichen Bereich habe ich bereits zum vierten Mal ein Seminar an der Verwaltungsakademie durchgeführt, sowie dort eine Projektgruppe beraten, die Vorstellungen über den Umgang mit nicht automatisierten Datensammlungen entwickelt hat.

Im Oktober habe ich ein Datenscheckheft herausgegeben. Es ist als Hilfsmittel für den Bürger gedacht, das ihm den Umgang mit den Behörden erleichtern soll.

Die starke Resonanz[7] läßt erkennen, daß die in der Vergangenheit vielfach beobachtete geringe Zahl von Bürgeranfragen bei den speichernden Stellen auch damit zu erklären ist, daß das sehr komplizierte Datenschutzrecht die Bürger nicht ohne weiteres in die Lage versetzt, von ihren Rechten Gebrauch zu machen. Sie benötigen dazu leicht verständliche Hilfsmittel.

Durch die Benutzung des Scheckheftes von sehr vielen Bürgern ist auch offenbar geworden, wie sich einzelne Stellen auf Fragen der Bürger eingestellt haben.

Aufbau der Dienststelle

Der Aufbau der Dienststelle fiel von vornherein in die Phase zunehmender haushaltsmäßiger Beschränkungen. Damit war für mich eine sehr vorsichtige Personaldisposition geboten. Angesichts des ständig steigenden Arbeitsanfalles führte dies in diesem Jahr zu ganz erheblichen Belastungen und Engpässen.

Auch bei Anlegung eines strengen Maßstabes erscheint mir die schrittweise Erweiterung um zwei Planstellen, wie ich sie von vornherein vorgesehen hatte, notwendig. Vordringlich ist die Schaffung einer A 13 S-Stelle, um u. a. die gerade in letzter Zeit im Bereich der technischen und organisatorischen Überprüfungen stark gestiegenen Aufgaben bewältigen zu können.

2. Kontrolle der Einhaltung der Datenschutzvorschriften

- Schwerpunkte im Berichtszeitraum -

Die für 1981 vorgesehenen Schwerpunkte[8] Personaldaten, öffentliche Sicherheit und Strafverfolgung, Gesundheitswesen und erste Überprüfungen von Rechenzentren und Rechenstellen konnte ich - wie vorgesehen - in Angriff nehmen.

2.1 Gesundheitswesen

Zahlreiche Vorgänge haben mich veranlaßt, zu prüfen, ob Art und Umfang der Erhebung von Gesundheitsdaten, ihre Samm-

[4] Vom 1. Juni 1981 (20 U 96/81 KG) Neue Juristische Wochenschrift 1981 S. 2521 f

[5] Neuerdings insbesondere das Sozialgesetzbuch Buch X

[6] Die Reihenfolge nach dem Jahresbericht 1980 ist in Klammern dargestellt

[7] In einer Woche war die erste Auflage von 6.500 Stück vergriffen, so daß eine Nachauflage von nochmals 6.500 Stück erstellt werden mußte, die inzwischen ebenfalls vergriffen ist.

[8] Vgl. Jahresbericht 1980, 5.1 (S. 17)

lung in zentralen automatisierten Registern und ihre Übermittlung an Dritte etwa für Zwecke der Sozialverwaltung und der Forschung sowie ihre Aufbewahrung den Datenschutzbestimmungen entsprechen. Dabei ist zu berücksichtigen, daß neben den Vorschriften der Datenschutzgesetze die ärztliche Schweigepflicht als besondere Form der Verpflichtung zur Wahrung des Datengeheimnisses besteht. Obgleich sie dem Inhalt nach nicht geregelt ist (§ 203 StGB setzt sie voraus[9]), kann sie zu einer Beschränkung der Zulässigkeit von Datenübermittlungen auch dann führen, wenn diese nach den Vorschriften der Datenschutzgesetze zulässig wäre.

Folgende Fälle sind hervorzuheben:

Forschungsprojekt „Europäische Erfassung von Mißbildungen und Mehrlingen" (EUROCAT)

Der Rat der Europäischen Gemeinschaft hat ein „Zweites Programm für Forschungsaktionen im Bereich Forschung in Medizin und Gesundheitswesen" beschlossen[10]. Dazu gehört u.a. eine „mehrjährige konzertierte Aktion" für die perinatale Überwachung. Mit ihrer Hilfe soll das Risiko einer vorgeburtlichen Schädigung festgestellt und verringert werden. An diesem Projekt beteiligen sich auf deutscher Seite Hessen und Berlin (Freie Universität, Klinikum Steglitz - Frauenklinik -). In Berlin ist ein umfangreicher Fragebogen erstellt worden, der 69 Gruppen personenbezogener Daten enthält: U. a. detaillierte Angaben zum Kind, über die Mutter (z.B. vorausgegangene Geburten, Mißbildungen in der Familie, chronische Krankheiten, Krankheiten während der Schwangerschaft, Nikotin, Alkohol, Suchtmittel), zum Vater und über die festgestellten Mißbildungen (genaue Klassifikation nach der British Paediatric Classification) sowie die Art der Vererbung.

Die Daten sollen in Gesprächen mit den betroffenen Müttern erhoben, jeweils in regionalen Registern gesammelt und außerdem nach Belgien an eine Zentrale an der Universität Loewen übermittelt werden.

Belgien gehört zu den westeuropäischen Ländern, die bisher über keine Datenschutzbestimmungen verfügen.

In Berlin sind 20 öffentliche und private Krankenhäuser beteiligt, in denen Entbindungsabteilungen bestehen.

Auf die Berliner Beteiligung an dem Projekt bin ich nicht durch die zuständigen Stellen, sondern durch einen Hinweis aus dem Publikum einer öffentlichen Veranstaltung im Februar 1981 aufmerksam gemacht worden.

Meine Ermittlungen haben folgendes ergeben:

Das Verfahren sah vor, daß Daten der Kinder und der Eltern - ohne Wissen der Betroffenen - in unzureichend anonymisierter Form nach Belgien zur zentralen Speicherung übermittelt werden. Die Erhebungen liefen im Januar 1981 an.

Das geplante Verfahren verstößt gegen § 11 Berliner Datenschutzgesetz, da für die Übermittlung weder die Einwilligung der Betroffenen noch eine ausreichende Rechtsgrundlage vorliegt. Der Beschluß des Ministerrates kommt - unabhängig von der Frage seiner Rechtsqualität - als Rechtsgrundlage nicht in Betracht, da er lediglich die Förderung fremder Maßnahmen zum Gegenstand hatte und nicht die Rechtsgrundlage für das Projekt selbst darstellt.

Der für das Projekt Verantwortliche beim Klinikum Steglitz, Frauenklinik, erklärte sich bereit, die datenschutzrechtlich erforderlichen Veränderungen an dem Verfahren vorzunehmen.

Auf meine Anregung hin wurde vereinbart, daß nach Belgien lediglich hinreichend anonymisierte - d. h. nicht personenbezogene - Daten übermittelt werden.

Im übrigen wurde sichergestellt, daß die Mütter vor der Datenerhebung die Informationen erhalten, die erforderlich sind, um eine wirksame Einwilligung erteilen zu können.

Die Einhaltung der Datenschutzbestimmungen werde ich aufgrund von Stichproben überprüfen. Eine Meldung zum Dateienregister ist inzwischen erfolgt.

Wenn ich auch nachträglich die erforderlichen Maßnahmen durchsetzen konnte, so wird das Datenschutzdefizit in diesem Bereich anhand folgender Punkte deutlich:

- Ich habe von der Beteiligung Berlins an dem Projekt zufällig erfahren.
- Die Krankenhäuser haben - soweit ersichtlich - an dem Verfahren ohne Einwände mitgewirkt.
- Weder bei der EG noch bei den anderen beteiligten Stellen sind die Datenschutzbelange von vornherein hinreichend berücksichtigt worden.

Krebsregister

Der Senator für Gesundheit und Umweltschutz ist an mich herangetreten, mit der Bitte, die Datenschutzprobleme einer Registrierung von Gesundheitsdaten, insbesondere die Problematik von Krebsregistern, zu erörtern.

Ausgangspunkt für Überlegungen ist die in Berlin seit langem vorhandene Sammlung von Daten Krebskranker, die der nachgehenden Fürsorge (§§ 24, 26 Gesundheitsdienst-Gesetz) unterliegen. Diese Daten werden einmal bei den Gesundheitsämtern geführt, die sie von den Krankenhäusern auf Grund von „Einwilligungserklärungen" der Patienten in der Aufnahmeverhandlung erhalten. Beim Senator für Gesundheit, Soziales und Familie wird ein Doppel gesammelt, so daß dort eine zentrale Kartei über alle in Berlin der nachgehenden Fürsorge unterliegenden Krebspatienten besteht.

Soweit die Register ausschließlich der Nachsorge dienen, halte ich sie grundsätzlich für datenschutzrechtlich zulässig.

Die Einwilligung als Grundlage einer Datenübermittlung und Speicherung setzt allerdings voraus, daß der Einwilligende über die Konsequenzen seiner Einwilligung aufgeklärt wird. Dies erscheint auf Grund meiner bisherigen Erfahrungen zweifelhaft. Eine Verbesserung der Einwilligungserklärung - etwa durch Aufnahme eines Hinweises auf die Übermittlung an die Gesundheitsämter - kann diese Zweifel jedoch beseitigen. Die Einwilligung in Datenübermittlungen zum Zwecke der Nachsorge wird auch nicht dadurch unwirksam, daß in besonderen Fällen der Patient aus medizinischen Gründen über seinen wahren Gesundheitszustand im Unklaren belassen wird[11]. In diesen Ausnahmefällen kann es für eine wirksame Einwilligung des betroffenen Patienten in eine Datenübermittlung, die ausschließlich seinen Interessen dient, ausreichen, daß er den Zweck der Übermittlung kennt.

Klinische Nachsorgeregister wären entsprechend zu beurteilen.

Die Beurteilung der Register ändert sich jedoch, soweit sie nicht nur dem Interesse des individuell Betroffenen, sondern darüber hinaus auch öffentlichen Interessen, etwa der epidemiologischen Forschung oder der Planung von Gesundheitseinrichtungen dienen. Hier sind an die Wirksamkeit der Einwilligung relativ hohe Anforderungen zu stellen: Sie setzt die Kenntnis vom Inhalt der übermittelten Daten ebenso voraus, wie die Information über den Zweck der Übermittlung. Ein Patient, der über seinen wahren Gesundheitszustand nicht informiert ist, kann daher eine solche Einwilligung nicht wirksam erteilen.

Selbst wenn man unterstellt, daß für die Durchführung epidemiologischer Forschungsvorhaben und für die Planung von Gesundheitseinrichtungen regelmäßig die Kenntnis anonymisierter Daten ausreicht, ergeben sich erhebliche Probleme. Zwar ist die Übermittlung anonymisierter Daten an Forschungs- und Planungseinrichtungen datenschutzrechtlich zulässig, die Anonymisierung der Daten durch die erhebende Stelle, etwa den behandelnden Arzt, wirft jedoch regelmäßig personelle und nicht zuletzt finanzielle Fragen auf. Insbesondere die Nachmeldung

[9] Vgl. zur Auslegung auch die Berufsordnung der Ärztekammer Berlin v. 02.02.1978 Amtsblatt Nr. 23 S. 527 ff.

[10] Amtsblatt der Europäischen Gemeinschaften (ABL) Nr. L 52 vom 23. Februar 1978, S. 20 und ABL Nr. L 43 vom 14. Februar 1981, S. 12

[11] Das Recht des Patienten auf Auskunft und Einsichtnahme in die Krankenakten ist inzwischen auch von der Rechtsprechung anerkannt (vgl. Bundesgerichtshof, Neue Juristische Wochenschrift 1978, S. 2337)

von Daten im Rahmen von Langzeitstudien dürfte zum Teil unüberwindliche Schwierigkeiten bereiten.

So stellte sich die Frage, ob nicht eine gesetzliche Regelung zur Bereitstellung der für die Forschung und Planung erforderlichen Daten erwogen werden soll. Denn die Aufnahme von hochsensitiven Gesundheitsdaten in ein Register, das über den ursprünglichen Zweck der Behandlung hinausgeht, stellt rechtlich einen Eingriff in die Persönlichkeitsrechte der Betroffenen dar. Ein derartiger Eingriff wäre nur auf Grund eines Gesetzes zulässig. Niemand wird das Interesse der Allgemeinheit an einer verstärkten Forschung, z.B. auf dem Sektor der Krebsbekämpfung, leugnen können. Diesem Interesse kann jedoch die besondere menschliche Situation dessen entgegenstehen, der bereits durch die Krankheit getroffen ist und nun auch noch befürchtet, zum Forschungsobjekt degradiert zu werden. Die Abwägung dieser Interessen ist dem Gesetzgeber vorbehalten. Daß es sich hierbei um eine schwierige Aufgabe handelt, macht auch der 1981 gefaßte Beschluß der Hauptversammlung der ärztlichen Vereinigung „Hartmannbund" deutlich:

„Die Delegierten des Hartmannbundes fordern, daß die ärztliche Schweigepflicht auch bei Forschungsvorhaben beachtet wird.

Sie bekräftigen die Aussage des 84. Deutschen Ärztetages, wonach auch das steigende Interesse an der Krankheitsursachenforschung das Verfügungsrecht des Patienten über seine persönlichen Daten nicht außer Kraft setzen kann. Daraus folgt, daß behandelnde Ärzte Patientendaten auch für Forschungszwecke nur mit Einwilligung der betroffenen Patienten oder in anonymisierter Form weitergeben dürfen.

Es wird erneut an den Gesetzgeber in Bund und Ländern appelliert, die schutzwürdigen Belange der Bürger nicht durch immer neue Ausnahmen oder spezialgesetzliche Regelungen abzubauen oder einzuengen."

Ergebnis

Die Führung von Krebsregistern zum (ausschließlichen) Zweck der Nachsorge ist mit Einwilligung des Patienten zulässig.

Es sollte in absehbarer Zeit geklärt werden, ob darüber hinaus zum Zwecke der epidemiologischen Forschung und der Planung von Gesundheitseinrichtungen die Einrichtung eines zentralen Krebsregisters gesundheitspolitisch erforderlich ist.

Aus der Sicht des Datenschutzes sollten bei einer Entscheidung folgende Gesichtspunkte berücksichtigt werden:

- Die Sammlung personenbezogener Daten in zentralen Registern betrifft entscheidend das Grundverhältnis Arzt-Patient. Jede Information, die eine dritte Stelle über den Gesundheitszustand des Patienten von diesem Register direkt oder indirekt erhält, kann das Verhältnis des Patienten zu seinem Arzt belasten.
- Daher ist die Sammlung personenbezogener Gesundheitsdaten in zentralen Registern soweit wie möglich zu beschränken.
- Die Datenverarbeitung sollte in aller Regel nur mit Einwilligung des Betroffenen erfolgen.
- Etwaige Ausnahmen sollten eng umgrenzt werden.
- In jedem Fall soll der Patient ein Auskunftsrecht haben.
- Ein Gesundheitsregister, dessen Zweck über die unmittelbare Behandlung hinausgeht, setzt eine konkrete Güterabwägung zwischen dem Arztgeheimnis und dem epidemiologischen Forschungsinteresse voraus, und wäre nur auf Grund eines speziellen Gesetzes zulässig.

Ich gehe davon aus, daß ich frühzeitig beteiligt werde, sofern in Berlin entschieden wird, einen Gesetzesentwurf vorzubereiten.

Sonstige Forschungsvorhaben

Daneben bin ich auch mit anderen Forschungsprojekten aus dem Gesundheitsbereich befaßt gewesen. So etwa mit Vorhaben über Wohngruppen Behinderter, spezielle gesundheitliche Risiken ausländischer Frauen, wissenschaftliche Nachuntersuchungen früherer Patienten und Erfassung und Auswertung von Schulsportunfällen.

In diesen Fällen entstand die Frage, wo eine sachgerechte Grenze zwischen den Interessen des Einzelnen an seinen Gesundheitsdaten und den Interessen des Forschers gezogen werden soll, ob Einwilligungserklärungen der Betroffenen beigebracht werden müssen oder bereits abgegebene Erklärungen ausreichen. Diese Abgrenzung konnte in den einzelnen Fällen auch gefunden werden.

Die Schwierigkeit besteht jedoch darin, daß eine spezielle Norm über die Behandlung datenschutzrechtlicher Fragen im Forschungsbereich fehlt. Ich gehe jedoch davon aus, daß im Rahmen der Novellierungsdebatte über das Bundesdatenschutzgesetz auch dieser Fragenkomplex erörtert und über die Schaffung einer Forschungsklausel auf Bundesebene entschieden wird, an der sich die Landesgesetzgeber orientieren können.

Krankenhäuser

Die Erhebung, Speicherung und Übermittlung von Patientendaten durch das Krankenhaus bedarf besonderer Sorgfalt. Daß auch in diesem Bereich die Anpassung an den Datenschutz noch nicht vollständig vollzogen ist, wird im folgenden deutlich. Dabei wird zugleich erkennbar, daß eine Reihe weiterer Fragen des Datenschutzes im Krankenhausbereich in naher Zukunft geklärt werden muß.

Der Senat hat eine „Allgemeine Anweisung über Aufnahme, Aufenthalt und Entlassung von Kranken in den Krankenhäusern des Landes Berlin (Aufenthaltsanweisung)" erlassen, zu der ich vorher Stellung genommen habe. Ziel meiner Stellungnahme war es, klarzustellen, in welchem Rahmen der Patient selbst entscheiden kann, an wen seine Daten übermittelt werden.

Ein Beispiel hierfür ist die Übermittlung von *Patientendaten* an die Krankenversicherung. Im Hinblick darauf, daß jedermann die Möglichkeit hat, den Krankenhausaufenthalt selbst zu bezahlen, ist die Übermittlung von Patientendaten an die Krankenversicherung nicht schon durch den Behandlungsvertrag gedeckt. Vielmehr setzt die Zulässigkeit eine gesonderte Einwilligungserklärung des Patienten voraus. Nunmehr ist in dem Vordruck für den Behandlungsvertrag (Aufnahmeverhandlung) eine entsprechende Erklärung enthalten, die gegebenenfalls vom Patienten gestrichen werden kann.

Nach einer Eingabe von Nachbarn eines Städtischen Krankenhauses können Mitteilungen über die im Krankenhaus mit Genehmigung der Deutschen Bundespost betriebene Personenrufanlage über herkömmliche Rundfunk- und teils auch Fernsehgeräte empfangen werden. Das Krankenhaus mußte ich im Interesse des Schutzes der Patientendaten darauf hinweisen, daß sensitive Patienten- aber auch Personaldaten nicht durch die Anlage übermittelt werden dürfen, solange nicht garantiert werden kann, daß unbeteiligte Dritte von diesen Daten keine Kenntnis erhalten.

Häufig ist unbekannt, daß bereits die bloße Tatsache des Aufenthaltes eines Patienten in einer Krankenanstalt der ärztlichen Schweigepflicht unterliegt. Grundsätzlich ist daher die Auskunft über den Aufenthalt eines Patienten nur zulässig, wenn dieser eingewilligt hat oder ein Gesetz die Übermittlung zuläßt[12].

Von einem Bürger wurde ich darauf aufmerksam gemacht, daß in seinem Keller ca. 100 Krankenakten einer psychiatrischen Klinik lagern. Die Akten stammten aus den Jahren 1977 bis 1980 und befanden sich in einem Karton. Sie enthielten u. a. Krankenblätter, Röntgenaufnahmen, Krankenberichte, Einwilligungserklärungen, Einweisungen, handgeschriebene Lebensläufe, Anträge für Gebrechlichkeitspflegschaften, Alkoholanamnesen, Aufnahmeberichte, Aufnahmebefunde der Neurologisch-Psychiatrischen Abteilung, EKG, Intelligenztests, Krankengeschichten, Anfragen der Gesundheitsämter, Überweisungen mit Untersuchungsberichten, Verordnungen, Beurlaubungen, Begleitscheine für Untersuchungsmaterial, Ausgangsbogen und Ausgangskarten.

[12] Für die polizeiliche Fahndung vgl. die Entscheidung des Bundesverfassungsgerichts Band 32 S. 373, 381

Damit sind in den Akten Daten höchster Sensitivität enthalten, da sie über ihren Charakter als medizinische Daten hinaus Suchtkranke (insbesondere Alkoholkranke) betreffen und ihre Kenntnisnahme durch Unbefugte zu schwersten Beeinträchtigungen schutzwürdiger Belange der Patienten führen können.

Soweit in den Akten Daten enthalten sind, die aus Dateien stammen, stellt die Entfernung der Akten aus dem Verfügungsbereich des Krankenhauses einen Bruch des Datengeheimnisses (§§ 8, 6, 11 Berliner Datenschutzgesetz) dar. Im übrigen liegt objektiv ein Verstoß gegen § 203 Abs. 1 Strafgesetzbuch vor.

Gegen den mutmaßlichen Täter wurde ein Ermittlungsverfahren eingeleitet, das jedoch vorläufig eingestellt werden mußte, da sich der Verdächtige nicht mehr im Inland befindet.

Die Vorkommnisse haben in dem betroffenen Krankenhaus dazu geführt, daß Vorkehrungen zur Reorganisation der Krankenaktenhaltung getroffen worden sind.

Bei Gelegenheit werde ich - auch in anderen Krankenanstalten - die ordnungsgemäße Aufbewahrung der Unterlagen über die Patienten überprüfen.

Die Behandlung psychiatrischer Daten

Häufig fühlen sich Bürger über den Umgang mit solchen Daten in ihren Persönlichkeitsrechten verletzt, die in psychiatrischen Gutachten enthalten sind. Entsprechende Eingaben betrafen die Bereiche Personalwesen, Familienfürsorge, Behindertenfürsorge und Schulwesen.

Bei der Erhebung, Speicherung und Übermittlung psychiatrischer Daten, insbesondere für psychiatrische Gutachten muß beachtet werden, daß

- diese Daten besonders sensitiv sind und jede mißbräuchliche Verwertung zu erheblichen, gegebenenfalls irreparablen Schäden führen kann,
- die wissenschaftlichen Erkenntnisse über Krankheitsbilder und sichere Anzeichen von psychiatrischen Erkrankungen einem erheblichen Wandel unterliegen.

Daraus ergibt sich die Notwendigkeit äußerster Vorsicht in allen Phasen der Datenverarbeitung. Um den Datenschutz in diesem kritischen Bereich zu fördern, habe ich Kriterien für die datenschutzrechtliche Beurteilung der Erhebung, Speicherung und Übermittlung psychiatrischer Daten, insbesondere in psychiatrischen Gutachten, zusammengestellt, die für Zwecke der Verwaltung von Dienststellen des Landes Berlin benötigt werden[13]. Diese werde ich bei Beratung und Prüfung zugrundelegen.

Die Verwendung von Vordrucken im Gesundheitsdienst

Auf Grund mehrerer Eingaben hatte ich mich mit der Frage zu beschäftigen, wie die Fragebogen für amtsärztliche Untersuchungen zu beurteilen sind. Anlaß war einmal der vom Senator für Justiz - Ärztlicher Dienst - verwendete zweiseitige - sehr detaillierte - Fragebogen, der auch für die 6-monatige Beschäftigung von Praktikanten verwendet worden ist. Der Fragebogen war mit einer generellen „Erklärung" verbunden, wonach der Bewerber pauschal alle Stellen von der ärztlichen Schweigepflicht entbindet. Gegen zahlreiche Einzelfragen sowie die im Formular enthaltene Erklärung habe ich datenschutzrechtliche Bedenken erhoben mit der Folge, daß der Senator für Justiz sich bereit erklärte, diesen Fragebogen für Praktikanten einzuziehen.

Was die Verwendung für andere Personen angeht, gilt folgendes:

Verschiedene Bürger haben ebenfalls Einwände gegen den Vordruck erhoben, der allgemein zur vertrauensärztlichen oder amtsärztlichen Untersuchung vom öffentlichen Gesundheitsdienst verwendet wird. Die Bedenken, die ich gegenüber dem damaligen Senator für Gesundheit und Umweltschutz geäußert habe, führten zu einer Neugestaltung des Erhebungsbogens, die die Belange des Datenschutzes hinreichend berücksichtigt.

Folgende datenschutzrechtliche Anforderungen hatte ich gestellt:

- Daten dürfen nur erhoben werden, soweit sie für die Aufgabe erforderlich sind.
- Einwilligungen zu Auskünften können nicht pauschal eingeholt werden.
- Der Bürger muß in der Lage sein, Art und Umfang der mit der Einwilligung verbundenen Konsequenzen zu übersehen.

2.2 Öffentliche Sicherheit und Ordnung

Landesmeldegesetz

Auf Grund des vom Bundestag verabschiedeten Melderechtsrahmengesetzes ergibt sich für die Länder die Notwendigkeit, ihre Meldegesetze neu zu fassen.

Dementsprechend wird im Auftrag der Innenministerkonferenz ein Musterentwurf für ein Landesmeldegesetz von einem Ausschuß vorbereitet. Die Datenschutzbeauftragten haben zu diesem Vorhaben detaillierte Vorstellungen hinsichtlich der Ausgestaltung des Datenschutzes in den Landesmeldegesetzen beschlossen:

Sie wollen erreichen, daß die in dem vom Bundestag verabschiedeten Melderechtsrahmengesetz vorgesehene Zielsetzung, das Einwohnermelderegister nicht als universelles Verwaltungsinformationssystem zu verwenden, auch im Bereich der Landesmeldegesetze beibehalten wird. Die Phase der Umsetzung des Bundesmelderechtsrahmengesetzes in das Landesrecht birgt eine Reihe von Gefahren für den Datenschutz. Diese wollen die Datenschutzbeauftragten mit ihren Vorschlägen vermeiden.

Sie betreffen vor allem:

- den Umfang der Speicherung von Daten
- die Ordnungsmerkmale (früher: „Personenkennzeichen")
- Art und Umfang der Meldepflicht
- die Mitwirkungspflicht des Wohnungsgebers bei der An- und Abmeldung
- die Datenübermittlung.

Meine Bedenken und Vorschläge habe ich im Mai 1981 in einer detaillierten Stellungnahme dem Senator für Inneres mitgeteilt.

Dabei habe ich die Notwendigkeit hervorgehoben, den direkten Anschluß von Abfragestationen an das Einwohnersystem konkret zu regeln. Im Einzelfall sollte durch Verordnung geregelt werden, welche Daten für den Abruf durch andere Stellen bereitgehalten werden dürfen.

Gerade in Berlin wirft die zunehmende Anzahl von gemeldeten Ausländern die Frage auf, inwieweit es möglich ist, die korrekte Schreibweise der ausländischen Namen auch im automatisch geführten Melderegister - in Berlin der Einwohnerdatenbank - darzustellen. Für eine solche Maßnahme spricht das persönliche Interesse der Personen mit ausländischen Namen an der korrekten Schreibweise ihres Namens und das öffentliche Interesse an der eindeutigen Identifizierbarkeit der Personen über den Namen. Die Wahrung dieser Interessen ist insbesondere im Hinblick auf eine zukünftige Automatisierung des Personenstandswesens von Bedeutung.

Technische und ökonomische Einwände, die einer Speicherung bisher entgegengehalten worden sind, bestehen angesichts normierter Verfahren zur Speicherung diakritischer Zeichen und neuerer Entwicklungen im Bereich druckender Ausgabemedien nicht mehr. Deshalb sollte bei der Konzeption des neuen Datensatzes für das Einwohnerwesen die korrekte Repräsentation ausländischer Namen auch dann berücksichtigt werden, wenn ein korrekter Ausdruck noch nicht sofort möglich ist.

Meine Vorstellungen werde ich auch in die Stellungnahme einfließen lassen, die ich zu dem Entwurf für ein Landesmeldegesetz abgeben werde, den mir der Senator für Inneres inzwischen übersandt hat.

[13] Die Kriterien sind als Anlage 1 beigefügt

Meldewesen

Anfang Mai erhielt ich eine Eingabe, mit der gerügt wurde, daß ein Wahlberechtigter für die Wahlen am 10. Mai 1981 keine Wahlberechtigungskarte erhalten habe.

Die Ermittlungen ergaben, daß eine Eintragung im Einwohnerdatensatz des Bürgers vorlag, nach der der Betreffende wegen geistiger Gebrechen unter Pflegschaft stand. Ein entsprechender Beschluß eines Amtsgerichts war jedoch nicht ergangen. Das angegebene Aktenzeichen bezog sich auf eine andere Person, deren Pflegschaft korrekt in der Datenbank eingetragen war. Da die Eintragungen fünf Jahre zurücklagen, war eine genaue Rekonstruktion der Vorgänge bei der Fehleintragung nicht mehr möglich. Alles deutet jedoch darauf hin, daß der Eintrag erst in einem falschen Datensatz vorgenommen, und daß nach einer späteren Überprüfung die Eintragung im richtigen Datensatz wiederholt wurde. Diese Annahme wird dadurch gestützt, daß die zwölfstelligen Aktenzeichen in beiden Fällen sehr ähnlich sind. In einem solchen Fall ist die Fehleintragung nur durch Zufall zu entdecken, so daß eine Löschung der Fehleintragung nicht erfolgen konnte. Auch die Verwendung einer Prüfziffer im Aktenzeichen hatte in diesem Fall versagt, da auch dieser Teil identisch war.

Der festgestellte Mangel ist höchstwahrscheinlich auf menschliches Versagen zurückzuführen, welches typischerweise beim Umgang mit Computern auftreten kann.

Bei meinen Überprüfungen im Zusammenhang mit der genannten Eingabe stieß ich jedoch auf weitere Mängel und Ungenauigkeiten bei der Behandlung von Pflegschaftseintragungen in der Einwohnerdatenbank.

So wurden mir bei einer Umfrage von den Bezirkseinwohnerämtern insgesamt 50 Personen genannt, denen zur Wahl am 10. Mai 1981 entweder Wahlunterlagen zugesandt wurden, obwohl sie wegen geistiger Gebrechen unter Pflegschaft standen oder keine Wahlunterlagen zugesandt wurden, weil in der Datenbank fehlerhaft Wahlausschlußgründe vermerkt waren. Weiterhin erhielt ich den Hinweis, daß zahlreiche Fälle dieser Art ohne formelle Einsprüche vor der Wahl bereinigt worden waren, ohne daß die Namen nachträglich feststellbar sind, und daß mit einer relativ hohen Dunkelziffer zu rechnen sei.

Bei der Überprüfung habe ich folgendes festgestellt:

1. Der Fehler wurde in der Mehrzahl aller Fälle durch Mängel des Belegflusses zwischen den die Pflegschaft oder die Aufhebung der Pflegschaft verfügenden Amtsgerichten und den Bezirkseinwohnerämtern verursacht, wie er für die sogenannten Mitteilungen in Zivilsachen vorgeschrieben ist. Entsprechende Entscheidungen der Amtsgerichte haben die Einwohnerdatenbank nicht erreicht, so daß bestehende Pflegschaften wegen geistiger Gebrechen nicht eingetragen waren oder aufgehobene Pflegschaften wegen geistiger Gebrechen nicht gelöscht worden waren. Welche Stellen für den Mangel des Belegflusses im einzelnen verantwortlich sind, ließ sich nachträglich nicht feststellen.
2. Der Aufruf eines Datensatzes für die Änderung oder Auskunft erfolgt entweder über das zwölfstellige Aktenzeichen der Meldebehörde oder über zwei bekannte Merkmale (wie z.B. Familienname und Vorname). In dem genannten Fall wurde z.B. durch die fehlerhafte Eingabe des Aktenzeichens eine Pflegschaft der falschen Person zugeordnet. Der Zugriff über nur zwei Merkmale führt zumindest bei häufigen Namen zu einem großen Angebot von Zieldatensätzen. Es bedarf daher der erhöhten Aufmerksamkeit des Eingebenden, um die Eintragung bei der richtigen Person durchzuführen. Daraus ergibt sich naturgemäß eine Fehlerquelle.
3. Änderungen eines Datensatzes können von allen änderungsberechtigten Personen und an allen änderungsberechtigten Terminals vorgenommen werden. Das bedeutet auch, daß jedes Bezirkseinwohneramt die Datensätze von Bürgern anderer Bezirke ohne Abstimmung mit dem Bezirksamt, welches für die betroffene Person zuständig ist, ändern kann. In mindestens einem Fall ist durch diese Eigenschaft des Systems ein Datensatz ohne Kenntnis des zuständigen Bezirksamtes geändert worden. Dies entspricht nicht den Grundsätzen ordnungsgemäßer Datenverarbeitung.

Ich habe in den einzelnen Fällen die entsprechenden Bezirksämter um Korrektur der Daten und um Stellungnahme gebeten. Generell haben sich jedoch Mängel des technisch-organisatorischen Gesamtsystems ergeben. Die Gespräche darüber, wie die Mängel zu beheben seien, sind noch nicht abgeschlossen.

Ich habe bisher folgende Anregungen gegeben:

1. Kontrolle des Belegflusses zwischen den auslösenden Amtsgerichten und der Einwohnerdatenbank durch die Amtsgerichte:

   Die Amtsgerichte sollten durch geeignete organisatorische Maßnahmen sicherstellen, daß ihnen innerhalb einer angemessenen Frist die die Pflegschaftsdaten betreffenden Originalauszüge aus der Einwohnerdatenbank zugesandt werden, damit sie auf Richtigkeit geprüft werden können. Sie sind nach Prüfung und ggf. Korrektur oder Vervollständigung dann in die jeweilige Pflegschaftsakte zu legen.
2. Verbesserung des gezielten Zugriffs auf Datensätze:

   Der Zugriff auf Datensätze soll entweder nur durch Eingabe der Meldebehörde-Aktenzeichen und der Familiennamen oder durch Eingabe von mindestens *drei* Merkmalen möglich sein. Dies würde sowohl der Sicherheit des korrekten Zugriffs dienen, als auch bei häufigen Namen zur Reduktion des Datensatzangebotes und damit zur Arbeitserleichterung führen.
3. Beschränkung des Datenzugriffs auf die zuständigen Bezirkseinwohnerämter sowie die zentralen Behörden:

   Jeder Datensatz eines Einwohners erhält Eintragungen über das zuständige Bezirksamt, in dem der Einwohner gemeldet ist. Die Terminals sind im System differenziert und lassen sich den Standorten zuordnen. Durch eine geeignete Programmergänzung könnte sichergestellt werden, daß das Programm bei ändernden Zugriffen überprüft, ob diese von einer zuständigen Behörde aus erfolgen. Andere Bezirksämter müssen sich bei Änderungswünschen jeweils mit dem zuständigen Bezirksamt abstimmen und diese um Änderung bitten.

Obwohl ich meine Überprüfung auf die Eintragungen der Wahlausschlußgründe beschränkt habe, gehe ich davon aus, daß auch andere Bereiche des Einwohnerdatensatzes von ähnlichen Mängeln betroffen sein können. Dies gilt z. B. für Daten über Eheangelegenheiten, Anstaltsunterbringungen, Lohnsteuermerkmale und Suchvermerke.

Schließlich fiel anläßlich der Überprüfung auf, daß über die Voraussetzungen der Eintragung von Wahlausschlußgründen Unklarheiten bestehen. Es sollte geprüft werden, ob nicht die dadurch bedingten Unsicherheiten bei der Führung des Melderegisters durch eine gesetzliche Klarstellung beseitigt werden könnten. Man könnte gemäß einer Empfehlung der Gesundheitsministerkonferenz vom 19. November 1981 daran denken, entsprechend der Regelung des § 45 Abs. 5 Strafgesetzbuch eine Bestimmung einzuführen, nach der ein Wahlausschlußgrund nicht quasi als automatische und unausgesprochene Nebenfolge anderer Maßnahmen, sondern nur auf Grund eines ausdrücklichen richterlichen Beschlusses festgestellt wird.

Lohnsteuerkarten

Den offenen Versand von Lohnsteuerkarten habe ich bereits im letzten Jahresbericht als nicht den Vorschriften entsprechend bemängelt.[14]

Die Einwendungen, die der Senat[15] hiergegen in seiner Stellungnahme zum Jahresbericht 1980 erhoben hat, schlagen nicht durch. Die Zahl der Eingaben und die Art der festgestellten Vorfälle zeigen, daß das gewählte Verfahren nicht sicher genug

[14] Jahresbericht 1980 S. 15 unter 2.6

[15] Stellungnahme des Senats - Drucksache 8/786 vom 5. Mai 1981 S. 4 zu 2.6

ist. Auch liegen die Sicherheitsanforderungen unter dem Standard zahlreicher anderer Bundesländer.

Entgegen der Stellungnahme des Senats war es bereits im Berichtsjahr möglich, die Lohnsteuerkarten kuvertiert zu verteilen. Damit wurde meiner Auffassung Rechnung getragen.

Volksbegehren

Zahlreiche Bürger haben sich an mich gewandt und um Auskunft darüber gebeten, auf welche Weise der Datenschutz bei der Durchführung des Antragsverfahrens für ein Volksbegehren zur Auflösung des Abgeordnetenhauses gewährleistet sei. Insbesondere stieß bei den Bürgern auf Bedenken, daß bei der Überprüfung der Unterschriften ein Vermerk in die Einwohnerdatenbank aufgenommen wurde, aus dem hervorgeht, von wem und auf welcher Liste eine Unterschrift geleistet wurde. Zweifel rührten wohl vor allem von dem bisher unbekannten und gegenüber Wahlen abweichenden Verfahren her.

Dem Charakter des Volksbegehrens entspricht es, daß sich der Bürger offen zu einer bestimmten Auffassung bekennen kann. Damit ist zwangsläufig verbunden, daß auch andere Bürger, die sich etwa auf der gleichen Unterschriftenliste eintragen, davon Kenntnis erhalten, welche Personen vor ihnen unterschrieben haben. Auf diese Weise wird jedoch nicht eine Wahlentscheidung, sondern in erster Linie die Förderung des Antrages auf ein Volksbegehren kundgetan.

Von den Verwaltungen sind die Unterschriften allerdings wie Wahlunterlagen zu behandeln. Die Landeswahlordnung bestimmt, daß diese Unterlagen spätestens ein Jahr nach dem Wahltag zu vernichten sind. Sie dürfen ausschließlich zur Durchführung des Volksbegehrens verwertet werden, also auch nicht z.B. zur Wahlwerbung bei anschließendem Wahlkampf. Eine unbefugte Verwertung würde einen Bruch des Daten- sowie des Amtsgeheimnisses der beteiligten Bediensteten darstellen. Soweit die Listen im Vorfeld vom Antragsteller ausgelegt werden, unterliegen sie ebenfalls datenschutzrechtlichen Bestimmungen. Bei einer Neufassung der Vorschriften wäre es empfehlenswert, daß auf diese Sachverhalte in den Vorschriften genau hingewiesen wird.

Mißbräuche der Unterschriftenlisten sind nicht bekannt geworden. Dies liegt auch daran, daß bereits im Vorfeld mit den beteiligten Stellen ein enger Kontakt stattgefunden hat mit dem Ziel, eine datenschutzgemäße Behandlung und alsbaldige Vernichtung sicherzustellen.

Meine Überprüfung der Aufbewahrung der Listen hat ergeben, daß die Listen zwischenzeitlich vernichtet worden sind.

Als ein Problem hat sich erwiesen, daß für einen bestimmten Zeitraum im Einwohnerdatensatz die Tatsache gespeichert wird, daß jemand für eine bestimmte Liste seine Unterschrift abgegeben hat.

Nach dem Gesetz über Volksbegehren und Volksentscheid zur Auflösung des Abgeordnetenhauses haben die Bezirksämter die Aufgabe, zu prüfen, ob die Unterzeichner am Tage der Unterschriftsleistung stimmberechtigt waren. Zudem darf je Liste nur eine Unterschrift geleistet werden. Dies bedeutet, daß, insbesondere wenn Antragsteller verschiedener politischer Richtungen miteinander konkurrieren, in bestimmten Einwohnerdatensätzen zeitweise die Tatsache der Unterzeichnung auf einer bestimmten Liste eingetragen wird. Daraus ließe sich mit einer gewissen Wahrscheinlichkeit auf die politische Haltung schließen. Die Registrierung derartiger Daten im Einwohnerdatensatz muß prinzipiell als bedenklich angesehen werden[16]. Auf Grund der erlassenen Gesetze ist diese Registrierung für einen möglichst kleinen Zeitraum jedoch zulässig. Es wäre allerdings wünschenswert, wenn im Hinblick auf einen möglichen Mißbrauch bei einer etwaigen Gesetzesänderung erwogen wird, die Dauer derartiger Speicherungen und den Kreis der Zugriffsberechtigten genau zu bestimmen.

[16] Vgl. dazu entsprechende ausländische Vorschriften, etwa Art. 31 des französischen Datenschutzgesetzes (Gesetz Nr. 78 - 17 vom 6. Januar 1978 betr. die Automation, Dateien und Grundrechte), der derartige Registrierungen prinzipiell - allerdings mit Erlaubnisvorbehalt - untersagt.

Ich habe mich vergewissert, daß die entsprechenden Einträge im Einwohnerdatensatz zwischenzeitlich wieder gelöscht sind.

Im Hinblick darauf, daß ggf. Erwägungen angestellt werden über die künftige Ausgestaltung des Verfahrens für ein Volksbegehren, möchte ich noch auf folgende Bedenken hinweisen, die mir von Seiten der Bevölkerung bekannt gemacht worden sind. So erklärten mir gegenüber etwa ältere Mitbürger, daß sie sich bei der „Haussammlung" von Unterschriften durch den Vermieter in ihrer Entscheidungsfreiheit stark eingeschränkt gesehen hätten. Es sollte parlamentarisch entschieden werden, ob derartige Begleiterscheinungen plebiszitärer Entscheidungen in Kauf genommen werden sollen.

Wahlen

Anläßlich der Wahlen stellten einige Bürger die Frage, ob die Parteien, von denen sie Wahlwerbung erhalten hatten, ihre Anschriften rechtmäßig verwendet hätten.

Dahinter steht folgendes Verfahren: Vor der Wahl wurden an die beteiligten politischen Parteien zu Zwecken der Wahlwerbung Listen ausgegeben, die, nach Wohngebiet sowie Wählergruppen (Jungwähler, Wähler über 60 Jahre) sortiert, Namen und Adresse der Wähler enthielten.

Diese auch vor Bundestags- und Europawahlen geübte Praxis findet ihre Grundlage in § 24 Landeswahlordnung. Danach sind die Bezirkswahlämter berechtigt, Abschriften oder Auszüge aus der Wählerliste mit allen vorhandenen Daten (z. B. auch Geburtsdatum der Betroffenen) an die Parteien herauszugeben.

Im Hinblick auf die einschränkenden Bestimmungen des § 22 Melderechtsrahmengesetz vom 18. August 1980 wurde von dieser weitergehenden Möglichkeit nicht Gebrauch gemacht, sondern auf den Ausdruck der Geburtsdaten verzichtet.

Die Landeswahlordnung beschränkt die Benutzung dieser Daten auf Zwecke zur Wahlwerbung. Eine weitergehende Nutzung ist ausgeschlossen. Für den Schutz dieser Daten sind zunächst die politischen Parteien selbst verantwortlich. Anhaltspunkte für einen Datenmißbrauch sind mir anläßlich dieser Wahl bisher nicht bekanntgeworden.

Ablichtung von Personalausweisen

Bereits im Vorjahr[17] sind mir mehrere Fälle bekanntgeworden, daß öffentliche Stellen vorgelegte Personalausweise ablichten und Ablichtungen aufbewahren. Bei der Beurteilung dieser Praxis gehe ich von folgendem aus:

- Die Ablichtung von Personalausweisen oder Teilen des Personalausweises muß für die Aufgabenerledigung erforderlich sein, d.h. es müssen besondere Gründe, in der Regel Sicherheitsgründe, dieses Verfahren erfordern.
- Die Sammlung von Fotokopien stellt eine Datei im Sinne des Berliner Datenschutzgesetzes dar.
- Da der Zweck der Datei in der Regel spätestens erfüllt ist, wenn der Besucher die öffentliche Stelle verlassen hat, sind die Daten danach unverzüglich zu löschen (in der Regel also spätestens am folgenden Werktag).
- In besonderen Fällen mußte ich die Notwendigkeit der „Spätidentifizierung" anerkennen, d. h. die nachträgliche Identifizierung von Personen, die eine öffentliche Stelle offensichtlich mit falschen Ausweisen betreten haben. Auch in diesem Fall erscheint es erforderlich, daß die Speicherung zeitlich befristet wird und sichergestellt ist, daß die schutzwürdigen Belange der übrigen Besucher gewahrt werden.

Auf dieser Grundlage bestanden z. B. gegen das Verfahren der Ausweisablichtung anläßlich der Wahlnacht im Abgeordnetenhaus keinerlei Bedenken. Die Ablichtungen sind auch unverzüglich vernichtet worden.

Die Praxis der Justizvollzugsanstalten mußte - was die Aufbewahrung der Ablichtungen angeht - geändert werden.

[17] Vgl. meinen Jahresbericht 1980 unter 2.6, S. 14

In jedem Fall ist hervorzuheben, daß das Verfahren der Ausweisablichtung nur in wohlbegründeten Ausnahmefällen verwendet werden kann.

Richtlinien für die Führung Kriminalpolizeilicher personenbezogener Sammlungen

Um den Datenschutz auch im Bereich der Kriminalpolizei sicherzustellen und Kriterien für die Ermessensentscheidungen insbesondere bei der Auskunftserteilung festzulegen, hat die Innenministerkonferenz im Januar 1981 Richtlinien für die Führung Kriminalpolizeilicher personenbezogener Sammlungen (KpS) verabschiedet, die im Lande Berlin am 15. April 1981 unverändert durch Erlaß des Senators für Inneres eingeführt worden sind. Die Richtlinien zielen im wesentlichen darauf ab, die in den Datenschutzgesetzen festgelegten Grundsätze (Beschränkung der Zulässigkeit von Datenspeicherung und -übermittlung auf dasjenige Ausmaß, das zur rechtmäßigen Aufgabenerfüllung erforderlich ist; Verpflichtung zur Datensicherung) auf alle kriminalpolizeilichen Sammlungen, also auch auf Akten, zu übertragen.

Bei der Auskunftserteilung an den Betroffenen wird von der bislang üblichen Praxis abgegangen, die Auskunft unter generellem Verweis auf das Datenschutzgesetz zu verweigern. Nunmehr ist bestimmt, daß auf Antrag Auskunft darüber erteilt wird, ob und ggf. welche Unterlagen zur Person vorhanden sind, es sei denn, daß die Belange des Bürgers hinter dem öffentlichen Interesse an der Nichtherausgabe der jeweiligen Daten zurücktreten müssen. Im Gegensatz zu bisher wird die Aufbewahrungsdauer beschränkt (in der Regel auf 10 Jahre nach der letzten Eintragung).

Die Konferenz der Datenschutzbeauftragten hatte zu dem Entwurf der Richtlinien eine ausführliche Stellungnahme abgegeben, die allerdings nicht in allen Punkten Berücksichtigung fand. Ich werde im kommenden Jahr mein besonderes Augenmerk darauf richten, auf welche Weise die Richtlinien Niederschlag in der polizeilichen Arbeit finden und ob derartige Verwaltungsvorschriften das geeignete Mittel sind, den Datenschutz in Polizeibehörden zu gewährleisten.

2.3 Personalwesen

Erhebliche Datenschutzdefizite

Datenschutzfragen aus dem Bereich des Personalwesens der öffentlichen Verwaltung haben sich mir seit Beginn meiner Tätigkeit als Berliner Datenschutzbeauftragter aufgedrängt.

Zwar vermag ich in der bloßen Schaffung zusätzlicher Rechtsvorschriften an sich keinen Fortschritt zu erkennen, es kommt vielmehr auf die Gesinnung und ein entsprechendes Verhalten der Bürger und der seinen Zielen dienenden staatlichen Amtswalter an. Trotzdem erscheint mir eine durchgreifende Veränderung der Praxis des Umgangs mit Personaldaten nur möglich, wenn die Ziele rechtlich vorgegeben werden.

Fortentwicklung des Beamtenrechts Datenschutzrechtliche Vorstellungen zur Verbesserung des Personaldatenschutzes

In meinem Jahresbericht 1980 habe ich eine Reform der personaldatenrechtlichen Regelungen im Landesbeamtengesetz angesprochen[18]).

Mittlerweile hat die Bundesregierung das 4. Gesetz zur Änderung dienstrechtlicher Vorschriften vorgelegt, das u.a. eine Ergänzung der personalaktenrechtlichen Regelungen des Bundesbeamtengesetzes vorsieht. Es bietet sich m. E. an, daß der Landesgesetzgeber auf Grund des Gesetzgebungsvorhabens des Bundes erwägt, auch den Personaldatenschutz der Berliner Landesbeamten zu verbessern.

Meine zu diesem Zweck vorgelegten Vorstellungen beruhen auf den Erfahrungen, die ich mit zahlreichen Eingaben gemacht habe.

Meine Anregungen verfolgen insbesondere drei Ziele:

- Ausdrückliche gesetzliche Regelung der Ermittlung und Speicherung von personenbezogenen Daten im Beamtenverhältnis selbst sowie in dessen Vorverhältnis,
- Harmonisierung des Personaldatenrechts der Beamten (bereichsspezifischer Datenschutz) mit dem allgemeinen Datenschutzrecht sowie dem arbeitsrechtlichen Datenschutz,
- Abkehr vom sogenannten Vollständigkeitsprinzip durch Verpflichtung des Dienstherrn, bestimmte in der Personalakte gespeicherte Daten sofort oder nach Zeitablauf wieder zu tilgen.

Der von mir unter Datenschutzgesichtspunkten entwickelte, als Anlage 2 beigefügte Vorschlag beschränkt sich auf eine Regelung des Personaldatenrechts, soweit es unmittelbar den grundrechtsrelevanten Bereich des Beamten betrifft. Die verwaltungstechnische Regelung des Personaldatenrechts könnte m.E. durch eine Rechtsverordnung erfolgen.

Unbeschränkte Auskünfte aus dem Bundeszentralregister

Bereits in meinem Jahresbericht 1980 hatte ich darauf hingewiesen, daß Berliner Behörden bei verschiedenen Verwaltungsvorgängen (insbesondere bei Einstellungen in den öffentlichen Dienst, aber auch z. B. bei der Feststellung der Eignung als Kleinsiedler auf einer Erbbauheimstätte) in m. E. unverhältnismäßigem Ausmaß von der Möglichkeit Gebrauch machen, eine unbeschränkte Auskunft aus dem Bundeszentralregister einzuholen. Nach Mitteilung des Senats[19]) ergab eine Umfrage an den Verwaltungen, daß für den Zeitraum von 11 Monaten bei insgesamt rd. 6.000 Ersuchen um unbeschränkte Auskunft nur in 28 Fällen Erkenntnisse zu verzeichnen waren, die nicht ohnehin auch in das Führungszeugnis aufgenommen worden wären.

Eine erneute Auswertung beim Bundeszentralregister im Mai 1981 hat ergeben, daß sich bislang an dieser Praxis nichts geändert hat.

Durch eine Eingabe wurde die Problematik noch erhellt: Im Zusammenhang mit der Einstellung für eine kurzfristige Tätigkeit als Erzieher für Sondergruppen in Obdachlosenheimen war über einen 26jährigen eine unbeschränkte Auskunft eingeholt worden. Darin waren Jugendstrafen enthalten, die in einem kurzen Zeitraum begangen worden waren, der über 8 Jahre zurücklag. Diese Strafen waren in ein Führungszeugnis nicht mehr aufzunehmen, der Betroffene konnte sich insoweit als nicht vorbestraft bezeichnen. Nichtsdestoweniger wurden die Strafen nun auf dem Wege der unbeschränkten Registerauskunft aufgedeckt, mit der Folge, daß sich der Betroffene Vorhaltungen ausgesetzt sah und eine Möglichkeit der Weiterbeschäftigung nicht mehr bestand.

Ich habe die Einholung der unbeschränkten Auskunft durch den Senator für Inneres, die Weiterleitung der Kopie der Auskunft an das betroffene Bezirksamt sowie die weitere Aufbewahrung der Auskunft beanstandet. Die Einholung einer unbeschränkten Auskunft durch die oberste Landesbehörde sowie die Weiterleitung an eine ihrer Aufsicht unterstehende Behörde ist nur zulässig, wenn dies zur Vermeidung von Nachteilen für den Bund oder ein Land unerläßlich ist oder wenn anderenfalls die Erfüllung öffentlicher Aufgaben erheblich gefährdet oder erschwert würde (§ 41 Bundeszentralregistergesetz). Im vorliegenden Fall sah ich die Voraussetzungen nicht für gegeben an.

Um die insbesondere auch im Vergleich zu anderen Bundesländern unverhältnismäßig hohe Anzahl an unbeschränkten Auskunftsersuchen in Berlin zu verringern, hatte ich Leitsätze formuliert und diese mit dem Senator für Inneres beraten. Insbesondere wegen der Haltung der Senatsschulverwaltung, die die Forderung der Bezirksämter nach unbeschränkten Auskünften unterstützt, sind die Beratungen noch nicht zu einem Ende geführt worden. Dessen ungeachtet werde ich fortfahren, die Einholung und Aufbewahrung solcher Auskünfte zu überprüfen und erforderlichenfalls zu beanstanden.

Die Verwaltungspraxis sollte von folgenden Leitsätzen ausgehen:

[18]) a. a. O. S. 13

[19]) Stellungnahme des Senats zum Jahresbericht 1980, Drucksache 8/786, S. 4

1. Das Ersuchen nach einer unbeschränkten Auskunft in einer Vielzahl von Fällen kann nicht der Regelfall sein. Die obersten Landesbehörden sollen nach dem Zweck des Bundeszentralregistergesetzes (BZRG), der besonders aus dem Zusammenspiel der §§ 39, 41, 51 BZRG deutlich wird, und dem Grundsatz der Verhältnismäßigkeit nur in bestimmten Fällen mit erheblicher Bedeutung Anfragen an das Bundeszentralregister richten, sofern das Führungszeugnis den Verwaltungszweck nicht erfüllt.

   Bei der Beurteilung ist zu berücksichtigen, daß die gegenüber dem dreistufigen Aufbau der Flächenländer andere Struktur der Berliner Verwaltung nicht eine weitergehende Praxis der unbeschränkten Auskünfte rechtfertigt. Dies folgt bereits aus Artikel 3 Grundgesetz.

2. Nur in schwerwiegenden Ausnahmefällen ist es zulässig, für nachgeordnete Behörden im Auftrag die Auskünfte zu beantragen und in diesen Fällen Entscheidungsempfehlungen oder Hinweise an eine nachgeordnete Behörde zu geben. Eine Ausnahme gilt, wenn
   - die oberste Landesbehörde im Einzelfall berechtigt wäre, die Entscheidung an sich zu ziehen und dies auch tatsächlich getan hat, oder
   - die Anfrage und Weitergabe zur Vermeidung von Nachteilen für den Bund oder das Land unerläßlich ist, oder
   - die Erfüllung öffentlicher Aufgaben erheblich gefährdet oder erschwert würde.

3. In Fällen, in denen die Anfrage berechtigt ist, muß sich die Behörde darauf beschränken, die erhaltenen Auskünfte nur in einem solchen Umfange aufzubewahren, als es für die Bearbeitung eines Verwaltungsvorganges unumgänglich ist. Ein Bedürfnis nach dauernder Aufbewahrung der erhaltenen Auskünfte besteht im Regelfall nicht, weil die oberste Landesbehörde ohnehin im Einzelfall jederzeit erneut Auskunft verlangen kann und der Hinweis, daß die Auskunft vorgelegen hat, ausreicht. Soweit in Ausnahmefällen eine Aufbewahrung unumgänglich sein sollte, muß sie gegen unberechtigte Einsichtnahme gesichert sein. Die Führung zahlreicher Auskünfte in den vielen Personen zugänglichen Sachakten ist unangemessen.

Es erscheint nunmehr an der Zeit, daß der Senat über eine neue Regelung entscheidet.

Offenbarung von Personaldaten

Anschriften öffentlicher Bediensteter dürfen in Berlin grundsätzlich nicht an private Stellen übermittelt werden (§ 11 Berliner Datenschutzgesetz), die diese dann zu Werbezwecken verwenden.

Dieser Grundsatz kann auch nicht dadurch umgangen werden, daß im öffentlichen Dienst Beschäftigte zugleich „Vertrauensleute" privater Organisationen sind und in dieser Eigenschaft Anschriftenlisten übermitteln. Die Tätigkeit als „Vertrauensmann" ist nur in den engen vom Dienstrecht gezogenen Grenzen zulässig[20]. Die Tätigkeit der „Vertrauensleute" hat sich danach auf kurze persönliche Kontaktaufnahmen und Terminvereinbarungen für außerhalb der Arbeitszeit liegende Gespräche und Verhandlungen zu konzentrieren. Die Übermittlung von Anschriftenlisten, etwa aller in einem bestimmten Zeitraum eingetretener Mitarbeiter, wäre eine Verletzung des Amtsgeheimnisses (Personalgeheimnisses) und als solche unzulässig. Anders liegt die Situation lediglich in dem Fall einer konkreten Kontaktaufnahme, die ggf. auch zur Übermittlung der jeweiligen Anschriften führen kann.

Die Zahlung von Gewerkschaftsbeiträgen unmittelbar durch die Arbeitgeber („Quellabzugsverfahren") ist schon mehrfach aus verschiedenen Rechtsgründen kritisiert worden. Auch datenschutzrechtlich ist dieses Verfahren nicht unproblematisch: Da die Gewerkschaftsbeiträge stets einen bestimmten Prozentsatz der Bezüge darstellen, wird mit der Zahlung der Beiträge durch den Arbeitgeber gleichzeitig die Höhe des Einkommens an die Gewerkschaft übermittelt.

Auf Grund eines Hinweises habe ich bei den Berliner Stadtreinigungsbetrieben das dort praktizierte Quellabzugsverfahren überprüft. Dabei habe ich festgestellt, daß das Verfahren nur durchgeführt wird, wenn die Bediensteten darin eingewilligt haben. Die Überprüfung der hierfür verwendeten Einzugsaufträge hat jedoch ergeben, daß ein Widerruf nur gegenüber der Gewerkschaft (hier der Gewerkschaft ÖTV) möglich sein sollte. Angesichts der mit dem Zahlungsauftrag verbundenen Übermittlung personenbezogener Daten an die Gewerkschaft halte ich diese Klausel für bedenklich. Die Einwilligung in die Übermittlung personenbezogener Daten kann nur gegenüber der übermittelnden Stelle abgegeben und somit jederzeit auch gegenüber dieser Stelle widerrufen werden. Die Berliner Stadtreinigungsbetriebe haben sich meiner Auffassung angeschlossen und werden in Übereinstimmung mit der ÖTV das Verfahren entsprechend ändern.

Die Höhe der Bezüge der einzelnen Bediensteten gehört zu den personenbezogenen Daten, auf deren Geheimhaltung trotz der Überprüfbarkeit an Besoldungstabellen stets großer Wert gelegt wird. So versendet das Landesamt für elektronische Datenverarbeitung im Auftrag des Landesverwaltungsamtes und anderer Dienststellen die Mitteilungen über die Höhe der Bezüge mit Hilfe von speziellen EDV-Ausdrucken, die erst gelesen werden können, wenn sie vom Bediensteten geöffnet sind.

Im Widerspruch zu dieser Übung steht das Verfahren, das in einer Reihe von Dienststellen bei der Rückgabe der ausgefüllten Lohnsteuerkarten an die Bediensteten geübt wird. Diese werden von der Stelle, die die Eintragungen vornimmt (z. B. Landesverwaltungsamt) gebündelt an bestimmte Anlaufstellen versandt (z. B. Büroleitung, Sekretariate u. ä.). Dort werden die Umschläge geöffnet und die Lohnsteuerkarten offen an die einzelnen Bediensteten verteilt. In diesem Verfahren sehe ich einen Mangel, da weit über das erforderliche Maß hinaus Einkommensdaten an verschiedene Mitarbeiter der Dienststellen bekanntgegeben werden. Ich habe empfohlen, ähnlich wie bei den Mitteilungen der Bezüge ein Verfahren zu entwickeln, das den Verschluß der ausgefüllten Lohnsteuerkarten ermöglicht.

Zwar wird in einigen Verwaltungen die Einwilligung der Bediensteten zur offenen Verteilung eingeholt. Die Einführung eines pauschalen Einwilligungsverfahrens kann jedoch die Verwaltung nicht von ihrer Verpflichtung entbinden, Verfahren einzuführen, die von vornherein eine Offenbarung von Personaldaten verhindern.

2.4 Studenten- und Schülerdaten

Ich habe an sechs Berliner Hochschulen Informationsgespräche über den Umgang mit Studentendaten geführt. Dabei konnte ich im Hinblick auf die organisatorischen und technischen Maßnahmen feststellen, daß den Datenschutzfragen ein sehr unterschiedliches Gewicht beigemessen wird. So konnten etwa an der Technischen Universität teilweise bemerkenswerte Vorkehrungen zur Datensicherung festgestellt werden. An anderen Hochschulen haben die Datenschutzgesetze dagegen kaum zu organisatorischen oder technischen Konsequenzen geführt.

Im einzelnen habe ich zu folgenden Punkten Empfehlungen gegeben:

Nach § 16 Satz 2 Ziff. 1 Berliner Datenschutzgesetz haben auch die Hochschulen eine Übersicht über die Art der von ihnen gespeicherten personenbezogenen Daten und über die Aufgaben, zu deren Erfüllung die Kenntnisnahme dieser Daten erforderlich ist, sowie über deren regelmäßige Empfänger zu führen. Diese Übersicht sollte insbesondere im Hinblick auf die erforderlichen Maßnahmen für die Datensicherung auch die sogenannten internen Dateien umfassen, die ansonsten aus dem Geltungsbereich des Datenschutzgesetzes ausgenommen sind. Nur eine Hochschule hatte eine Erhebung vorgenommen, in der auch diese internen Daten einbezogen sind.

Im Amtsblatt für Berlin und im Landespressedienst sind die Dateien zu veröffentlichen (§ 12 Berliner Datenschutzgesetz). Solche Veröffentlichungen sind zwar von allen Hochschulen vor-

[20] Vgl. etwa das Rundschreiben II Nr. 38/1979 des Senators für Inneres von Berlin, Betr.: Nebentätigkeit der Vertrauensleute von Selbsthilfeeinrichtungen

genommen worden. Ich habe allerdings festgestellt, daß die Hochschulen nicht alle veröffentlichungspflichtigen Dateien aufgenommen haben (z.B. fehlen in der Regel die Karteien der akademischen Auslandsämter); bei den veröffentlichten Dateien wurden bei der Art der Daten Merkmale genannt, die keine hinreichende Transparenz gewährleisten (z. B. „hochschulspezifische Daten").

Die Erhebung personenbezogener Daten von Studenten stützt sich auf zwei Rechtsgrundlagen: Zum einen werden die Daten zur Erfüllung der eigenen Aufgabe der Hochschule (Lehre und Forschung) erhoben, zum anderen schreibt das Hochschulstatistikgesetz die Erhebung einer Reihe von Daten vor, die sich z. T. mit den für eigene Zwecke erhobenen Daten decken. Die Aufklärung über die Rechtsgrundlage (§ 9 Abs. 2 Berliner Datenschutzgesetz) berücksichtigt in keinem Fall diese doppelte Aufgabenstellung. Ich habe darauf hingewiesen, daß es für die Studenten erkennbar sein müsse, welche Daten für welche Aufgaben erhoben werden. Dies ist vor allem deshalb von Bedeutung, weil mangels entsprechender Rechtsvorschrift die Immatrikulation nicht an die Abgabe der ausschließlich statistischen Daten gekoppelt werden darf (§ 36 Abs. 1 Verwaltungsverfahrensgesetz).

Gegenstand z. T. ausführlicher Erörterung waren Datenübermittlungen, die von Hochschulen an andere Stellen vorgenommen werden. Dabei konnte ich feststellen, daß alle Hochschulen Wert auf die Einhaltung der Bestimmungen über Datenübermittlungen legen. Zur Zeit wird noch geprüft, in welchem Umfang Daten zwischen den Studentenwerken und den Hochschulen zum Zweck der Ausbildungsförderung sowie zwischen Ausländerbehörden und Hochschulen ausgetauscht werden dürfen. Das Hauptproblem besteht hierbei darin, den Datenaustausch auf das erforderliche Maß zu beschränken.

Der Veröffentlichung von Studentendaten stehen keine Bedenken entgegen, wenn diese ihre Einwilligung in die Aufnahme entsprechender Adreßlisten gegeben haben.

Auffällige Mängel wurden hinsichtlich der räumlichen Sicherung von Studentendateien festgestellt. Teilweise auf Grund baulicher Gegebenheiten, teilweise aber auch auf Grund mangelhafter finanzieller Ausstattung werden Studentendaten in nicht verschließbaren Schränken, in Räumen zu ebener Erde (bei einfacher Fensterverglasung) oder in Räumen aufbewahrt, zu denen eine Vielzahl von Personen Zutritt haben. Einige Hochschulen sind bereits im wesentlichen meinen Empfehlungen gefolgt. Ich gehe davon aus, daß auch an den übrigen Hochschulen weitere Maßnahmen zur Verbesserung des Datenschutzes ergriffen werden.

In meinem Jahresbericht 1980 hatte ich auf Probleme hingewiesen, die sich mit der Führung von Schülerdaten, insbesondere in den Schülerbogen ergeben. Gegenüber dem Senator für Schulwesen habe ich Ende 1980 eine ausführliche Stellungnahme abgegeben. Daraufhin wurde ein Sonderauftrag mit dem Ziel vergeben, neue Ausführungsvorschriften für den Umgang mit Schülerdaten zu entwickeln. Meine Anregungen sollen dabei weitgehend berücksichtigt werden. Zu einem Rohentwurf konnte ich bereits eine positive Stellungnahme abgeben.

2.5 Sozialwesen

Am 1. Januar 1981 ist das 1. und 2. Kapitel des X. Buches des Sozialgesetzbuches[21] (SGB X) in Kraft getreten. Das in § 35, I. Buch des Sozialgesetzbuches[22] (SGB I) geregelte Sozialgeheimnis umfaßt den Anspruch, daß Einzelangaben über die persönlichen und sachlichen Verhältnisse eines jeden Bürgers von den Leistungsträgern als Sozialgeheimnis gewahrt werden müssen und nicht unbefugt offenbart werden dürfen. Die Offenbarungsbefugnisse sind durch das 2. Kapitel des SGB X in den §§ 67 bis 77 geregelt worden.

Die Datenschutzbeauftragten des Bundes und der Länder hatten schon vor 1980 im Gesetzgebungsverfahren ihre Vorstellungen über die zu schaffenden Normen eingebracht. Nicht alle Anregungen sind vom Gesetzgeber aufgegriffen worden. Gleichwohl markiert die verabschiedete Fassung einen wichtigen Schritt zum Datenschutz. Die Offenbarungstatbestände der §§ 67 ff SGB X ergänzen das in § 35 SGB I mehr deklaratorisch geregelte Persönlichkeitsrecht um Tatbestände, von deren Vorliegen die Zulässigkeit von Eingriffen abhängt. Bemerkenswert ist, daß die neuen Regelungen des Sozialgesetzbuches eindeutig bestimmen, daß sich der Datenschutz nicht nur auf Dateien, sondern auch auf Akten und sonstige Informationssammlungen erstreckt.

Allerdings bereitet die Umsetzung der neuen Regelungen in die Praxis der Sozialbehörden z. T. erhebliche Schwierigkeiten.

So habe ich festgestellt, daß der Anwendungsbereich des § 74 SGB X bei der Geltendmachung von Unterhaltsansprüchen für den Unterhaltsberechtigten durch die Jugendämter der Bezirke[23] mißverstanden worden ist. Die Datenschutzregelungen des SGB X, insbesondere auch des § 74 als Offenbarungstatbestand beziehen sich nur auf die von Sozialbehörden gespeicherten Daten, nicht jedoch auf Daten, die außerhalb von Behörden (z. B. bei Arbeitgebern) gespeichert sind und in einem sachlichen Zusammenhang mit den Offenbarungstatbeständen der §§ 67 ff SGB X stehen. Adressat der Datenschutzregelungen sind nur die Sozialbehörden, nicht aber Arbeitgeber oder andere Stellen und Personen, die in ein Sozialhilfeverfahren einbezogen werden können oder müssen. Mein Hinweis, daß § 74 SGB X keine Mitteilungsrechte oder gar -pflichten des Arbeitgebers begründet, wird von den zuständigen Stellen künftig berücksichtigt.

In mehreren Fällen haben sich ausländische Sozialhilfeempfänger darüber beschwert, daß ihre Namen von Sozialbehörden an die Ausländerpolizei gemeldet wurden. Der Offenbarungskatalog des Sozialgesetzbuches sieht in § 71 Ziff. 2 SGB X als Offenbarungstatbestand nur die in § 10 Abs. 1 Nr. 9 und Abs. 2 Ausländergesetz geregelten Voraussetzungen vor. Danach dürfen den mit der Ausführung des Ausländergesetzes betrauten Behörden die erforderlichen Auskünfte erteilt werden, wenn ein Ausländer die öffentliche Gesundheit und Sittlichkeit gefährdet. Der in § 10 Abs. 1 Nr. 10 Ausländergesetz geregelte Tatbestand des Sozialhilfeempfangs begründet dagegen kein Mitteilungsrecht nach § 71 SGB X. Der damalige SenArbSoz hat auf Grund meiner Anregung die Verwaltungsvorschriften insoweit geändert und die Sozialbehörden auf die neue Rechtslage hingewiesen.

Nach § 27 Abs. 1 Ziff. 5 SGB I gehören die Vormundschafts- und Gerichtshilfe zu den Sozialleistungen, auf die auch die Datenschutzregelungen der §§ 67 ff. SGB X anzuwenden sind. In § 38 Abs. 1 Satz 6 und Abs. 2 Jugendgerichtsgesetz ist die Mitwirkung der Jugendgerichtshilfe während des gesamten Verfahrens einer Jugendstrafsache vorgesehen. Da die Vertreter der Jugendgerichtshilfe erzieherische, soziale und fürsorgerische Gesichtspunkte zur Geltung bringen sollen, sehe ich in dieser Regelung einen Ermächtigungstatbestand, der die Übermittlung der erforderlichen personenbezogenen Daten des Jugendlichen und seines sozialen Umfeldes im Rahmen des Verfahrens zuläßt. Die in Ziff. 20 der Jugendgerichtshilfevorschriften geregelte Übersendung des Berichtes an die dort vorgesehenen Stellen halte ich im Rahmen einer an der Erforderlichkeit orientierten Auslegung für zulässig. Bedenken habe ich aber gegen die in Abs. 2 geregelte Voraussetzung der Übersendung geäußert, die lediglich ein „berechtigtes Interesse" verlangt. Bei den sozialen Diensten ist nicht grundsätzlich von einem berechtigten Interesse auszugehen, sondern dieses muß vielmehr in jedem einzelnen Fall nachweisbar sein.

Öffentliche Aufmerksamkeit erregte das später auch in anderen Bundesländern bekannt gewordene Verfahren bei der Überweisung von Sozialhilfe an die Antragsteller. Die Angabe des Zahlungsgrundes auf den Überweisungsträgern wurde in der Öffentlichkeit und von den Datenschutzbeauftragten kritisiert. Nach meinem Hinweis hat der Senator für Gesundheit, Soziales und Familie angekündigt, daß die Angabe des Zahlungsgrundes auf Überweisungsträgern ersetzt wird. Von anderer Stelle sind dagegen zwar Bedenken erhoben worden, durch eine Bezugnahme auf entsprechende Erläuterungen im Bewilligungsbescheid kann jedoch in den meisten Leistungsbereichen den Erfordernissen

[21] Bundesgesetzblatt I, S. 1469, 2218 vom 18.8.1980

[22] Bundesgesetzblatt I, S. 3015 vom 11.12.1975

[23] nach §§ 1605 ff. BGB

einer bürgerfreundlichen Verwaltungspraxis und des Datenschutzes Rechnung getragen werden. Nur in wenigen Ausnahmefällen (z. B. Zuwendungen ohne Antrag und ohne Bescheid) wird weiterhin die Angabe des Zahlungsgrundes erforderlich sein. Diese Verfahrensweise könnte auch für andere Leistungsbereiche beispielgebend sein, in denen die Bezugnahme auf einen vorweggegangenen Verwaltungsakt möglich ist. Ich bin bestrebt, mit allen beteiligten Stellen eine einheitliche Handhabung herbeizuführen.

Von besonderer Bedeutung ist die Regelung des Offenbarungstatbestandes für Forschung und Planung in § 75 SGB X. Die nach Abs. 2 dieser Vorschrift erforderliche Genehmigung durch die oberste Landesbehörde sollte nicht zu einer Inflationierung von Genehmigungserklärungen ohne Einwilligung der Betroffenen oder sonstiger Beteiligter des Sozialverfahrens führen. Vielmehr sollte regelmäßig zunächst die Unzumutbarkeit, eine Einwilligung Betroffener einzuholen, positiv festgestellt werden, oder es muß geklärt sein, daß der Zweck der Forschung bzw. Planung auf andere Weise nicht zu erreichen ist. Auch sollte sichergestellt sein, daß nur für förderungswürdige Forschungsprojekte Zugang zu den Bürgerdaten gegeben wird. Es muß ausgeschlossen bleiben, daß wissenschaftliche Forschung als Vorwand für eine nicht gerechtfertigte Offenbarung von Sozialdaten dient. Auch Ausbildungszwecke können nicht mit dem Hinweis auf „wissenschaftliche Forschung" eine Offenbarung rechtfertigen. Um eine geregelte Verfahrensweise der obersten Landesbehörden beim Genehmigungsverfahren zu gewährleisten, sollten Richtlinien für Offenbarungsbedingungen aufgestellt werden, wie dies z. B. auch in Hessen geplant ist.

Gerade die Problematik der Datenoffenbarung für die sozialempirische Forschung wird in § 75 SGB X besonders deutlich. Ich sehe in dieser Regelung einen Präzedenzfall für den Umgang mit personenbezogenen Daten in der öffentlichen Verwaltung zu Forschungszwecken gegenüber allen Forschungseinrichtungen, seien sie privater oder öffentlich-rechtlicher Natur. Hier liegt der Gedanke zugrunde, daß eine Datenübermittlung, auch wenn sie zu Forschungszwecken geschieht, ein Eingriff in das Persönlichkeitsrecht Betroffener ist, für dessen Zulässigkeit eine gesetzliche Ermächtigung oder die Einwilligung der Betroffenen vorliegen muß. Angesichts dieser richtungsweisenden Regelung muß auch die Übermittlung personenbezogener Daten zu Forschungszwekken aus anderen Verwaltungsbereichen, in denen § 75 SGB X keine Anwendung finden kann, besonders zurückhaltend gehandhabt werden, sofern nicht entweder eine gesetzliche Ermächtigung oder eine Einwilligung des Betroffenen vorliegt.

Auch zum Recht auf Einsicht in Sozialakten sind mir Beschwerden von Bürgern zugegangen. Es handelt sich um das Akteneinsichtsrecht in Sozialakten durch den Betroffenen selbst. Der allgemeinen Regelung des § 29 Verwaltungsverfahrensgesetz entspricht im Sozialbereich nunmehr § 25 SGB X. Dort ist eine Verpflichtung der Behörde geregelt, den Beteiligten Akteneinsicht zu gewähren, soweit dies zur Geltendmachung oder Verteidigung ihrer rechtlichen Interessen erforderlich ist. Eine mögliche Gesundheitsgefährdung durch die Akteneinsicht kann kein Verweigerungsgrund sein, da nach Abs. 2 in derartigen Fällen lediglich zum gesundheitlichen Schutz des Beteiligten ein Arzt zur Unterstützung bzw. zur Vermittlung des Akteninhaltes zugegen sein soll. Bei der Auslegung dieser Regelung sollte ein Kammergerichtsurteil berücksichtigt werden, nach dem Patienten selbst in psychiatrische Gutachten von Krankenhäusern Akteneinsicht nehmen können.

Erfreulich war es festzustellen, daß der Datenschutz im Bereich der Sozialstatistik dadurch verbessert worden ist, daß die entsprechenden Fragebögen einen direkten Personenbezug nicht mehr enthalten.

2.6 Bildschirmtext

Allgemeines

In Berlin wurde die praktische Erprobung des Bildschirmtextes auf der Grundlage des Bildschirmtexterprobungsgesetzes (BiTEG)[24] fortgesetzt.

Auf Bundes- und Länderebene sind folgende Entwicklungen hervorzuheben:

- das Rundfunkurteil des Bundesverfassungsgerichts[25]
- die Bildung der Enquête-Kommission Neue Medien im Bundestag
- die Ergebnisse der baden-württembergischen Expertenkommission Neue Medien[26]
- das rheinland-pfälzische Landesgesetz über einen Versuch mit Breitbandkabel[27]
- der Beschluß der Bundesregierung[28] zur Einführung des Bildschirmtextes

Die Datenschutzbeauftragten des Bundes und der Länder haben als Ergebnis einer ersten Bestandsaufnahme ihre Zielvorstellungen über notwendige Regeln als „Grundsätze für den Datenschutz bei den Neuen Medien (insbesondere bei Bildschirmtext und Kabelfernsehen)"[29] zusammengefaßt. Sie sollen sicherstellen, daß die anlaufenden Erprobungen und die ihnen zugrundeliegenden Vorschriften den Datenschutz von vornherein mit berücksichtigen und erste Anregungen für die zukünftige Ausgestaltung des Datenschutzes bei den Neuen Medien geben.

Dementsprechend habe ich überprüft, ob der Versuchsbetrieb den datenschutzrechtlichen Anforderungen des BiTEG entspricht. Dabei habe ich auch Regelungsdefizite festgestellt, die bei der endgültigen Normierung beseitigt werden sollten. Auf einige Probleme wird im folgenden eingegangen[30]. Dabei spreche ich auch solche an, die sich durch die Teilnahme Privater ergeben haben. Denn auch insoweit ist das Land Berlin als Veranstalter dafür verantwortlich, daß nicht mit Hilfe von Bildschirmtext schutzwürdige Belange von Teilnehmern und Dritten verletzt werden.

Beispiele für unzulässige Datenübermittlungen

Bei der Durchsicht einiger Angebote war festzustellen, daß zahlreiche Anbieter als *Begrüßungsseite* eine sog. „Antwortseite" gebrauchten, die von der Bildschirmtextzentrale mit Namen und Anschrift des Benutzers versehen wurde und als solche durch eine entsprechende Tasteneingabe des Benutzers an den Anbieter abgesandt werden konnte. Die Übersendung der Seite konnte auch aus Versehen bewirkt werden.

Auf diese Weise konnten Anbieter die Daten des Teilnehmers erhalten, ohne daß dies dem Teilnehmer deutlich wurde. Dies widerspricht dem allgemeinen Prinzip fairer Datenverarbeitung wie es auch in § 4 Abs. 4 BiTEG zum Ausdruck kommt.

Diese Praxis der Gestaltung der Begrüßungsseiten ist durch die Anbieter selbst auf Grund einer Empfehlung des Senators für Kulturelle Angelegenheiten verändert worden. Bei den letzten Kontrollen konnte ich derartige Verstöße gegen § 4 Abs. 4 BiTEG nicht mehr feststellen.

Anläßlich der Neuwahlen in Berlin wurde von einem Berliner Anbieter eine *Wahlumfrage* über Bildschirmtext durchgeführt, an der sich die Bildschirmtextteilnehmer und bis zu zwei weitere wahlberechtigte Angehörige beteiligen konnten. Der Veranstalter der Umfrage hat auf diesem Weg von 714 Berliner Bildschirmtextteilnehmern Daten zum Familienstand und zur politischen Meinung der einzelnen Familienmitglieder erheben können.

Auch gegen diese Aktion habe ich gegenüber dem zuständigen Senator Bedenken aus § 4 Abs. 4 erhoben. Ein vertragsähnliches Verhältnis bestand nicht und konnte auch nicht durch die Übersendung der Antwortseite hergestellt werden, da die Zulässigkeit einer derartigen Übersendung bereits das Bestehen eines

[24] Gesetz über die Erprobung von Bildschirmtext in Berlin - Bildschirmtexterprobungsgesetz (BiTEG) - vom 4. Juni 1980, GVBl. S. 1001 ff.

[25] BVerfG, Urteil vom 16. Juni 1981 (1 BVL 89/78), Neue Juristische Wochenschrift 1981 S. 1774 ff.

[26] Expertenkommission Neue Medien Baden-Württemberg: Abschlußbericht, Stuttgart 1980

[27] GVBl. vom 15. Dezember 1980

[28] vom 24. Juni 1981 (Bulletin, Presse- und Informationsamt der Bundesregierung Nr. 63 / S. 533, vom 27. Juni 1981)

[29] Vgl. Anlage 3

[30] Auf die rechtlichen Probleme bin ich im übrigen im Jahresbericht 1980 auf S. 9 ff., 2.3 eingegangen

vertragsähnlichen Vertrauensverhältnisses voraussetzt. Der in § 4 Abs. 4 enthaltene Schutzgedanke muß besondere Beachtung bei der Abfrage derart höchstpersönlicher Informationen wie der politischen Meinung des Teilnehmers und seiner Familienangehörigen finden.

Für eine endgültige Regelung könnte § 3 Nr. 6 des rheinland-pfälzischen Gesetzes über einen Versuch mit Breitbandkabel Vorbild sein. Dort ist bestimmt:

> „Abstimmungen und Wahlen mittels eines Rückkanals sind unzulässig; dies gilt nicht für die Beurteilung unterhaltender Sendungen und bei Spielen."

Es sollte klargestellt werden, daß hierunter auch Meinungsumfragen fallen.

Ein Verlag hat eine "Bildschirmtext-*Glückwunschaktion*" zur Hochzeit des englischen Thronfolgerpaares veranstaltet.

Personen konnten gegen ein Entgelt ihre Glückwünsche aufgeben, die an das englische Bildschirmtextsystem „Prestel" übermittelt werden sollten. Gegen diese Aktion bestehen insoweit Bedenken, als die Namen der Beteiligten zugleich auf über 50 Seiten im deutschen Bildschirmtext veröffentlicht wurden. Diese Veröffentlichung entspricht nicht den Grundsätzen fairer Datenverarbeitung und begegnet auch nach geltendem Recht Bedenken aus § 4 Abs. 4 BiTEG, da die Einwilligung zur Übermittlung nach England nicht mit der Einwilligung zur Veröffentlichung in Deutschland gleichzusetzen ist.

Verwechselungsgefahr

Die Wahrscheinlichkeit, sich versehentlich seiner Daten zu begeben mit z. T. erheblichen Folgen - wie z. B. der Bestellung von Waren oder Reisen etc. - hat sich in der Erprobungszeit bisher als zu hoch erwiesen. Ich habe daher gefordert, daß der Befehl „absenden" nur durch die Tasten zweier Zahlen möglich sein sollte, um eine Verwechselung mit „nicht absenden" zu vermeiden. Diese Forderung ist seit kurzem in mehreren Fällen bereits realisiert worden.

Bankverkehr

In der Erprobungsphase besteht auch die Möglichkeit, Bankgeschäfte über Bildschirmtext abzuwickeln (sog. home-banking). Gegenwärtig ist dies bereits mit einem Kreditinstitut möglich. Die Sparkasse der Stadt Berlin West hat allerdings auf der Internationalen Funkausstellung 1981 ebenfalls die Einführung eines entsprechenden Verfahrens angekündigt. Für die Zukunft entsteht die Frage, wie der Datenschutz bei diesen Verfahren geregelt werden sollte. Hierbei geht es darum, unbefugte Zugriffe auf die Konten zu verhindern. Dies gilt sowohl für die unbefugte Einsichtnahme in die Konten als auch für die unbefugte Vermögensdisposition. Die Besonderheit dieses Verfahrens liegt vor allem darin, daß die Sicherheit im wesentlichen über Code-Zahlen erreicht wird, die in bestimmten Zeitabständen gewechselt werden. Ich nehme z. Z. an diesem Verfahren teil, um mich über den Sicherheitsstandard zu informieren.

Bei diesem Verfahren stellt sich insbesondere die Frage, ob nicht die mißbräuchliche Verwendung von Code-Zahlen rechtlich besonders geschützt werden muß.

M. E. müssen geprüft werden:

- Ein Verbot aller Akte zur Ermittlung derartiger Codes.
- Ein Verbot der Aufbewahrung, Weitergabe und Verwendung von Codes durch Unbefugte, die Codes - sei es auch durch Zufall - erfahren haben.

Entsprechende Strafrechtsbestimmungen müßten für die endgültigen Bildschirmtextgesetze (ggf. auch für das Strafgesetzbuch) vorbereitet werden, da diese Fälle von geltendem Strafrecht nicht erfaßt werden.

Bei einer Prüfung dieser Fragen muß berücksichtigt werden, daß die Codes Schlüssel darstellen, die den Zugang zu Rechtsgütern gewähren. Sie sind selbst keine eigenständigen Rechtsgüter. Die Notwendigkeit einer Schaffung entsprechender Straftatbestände läßt sich jedoch mit der Annahme begründen, daß die Technisierung und Anonymisierung eine kriminogene Wirkung entfalten, die dahingeht, daß die Bereitschaft zur Straftat wächst und Hemmungsmechanismen abnehmen. Daher sind teilweise vergleichbare Tatbestände, wie die Verletzung von Privatgeheimnissen und der Mißbrauch von Ausweispapieren als Straftaten geregelt (§§ 203, 204, 281 Strafgesetzbuch).

Ergebnis

Die vorstehenden Überlegungen sind ein erstes Ergebnis meiner Beteiligung an der Bildschirmtexterprobung als Anbieter[31] und Teilnehmer wie auch der Kontakte mit den beteiligten Institutionen, u. a. auch einem Informationsbesuch in der Berliner Bildschirmtextzentrale, die gemeinsam mit dem Bundesbeauftragten erfolgte.

Aus ihnen ergibt sich eindeutig, daß vor der Verabschiedung eines endgültigen Bildschirmtextgesetzes insbesondere zu klären ist, welche Daten für den Betrieb erhoben, gespeichert und übermittelt werden sollen.

Ich halte es für erforderlich, daß ein auf Dauer angelegtes Gesetz eindeutiger als das Erprobungsgesetz definiert, in welchem Umfang personenbezogene Daten verarbeitet werden dürfen.

Das entspricht auch dem Auftrag des Gesetzgebers, eine Begleituntersuchung durchzuführen (§ 2 BiTEG). Bedenklich ist, daß sich die Vergabe entsprechender Arbeiten verzögert hat. Darüber hinaus erscheint das Verhältnis zwischen Landes- und Bundesaufgaben nach wie vor klärungsbedürftig, da zwischen dem Wortlaut des BiTEG und dem Beschluß des Bundeskabinetts ein Widerspruch besteht. Denn § 2 Abs. 5 BiTEG sieht im Gegensatz zum Beschluß des Bundeskabinetts vor, daß vor einer Beschlußfassung über die Begleituntersuchung keine Entscheidung über die endgültige Einführung des Bildschirmtextes getroffen werden darf. Es erscheint geboten, beide Fragenkomplexe so schnell wie möglich zu klären.

2.7 Justizverwaltung

Mit Ausnahme der Rechtsprechung, die angesichts ihrer verfassungsmäßig gewährleisteten Unabhängigkeit naturgemäß meiner Kontrolle entzogen ist, überprüfe ich auch die Einhaltung des Datenschutzes in der Justiz. Als speichernde Stellen sind hier insbesondere die Staatsanwaltschaft sowie die Justizvollzugsanstalten zu nennen, aber auch die registerführenden Gerichte.

Staatsanwaltschaft

Die Staatsanwaltschaft beim Landgericht führt zur Erleichterung ihrer Arbeit insbesondere bei parallel laufenden Strafverfahren eine Zentralkartei, die ich überprüft habe. Dabei habe ich festgestellt, daß der Umfang der in der Zentralkartei enthaltenen Daten auf das Mindestmaß beschränkt ist und Auskunft nur im erforderlichen Umfang erteilt wird. Zu der geplanten Automatisierung der Zentralkartei konnte bislang noch keine Stellung genommen werden, da ein verbindliches Konzept noch nicht vorliegt. Im Hinblick auf die bereits vorliegenden Mindestanforderungen bei den zentralen Namenskarteien der Staatsanwaltschaften, die die Konferenz der Datenschutzbeauftragten des Bundes und der Länder beschlossen hat, werde ich die Automation in diesem Bereich aufmerksam beobachten.

Im letzten Jahresbericht habe ich von den Eingaben berichtet, die sich gegen die Berliner Praxis gerichtet haben, die Glaubwürdigkeitsprüfung kindlicher Zeugen durch den Polizeipräsidenten mit Hilfe eines Fragebogens vorzunehmen. Inzwischen ist meine im Jahresbericht abgegebene Empfehlung vom Senator für Justiz aufgegriffen und in einer Anweisung an die Generalstaatsanwaltschaft verwirklicht worden.

[31] In der Zeit vom 1. 9. 1980 bis 31. 8. 1981 wurde das angebotene Programm wie folgt genutzt
- Bestellungen von Jahresberichten, Informationsmaterial über Bildschirmtext über 200 x
- Aufruf des Inhaltsverzeichnisses ca. 1500 x
- Aufruf der Seite Datenschutzrecht ca. 500 x

Angeboten werden z. Z. 45 Seiten

Forschungsprojekt des Max-Planck-Instituts für ausländisches und internationales Strafrecht in Freiburg

Strafgefangene der JVA Tegel haben sich an mich gewandt und geltend gemacht, die Persönlichkeitsrechte der Strafgefangenen würden wegen der Art der Durchführung des Forschungsprojektes verletzt. Insbesondere beschwerten sie sich über die Übermittlung von Daten aus Gefangenenpersonalakten.

Meine Überprüfung hat bisher folgendes ergeben:

Um wissenschaftlich abgesicherte Erkenntnisse über die Wirksamkeit des sozialtherapeutischen Behandlungsvollzuges in der Teilanstalt IV der JVA Tegel zu gewinnen, führt das Max-Planck-Institut seit 1976 ein Forschungsprojekt in der Anstalt durch.

In der derzeit laufenden Projektphase soll ein Vergleich zwischen den Lebensumständen, insbesondere dem strafrechtlichen Werdegang der Insassen der Modell-Teilanstalt IV und der übrigen Teilanstalten vorgenommen werden. Hierzu werden zu verschiedenen Zeitpunkten ausführliche Befragungen der beteiligten Strafgefangenen durchgeführt.

Während in der Teilanstalt IV grundsätzlich alle Gefangenen in die Untersuchung einbezogen und über das Forschungsprojekt informiert werden, wird bei den übrigen Teilanstalten eine Auswahl unter den Gefangenen vorgenommen. Diese Auswahl wird vom Max-Planck-Institut auf Grund einer Reihe von personenbezogenen Daten sämtlicher Strafgefangener vorgenommen, die zuvor an das Max-Planck-Institut übermittelt worden sind. Die übermittelten Daten stellen einen Auszug der Daten dar, die für Verwaltungszwecke in einer Gefangenenkartei geführt werden.

In einem persönlichen Gespräch habe ich dem Senator für Justiz meine Bewertung vorgetragen.

Danach ist die Übermittlung von Daten an das Max-Planck-Institut rechtmäßig, soweit die Einwilligung der Gefangenen vorliegt. Hierzu habe ich empfohlen, die Einwilligungen zu dokumentieren. Nach Mitteilung des Senators für Justiz geschieht dies inzwischen.

Soweit personenbezogene Daten ohne Einwilligung der Gefangenen an das Max-Planck-Institut übermittelt werden, habe ich einen Verstoß gegen die §§ 6 Satz 1, 11 Berliner Datenschutzgesetz festgestellt.

Beim Fehlen eines speziellen Gesetzes läßt das wegen der Art der Aufbereitung der Daten unmittelbar anzuwendende Berliner Datenschutzgesetz eine Übermittlung an nicht-öffentliche Stellen nur zu, wenn zuvor die Einwilligung der Betroffenen eingeholt worden ist.

Die Vorschriften des Strafvollzugsgesetzes machen die Einwilligung nicht entbehrlich.

Gemäß § 166 StVollzG obliegt es zwar dem kriminologischen Dienst, in Zusammenarbeit mit den Einrichtungen der Forschung, den Strafvollzug wissenschaftlich fortzuentwickeln. Hierin vermag ich nur eine Aufgabenzuweisung, jedoch keine Ermächtigungsgrundlage dafür zu sehen, im Rahmen dieser Aufgaben personenbezogene Daten von Häftlingen an private Forschungseinrichtungen zu übermitteln. Weder aus der Entstehungsgeschichte des § 166 StVollzG noch aus dem Zusammenhang mit anderen Regelungen dieses Gesetzes läßt sich eine solche Bedeutung ermitteln.

Der Senator für Justiz geht von einer anderen rechtlichen Bewertung aus, hat jedoch insoweit eine rechtliche Überprüfung dieser Frage zugesagt.

Er bereitet außerdem eine schriftvertragliche Regelung mit dem Max-Planck-Institut vor, die die getroffenen Abreden klarstellen soll.

In einer Sitzung des Rechtsausschusses des Abgeordnetenhauses wurden die Standpunkte vorgetragen. Dabei erklärte der Senator für Justiz, man werde künftig im Interesse aller Beteiligten den datenschutzrechtlichen Bedenken Rechnung tragen und die Einwilligung einholen.

Schuldnerverzeichnis

Eine nicht unbedeutende Rolle im Geschäftsverkehr spielt das sogenannte „Schuldnerverzeichnis", in das nach § 915 Zivilprozeßordnung alle Personen einzutragen sind, die die eidesstattliche Versicherung nach § 807 ZPO (früher Offenbarungseid) abgegeben haben, gegen die zur Erzwingung dieser Versicherung die Haft angeordnet ist oder die die eidesstattliche Versicherung nach § 284 der Abgabenordnung abgegeben haben. Nach § 915 Abs. 3 ZPO ist jedermann auf Antrag Auskunft aus dem Verzeichnis zu erteilen, es kann auch Einsicht gewährt werden.

Insbesondere zur Entlastung der Amtsgerichte werden Abschriften aus dem Verzeichnis gefertigt und Rechtsanwaltskammern, Industrie- und Handelskammern sowie anderen vertrauenswürdigen Körperschaften, Personen oder Unternehmen zur Verfügung gestellt. Die Berufsvertretungen können ihrerseits die Listen ihren Mitgliedern verfügbar machen, wobei sie sich der Hilfe anderer Organisationen (z. B. der Schutzgemeinschaft für allgemeine Kreditauskünfte) bedienen können.

Auf diese Weise werden die Eintragungen einem unabsehbar großen Personenkreis bekannt. Zwar ist vorgeschrieben, daß die Eintragungen nach dem Ablauf bestimmter Fristen zu löschen bzw. die Listen zu vernichten sind, angesichts der Vielzahl der Adressaten ist eine Überprüfung allerdings nicht möglich.

U. a. auf Drängen des Bundesbeauftragten für den Datenschutz hat der Bundesminister der Justiz einen Entwurf für eine Verordnung über Abschriften aus den Schuldnerverzeichnissen vorgelegt, der den datenschutzrechtlichen Belangen der Betroffenen verstärkt entgegenkommt. Ich habe den Senator für Justiz gebeten, den Verordnungsentwurf zu unterstützen, dabei allerdings darauf hingewiesen, daß auch dieser Entwurf noch verbesserungsfähig ist. Wesentlich erscheint mir insbesondere, daß eine listenmäßige Übermittlung der Daten allenfalls an Stellen hinnehmbar ist, die zumindest mittelbar staatlicher Aufsicht unterliegen. Dies trifft einerseits für öffentliche Stellen, andererseits für solche Stellen zu, die nach dem 4. Abschnitt des Bundesdatenschutzgesetzes von der Aufsichtsbehörde für den Datenschutz kontrolliert werden. Nur eine solche Aufsicht gewährleistet die Einhaltung der Beschränkungen, die § 915 ZPO mit der Herstellung von Abschriften aus dem Schuldnerverzeichnis verbindet.

Der Verordnungsentwurf sieht dagegen weiterhin vor, daß die öffentlich-rechtlichen Berufsvertretungen (insbesondere die Industrie- und Handelskammer) ihren Mitgliedern weiterhin listenmäßige Abschriften zur Verfügung stellen können. Demgegenüber habe ich betont, daß eine Weiterleitung von Daten aus dem Schuldnerverzeichnis durch andere Stellen als durch das Vollstreckungsgericht nur nach einer Abwägung der Erforderlichkeit im Einzelfall erfolgen sollte. Dies schließt auch die Weiterleitung von Listen durch die Industrie- und Handelskammer an ihre Mitglieder aus. Die Industrie- und Handelskammer hat meinem Standpunkt widersprochen und darüber hinaus für wünschenswert gehalten, daß die Praxis, das Schuldnerverzeichnis durch private Dritte zu veröffentlichen und Dritten zuzuleiten, beibehalten wird. Der Senator für Justiz hat sich nicht bereitgefunden, meine Anregungen zu unterstützen, sondern sich den Bedenken der Industrie- und Handelskammer angeschlossen. Demgegenüber halte ich an meiner Stellungnahme fest. In meiner Auffassung fühle ich mich durch eine in diesem Jahr ergangene Entscheidung des Schweizerischen Bundesgerichtes bestätigt, das unter dem Hinweis auf einen unzulässigen Eingriff in die persönliche Freiheit des Schuldners einer Veröffentlichung des Namens eines Schuldners für verfassungswidrig erklärte, bei dem ein erfolgloser Pfändungsversuch unternommen worden war.

Auch die Führung des Schuldnerverzeichnisses bei den Amtsgerichten selbst ist nicht unproblematisch. Der Umstand, daß bei vielen Eintragungen hinreichend identifizierende Daten der Schuldner, insbesondere das Geburtsdatum, nicht bekannt sind, führt dazu, daß eine hohe Verwechselungsgefahr besteht. Dies insbesondere deswegen, weil angesichts der großen Wohnungsmobilität säumiger Schuldner die Wohnung nicht als verläßliches Identifizierungsmerkmal verwendet werden kann.

So kann es leicht zu Verwechselungen kommen, die für den Betroffenen durchaus erhebliche wirtschaftliche Auswirkungen haben können. So vermutete ein Petent, daß ihm ein Makler eine

Wohnung deshalb nicht vermittelt habe, weil er vom Schuldnerverzeichnis eine ungünstige Auskunft über eine andere Person gleichen Namens erhalten habe.

Auch meine Empfehlungen, nach Möglichkeit das Geburtsdatum in das Schuldnerverzeichnis aufzunehmen und die Auskunft nur dann zu erteilen, wenn der Betroffene hinreichend identifiziert ist, stieß auf Widerstand bei der Justizverwaltung, die auf den damit verbundenen hohen Arbeitsaufwand hinwies.

Ich habe den Bundesbeauftragten für den Datenschutz hierauf aufmerksam gemacht und ihn gebeten, auch dieses Problem in die Diskussion um die Reform des Schuldnerverzeichnisses einzubringen.

2.8 Wirtschaft und Verkehr

Gewerberegister

Die Sammlung der Anmeldungen nach § 14 Gewerbeordnung (Gewerberegister) wurde über ihren unmittelbaren Zweck als Hilfsmittel für die Gewerbeaufsichtsbehörde als Informationsquelle für Gläubiger genutzt, die zur Durchsetzung ihrer Forderungen präzise Angaben über ihre Schuldner benötigen. Dies ist vor allem für solche Schuldner von Bedeutung, die nur ein Kleingewerbe betreiben und nicht zum Handelsregister meldepflichtig sind.

Entgegen der Bedeutung, die demnach dem Gewerberegister im Wirtschaftsleben zukommt, sieht die Gewerbeordnung die Auskunftserteilung nicht ausdrücklich vor. Dies hat zur Folge, daß die die Auskunft regelnden Verwaltungsvorschriften[32], die im Prinzip bundesweit gelten, hinter den datenschutzrechtlichen Vorschriften zurücktreten. Da § 11 Berliner Datenschutzgesetz die Übermittlung personenbezogener Daten an nicht-öffentliche Stellen an die Einwilligung der Betroffenen bindet, ist eine Auskunft nur noch in den Fällen möglich, in denen die Einwilligung vorliegt (eine entsprechende Erklärung kann nunmehr bei der Anmeldung eines Gewerbes angegeben werden) oder wenn in anderweitigen Vorschriften den Daten Publizität zukommt (z. B. auf Grund handelsrechtlicher Vorschriften).

Obwohl für eine Reihe von Fällen unter Einbeziehung der Melderegisterauskunft nach § 17 a Meldegesetz eine befriedigende Regelung gefunden werden konnte, bleiben doch Fälle übrig, in denen diese Rechtslage zu Erschwernissen für den Gläubiger führt. Dies ist insbesondere der Fall bei Gewerbebetrieben, die sogenannte „Etablissement-Bezeichnungen" verwenden, d. h. bei denen in der Geschäftsbezeichnung der Name des Inhabers nicht zum Ausdruck kommt (z.B. Gaststätten, Boutiquen).

Da sich wegen der insoweit fehlenden Rechtsgrundlage die Gewerbeämter weigerten, Auskünfte zu erteilen, wandten sich eine Reihe von Anwälten mit der Bitte um Aufklärung an mich. In diesen Fällen habe ich auf die Rechtslage hingewiesen, insbesondere auch darauf, daß es der Bundesgesetzgeber ausdrücklich abgelehnt hat, anläßlich der letzten Novellierung des Gewerberechts entsprechende Bestimmungen zu erlassen.

Ich räumte ein, daß diese rechtliche Situation im Hinblick auf die Verfolgung rechtlicher Interessen zu unbefriedigenden Ergebnissen führen kann. Andererseits sei es aber auch nicht Aufgabe der Gewerbeämter, die Verfolgung privater Rechtsinteressen zu ermöglichen. Hierfür stünden nicht zuletzt privatwirtschaftliche Organisationen wie Auskunfteien und Detekteien zur Verfügung.

Sollte die Wirtschaft, statt sich der genannten Instrumente zu bedienen, staatliche Tätigkeit fordern, wäre anzustreben, daß sich der Gesetzgeber erneut der Materie annimmt und eine eindeutige spezialgesetzliche Regelung über Voraussetzungen und Verfahren bei Auskünften bei den Gewerbeanmeldungen schafft.

Datei der Taxifahreranmeldungen

Durch die Eingabe eines Taxiunternehmers bin ich darauf aufmerksam gemacht worden, daß der Polizeipräsident von Taxiunternehmern die Übermittlung personenbezogener Daten der beschäftigten Fahrer verlangt und diese in einer Datei speichert. Die Überprüfung hat ergeben, daß diese Datei nicht der Übermittlung an dritte Stellen dient und damit als interne Datei im Sinne des § 3 Abs. 3 Berliner Datenschutzgesetz zu betrachten ist.

Im Hinblick darauf, daß die Führung auch solcher Dateien dem Verfassungsgrundsatz der Verhältnismäßigkeit entsprechen muß, habe ich gegenüber dem die Fachaufsicht führenden Senator für Wirtschaft und Verkehr darauf hingewiesen, daß eine Rechtsgrundlage für die Erhebung der Daten und damit auch für die Speicherung der Daten fehlt. Gemäß § 16 Personenbeförderungsgesetz können zwar mit der Genehmigung eines Taxiunternehmens Auflagen verbunden werden. Diese Auflagen sind jedoch nur im Rahmen des Gesetzes zulässig, d. h. die Auflage muß im Zusammenhang mit einer im Personenbeförderungsgesetz genannten Verpflichtung stehen. Hier kommt allenfalls § 54 Abs. 2 i.V.m. § 21 Personenbeförderungsgesetz in Betracht, der nur die Überprüfung im Einzelfall, jedoch nicht die umfassende Vorratshaltung von Daten gestattet.

Ich habe angeregt, zu überprüfen, ob nicht auf diese besondere Form der Fahreranmeldungen verzichtet werden kann und empfohlen, gegebenenfalls eine ausdrückliche Regelung zu erwägen. Der Senator für Wirtschaft und Verkehr ist zwar meiner Auffassung nicht beigetreten, will jedoch nach Möglichkeit meiner Anregung auf ausdrückliche Normierung folgen und eine zweifelsfreie rechtliche Grundlage - etwa im Rahmen der 5. Novelle zum Personenbeförderungsgesetz - fördern.

3. Organisatorische und technische Maßnahmen

3.1 Grundsätzliche Fragen

Verhältnis der speichernden Stelle zum Rechenzentrum

Die bisher in der Verwaltung herrschende Form zentraler Datenverarbeitung ist dadurch gekennzeichnet, daß bei den Fachverwaltungen das Gefühl der Verantwortung für die Daten insoweit zurückgegangen ist, als die Verarbeitung an andere Stellen abgegeben worden ist. Meine Überprüfungen haben gezeigt, daß die nachteiligen Auswirkungen dieses Trends trotz der gesetzlichen Regelung noch nicht vollständig überwunden sind. Ich habe immer wieder Verwaltungen angetroffen, die trotz ihrer fachlichen Zuständigkeit nicht über die Art und Weise des Umgangs mit ihren Daten in den Rechenzentren hinreichend unterrichtet waren und damit ihrer Aufgabe als voll verantwortlicher speichernder Stelle nicht genügten. Im Interesse einer Klarstellung der Verantwortung wird es darauf ankommen, daß die Fachverwaltungen sich in Erinnerung rufen, daß sie für den Umgang mit ihren Daten voll verantwortlich bleiben auch soweit sie sich zur Erfüllung ihrer Aufgaben zentraler Einrichtungen bedienen. Die Rechenzentren sind insoweit nur Verrichtungshilfen, ebenso kleinere Rechenstellen, in denen im Auftrag Daten verarbeitet werden.

Diese Auffassung von der Verantwortung der Fachverwaltung führt dazu, daß das Landesamt für Elektronische Datenverarbeitung, soweit es Aufgaben für Fachverwaltungen wahrnimmt, nicht speichernde Stelle im datenschutzrechtlichen Sinne ist. Die fachliche Verantwortung verbleibt auch in diesem Fall bei der Fachverwaltung. Daneben sind die Rechenzentren verpflichtet, die technischen und organisatorischen Maßnahmen zu treffen, die für den Datenschutz erforderlich sind.

Rechner außerhalb der Rechenzentren

Bei den Prüfungen hat sich ergeben, daß der zunehmende Trend zur Dezentralisierung der Datenverarbeitung - insbesondere des Zugangs zu ihr - es erforderlich macht, neben den Rechenzentren selbst auch die verstreuten Benutzerschnittstellen einschließlich der über Direktzugriff verbundenen Abfragestationen zu kontrollieren. Die Rückverlagerung der Datenverarbeitung an den Arbeitsplatz des Sachbearbeiters sowie die Kopplung von Rechnern zu Rechnernetzen über Datenfernübertragungsmedien sind die prägenden Tendenzen bei der Entwicklung von neuen Anwendungsformen.

[32] Ausführungsvorschriften zu den §§ 14, 15 und 55 c der Gewerbeordnung sowie zu Gewerbeanzeigen - Verordnung vom 24. Oktober 1980, Amtsblatt S. 1905, Dienstblatt I Nr. 17

Darüber hinaus nimmt die Zahl solcher Rechenstellen zu, die isoliert sind und ohne Einbindung in eine arbeitsteilige Rechenzentrumsorganisation sowie ohne Datenfernverarbeitungsverbindung mit anderen Rechenstellen betrieben werden. Solche Anlagen werden meist für die Datenerfassung, für die Textverarbeitung oder für andere Aufgaben, für die großer organisatorischer Aufwand nicht angemessen ist, verwendet.

Ich halte es für geboten, für solche sogenannten „Stand-Alone-Rechner" Mindestanforderungen zu definieren, um die Beachtung der Datenschutzvorschriften auch in diesem ständig wachsenden Bereich sicherzustellen. Entsprechende Hinweise, die auch die Verhältnismäßigkeit zwischen Umfang der Maßnahmen und Kosten der Verfahren berücksichtigen, werden gegenwärtig von mir vorbereitet. Dazu gehört - wie aus gegebenem Anlaß auszuführen ist - auch die Forderung, daß öffentliche Stellen, die personenbezogene Daten auf isolierten Kleinrechnern verarbeiten und die erforderlichen Programme bei Software-Firmen erstehen, soweit über die Verfahren informiert sind, daß sie ihrer Verantwortung als speichernder Stelle vollauf genügen können.

Verhältnis zwischen Herstellerfirmen und öffentlichen Stellen

Das Zusammenwirken von öffentlichen Stellen und Herstellerfirmen für ADV-Hard- und Software war in zwei Fällen Gegenstand datenschutzbezogener Erörterungen.

Während der *Installation* eines umfangreichen ADV-Verfahrens in einem Krankenhaus sollte im Hause der Herstellerfirma auf einer identischen Anlage die *Einarbeitung* der Datenerfasser durchgeführt werden. Um Zeit zu sparen und um die praktische Inbetriebnahme des Systems im Krankenhaus zu einem vorgegebenen Zeitpunkt gewährleisten zu können, sollte bei der Schulung gleichzeitig die Ersterfassung echter Datensätze erfolgen. Ich habe eine Modifizierung dieses Vorgehens gefordert, da der geplante Ablauf das unnötig hohe Risiko beinhaltet hätte, daß Mitarbeiter der Herstellerfirma von Daten Kenntnis nehmen würden, die der ärztlichen Schweigepflicht unterliegen. Eine Vereinbarung zwischen Krankenhaus und Hersteller für diese Übergangsphase soll regeln, daß zunächst eine gründliche Schulung des Erfassungspersonals an Testdaten erfolgt, und daß eine Echtdatenerfassung danach ohne eine Unterstützung des Herstellerpersonals erfolgt, die über das hinausgeht, was bei der Wartung eines ausgereiften Verfahrens unvermeidbar ist.

Beim Landesamt für Elektronische Datenverarbeitung ist die von einem Hersteller angebotene Möglichkeit der *Fernwartung* über Datenfernübertragung eingeführt worden. Dabei handelt es sich um Datenverarbeitung, die von der Herstellerfirma im Auftrag des LED erfolgt, so daß das LED als Auftraggeber für Datenschutz und Datensicherung verantwortlich ist. Bei der Fernwartung bedarf es der hohen Aufmerksamkeit des Auftraggebers, um sicherzustellen, daß nicht personenbezogene und andere zu schützende Daten sowie Programme unkontrolliert zu externen Stellen - auch in das Ausland - übertragen werden. Der Hersteller hat bei diesem Verfahren die Aspekte der Datensicherung berücksichtigt, ohne daß letzten Endes alle Unwägbarkeiten ausgeschlossen werden konnten. Das LED hat für die Durchführung der Fernwartung eine Arbeitsanweisung erarbeitet, die nach meiner Auffassung vorbildlich ist, da sie die Möglichkeiten der Fernwartung soweit nutzt, wie für die Sicherheit der Daten kein Risiko besteht und damit Risikofaktoren ausschließt. Die Arbeitsanweisung enthält das Verbot der Software-Fernwartung, da dabei zuverlässige technische Datensicherungsmaßnahmen auf Grund des technischen Prinzips nicht möglich sind und gebietet die Löschung oder physische Abkoppelung aller angeschlossenen Datenträger mit zu schützenden Inhalten vor jeder Hardware-Fernwartung.

Nach weiteren praktischen Erfahrungen mit dieser Regelung erwäge ich, in Kontakt mit dem LED Grundsätze für die Durchführung von Fernwartung zu gewinnen, da diese Dienstleistung der Hersteller mit dem Ausbau der Datenfernübertragungsmedien eine immer größere Verbreitung finden wird.

3.2 Stellungnahme zu Datenverarbeitungsverfahren

Aus technischer Sicht wurde in diesem Jahr zu verschiedenen Verfahren Stellung genommen.

Soweit es sich dabei nicht um Stellungnahmen handelte, die sich aus konkretem Anlaß auf technische oder organisatorische Detailvorschläge konzentrierten, betrafen sie Verfahren, die fertig geplant waren und zur Realisierung anstanden.

Die vorgesehene Einführung der Pilotanwendung der *Einheitlichen Patientendatenverwaltung (EPDV)* im Humboldt-Krankenhaus und der *Online-Verbundkatalogisierung* für die Berliner Bibliotheken habe ich anhand der vorgelegten Hauptuntersuchungsberichte prüfen können. Ich habe dabei vorsorglich auf Lücken oder Ungenauigkeiten hinsichtlich der technisch-organisatorischen Maßnahmen hingewiesen, soweit sie den Planungsunterlagen entnommen werden konnten.

Die ADV-Unterstützung des *Vollzugs* nach dem *Bundesausbildungsförderungsgesetz* (BAföG) ist ein Beispiel für ein Verfahren, in dem sensitive Daten dezentral bei den Bezirksämtern (Ämter für Ausbildungsförderung) erfaßt und zentral im Landesamt für Elektronische Datenverarbeitung verarbeitet werden. Ich habe in einer Stellungnahme zu einer geplanten Neufassung der Bearbeitungsrichtlinien auf die Verantwortung der Ämter für Ausbildungsförderung als speichernde Stelle besonders hingewiesen. Es entspricht ordnungsgemäßer Datenverarbeitung, wenn der Umgang mit sensitiven Daten und ihren Datenträgern im Detail mit dem LED geregelt ist. Gleichzeitig habe ich gefordert, daß im Zuge des Datenträgeraustausches nur gelöschte Datenträger vom LED an die Bezirksämter zurückgesandt werden.

Beim Rechnerverbund der Berliner Hochschulen erfolgt eine *projektbezogene* Auswertung von Protokollen über die Verwendung von Betriebsmitteln und es wird außerdem die Möglichkeit gegeben, die aktuellen Aktivitäten eines Benutzers an jedem Bildschirm projektbezogen darzustellen. Weil ein großer Teil der Projekte von einer Einzelperson durchgeführt wird, sind diese Daten gleichzeitig personenbezogene Daten. Da eine Unterbindung dieser Verfahren wegen des relativ freien Datenflusses in einem Hochschulrechenzentrum nicht sachgerecht war, habe ich darum gebeten, die Einwilligung der Benutzer zu diesen Verfahren in geeigneter Form einzuholen. An der Technischen Universität ist eine entsprechende Änderung der Benutzerordnung in Vorbereitung.

Von der Verwaltung der Freien Universität bin ich gebeten worden, zur dort praktizierten Erfassung von Daten über *Ferngespräche* von Dienstanschlüssen Stellung zu nehmen. Ich habe hinsichtlich der Erfassung der angewählten Rufnummer bei Privatgesprächen Bedenken geäußert und empfohlen, die technischen Voraussetzungen zu schaffen, um die ordnungsgemäße Abrechnung auch ohne Speicherung der Zielnummer sicherzustellen. Die Freie Universität hat zugesagt, entsprechend meinen Empfehlungen zu verfahren.

Meine Empfehlungen zur technisch-organisatorischen Umgestaltung der *Einwohnerdatenbank* wurden an anderer Stelle dieses Berichtes (Abschnitt 2.2 - Meldewesen) behandelt.

Grundsätzlich ist festzuhalten, daß ich mit meinen Stellungnahmen zu geplanten Verfahren in keinem Falle dem zweifellos verständlichen Wunsch entsprechen kann, bereits im Vorfeld der Verfahrensrealisierung ein verbindliches, zustimmendes Votum des Datenschutzbeauftragten zu erhalten. Ich halte es jedoch für sehr begrüßenswert, wenn ich frühzeitig in die Planung von ADV-Verfahren einbezogen werde, da ich dann rechtzeitig Mängeln vorbeugen kann, die nach der Realisierung nur mühsam korrigierbar sind.

3.3 Aktenvernichtung und Vernichtung von Computerausdrucken

In einigen Fällen bin ich um Stellungnahme zur Vernichtung von Akten und Computerausdrucken gebeten worden.

Im Zusammenhang mit dem Volksbegehren war sicherzustellen, daß nach der Prüfung der Unterschriftslisten diese auch vernichtet wurden. Dieses ist geschehen, wenn auch von den einzelnen Bezirksämtern in verschiedener Weise dabei vorgegangen wurde.

Die Vernichtung von Datenträgern bei der Müllverbrennungsanlage Ruhleben war Gegenstand eines Informationsbesuches bei dieser Anlage. Ich stellte dabei fest, daß eine Vernichtung der

Datenträger nur dann ordnungsgemäß durchgeführt wird, wenn die Verwaltungen das zu vernichtende Material selbst anliefern und durch eigenes Aufsichtspersonal sicherstellen, daß das Material in den Aufgabetrichter eingegeben wird. Erfolgt dies nicht, kann nicht sichergestellt werden, daß das Material tatsächlich sofort und ohne die Möglichkeit Dritter, gewollt oder ungewollt Kenntnis zu nehmen, vernichtet wird.

Das Landesverwaltungsamt trat mit der Bitte an mich heran, bei der Beschaffung einer Aktenvernichtungsanlage für große Mengen von Computerausdrucken zu der erforderlichen Schnittbreite Stellung zu nehmen. Anlagen mit größerer Schnittbreite sind bei gleicher Anforderung an den Durchsatz kostengünstiger. Bei der Vorführung einer Anlage konnte ich mich davon überzeugen, daß eine Schnittbreite von 8 mm nicht ausreicht, um eine den Anforderungen des Datenschutzes genügende Vernichtung zu gewährleisten. Ich betrachte derartiges Material auch dann nicht als vernichtet, wenn es mit den an diese Zerschneideanlagen angeschlossenen Pressen gepreßt wurde. Die Mindestanforderung für die Vernichtung von Computerausdrucken, die personenbezogene Daten enthalten, welche nicht einem besonderen Geheimschutz unterliegen, ist eine Schnittbreite von höchstens 4 mm.

4. Information über die Datenverarbeitung in der Berliner Verwaltung

4.1 Dateienregister

Das im Berliner Datenschutzgesetz (§ 22) vorgesehene Dateienregister soll die automatische Datenverarbeitung in der Berliner Verwaltung vor allem für den Bürger überschaubar machen. Die für den Aufbau des Registers beim Berliner Datenschutzbeauftragten erforderliche Rechtsverordnung ist im Frühjahr 1981 in Kraft getreten[33]. Ich halte die Regelung für beispielhaft.

Dem „allgemeinen" Dateienregister kann jeder Bürger entnehmen, wo möglicherweise Daten über ihn gespeichert sind (Art der Daten, Stellen an die übermittelt wird). Nicht gespeichert ist, ob gerade seine Daten in den einzelnen Dateien geführt werden. Dies kann der Bürger erfahren, indem er eine Auskunft bei der betreffenden Stelle einholt. Jeder Bürger kann als Orientierungshilfe in das allgemeine Register und in die bei mir geführte Registerübersicht einsehen.

Soweit öffentliche Stellen von der Meldepflicht zum allgemeinen Dateienregister ausgenommen sind, haben sie, mit der Ausnahme des Landesamtes für den Verfassungsschutz, zum „besonderen" Dateienregister zu melden, welches bei mir unter Verschluß geführt wird. Hier hat der Bürger selbst zwar kein Einsichtsrecht, die Meldungen sind aber ein wichtiges Hilfsmittel bei meinen Kontrollen.

Bei einer Novellierung des Berliner Datenschutzgesetzes sollte nach meinen Erfahrungen auch § 22 Berliner Datenschutzgesetz überdacht werden. Es wäre zu prüfen, wie weit es tatsächlich sinnvoll ist, öffentliche Stellen, die in einem tatsächlichen oder nur vermuteten Wettbewerbsverhältnis mit privaten Organisationen stehen (z.B. Krankenhäuser oder Eigenbetriebe), von der Meldepflicht zum allgemeinen Dateienregister auszunehmen.

Bisher sind ca. 400 Dateien zu den Registern gemeldet. Ich gehe davon aus, daß die Stellen, die ihre Dateien noch nicht gemeldet haben, die Meldung alsbald nachholen.

4.2 Information des Datenschutzbeauftragten durch die Verwaltung

Die Verwirklichung des Datenschutzes wird durch eine frühzeitige Information über wesentliche Vorhaben erleichtert. Die Informationspflichten sind noch einmal in einem Rundschreiben des Senators für Inneres zusammengefaßt[34].

Auf Grund der bisherigen Erfahrungen möchte ich den Passus des Rundschreibens hervorheben, der vorsieht, daß ich Gelegenheit erhalte, zu Entwürfen von Rechts- und Verwaltungsvorschriften, die eine automatische oder manuelle Verarbeitung personenbezogener Daten zum Gegenstand haben, Stellung zu nehmen. In Einzelfällen ist dieser Punkt bisher nicht beachtet worden. Ich gehe jedoch davon aus, daß es sich hierbei um Anlaufschwierigkeiten handelt, so daß meine rechtzeitige Beteiligung in Zukunft sichergestellt wird.

5. Zusammenarbeit mit anderen Stellen

5.1 Beauftragte des Bundes und der Länder

Die Konferenz der Datenschutzbeauftragten, zu der sich die Datenschutzbeauftragten des Bundes und der Länder zusammengeschlossen haben, hat in drei Sitzungen in Berlin unter meinem Vorsitz beraten.

Die wichtigsten Ergebnisse dieser Konferenzen lassen sich in folgender Weise zusammenfassen:

7. Konferenz am 11. Dezember 1980

- Beschluß über die „Grundsätze für den Datenschutz bei den Neuen Medien" (insbesondere bei Bildschirmtext und Kabelfernsehen) (vgl. oben 2.6 und Anlage 3)
- Feststellung, daß die Technischen Prüfstellen für den Kraftfahrzeugverkehr öffentliche Stellen im Sinne der Datenschutzgesetze sind und der Kontrolle der Datenschutzbeauftragten unterliegen

8. Konferenz am 2. April 1981

- Stellungnahme zum „Formulierungsvorschlag für ein Landesmeldegesetz" (vgl. oben 2.2)
- Stellungnahme zu Fragen der Auslegung des SGB X (vgl. oben 2.5)

9. Konferenz am 28./29. September 1981

- Beschluß der „Mindestanforderungen für den Datenschutz bei den Zentralen Namenskarteien der Staatsanwaltschaften" (vgl. oben 2.7)
- Stellungnahme zum „Datensatz für das Meldewesen" (vgl. oben 2.2)
- Stellungnahme zum „Sozialbericht - psychosoziale Grunddaten -"
- Stellungnahme zum Erhebungsverfahren bei der „Sozialhilfestatistik - Empfängernachweis" (vgl. oben 2.5)

Nach einer letzten Sitzung im Dezember 1981 wird der Vorsitz mit dem Jahreswechsel auf Baden-Württemberg übergehen.

5.2 Aufsichtsbehörde für nicht-öffentliche Stellen und sonstige Stellen

In den turnusmäßigen Sitzungen mit dem Senator für Inneres als Aufsichtsbehörde für den Datenschutz wurden zahlreiche Grundsatz- und Einzelfragen behandelt (u.a. Auslegungsprobleme, die sich aus dem Sozialgesetzbuch X Kapitel 1 und 2 ergeben; datenschutzrechtliche Behandlung nicht-öffentlicher Stellen, die Aufgaben der öffentlichen Verwaltung wahrnehmen, insbesondere Datenübermittlung an diese Stellen; datenschutzrechtliche Beurteilung der automatischen Telefondatenerfassung; Datenschutzfragen im Krankenhaus).

Schließlich habe ich Kontaktgespräche mit den Datenschutzbeauftragten der Religionsgemeinschaften geführt, in denen vor allem Fragen der Übermittlung von Daten zwischen dem öffentlichen Bereich und den Religionsgemeinschaften erörtert worden sind.

6. Ausblick

6.1 Voraussichtliche Schwerpunkte der künftigen Arbeit des Berliner Datenschutzbeauftragten

Auf Grund der bisherigen Erfahrungen ergeben sich die Schwerpunkte für meine künftige Arbeit in folgender Reihenfolge:

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

Damit soll vor allem auch die zunehmende Diskrepanz zwischen Bürger und Verwaltung, die zweifellos durch die

[33] Berliner Datenschutzregisterordnung vom 16.2.1981 (GVBl. vom 12.3.1981)

[34] Dienstblatt des Senats Teil I S. 30 vgl. Jahresbericht 1980 3.2, S. 15

Technisierung gefördert worden ist, verringert werden. Die Unterrichtung der Bürger und der Verwaltung über Datenschutzrechte und -pflichten wird fortgesetzt.

b) Weiter sind folgende Schwerpunkte absehbar:
- Überprüfung von Rechenzentren und Rechenstellen
- Überprüfungen im Bereich Bau- und Wohnungswesen
- Neue Medien
  - Begleitung des Bildschirmtextversuchs
  - Stellungnahme zum Datenschutz bei der Kabelkommunikation
- Überprüfungen im Bereich Öffentliche Sicherheit und Strafverfolgung

6.2 Absehbare Entwicklungen

Novellierung des Bundesdatenschutzgesetzes

Für diese Legislaturperiode ist eine Novellierung des Bundesdatenschutzgesetzes vorgesehen. Dabei ist davon auszugehen, daß inhaltlich an die Vorschläge angeknüpft wird, die alle drei Bundestagsparteien bereits gegen Ende der letzten Legislaturperiode vorgelegt haben. Zwischenzeitlich sind zwei sehr interessante Stellungnahmen zur Frage der Novellierung abgegeben worden:

Einmal eine umfassende Ausarbeitung des Bundesbeauftragten für den Datenschutz, Professor Bull[35], und zum anderen ein Bericht der Bayerischen Staatsregierung über die Erfahrung mit dem Bayerischen Datenschutzgesetz und dem Bundesdatenschutzgesetz[36].

Bei der Neugestaltung der Gesetze werden neben den Erfahrungen, die die Datenschutzbeauftragten des Bundes und der Länder wie die Aufsichtsbehörden für den Datenschutz inzwischen gewonnen haben, auch die zunehmend anfallenden Erkenntnisse der Rechtsprechung einzubeziehen sein.

So wird zu erwägen sein, ob nicht angesichts der formalen Auslegung des Pressebegriffs durch die Rechtsprechung (die in Berlin etwa der Notgemeinschaft für die Freie Universität im Hinblick auf die Veröffentlichung von Personen, die sich in den vergangenen Jahren an Universitätswahlen beteiligt hatten, die Stellung eines Presseunternehmens einräumte)[37] eine auch für den öffentlichen Bereich relevante Klarstellung dahingehend erfolgen sollte, daß nicht die Herstellung eines beliebigen Druckerzeugnisses die Datenschutzrechte außer Kraft setzt. Aufgegriffen werden sollte die Rechtsprechung des Kammergerichts zu Fragen des Einsichtsrechts in (hier psychiatrische) Krankenunterlagen, in der auch dem kranken Menschen umfassende Informationsrechte eingeräumt werden[38]. Die aufsehenerregende Entscheidung des Bundesgerichtshofs, in der dem Betroffenen kein Anspruch auf Auskunft über die Personen eingeräumt wird, an die Daten weitergegeben wurden[39], gilt jedenfalls nicht für den öffentlichen Bereich in Berlin. Denn insoweit enthält das Berliner Datenschutzgesetz eine datenschutzfreundlichere Regelung.

Interessante Anregungen können auch aus den in der Zwischenzeit in Kraft getretenen Regelungen im Ausland und bei zwischenstaatlichen Einrichtungen gezogen werden.

So hat der Schweizerische Bundesrat zur Vorbereitung eines entsprechenden Bundesgesetzes „Richtlinien für die Bearbeitung von Personendaten in der Bundesverwaltung" erlassen Sie erscheinen mir sowohl vom Verfahren (Erlaß vorläufiger Richtlinien zur Erprobung und Förderung einer künftigen gesetzlichen Regelung) als auch vom Inhalt her beachtenswert.

Insbesondere wurde hier eine interessante Lösung für das Spannungsverhältnis zwischen dem Erfordernis der Einwilligung zur Rechtmäßigkeit von Datenübermittlungen und einer auf Grund Gesetzes zulässigen Datenübermittlung ohne Einwilligung gefunden: Danach braucht die zunächst erforderliche Einwilligung dann nicht eingeholt werden, wenn die Zustimmung nach den Umständen vorausgesetzt werden kann oder wenn erwiesen ist, daß die betroffene Person die Zustimmung nur verweigert, um sich einer gesetzlichen Verpflichtung zu entziehen. Die Lösung ermöglicht es, in Fällen, bei denen der Aufwand für die Einholung einer Einwilligung in keinem Verhältnis zum Ausmaß der zu befürchtenden Beeinträchtigung steht, die Datenübermittlung nur im Falle des Widerspruchs des Betroffenen für unzulässig zu erklären. Ebenso verhindert sie, daß unter dem Schutzmantel des Datenschutzes die Verfolgung anerkennenswerter rechtlicher Interessen erschwert oder verhindert wird.

Derartige Versuche, ein gesetzliches Ventil für bestimmte Datenübermittlungen zu schaffen, begegnen andererseits Bedenken, daß dadurch in größerem Umfange Datenschutzbestimmungen umgangen werden können.

Vor einer endgültigen Bewertung dieser oder verwandter Lösungen sollte die Entscheidung dieser Frage durch den Bundesgesetzgeber im Rahmen der geplanten Novellierung des Bundesdatenschutzgesetzes abgewartet werden.

Berlin, den 28. Dezember 1981

Der Berliner Datenschutzbeauftragte

Dr. Kerkau

---

[35] Zur Novellierung des Bundesdatenschutzgesetzes, gedruckt unter dem Titel: Ziele und Mittel des Datenschutzes, Forderungen zur Novellierung des Bundesdatenschutzgesetzes (Königstein: Athenäum 1981)

[36] Dem Bayerischen Landtag auf Grund des Beschlusses vom 30. Januar 1980 (Drucksache 9/3863) mit Schreiben vom 12. Juni 1981 erstattet

[37] Urteil des Landgerichts Berlin vom 18.12.1980 - 27 O 435/80

[38] Urteil des Kammergerichts vom 1.6.1981 - 20 K 96/81

[39] Urteil des Bundesgerichtshofs vom 19.5.1981 - VI ZR 273/79

Anlage 1

Kriterien für die datenschutzrechtliche Beurteilung der Erhebung, Speicherung und Übermittlung psychiatrischer Daten, insbesondere in psychiatrischen Gutachten, die für Zwecke der Verwaltung von Dienststellen des Landes Berlin benötigt werden.

Bei der Erhebung, Speicherung und Übermittlung psychiatrischer Daten, insbesondere psychiatrischer Gutachten muß beachtet werden, daß

- diese Daten höchstsensibel sind und jede mißbräuchliche Verwertung zu erheblichen, unter Umständen irreparablen Schäden führen kann,
- die wissenschaftlichen Erkenntnisse über Krankheitsbilder und sichere Anzeichen von psychiatrischen Erkrankungen einem erheblichen Wandel unterliegen.

Daraus ergibt sich die Notwendigkeit äußerster Vorsicht in allen Phasen der Datenverarbeitung.

I.

Erhebung, Speicherung und Übermittlung psychiatrischer Daten durch den untersuchenden Arzt

1. Die Erhebung der Daten zur Vorbereitung psychiatrischer Gutachten ist ausschließlich Angelegenheit des untersuchenden Arztes. Bei der Untersuchung sollten nur Daten erhoben und gespeichert werden, die für die Erstellung des Gutachtens erforderlich sind. Auch wenn der Arzt im Auftrag einer dritten Stelle, z. B. der Dienstbehörde handelt, bleibt er bezüglich der erhobenen Daten „speichernde Stelle".

2. Die Art und Weise der Untersuchung muß mit dem Persönlichkeitsrecht des Betroffenen vereinbar sein. Sie kann daher nicht durch Akten, andere Gutachten oder sogenannte Ferngutachten ersetzt werden.

3. In der Regel sind vom Arzt nur die Ergebnisdaten, nicht jedoch die Befunddaten an die auftraggebende Verwaltung zu übermitteln. Die Weiterleitung der Befunddaten für Verwaltungszwecke der auftraggebenden Stelle ist nur zulässig, wenn die Weiterleitung des Ergebnisses für den gesetzlichen ausdrücklich vorgeschenen Zweck nicht ausreicht (z. B. § 78 Abs. 1 Landesbeamtengesetz).

   Soweit nicht eine gesetzliche Grundlage besteht, ist die Übermittlung nur mit Zustimmung des Betroffenen zulässig.

4. Für die Übermittlung psychiatrischer Gutachten und deren Ergebnisse an die auftraggebende Verwaltung gilt der Grundsatz der Zweckbindung. Daten dürfen daher nur insoweit übermittelt werden, als der - in der Regel eine - Zweck, zu dem das Gutachten erstellt worden ist, dies verlangt.

II.

Erhebung, Speicherung und Übermittlung durch die auftraggebende Verwaltung

1. Auch die auftraggebende Verwaltung hat den Grundsatz der Zweckbindung zu beachten, d.h. das psychiatrische Gutachten bzw. die Ergebnisse des psychiatrischen Gutachtens dürfen nur für den - in der Regel einen - Zweck verwertet werden, für den die Erstellung des Gutachtens erbeten wurde.

2. Soweit psychiatrische Gutachten und Ergebnisse solcher Gutachten in Akten aufgenommen werden, sind sie besonders zu behandeln. Über das Einsichtsrecht ist gesondert zu entscheiden. In jedem Einzelfall muß daher unter Anlegung strenger Maßstäbe geprüft werden, welche Gründe die Einblicknahme in die Ergebnisse oder sogar in das Gutachten selbst rechtfertigen.

3. Die Gültigkeit psychiatrischer Daten ist zeitlich begrenzt. Auch innerhalb der Zweckbindung ist eine Verwertung dann auszuschließen, wenn wegen des Zeitpunkts der Erstellung des ihnen zugrundeliegenden Gutachtens Zweifel an der Verwertbarkeit der Daten bestehen.

4. Psychiatrische Gutachten sowie die Ergebnisse psychiatrischer Gutachten, die entgegen diesen Richtlinien im Besitz von Dienststellen sind, müssen vernichtet werden. Sind auf rechtswidrig erlangte psychiatrische Daten bereits Verwaltungsentscheidungen gestützt worden, ist für die Vorgänge, in denen diese Daten Erwähnung finden, eine Aufbewahrungsform zu wählen, die die weitere Verwertung der Daten verhindert (z. B. Aufbewahrung in versiegelten Umschlägen).

5. Können psychiatrische Daten von Bedeutung für ein anderes Verwaltungsverfahren sein und ist dies der Stelle bekannt, die über diese Gutachten verfügt, ist nur ein Hinweis auf die Existenz der Daten, nicht aber die Übermittlung der Daten an die andere Stelle zulässig.

Anlage 2

Datenschutzrechtliche Vorstellungen zur Verbesserung des Personaldatenschutzes

1. Vorschläge zur Regelung im Vorverhältnis

Im Rahmen des Bewerbungsverhältnisses ist die Erhebung und Speicherung der personenbezogenen Daten zulässig, die erforderlich sind, um über die Ernennung des Bewerbers zum Beamten zu entscheiden (§ 9 Abs. 1 LBG). Bei der Erhebung sind die in anderen Gesetzen festgelegten Verwertungsverbote (namentlich des Bundeszentralregistergesetzes) zu berücksichtigen. Wird der Bewerber nicht eingestellt, sind die von ihm eingereichten Unterlagen zurückzugeben, sobald ein anderer Bewerber ernannt worden ist. Die Aufbewahrung anderer Unterlagen, die abgelehnte Bewerber betreffen, sollte auf das unbedingt erforderliche Maß beschränkt werden.

2. Vorschläge zur Regelung während des Dienstverhältnisses

Während des Dienstverhältnisses ist die Erhebung personenbezogener Daten und deren Aufbewahrung in einer Personalakte (einschließlich aller Datensammlungen, die Personaldaten enthalten) zulässig, soweit diese zur Abwicklung des Dienstverhältnisses erforderlich sind. Bei der Erhebung sind die gesetzlichen Verwertungsverbote zu berücksichtigen. Unzulässigerweise erhobene Daten sind aus der Personalakte zu entfernen.

Darüber hinaus sind Vorgänge auf Antrag des Beamten zu tilgen, die ursprünglich zulässig in die Personalakte aufgenommen worden sind, deren Kenntnis für die Erfüllung der Pflichten und Wahrung der Rechte des Dienstherrn jedoch nicht mehr erforderlich ist.

Vorgänge in der Personalakte über die Prüfung der Einstellungsvoraussetzungen (§ 9 Abs. 1 Nr. 2 LBG) sind nach Beendigung der Probezeit auf Antrag des Beamten zu tilgen.

Eintragungen in der Personalakte über Disziplinarmaßnahmen und Disziplinarvorgänge sind nach Maßgabe des § 112 Landesdisziplinarordnung zu tilgen. Für Vorgänge und Eintragungen über strafgerichtliche Verurteilungen, strafrechtliche Ermittlungsverfahren, berufsgerichtliche Verfahren oder Ordnungswidrigkeiten gilt das gleiche, wenn ein sachgleicher Vorgang besteht.

Vorgänge und Eintragungen in der Personalakte über strafrechtliche Ermittlungsverfahren und Ordnungswidrigkeiten sind zu tilgen, sobald feststeht, daß der Sachverhalt keinen Anlaß zu disziplinarrechtlichen Ermittlungen gibt. Vorgänge und Eintragungen in der Personalakte über strafgerichtliche Verurteilungen und berufsgerichtliche Verfahren, die keinen Anlaß zu disziplinarrechtlichen Ermittlungen gegeben haben, sind nach drei Jahren zu tilgen. Die Frist beginnt mit dem Tage der das Verfahren abschließenden Entscheidung. Ist diese anfechtbar, beginnt die Frist mit dem Tage, an dem die Entscheidung unanfechtbar ist.

Die Personalakte darf einer anderen Stelle nur mit schriftlicher Einwilligung des Beamten zugänglich gemacht werden, es sei denn, es handelt sich um die erforderliche Vorbereitung einer ohne seine Zustimmung zulässigen Versetzung (§ 61 LBG) oder Abordnung (§ 62 LBG).

Der Inhalt von Personalakten unterliegt einer besonderen Verschwiegenheitspflicht (Personaldatengeheimnis).

Die Einzelheiten der Personaldatenführung sollten einheitlich im Verordnungswege geregelt werden.

Anlage 3

Grundsätze für den Datenschutz bei den Neuen Medien (insbesondere bei Bildschirmtext und Kabelfernsehen)

Beschluß der 7. Konferenz der Datenschutzbeauftragten des Bundes und der Länder in Berlin
am 11. Dezember 1980
- in der Fassung vom 21. Januar 1981 -

Vorbemerkung

Die nachstehenden Grundsätze für den Datenschutz bei den Neuen Medien sollen sicherstellen, daß die anlaufenden Erprobungen und die ihnen zugrundeliegenden Vorschriften den Datenschutz von vornherein berücksichtigen und dieser dem Einsatz neuer Technologien nicht nachfolgt.

Die Grundsätze können dem Stand der Vorhaben und der technischen Entwicklung entsprechend nicht abschließend sein.

1. **Informationssammlung über Teilnehmer**

1.1 Bei der Einführung Neuer Medien ist der Datenschutz sicherzustellen. Dies gilt auch für die Versuchsphase. Bereits hierfür sollten gesetzliche Regelungen getroffen werden.

1.2 Personenbezogene Benutzerdaten dürfen nur erhoben, gespeichert oder übermittelt werden, soweit ihre Verarbeitung für den Betrieb unumgänglich ist und ohne sie eine der gesetzlich zugelassenen Kommunikationsformen der Neuen Medien nicht durchgeführt werden kann.

1.3 Der Schutz der in den Neuen Medien anfallenden personenbezogenen Teilnehmerdaten kann nicht auf deren Verarbeitung in Dateien beschränkt werden.

1.4 Sofern bei bestimmten Diensten eine unmittelbare Teilnehmer-Anbieter-Kommunikation vorgesehen ist, dürfen Daten nur in dem Umfang festgehalten und übermittelt werden, wie dies zur Durchführung des jeweiligen Dienstes erforderlich und auf Grund der einschlägigen gesetzlichen Regelung zulässig ist.

1.5 Gebühren und Entgelte sind in anonymer Form zu berechnen und abzurechnen, soweit eine individualisierbare Registrierung von einzelnen Kommunikationsvorgängen zur Abwicklung von Vertragsverhältnissen nicht erforderlich ist. Sollte eine zusätzliche Kontrolle erforderlich werden, so könnte beim Benutzer eine Zähleinrichtung installiert werden.

2. **Bedeutung des Versuchsstadiums (Pilotprojekte)**

2.1 Bereits in der Versuchsphase ist ein möglichst wirksamer Datenschutz sicherzustellen, da diese Phase die spätere Nutzung der Neuen Medien prägt.

2.2 In der Versuchsphase ist zu prüfen, ob weitere Datenschutzregelungen auf dem Gebiet der Neuen Medien nötig sind oder ob vorhandene Vorschriften modifiziert werden müssen.

2.3 Im Rahmen wissenschaftlicher Begleituntersuchungen ist dafür zu sorgen, daß auch die Datenschutzfragen besonders geprüft werden.

2.4 Im Rahmen einer wissenschaftlichen Begleituntersuchung ist der Zugriff auf gespeicherte Datenbestände nur gestattet, sofern diese Daten anonymisiert worden sind. Darüber hinausgehende Daten dürfen nur von den Teilnehmern direkt erfragt werden.

Die Datenverarbeitung sollte in allen Phasen nur mit Einwilligung des Teilnehmers erfolgen (vgl. dazu Ziff. 3).

3. **Die Bedeutung der „Einwilligung" bei der Speicherung von Teilnehmerdaten**

3.1 Die Speicherung von Teilnehmerdaten in einer Form, die die Erstellung individueller Persönlichkeitsprofile gestattet, ist zu verbieten. Darüber hinaus kann in einzelnen Diensten die Speicherung besonders sensibler Daten aus dem „unantastbaren Bereich privater Lebensgestaltung" (vgl. BVerfGE 27, 1, 7; s. a. § 27 Abs. 3 Satz 3 BDSG) grundsätzlich verboten werden. Eine Einwilligung des Teilnehmers hebt das Verbot nicht auf.

3.2 Im übrigen ist eine Speicherung von Teilnehmerdaten erlaubt,

a) wenn eine gesetzliche Regelung dies zuläßt;

b) wenn der Teilnehmer seine Einwilligung gibt.

Diese Einwilligung ist nur wirksam, wenn der Teilnehmer zuvor sorgfältig über ihre Konsequenzen aufgeklärt worden ist (informed consent). Dies gilt auch für den Abschluß von Verträgen.

4. **Rückkanal und sonstige technische Vorkehrungen, über die Äußerungen der Teilnehmer dem System gegenüber kundgegeben werden können**

4.1 Nutzungsmöglichkeiten des Rückkanals und aller sonstigen technischen Vorkehrungen, über die Äußerungen der Teilnehmer dem System gegenüber kundgetan werden können, sollen nach Möglichkeit gesetzlich geregelt werden. Soweit Teilnehmerdaten gespeichert werden können, dürfen sie nur zu dem Zweck verwertet werden, zu dem sie offenbart wurden.

4.2 Persönlichkeitsprofile der Teilnehmer dürfen anhand der in der Betriebszentrale anlaufenden Kommunikationsdaten nicht erstellt werden. Dies gilt für jede Betriebszentrale, unabhängig von der angewendeten Technologie.

4.3 Abstimmungen und Wahlen über den Rückkanal dürfen nicht durchgeführt werden.

5. **Medienprivileg**

5.1 Das Verhältnis des Medienprivilegs zu den Neuen Medien bedarf insgesamt einer eingehenden Untersuchung.

5.2 Dabei muß insbesondere geprüft werden,

- ob die einzelnen Neuen Medien als Presse bzw. Rundfunk anzusehen sind oder ob es sich um Medien sui generis handelt,
- in welchen Fällen nach geltendem Recht personenbezogene Daten ausschließlich zu publizistischen Zwecken verarbeit werden,
- ob der Geltungsbereich des Medienprivilegs im Hinblick auf die für die Benutzer bestehenden Gefahren sachgerecht geregelt ist,
- falls dies bejaht wird:
  ob der Geltungsbereich zur Klarstellung gesetzlich geregelt werden soll,
- falls dies verneint wird:
  inwieweit der Geltungsbereich nur geregelt werden sollte.

Schließlich bedarf besonderer Erörterung die Gefahr, daß in Medienarchiven gespeicherte, personenbezogene Daten in die Speicherzentralen eingegeben werden und unter Berufung auf das Medienprivileg (§ 1 Abs. 3 BDSG und entsprechende Regelungen in den Ländergesetzen) frei zugänglich gemacht werden. Unter diesem Gesichtspunkt verdienen auch die im Urteil des Bundesverfassungsgerichts vom 5. Juni 1973 - 1 BvR 536/72 - (BVerfGE 35, S. 202 ff. [219 ff.] „Lebach") aufgestellten Grundsätze zum Schutze der Persönlichkeit vor dem Zugriff der Öffentlichkeit besondere Berücksichtigung.

6. **Fernmeldegeheimnis und Neue Medien**

6.1 Im gesamten Netzbereich werden die zentralen Einrichtungen der Neuen Medien ebenso wie die Übertragungswege vom Fernmeldegeheimnis im Sinne von Art. 10 GG umfaßt, sofern es sich dabei um juristische Personen des öffentlichen Rechts handelt.

6.2 Folgt man der Auffassung, daß die zentralen Einrichtungen der Neuen Medien keine Fernmeldeanlagen sind, ist ein dem Fernmeldegeheimnis vergleichbares Amtsgeheimnis für den Nutzungsbereich - unter Umständen in Verfassungsrang - zu schaffen.

6.3 Die Einblicknahme in und die Übermittlung von personenbezogenen Daten aus Speichereinrichtungen einer Bildschirmtext- bzw. Kabelfernsehzentrale sind nur auf Grund gesetzlicher Voraussetzungen zulässig. Unter Datenschutzgesichtspunkten ist es bedenklich, die Regelungen des Gesetzes zu Art. 10 GG uneingeschränkt anzuwenden.

6.4 Für die in den zentralen Einrichtungen der Neuen Medien beschäftigten Bediensteten ist ein Zeugnisverweigerungsrecht und für alle dort gespeicherten Daten ein Beschlagnahmeverbot (vgl. § 97 StPO) zu verlangen.

7. **Datenschutzkontrolle und Datensicherung**

7.1 Die Kontrolle des Datenschutzes bei den Neuen Medien sollte Aufgabe der Datenschutzbeauftragten des Bundes und der Länder sein.

7.2 Beim Anschluß von ADV-Einrichtungen durch Teilnehmer sind hinreichende technische und organisatorische Maßnahmen zu fordern, sowohl hardware- als auch softwaremäßig, z. B. Schlüsselschalter, Paßwortroutinen usw.