HESSISCHER LANDTAG

7. Wahlperiode . Drucksache 7/3137

29. 03. 73

Vorlage des Datenschutzbeauftragten

betreffend den Zweiten Tätigkeitsbericht

Mit Schreiben vom 29. März 1973 legt der Datenschutzbeauftragte gemäß § 14 Abs. 1 des Datenschutzgesetzes vom 7. Oktober 1970 (GVBl. I S. 625) dem Landtag den folgenden Zweiten Tätigkeitsbericht vor:

Eingegangen am 29. März 1973 . Ausgegeben am 27. April 1973

Druck: Carl Ritter & Co. Wiesbaden . Vertrieb: Verlag Dr. Hans Heger 53 Bonn-Bad Godesberg Goethestr. 56 Tel. 63551

Zweiter Tätigkeitsbericht

des

Hessischen Datenschutzbeauftragten

vorgelegt zum 31. März 1973

gemäß § 14 des Hessischen Datenschutzgesetzes vom 7. Oktober 1970

INHALTSVERZEICHNIS

1. VORBEMERKUNGEN

1. Vorbemerkungen

Der vorliegende Zweite Tätigkeitsbericht des Datenschutzbeauftragten umfaßt zum ersten Mal einen Zeitraum von 12 Monaten. Der erste Bericht hatte nur die neun Monate nach der Wahl des ersten Datenschutzbeauftragten behandelt. In dieser Zeit mußten zunächst die Dienststelle aufgebaut und Arbeitsschemata entwickelt werden. Der erste Bericht beschränkte sich deshalb weitgehend darauf, einen Überblick über die Entwicklung der maschinellen Datenverarbeitung und des Datenschutzes ganz allgemein und im besonderen in der öffentlichen Verwaltung in Hessen zu geben; die Problemkreise Persönlichkeitsschutz und Schutz der verfassungsmäßigen Machtbalance wurden umrissen, ungelöste Fragen wurden aufgezeigt und Anregungen zur Verbesserung des Datenschutzes und der Datensicherheit gegeben. Der Zweite Tätigkeitsbericht kann auf theoretische Erörterungen nicht verzichten, da die Diskussion über den Inhalt und die Organisation des Datenschutzes noch im vollen Gang ist. Vor allem aber berichtet er über die Beobachtungen, Erkenntnisse und Erfahrungen, die der Datenschutzbeauftragte bei seiner Tätigkeit im Berichtszeitraum gemacht hat.

Die positive Aufnahme des Ersten Tätigkeitsberichts und seiner Aufgliederung im Landtag, in der Regierung und in der Öffentlichkeit veranlaßt den Datenschutzbeauftragten, für den Zweiten Tätigkeitsbericht die Gliederung beizubehalten und ihn als eine Art Fortschreibung des ersten Berichts weiterzuführen. Dadurch können die Entwicklungen in den verschiedenen Problemkreisen leichter miteinander verglichen werden. Bestand kein Anlaß zur Fortschreibung, so wurden die Ziffern als Leertitel geführt. Wo es notwendig war, wurde die Untergliederung allerdings abgewandelt oder ergänzt. Wird im Bericht auf Ausführungen in anderen Abschnitten Bezug genommen, so werden die arabischen Ziffern angeführt. Bezieht sich der Hinweis auf Teile des Ersten Tätigkeitsberichts, so wird vor die arabischen Ziffern eine I gestellt.

1.1 Die EDV und das Datenschutzverständnis

Im Berichtszeitraum 1972/73 hat die öffentliche Verwaltung in Bund und Ländern ständig weitere Aufgaben der maschinellen Datenverarbeitung zugeführt. Ende 1972 waren rund 12 000 Datenverarbeitungsanlagen in der Bundesrepublik installiert*). Andere Quellen sprechen von 22 000 Anlagen**). Die Zahl der Kleincomputer belief sich auf etwa 35 000***). Im Bereich der öffentlichen Verwaltung arbeiteten Ende 1972 ca. 1 000 EDV-Anlagen. Nach der fortgeschriebenen Bestandsaufnahme waren in der öffentlichen Verwaltung in Hessen am 31. 12. 1972 rund 80 Anlagen in Betrieb. Diese Entwicklung geht weiter. Die Datenverarbeitung wird immer mehr für Massenaufgaben der Verwaltung, aber auch für die Planung einer modernen Gesellschafts- und Sozialpolitik verwendet. Gäbe es keine maschinelle Datenverarbeitung, so müßten z. B. für die Berechnung und Auszahlung von Löhnen und Renten, von Wohngeld und anderen Sozialbeihilfen eine große Zahl zusätzlicher Arbeitskräfte eingestellt werden. In zunehmendem Maße werden auch die bei der Verwaltungsarbeit anfallenden Unterlagen und Daten für andere als die ursprünglich vorgesehenen Verwaltungszwecke sowie für wissenschaftliche und statistische Aufgaben gespeichert und ausgewertet. Hersteller und Anwender bemühen sich intensiv und mit Erfolg, ihre Anlagen, Programme und Organisationen so zu gestalten, daß sie „benutzerfreundlich" sind. Ein entsprechender Begriff für den Betroffenen, dessen Daten gespeichert und vielfach weitergegeben werden, ohne daß er davon erfährt, fehlt dagegen in der Fachwelt. „Betroffenenfreundliche" Systeme wurden noch nicht bekannt. Dies kennzeichnet die derzeitige Einschätzung dieses Problems.

In den Verwaltungen des Bundes und der Länder wurde bereits mit dem Aufbau integrierter Datenverarbeitungssysteme begonnen. Es entstehen auf Landes- und Bundesebene Teilsysteme, wie z. B. die Informationssysteme der Kriminalpolizei (vgl. 4.1.1.3 c) und der Nachrichtendienste (vgl. 4.1.1.3 e). Dabei wird die Grundstruktur des staatlichen Informationswesens schon heute festgelegt. Die Techniker der Verwaltung und der Elektronik entwickeln benutzerfreundliche Programme, Verfahrensregeln und Organisationsmuster, die den Informationsbedarf der Verwaltung optimal erfassen und den reibungslosen Datenfluß sicherstellen. Die Fragen nach den demokratischen Kontrollen, nach dem Schutzbedürfnis der Persönlichkeitsrechte des Bürgers und der verfassungsmäßigen Gewaltenbalance werden dabei meist vernachlässigt.

Wissenschaftler und Politiker haben diese Gefahren erkannt und nach Lösungen gesucht. Auch im Berichtszeitraum wurden neue Vorschläge und Gesetzentwürfe bekannt. Im In- und Ausland veröffentlichte Untersuchungen und Gutachten von wissenschaftlichen Gremien und Regierungskommissionen haben sich im Zusammenhang damit auch mit dem hessischen Datenschutzgesetz und der Institution des Datenschutzbeauftragten befaßt (vgl. 1.4 und 2.1—2.3). Zu gesetzgeberischen Maßnahmen ist es jedoch nicht gekommen.

1.2 Die Reaktion auf den Ersten Tätigkeitsbericht

Der Erste Tätigkeitsbericht des Datenschutzbeauftragten gab der Diskussion über den Datenschutz gewisse neue Akzente. Er wurde gemäß § 14 Abs. 1 DSG am 29. 3. 1972 dem Präsidenten des Landtags und dem Ministerpräsidenten vorgelegt und in der 41. Plenarsitzung des Landtags

*) Nach Diebold; zitiert in: Handbuch der modernen Datenverarbeitung 13/4, 49. Lief., Forkel Verlag Stuttgart/Wiesbaden.

**) „Die Zeit" Nr. 9 vom 23. 2. 1973, S. 29.

***) Genaue Zahlenangaben sind nicht möglich, weil es keine einheitliche Abgrenzungen von Datenverarbeitungsanlagen, Groß- und Kleincomputern gibt.

am 31. 5. 1972 behandelt. Zusammen mit der Stellungnahme der Landesregierung vom 18. 5. 1972 (LT-Drucks. 7/1705) wurde der Bericht vom Plenum dem Hauptausschuß überwiesen (Stenographischer Bericht 7/41). Der Ausschuß hat seine Beratungen noch nicht abgeschlossen. Er hat jedoch seine Zuständigkeit für den Teil des Berichts festgestellt, der sich mit der Wahrung der Grundrechte der Bürger befaßt. Mit der Vorlage des zweiten Berichts stellt sich nunmehr die Frage nach der weiteren parlamentarischen Behandlung der Tätigkeitsberichte.

Die Stellungnahme der Landesregierung zum Ersten Tätigkeitsbericht und seine Behandlung im Landtag und in der Öffentlichkeit haben gezeigt, daß über die Unabhängigkeit der Stellung des Datenschutzbeauftragten und über seine Arbeitsweise keine Meinungsverschiedenheiten bestehen. Der Bericht stieß auch bei außerhessischen Behörden, bei Arbeitgeber- und Arbeitnehmerorganisationen, bei Fachverbänden und sonstigen Institutionen, sowie bei Wissenschaftlern und Journalisten auf großes Interesse.

Im Ausland war das Echo ebenfalls sehr lebhaft. Dies gilt besonders für den englischsprachigen Raum. Deshalb wurde eine Übersetzung des Berichts in englischer Sprache angefertigt, die im Dezember 1972 erschien.

1.3 Notwendigkeit des Datenschutzes

Die Notwendigkeit des Datenschutzes wird in Wissenschaft und Praxis nicht mehr bestritten. Das gilt auf jeden Fall für die Datenverarbeitung in der öffentlichen Verwaltung. Gegen eine allgemeine Regelung des Datenschutzes für die private Wirtschaft sind jedoch in der Diskussion über den Referentenentwurf eines Bundesdatenschutzgesetzes von verschiedenen Seiten Bedenken erhoben worden. Einige interessierte Gruppen forderten, die gesetzliche Regelung des Datenschutzes generell auf den Bereich der öffentlichen Verwaltung zu begrenzen.

Aber auch aus dieser Auffassung kann nicht gefolgert werden, daß der Datenschutz schlechthin für unnötig gehalten werde. In der Regel werden nur einzelne Elemente des Datenschutzes abgelehnt. So haben sich z. B. Auskunfteien gegen eine gesetzliche Auskunftspflicht ausgesprochen.

Welche Bedeutung Datenschutzmaßnahmen in der privaten Wirtschaft erlangen können, beleuchtet eine Pressemeldung*), wonach die Hermes-Kredit-Versicherung bei zwei EDV-Anwendern den Abschluß einer Computer-Mißbrauch-Versicherung mit der Begründung abgelehnt habe, das Versicherungsrisiko sei zu hoch. Bei den Antragstellern seien die Funktionen, z. B. Datenerfassung, Operating und Programmierung nicht klar genug voneinander getrennt, die Datensicherung sei mangelhaft und die Auswertung der Maschinenprotokolle ungenügend. Diese Meldung erhellt die Besonderheiten der maschinellen Datenverarbeitung gegenüber der herkömmlichen Informationsverarbeitung: Einerseits entsteht bei den EDV-Anwendern ein Versicherungsbedürfnis gegen die besonderen Schäden, die aus dem Diebstahl von Daten und Programmen, aus betrügerischen Programm-Manipulationen und -Unterdrückungen sowie durch Veränderung oder Einschieben von Datenträgern entstehen können; andererseits verlangt der Versicherer spezielle Datenschutzmaßnahmen als Vorbedingung für den Abschluß des Versicherungsvertrages, um so sein Risiko zu verringern.

*) Manager Magazin 1/73, S. 61.

1.3.1 EDV-Programme für Datenschutz

Auch bei den Anwendern der Datenverarbeitung wächst das Verständnis für die Notwendigkeit von Datenschutzmaßnahmen. Hersteller von Hard- und Soft-Ware berichten, daß ihre Kunden neuerdings Vorschläge und Hilfen für Datenschutz- und Datensicherungsmaßnahmen erwarten. Diese Anwender haben erkannt, daß die EDV nicht nur Nutzen bringen, sondern daß sie auch zum Datenmißbrauch und zum Schaden des Anwenders eingesetzt werden kann. Bekanntgeworden sind z. B. Diebstähle von Adressendateien bei Versandhäusern oder von Patentunterlagen bei Industrieunternehmen. Einige Hersteller prüfen z. Z. die Möglichkeiten, spezielle Dienstprogramme für Datenschutz und Datensicherung zu entwickeln, um mit Hilfe der Elektronik den mit der EDV verbundenen besonderen Gefahren entgegenzutreten.

1.3.2 Datenaustausch und Adressenhandel

Wie tief die elektronische Datenverarbeitung in die Intimsphäre eindringen kann und wie notwendig besondere Schutzmaßnahmen sind, ergibt sich ferner aus der Nutzung der elektronischen Datenverarbeitung durch verschiedene Anwender. Adressenverlage und Werbegesellschaften, Detekteien, Banken und Versicherungen tauschen bereits ihre Daten aus und führen sie zusammen, so daß Persönlichkeitsprofile entstehen, die die verschiedensten Merkmale erfassen. Eine große Werbegesellschaft offeriert in ihrem neuesten Katalog Adressenmaterial, das nach verschiedensten Kriterien aufgegliedert ist. Angeboten werden über tausend „Adressenstämme", z. B. von Teenagern und Twens, von Zahnprothesenträgern, von spendenfreudigen Personen, von Jagdscheininhabern, von Käufern pornographischer Artikel usw.

Auffällig ist, daß die Werbegesellschaft einen Teil ihrer Adressen offensichtlich von Behörden bezieht. Bei einer Reihe von Adressenstämmen heißt es: „aus behördlichen" oder „aus amtlichen" Unterlagen zusammengestellt. Die Gesellschaft ist bemüht, ihre Adressendatei zu vervollständigen. Sie sucht deshalb in ihrem Katalog nach Lieferanten von Adressen: So z. B. von Spielbankkunden, von ledigen Strafgefangenen, ledigen ehemaligen Fürsorgezöglingen, ledigen ehemaligen Kinderheimzöglingen und ledigen Müttern.

1.4 Der Datenschutzbeauftragte

Die unabhängige Stellung des Datenschutzbeauftragten (vgl. I 1.4.2) ist in der Behandlung des Ersten Tätigkeitsberichts im Parlament (1.2) bestätigt worden. Welche besondere Beachtung ihm auch außerhalb der staatlichen Verwaltung entgegengebracht wird, geht daraus hervor, daß grundsätzliche Fragen des Datenschutzes und der Datensicherung von verschiedenen Organisationen in vielen Gesprächen an ihn herangetragen worden sind.

Auf seiten der Landes- und Kommunalverwaltungen hatte der Datenschutzbeauftragte engen Kontakt mit den Stellen und Ausschüssen, die sich mit der Automation der Landesverwaltung befassen, insbesondere auch mit der Hessischen Zentrale für Datenverarbeitung (HZD) und den Kommunalen Gebietsrechenzentren (KGRZ). Besondere Schwerpunkte bildeten im Berichtszeitraum die Überlegungen über einen Datenkatalog (vgl. 3.2), der Schutz medizinischer (vgl. 4.1.2.3), kriminalpolizeilicher (vgl. 4.1.1.3 c) und nachrichtendienstlicher Daten (vgl. 4.1.1.3 e).

Obwohl die Reaktion auf die Empfehlungen, die der Datenschutzbeauftragte aufgrund seiner Beobachtungen und Erfahrungen vorgelegt hat, unterschiedlich war, lösten sie in der Regel Nachprüfungen aus und führten zur Beseitigung der beanstandeten Zustände.

Auch an der Datenschutzdiskussion außerhalb Hessens beteiligte sich der Datenschutzbeauftragte und war bemüht, die hessischen Beobachtungen und Erfahrungen — insbesondere bei Gesprächen mit dem zuständigen Beamten des Bundesinnenministeriums — in die Erörterungen um eine Bundesdatenschutzgesetzgebung einzubringen. An dem Hearing zu dem im Bundesinnenministerium erarbeiteten Referentenentwurf für ein Bundesdatenschutzgesetz nahm der Datenschutzbeauftragte mit einem Diskussionsbeitrag teil (vgl. Anlage I). Der Schutz medizinischer Daten stand im Mittelpunkt von Gesprächen mit dem Bundesministerium für Jugend, Familie und Gesundheit sowie mit Vertretern ärztlicher Organisationen.

Mit Herstellerfirmen und Anwendern erörterte der Datenschutzbeauftragte die Weiterentwicklung der EDV und den Einsatz technischer Verfahren und organisatorischer Maßnahmen für den Datenschutz und die Datensicherung.

In besonderem Maße beschäftigte sich der Datenschutzbeauftragte mit der Frage, was die Massenmedien beitragen könnten, um in der Bevölkerung das Verständnis für die Notwendigkeit von Datenschutzmaßnahmen zu vertiefen. In einer Anzahl von Interviews, Presseartikeln und Vorträgen griff er diesen Themenkreis auf. Er besprach ihn ferner mit Journalisten und mit Verantwortlichen der Verwaltung von Rundfunkanstalten.

Die Fülle von mündlichen und schriftlichen Anfragen, die der Datenschutzbeauftragte im Berichtszeitraum erhielt und in denen er um Auskunft über das Wesen des Datenschutzes oder um Material für wissenschaftliche Arbeiten gebeten wurde, zeigt das zunehmende Interesse in der Öffentlichkeit für diese Fragen. Des öfteren wandten sich auch Privatpersonen an den Datenschutzbeauftragten mit der Bitte um Stellungnahmen oder Ratschläge zu Problemen des Datenschutzes (vgl. 4.1.4). Er erhielt dabei Kenntnis von vielen Vorgängen, die nicht in seinen Zuständigkeitsbereich fielen, weil sie sich entweder außerhalb Hessens oder im Bereich der Datenverarbeitung durch private Institute abspielten. Diese zusätzlichen Informationen rundeten seine Eindrücke ab und ermöglichten ihm, ein Gesamtbild der Entwicklung zu gewinnen.

2. RECHTLICHE REGELUNGEN DES DATENSCHUTZES AUSSERHALB HESSENS

2.1 Andere Länder — Überblick

Seit dem im Ersten Bericht gegebenen Überblick über den Gesetzgebungsstand im Datenschutz haben sich kaum Veränderungen ergeben. Zur Verabschiedung weiterer gesetzlicher Regelungen ist es nicht gekommen. Dies heißt jedoch nicht, daß man Datenschutzregelungen heute für weniger dringlich hält. Vielmehr will man die erwarteten bundesgesetzlichen Regelungen abwarten, um die nach wie vor fest geplanten Landesgesetze inhaltlich und gesetzestechnisch darauf abstimmen zu können. Aus diesem Grunde wurden z. B. die in Rheinland-Pfalz, Nordrhein-Westfalen und Hamburg vorliegenden Gesetzentwürfe vorläufig nicht weiter verfolgt. Daneben spielt freilich auch das Bestreben eine Rolle, die noch immer vorhandene Unsicherheit über Nutzung, Kosten und Praktikabilität von Datenschutzregelungen in der verbleibenden Zeit durch Untersuchungen und systematisches Zusammentragen der Erfahrungen zu verringern.

2.1.1 Schleswig-Holstein

Die einzige neue Gesetzgebungsinitiative in den Ländern ist von der Opposition im Schleswig-Holsteinischen Landtag ausgegangen. Der von ihr am 12. 2. 1973 eingebrachte Entwurf eines Datenschutzgesetzes (LT-Drucks. 7/484) tendiert in allen Fragen zu möglichst umfassenden und weitreichenden Regelungen, wobei neben dem hessischen Datenschutzgesetz und den Entwürfen anderer Länder insbesondere der Referentenentwurf des Bundesinnenministers und der im letzten Bundestag aus seiner Mitte eingebrachte Entwurf (vgl. I 2.2.2) als Vorbilder dienen. Bemerkenswert erscheint der Vorschlag einer Datenschutzkommission, die ebenso wie der Hessische Datenschutzbeauftragte über den Schutz der personenbezogenen Daten wachen und die Auswirkungen der Datenverarbeitung auf das Verfassungsgefüge beobachten, darüber hinaus aber auch ein öffentliches Register aller maschinell geführten Sammlungen personenbezogener Daten im Bereich der öffentlichen Verwaltung führen soll.

Der Entwurf wurde nach der Beratung im Landtag am 27. Febr. 1973 an den Innen- und den Rechtsausschuß überwiesen. Die Landesregierung hat sich dafür ausgesprochen, zunächst das Bundesdatenschutzgesetz abzuwarten.

2.1.2 Bayern

Keine neuen Entwicklungen

2.1.3 Rheinland-Pfalz

Anläßlich einer parlamentarischen Debatte über einen von der Landesregierung erteilten Entwicklungsauftrag für ein Integriertes Planungs-, Entwicklungs- und Kontrollsystem (IPEKS) wurden eingehend Fragen einer parlamentarischen Beteiligung an den im Aufbau befindlichen Informationssystemen erörtert. Die Opposition vertrat die Ansicht, daß das Parlament bereits jetzt seinem Verfassungsauftrag, die Arbeit der Regierung zu kontrollieren und Alternativen zu ihren Planungen zu entwickeln, aus mangelnder Information und Aufklärung nicht ausreichend nachkommen könne. Sie stellte deshalb die Frage nach der geeignetsten Organisationsform zur Wahrnehmung und Unterstützung der parlamentarischen Informationsansprüche. Ihre Anregung, an Stelle oder neben dem im rheinland-pfälzischen Entwurf eines Datenschutzgesetzes vorgesehenen gemischten Ausschuß einen Datenschutzbeauftragten nach hessischem Vorbild einzurichten, wurde allgemein als näher zu prüfende Möglichkeit aufgenommen. Die Regierungsfraktion beabsichtigt jetzt, die geplante Institution eines Bürgerbeauftragten zugleich mit Datenschutzaufgaben zu betrauen.

2.1.4 Niedersachsen
2.1.5 Baden-Württemberg
2.1.6 Nordrhein-Westfalen
2.1.7 Hamburg
2.1.8 Berlin, Bremen, Saarland

Keine neuen Entwicklungen

2.2 Gesetzgebungsstand im Bund

Die Diskussionen über den Entwurf zum Bundesmeldegesetz und den Referentenentwurf für ein Bundesdatenschutzgesetz sind weitergeführt worden. Zu gesetzgeberischen Schritten ist es im Berichtszeitraum nicht gekommen.

2.2.1 Bundesmeldegesetz

Der Entwurf eines Bundesmeldegesetzes (BT-Drucks. VI/2654) ist mit der Auflösung des sechsten Bundestages formell untergegangen. Der Bundesinnenminister beabsichtigt, den Entwurf alsbald erneut einzubringen. Auf Grund der bisherigen Diskussion sind einige Änderungen vorgesehen, die z. T. auch die Regelung des Datenschutzes im Meldewesen betreffen. So ist die Ermächtigung des Bundesministers des Innern zur Festlegung eines bundeseinheitlichen Mindestdatensatzes in ihrer Zweckbestimmung präzisiert und eingeschränkt worden. Verordnungen dürfen nur noch die Durchführung von Datenübermittlungen zwischen mehreren Ländern oder zwischen einem Land und dem Bundesverwaltungsamt entsprechend den im Entwurf selbst vorgesehenen Vorschriften regeln (§ 16 n. F.). Die Protokollierungspflicht bei automatischer Datenübermittlung wird eingeschränkt, soweit der Datenverkehr in genereller Weise festgelegt und dokumentiert ist (§ 17 Abs. 2 Satz 3 n. F.). In Anpassung an den Referentenentwurf eines Bundesdatenschutzgesetzes wird das Merkmal Beruf in die Kategorie der freien Daten eingestuft. Dies hat zur Folge, daß ein berechtigtes Interesse für Privatauskünfte über den Beruf nicht mehr glaubhaft gemacht zu werden braucht.

Entsprechend einer Anregung des Bundesrates sollen „die Behörden der öffentlich-rechtlichen Religionsgesellschaften" mit Rücksicht auf deren verfassungsrechtliche Stellung die gleichen Rechte auf Datenübermittlung aus dem Einwohnerinformationssystem erhalten wie die Behörden der öffentlichen Verwaltung, d. h. „soweit die Kenntnis der Daten zur rechtmäßigen Erfüllung ihrer Aufgaben erforderlich ist". Die von den Kirchen wahrgenommenen Aufgaben sind umfangreich und breitgestreut. Sie reichen von seelsorgerischen über karitative bis zu administrativen Tätigkeiten. Verfassungsrechtliche Informationsansprüche haben die öffentlich-rechtlichen Religionsgesellschaften aber lediglich zur Realisierung ihres Rechts, „auf Grund der bürgerlichen Steuerlisten nach Maßgabe der landesrechtlichen Bestimmungen Steuern zu erheben" (Art. 140 GG i. V. m. Art. 137 WRV).

Der Anschluß an das Einwohnerinformationssystem eröffnet dagegen den Zugriff auf personenbezogene Daten in einem Umfang, der weit über die zur Festsetzung und Einziehung von Kirchensteuern benötigten Angaben hinausgeht. Problematisch ist die Regelung auch deshalb, weil sie Vorbild für eine Bestimmung im Referentenentwurf eines Bundesdatenschutzgesetzes geworden ist. Danach können die Religionsgesellschaften zur Erfüllung ihrer Aufgaben Informationen aus **allen** staatlichen Datensammlungen erhalten, sofern sichergestellt ist, daß bei ihnen ausreichende Datenschutzmaßnahmen getroffen sind (§ 7 II i. d. F. vom 15. 8. 1972).

Ein so weitgehender Einbezug von Religionsgesellschaften in das staatliche Informationssystem entspricht nicht den Zielen des Datenschutzes. Mit dem verfassungsrechtlichen Gebot des Schutzes der Intimsphäre des einzelnen und der Pflicht des Staates zu weltanschaulich-religiöser Neutralität*) ist eine uneingeschränkte Einbeziehung der Kirchen in die staatsbehördliche Amtshilfe nicht vereinbar (vgl. 4.1.1.3 f und I 4.1.2 a).

Eine gleichartige Informationsabgabe an staatliche Behörden und Religionsgesellschaften jeweils „im Rahmen der . . . Erfüllung (ihrer) Aufgaben" läßt auch außer Acht, daß die Kirchen weder bei der Bestimmung ihrer „Aufgaben" noch bei deren „Erfüllung" von den parlamentarischen und gerichtlichen Regelungen und Kontrollen des Staates abhängen und deshalb — anders als staatliche Stellen — den Umfang ihrer Informationsrechte letztlich selbst bestimmen können und müssen.

2.2.2 und 2.2.3 Keine neuen Entwicklungen

2.2.4 Entwurf eines Einführungsgesetzes zum Strafgesetzbuch

Der Entwurf eines Einführungsgesetzes zum Strafgesetzbuch, für den die Bundesregierung das Gesetzgebungsverfahren erneut eingeleitet hat, unternimmt eine abschließende strafrechtliche Regelung der Verletzung von Privatgeheimnissen durch Amtsträger. Dabei wird die Geheimhaltungspflicht — über den bisher maßgeblichen materiellen Geheimnisbegriff (§ 300 StGB) hinaus — auf „Einzelangaben über persönliche oder sachliche Verhältnisse eines anderen . . ., die für Aufgaben der öffentlichen Verwaltung erfaßt worden sind" ausgedehnt.

Der Entwurf trägt damit dem zunehmenden Umfang der Sammlung und Verarbeitung personenbezogener Daten durch die Verwaltung und den entsprechend vergrößerten Mißbrauchsgefahren Rechnung und zieht die zur Vereinheitlichung gebotenen Konsequenzen aus den auf Teilgebieten wie Statistik und Datenschutz schon existierenden Vorschriften mit ähnlich weiten Schutzbereichen (amtl. Begründung, BR-Drucks. 1/72 S. 231). Der Entwurf erweitert und verbessert den Datenschutz, soweit es um das Offenbaren personenbezogener Daten durch Amtsträger geht. Andererseits läßt er die Frage offen, ob und in welchem Umfang ergänzende strafrechtliche Datenschutzvorschriften erforderlich sind, um auch andere Handlungsformen (fahrlässiges Offenbaren, unzulässiges Beschaffen) und einen weiteren Personenkreis (Privatpersonen) zu erfassen.

2.3 Ausland

2.3.1 USA

Bei der Suche nach international bedeutsamen Fortschritten in der Datenschutzgesetzgebung konzentriert sich das Interesse naturgemäß auf die Vereinigten Staaten als Land mit der größten Computerdichte und als Ausgangspunkt der Datenschutzdiskussion. Der Datenschutzbeauftragte hat deshalb die Gelegenheit eines mehrwöchigen Aufenthaltes in den USA für einen Erfahrungsaustausch mit Mitgliedern von Arbeitsstäben der Bundeslegislative (Senat) und der -exekutive (Department of Health, Education and Welfare), mit Wissenschaftlern und mit Experten der Computerindustrie sowie der EDV-Anwender genutzt.

Anknüpfungspunkte waren u. a. öffentliche Äußerungen von Prof. A. Westin, die teilweise dahingehend interpretiert und kommentiert worden waren, daß man bisher die Gefahren übertrieben habe und eine realistische Bestandsaufnahme zu keiner Beunruhigung Anlaß gebe.

Prof. Westin gilt seit Jahren in den USA als einer der ersten Experten für Fragen des Privacy-Schutzes und der sozialen Konsequenzen der neuen Informationstechnologien. Er war Leiter einer von der National Academy of Sciences durchgeführten Untersuchung über Stand und Probleme der automatisierten Führung personenbezogener Daten, deren Ergebnisse kürzlich veröffentlicht wurden*).

Aufgrund der geführten Gespräche und nach Auswertung der empirischen Befunde der genannten Studie läßt sich die Situation folgendermaßen umreißen: Der gegenwärtige Stand der Datenverarbeitung ist weniger fortgeschritten, als bisher teilweise angenommen. Viele Möglichkeiten der Informationsaufbereitung und -verknüpfung werden — obgleich technisch nicht schwierig — heute noch nicht genutzt. Konkreter Mißbrauch in großem Maße ist nicht festgestellt worden. In diesen Befunden äußert sich aber

*) (Art. 1 Abs. 1, Art. 2 Abs. 1, Art. 4 Abs. 1 GG; Leibholz/Rinck Art. 2 Anm. 3, Art. 4 Anm. 1).

*) Alan F. Westin, Michael A. Baker: Databanks in a Free Society. Computers, Record-Keeping and Privacy. New York 1972, 522 S.

keine Tendenzwende. Es müssen nur einige übertriebene Vorstellungen korrigiert werden, die eine unkritische publizistische Computerwelle hinterlassen hat. An die Stelle von Euphorie und Angst tritt die distanzierte Bewertung einer realistischen Bestandsaufnahme.

Vor einer Unterschätzung der Gefahren wird gewarnt, besonders im Bereich der Überwachungsdaten der Verbrechensbekämpfung und der Nachrichtendienste. Bezeichnend für die Einschätzung der Aktualität der Problematik ist die Forderung, nicht länger bei wissenschaftlichen Untersuchungen und publizistischen Erörterungen stehen zu bleiben, sondern gesetzgeberische Initiativen und die Einrichtung ständiger parlamentarischer Beobachtungs- und Überwachungsgremien in die Wege zu leiten. Auch die EDV-Industrie scheint diese Einschätzung zu teilen; eine Herstellerfirma hat ein Entwicklungsprogramm für Techniken und Verfahren der Datensicherung in Höhe eines achtstelligen Dollarbetrages anlaufen lassen. Die maßgebenden Experten schlagen übereinstimmend die Schaffung unabhängiger, nicht in den allgemeinen Regierungsapparat eingegliederter Kontroll- und Beschwerdeinstitutionen vor*).

Während auf Bundesebene nach dem Credit-Reporting-Act keine weiteren Gesetzgebungsinitiativen in Gang gekommen sind, gibt es auf lokaler Ebene einige projektbezogene Experimente, die ungeachtet ihres beschränkten sachlich-örtlichen Charakters von allgemeinem Interesse sind.

So wurden in der Stadt Wichita Falls, Texas, im Rahmen der Entwicklung eines Gesamt-Informations-Systems ein besonderer Datenregistrator und ein Beirat geschaffen, die an der Aufstellung und Durchführung von Grundsätzen des Datenzugriffs und -zugangs mitwirken. Der Registrator, der dem City-Manager direkt unterstellt ist, entscheidet über alle Datenanforderungen außerhalb des routinemäßigen Datenverkehrs und protokolliert Empfänger, Zweck und Umfang der Datenabgabe. Der Beirat, dessen Mitglieder vom Bürgermeister und Stadtrat (board of aldermen) ernannt werden, berät den Registrator und den Stadtrat und erarbeitet Grundsätze für den Datenzugang und ggf. für die Erweiterung der Datenbasis. Die von Februar 1972 datierende Verordnung (ordinance), die die Rechtsgrundlage für beide Institutionen darstellt, gibt außerdem dem betroffenen Bürger Einsichts- und Korrekturrechte und ordnet an, daß beanstandete Daten vorläufig aus dem Datenverkehr gezogen werden.

In Berkeley, Kalifornien, wurde — ebenfalls durch städtische Verordnung — ein gemischtes Bürgerkommitee geschaffen, dessen Mitglieder die Bereiche Polizei, Stadtrat (city-council), Bürgerrechtsorganisationen, Öffentlichkeit und Informatik repräsentieren müssen und das die Aufgabe hat, ein Mikrofilmarchiv der Kriminalfälle im Hinblick auf die Gewährleistung von Datenschutz und -sicherheit zu überwachen. Die Verordnung enthält Grundsätze über den zulässigen Inhalt der Kriminalakten — z. B. werden „nicht verifizierte Daten, wie etwa aus geheimdienstlichen Quellen", ausgeschlossen — und über zugelassene Benutzer und Verwendungszwecke (Strafjustiz, Strafverteidigung). Die von der Polizei von Berkeley gesammelten Informationen dürfen in ein Informationsaustauschsystem erst dann eingebracht werden, wenn der City-Council die technischen und administrativen Schutzmaßnahmen geprüft und für ausreichend befunden hat.

*) z. B. Westin a.a.O. S. 351 ff., Hearings before the Subcommittee on Constitutional Rights of the Committee on the Judiciary, US Senate, 92 nd Congress, Part I S. 816 ff., Arthur Miller, Hearings a.a.O. S. 18 f., Robert P. Bigelow, Hearings a.a.O. S. 685 f.

2.3.2 Kanada

In Kanada hat eine gemische Arbeitsgruppe des Kommunikations- und des Justizministeriums eine Untersuchung über die Auswirkungen der EDV auf die Privatsphäre durchgeführt*). Ihre empirischen Ergebnisse decken sich überwiegend mit denen der erwähnten US-amerikanischen Studie, mit deren Verfassern auch enger Kontakt bestand. In der Bewertung werden jedoch die Akzente etwas anders gesetzt. Die Studie kommt zu dem Schluß, daß Datensammlungen in größerem Umfang betrieben werden als in der Öffentlichkeit bekannt ist. Zwischen Polizei, Kreditauskunfteien, Versicherungen, Ausbildungsstellen und Wohlfahrtsbehörden bestehen Austauschbeziehungen, von denen die Betroffenen meist nichts erfahren. Sensitive Daten werden gegenwärtig zwar erst in geringem Umfang, jedoch mit stark steigender Tendenz automatisch verarbeitet. Die Informationssysteme sind meist noch regional begrenzt, werden aber schnell der räumlichen Ausdehnung der Trägerorganisation angepaßt und erhalten damit häufig nationalen oder auch internationalen Charakter. Eine Umfrage ergab bei den Verantwortlichen zwar eine einhellig starke Beachtung der Datenschutzfragen, aber sehr unterschiedliche Einstellungen gegenüber Vorschlägen zur gesetzlichen Regelung und Überwachung der Datenbanken.

Die Arbeitsgruppe hält die Entwicklung eines allgemeinen Rechtsbegriffs der Privacy für wünschenswert, an welchem sich die erforderlichen einzelnen Regelungsansätze auf nationaler und auf Provinzebene und auf den verschiedenen Lebensgebieten orientieren könnten. Eine einheitliche und zugleich flexible Überwachung und Durchsetzung der einzelnen Regelungen soll durch eine unabhängige Stelle in der Form einer Behörde oder eines Ombudsmans erreicht werden. Sie soll außerdem die Aufgabe erhalten, technologische Trends zu untersuchen, neue Systemkonzepte zu beurteilen und durch Berichte Regierung und Öffentlichkeit zu beraten und zu informieren. Als erster Schritt zur Regulierung des stark entwickelten Datenverkehrs über die Grenze zu den Vereinigten Staaten hinweg wird die Einrichtung eines speziellen Registers zur Diskussion gestellt.

2.3.3 Großbritannien

Der von dem Unterhausabgeordneten Huckfield 1971 und erneut 1972 eingebrachte Control of Personal Information Bill unterscheidet sich von dem Data Surveillance Bill des Abgeordneten Baker von 1969 (vgl. I 2.3.2) in wesentlichen Punkten.

*) Privacy and Computers. A Report of a Task Force established jointly by Department of Communications/Department of Justice, Information Canada, Ottawa 1972.

Der Entwurf betrifft auch manuelle Sammlungen, jedoch nur solche mit über 100 000 Personen und solche, deren Gefährlichkeit von der Regierung besonders festgestellt wurde. Der Betrieb solcher Datenbanken ist nur in dem Umfang erlaubt, wie er von einem Datentribunal besonders zugelassen worden ist. Zulassungsbedürftig ist ebenfalls die Nutzung im Ausland gelegener Datenbanken der beschriebenen Art. Das Tribunal hat weitestgehende Rechte. Es kann Schadenersatzpflichten auferlegen, Zulassungen widerrufen und die Vernichtung von Datenbeständen anordnen. Seine Durchsetzungskraft wird durch scharfe Strafsanktionen und mit Hilfe von Aufsichtsbeamten abgesichert. Materielle Grundsätze, an denen die Tätigkeit des Tribunals zu orientieren ist, sind in dem Entwurf kaum enthalten.

Mitte 1972 hat das von der Regierung eingesetzte Committee on Privacy als Ergebnis einer über zweijährigen Untersuchung einen umfangreichen Bericht über die Notwendigkeit gesetzgeberischer Maßnahmen zum Schutze der Privatsphäre gegenüber modernen gesellschaftlichen und technischen Entwicklungen vorgelegt. Der Auftrag bezog sich ausschließlich auf den privaten Sektor. Die Entwicklung innerhalb der öffentlichen Verwaltung hält man aufgrund der vorhandenen Regelungen und der parlamentarischen Kontrolle für weniger kritisch.

Die Schaffung eines allgemeinen Right of Privacy wird von der Kommission abgelehnt, vor allem weil die rechtlichen und praktischen Konsequenzen eines solchen Schrittes nicht voll überschaubar seien. Statt dessen werden für die einzelnen Lebensbereiche wie Presse, Rundfunk, Kreditagenturen, Banken, Ausbildung, Medizin usw. jeweils eine Reihe von Detailmaßnahmen vorgeschlagen. Für den Bereich der automatischen Datenverarbeitung stellt die Kommission fest, daß die Privatsphäre zwar noch nicht aktuell bedroht sei. Man müsse jedoch mit künftigen Beeinträchtigungen rechnen. Die von der Kommission aufgestellten Grundsätze, die im wesentlichen die international bekannten Datenschutzforderungen enthalten, sollen deshalb nach ihrer Auffassung zunächst freiwillig angewendet werden. Die Regierung wird aufgefordert, mit Hilfe einer unabhängigen gemischten Kommission aus EDV- und Verwaltungsfachleuten die Entwicklung gründlicher zu analysieren und geeignetere Kontrollinstrumente zu entwickeln, die dann zu gegebener Zeit eingesetzt werden könnten.

Einer Selbstkontrolle der EDV-Fachwelt durch Berufs- oder Standesregeln steht die Kommission skeptisch gegenüber. An den Gesetzentwürfen von Baker und Huckfield wird bemängelt, daß die Aufgaben und Befugnisse der darin vorgesehenen Überwachungsinstanzen nicht hinreichend durch den Gesetzgeber bestimmt seien. Dagegen wird das Modell eines betrieblichen Sicherheitsbeauftragten nach dem Vorbild des englischen Minengesetzes von 1954 als überprüfenswert angesehen.

2.3.4 Frankreich

In dem noch unveröffentlichten Jahresbericht 1969/70 des Conseil d'Etat wird die Errichtung eines Haut-Comité vorgeschlagen, das die Rechte des einzelnen und das Prinzip des freien Zuganges zur Information durch gutachtliche Stellungnahmen zu einschlägigen Gesetzesvorhaben zur Geltung bringen soll.

Ferner soll es Datenbanken mit hohem Risiko genehmigen und überwachen. Es kann zum Erlaß von Verwaltungsvorschriften ermächtigt werden.

2.3.5 Schweden

Ein umfassendes Datenschutzgesetz wird in einem von einer königlichen Kommission Mitte 1972 vorgelegten Bericht vorgeschlagen. Der Betrieb von Datenbanken mit personenbezogenen Informationen auf EDV-Basis wird danach von einer besonderen Zulassung durch eine zu schaffende Datenaufsichts-Kommission abhängig gemacht. Die Zulassung soll erteilt werden, wenn keine Gründe vorliegen, die eine übermäßige Beeinträchtigung der Privatsphäre befürchten lassen. Die Kommission kann weitreichende Auflagen erteilen. Aus gegebenem Anlaß können die Auflagen nachträglich geändert werden. Selbst die Stillegung einer Datenbank ist zulässig. Die Genehmigung bezieht sich jeweils auf ein System mit bestimmten Angaben, Zielen, Verfahren und Outputs. Bei Änderungen ist eine erneute Zulassung notwendig. Die Kommission überwacht die Einhaltung des Gesetzes und der ihr erteilten Auflagen. Durch ihre Zusammensetzung aus Parlamentariern, EDV- und Verwaltungsfachleuten soll sie sowohl sachkundig als auch in engem Kontakt mit der öffentlichen Meinung arbeiten. Der Betroffene soll das Recht erhalten, einmal pro Jahr kostenlos die über ihn gespeicherten Angaben zu erfahren. Die Verbringung von Datenbeständen ins Ausland wird verboten. Dasselbe gilt für einzelne Daten, soweit sie zum Aufbau oder zur Unterhaltung von Informationssystemen dienen können. Der Entwurf enthält außerdem Geheimhaltungs-, Straf- und Schadensersatzvorschriften.

Das in Schweden seit langem als Verfassungsgrundsatz geltende Prinzip der Öffentlichkeit von Verwaltungsakten soll durch das Datenschutzgesetz nicht geschmälert werden.

2.4 **Tendenzen der Datenschutzgesetzgebung**

Das internationale Problembewußtsein für Datenschutz ist weiter gestiegen. In der Mehrzahl der technologisch führenden Länder haben die Regierungen — in den USA die National Academy of Sciences — die Initiative ergriffen und unter Inanspruchnahme wissenschaftlichen Sachverstandes erste grundlegende und empirisch untermauerte Problemanalysen durchgeführt.

Übereinstimmend wird gefordert, die Entwicklung mit verstärkter Aufmerksamkeit zu verfolgen. Umfassende gesetzgeberische Maßnahmen werden für geboten erachtet. Im Gegensatz zur Bundesrepublik neigt man aber nicht zu einer Lösung in der Form des „all at once", sondern zu einem sachlich differenzierteren und zeitlich gestaffelten Vorgehen, das die verschiedenen Lebensbereiche je nach Dringlichkeit erfaßt.

Aus diesem Grund spielen auch institutionelle Vorschläge meist eine zentrale Rolle: Datenschutzkommissionen, -beauftragte oder Registerbehörden werden als wichtige Instrumente für Ausbau und Fortentwicklung des Datenschutzes angesehen.

Wichtige Marksteine in der Gesamtentwicklung sind die aus den USA berichteten Ansätze zur Lösung von Datenschutzfragen auf der kommunalen Ebene. Während bisher alle wesentlichen Initiativen von wissenschaftlicher und Regierungsseite ausgingen, kommen nunmehr deutliche Impulse aus der Mitte der Bevölkerung. Immer mehr Bürger erkennen, daß ihre Belange durch Datensammlung und -austausch berührt werden, und beginnen, ihre Interessen durch gezielte politische Aktivität selbst wahrzunehmen. Verstärkt sich dieses demokratische Engagement, so dürfte dies die Aussichten, daß bei der weiteren Entwicklung der EDV die humanen Bedürfnisse gegenüber technokratischen Tendenzen die Oberhand behalten, entscheidend verbessern.

In der Bundesrepublik sind entsprechende Anzeichen zwar noch weniger ausgeprägt, soweit es um automatisierte Datensammlungen geht. Jedoch sind das im Betriebsverfassungsgesetz vom 15. 1. 1972 (BGBl. I S. 13) erstmals für den privatwirtschaftlichen Sektor durchgesetzte Recht des Arbeitnehmers auf Einsicht in seine Personalakten (§ 83) und die Erstreckung der Mitbestimmung des Betriebsrats auf Personalfragebogen und vergleichbare Unterlagen (§ 94 BetrVG) ebenfalls deutlicher Ausdruck einer sich verändernden Einstellung gegenüber der Sammlung und Verarbeitung personenbezogener Informationen. Die vorgefundene Praxis wird nicht mehr unbefragt hingenommen, sondern muß sich der Kritik der Betroffenen und ihrem Anspruch auf Einflußnahme stellen.

2.4.1 Anwendungsbereich

In der Frage der sinnvollsten Absteckung des Geltungsbereichs von Datenschutzvorschriften bestehen nach wie vor sehr unterschiedliche Auffassungen. Im großen und ganzen scheint sich jedoch — entsprechend den zunehmenden Erfahrungen — eine Tendenz in Richtung auf stärker differenzierende Lösungen durchzusetzen. Die einzelnen Datenschutzmaßnahmen und -rechte werden nicht mehr pauschal im gesamten Bereich der Informationsverarbeitung eingesetzt, sondern jedes Instrument entsprechend seinen speziellen Wirkungsmöglichkeiten, Kosten und sonstigen Vor- und Nachteilen. So können etwa Geheimhaltungs- und Strafvorschriften, Auskunfts- und Berichtigungsansprüche, Protokollierungsgebote, Datenbankregister und unabhängige Überwachungsinstanzen für jeweils unterschiedlich abgesteckte Bereiche vorgesehen werden. Die Differenzierungen erfolgen nicht nur nach technischen und formalen Kategorien (etwa: manuell/automatisch, öffentlich/privat, personenbezogen/sachbezogen, intern/extern), sondern auch nach inhaltlichen Zwecksetzungen oder nach der Zugehörigkeit zu bestimmten Lebensbereichen oder Wirtschaftsbranchen (etwa: Strafverfolgung, Personalwesen, Meinungsforschungsinstitute, Adressenhandel, Gesundheitswesen, Versicherungs- und Kreditwirtschaft).

Auch die bisherige Diskussion des Referentenentwurfs eines Bundesdatenschutzgesetzes ist weithin durch das Verlangen nach stärkeren Differenzierungen gekennzeichnet. Zwar ist bei einigen Interessentengruppen das Bestreben erkennbar, jeweils so zu differenzieren, daß die eigene Branche den organisatorischen und wirtschaftlichen Belastungen des Datenschutzes entgeht. So wurde z. B. verlangt, eine bestimmte Branche oder den Datenverkehr zwischen konzernverbundenen Unternehmen generell vom Datenschutz auszunehmen. Andererseits erscheint eine Reihe von Hinweisen auf die speziellen Verhältnisse, Interessenlagen und Gepflogenheiten einzelner Bereiche durchaus begründet und wird im weiteren Gesetzgebungsgang noch näher zu prüfen sein. Die Tendenz zu stärkerer Differenzierung macht zwar das Streben nach einem umfassenden und wirksamen Datenschutz keineswegs leichter. Trotzdem liegt hier der Schlüssel zu erfolgversprechenden Strategien. Denn ebenso wie für die Datenverarbeitung selbst verstärkt sich für den Datenschutz die Erkenntnis, daß Eingriffe in eine gewachsene Informationsstruktur nur dann den gewünschten Erfolg zeitigen, wenn sie den spezifischen Verhältnissen des jeweiligen Sozialbereiches ausreichend Rechnung tragen.

2.4.2 Zielsetzung

Abgesehen vom Entwurf der Opposition im Landtag von Schleswig-Holstein behandeln die neu bekanntgewordenen Gesetzesinitiativen zu Datenschutzregelungen allein die Regelung des Persönlichkeitsschutzes. Fragen des Informationsgleichgewichts werden, sofern sie überhaupt Beachtung finden, meist in anderem sachlichem Zusammenhang, etwa mit der Parlamentsreform*) oder der Förderung des Dokumentationswesens, erörtert.

2.4.3 bis 2.4.5 Datenbankregister, Protokollierung, Rechte des Betroffenen

Auch in den neueren Entwürfen und Vorschlägen finden sich die heute schon klassischen Datenschutzforderungen nach Errichtung von Datenbankregistern, nach automatischer Protokollierung der Maschinenfunktionen und nach Ausstattung der Betroffenen mit umfassenden Kontrollrechten. Neuartige Kontrollmethoden sind nicht zur Diskussion gestellt worden. Die Phase der Suche nach geeigneten Datenschutzinstrumenten scheint abgeschlossen zu sein. Die Überlegungen konzentrieren sich nunmehr auf Auswahl und Kombination. Dabei sind neben dem Ziel maximaler Wirksamkeit heute verstärkt Fragen der Praktikabilität und der Kosten zu beachten. Es kommt darauf an, die Regelungen so zu dosieren und abzustimmen, daß sie einerseits die Kernforderungen des Datenschutzes voll erfüllen und andererseits die Datenverarbeitung weder übermäßig behindern noch zu sehr verteuern. Kosten und sonstige Nachteile müssen in einem ausgewogenen Verhältnis zu dem Zweck und den Wirkungen der Datenschutzmaßnahmen stehen. Außerdem sollten die Regelungen so beschaffen sein und in einer solchen Weise eingeführt werden, daß sie bei möglicht allen Betroffenen auf Verständnis und Zustimmung stoßen. Nur dann besteht die Gewähr, daß auch solche Bestimmungen, deren Einhaltung nicht voll kontrollierbar ist — wie etwa Datengeheimnis oder Protokollierungspflicht —, in der Praxis weitgehend befolgt werden. Aus dem Zielkon-

*) (vgl. z. B. Zwischenbericht der Enquete-Kommission, BT-Drucks. VI/3829).

flikt „wirksamer Datenschutz contra geringe Belastung der Datenverarbeitung" ergibt sich ein Zwang, die einzelnen Instrumente des Datenschutzes so einzusetzen, daß die gewünschte Wirkung mit möglichst geringer Eingriffsintensität erreicht wird. Möglichkeiten der Optimierung in diese Richtung ergeben sich aus dem sachlichen und dem funktionellen Zusammenhang der einzelnen Instrumente. Diese Zusammenhänge müssen deshalb noch wesentlich genauer als bisher untersucht werden. Ziel dieser Bemühungen muß sein, die heute noch vorherrschende Theorie und Praxis des Datenschutzes als Katalog relativ unverbundener Forderungen bzw. Maßnahmen zu ersetzen durch ein auf Wirkungszusammenhängen aufbauendes systematisches Datenschutzkonzept.

Im Zentrum eines solchen „Datenschutzsystems" wird als strukturelle Voraussetzung für individuell oder institutionell auszuübende Kontrolle die Forderung nach Transparenz zu stehen haben. Nur wer die ihn betreffenden Informationsvorgänge wahrnehmen kann, ist auch in der Lage, seine Interessen geltend zu machen. Transparenz kann außer durch die Einrichtung eines Registers auch durch die Publikation der Datenkataloge und Datenflüsse hergestellt werden. Welches Instrument bevorzugt wird, hängt zunächst von der Einschätzung seiner Leistungsfähigkeit ab, außerdem davon, wie sich eine Registerstelle in die übrigen institutionellen Maßnahmen des Datenschutzes einpassen läßt.

Die Durchschaubarkeit des automatisierten Informationswesens ist aber nicht nur Voraussetzung für die Ausübung der Kontrollrechte; sie unterstützt und verstärkt auch deren Wirkungen. Je offener sich die Entwicklung der EDV vor den Augen des Bürgers und der verschiedenen an der Verwaltungskontrolle beteiligten Institutionen vollzieht, um so mehr werden die Systementwickler und -anwender schon von sich aus die Interessen der Betroffenen berücksichtigen. Nachträgliche Einzelfallkontrollen sind dann in erheblich geringerem Falle notwendig. Daraus wird zugleich deutlich, daß Transparenz kein Selbstzweck ist und nicht isoliert als alleiniges Instrument eingesetzt werden kann. Denn ihre präventive Funktion entfaltet sie gerade im Hinblick auf die im Hintergrund stehenden konkreten Kontroll- und Sanktionsmöglichkeiten.

Ein funktioneller Zusammenhang besteht auch zwischen den Rechten des Betroffenen und den Aufgaben einer Überwachungsinstanz. Beide haben das Ziel einer stärkeren Berücksichtigung der Interessen der Betroffenen, wobei einmal individuelle, das andere mal mehr gesellschaftliche oder Gruppeninteressen im Vordergrund stehen. Daraus wird folgen, daß institutionelle Kontrolle ihren Ort vor allem da hat, wo die unmittelbare Kontrolle durch die Betroffenen nicht funktioniert. Dies betrifft etwa das gesamte Informationsgebaren der Kriminalpolizei und der Nachrichtendienste, wo den Betroffenen aus taktischen Gründen keine Einsichts- und Korrekturrechte eingeräumt werden. Aber selbst wenn das Gesetz dem Einzelnen das rechtliche Instrument zur individuellen Interessenwahrung zur Verfügung stellt, kann eine institutionelle Ergänzung notwendig sein, etwa weil die Informationsprozesse den Betroffenen oft verborgen bleiben (z. B. bei Versicherungs- und Kreditinformation) oder weil der betroffene Personenkreis seine Rechte aus Unsicherheit oder Angst nicht wahrnimmt (untere Sozialschichten, z. B. Sozialdatenbank).

Die beschriebenen Interdependenzen lassen ausreichenden Spielraum für die Erarbeitung von Kompromissen in einigen aus wirtschaftlich-pragmatischen Gesichtspunkten bisher besonders kontroversen Fragen.

Eine von der EDV-Praxis aus Kostengründen abgelehnte Forderung betrifft die Benachrichtigung der Betroffenen von den über sie gespeicherten Daten. Die Einzelauskunft auf Anforderung des Betroffenen ist, jedenfalls bei Daten, die ohne Kenntnis des Betroffenen in die Datenbank gelangt sein können, unentbehrlich, da sie die einzige Möglichkeit darstellt, zu kontrollieren, ob die Datensammlung im Einzelfall vollständig und richtig ist. Es dürfte sich aber im allgemeinen als überflüssig erweisen, darüber hinaus die Datenbanken zur periodischen Zusendung individueller Datenauszüge an die Betroffenen zu verpflichten. Die in erster Linie davon erhoffte präventive Kontrolle läßt sich mit wesentlich geringeren Kosten auf anderem Wege herstellen. Die Betroffenen können zum Gebrauch ihrer individuellen Auskunftsrechte auch in der Weise in die Lage versetzt werden, daß ihnen Art und Umfang der Datensammeltätigkeit in allgemeiner Form zur Kenntnis gebracht wird, z. B. durch entsprechende Veröffentlichungen und/oder Eintragungen in öffentlichen Registern. Allerdings muß dieses Modell, da die präventive Kontrolle weniger ausgeprägt ist, durch eine institutionell ausgeübte Überwachung ergänzt werden, welche die Vollständigkeit und Richtigkeit der Publikationen sicherstellt. Die Aufteilung der Kontrolle zwischen Betroffenen und Überwachungsinstanz erfolgt also im Grundsatz so, daß ersterer die konkreten Dateninhalte, letztere die gespeicherten Informationskategorien und die Eigenschaften der Austauschkanäle abdeckt, wobei erstere punktuell-stichprobenweise, letztere umfassend und durchgehend ausgeübt wird.

Nach dem gleichen Prinzip kann auch der für die Protokollierung und Auskunftserteilung über Datenübermittlungen an andere Stellen erforderliche Aufwand entscheidend gesenkt werden. Derjenige Bereich des Datenverkehrs, der zur Routine zählt, könnte nach Datenempfängern und jeweils in Frage kommenden Datenarten in allgemeiner Form dokumentiert und publiziert werden, so daß jedermann den ihn betreffenden Informationsfluß abschätzen kann. Datenabgaben außerhalb des Routinebereichs wären dagegen konkret nach Datenart, Inhalt und Empfänger zu protokollieren und auf Anfrage mitzuteilen. Auch diese Abschichtung steht jedoch unter dem Vorbehalt, daß eine Kontrollinstanz die Einhaltung der dargelegten Grundsätze gewährleistet. In bestimmten Routinebereichen, insbesondere wo auch Daten höherer Empfindlichkeit erfaßt werden (z. B. Kriminalpolizei), sollte man freilich nur auf die besonders aufwendigen Aufbereitungsarbeiten verzichten, die erforderlich sind, um jederzeit gezielte Auskünfte aus dem Protokoll geben zu können. Dagegen sollte man die vergleichsweise einfache Protokollierung selbst beibehalten, um die Rekonstruierbarkeit aller Abrufe zum Zwecke von

Stichproben oder aus Anlaß konkreter Nachprüfungen sicherzustellen.

Unzutreffend ist der gegenüber den Ausführungen im Ersten Tätigkeitsbericht (I 2.4.4) erhobene Einwand, eine Protokollierung sei funktionslos, weil bereits durch Programme (Berechtigungstabellen, Paßwort-Strukturen) sichergestellt werden könne, daß Daten immer nur im Umfang der bestehenden Berechtigung abgerufen werden. Er läßt außer Acht, daß sich der Umfang einer Berechtigung stets nur nach abstrakten Merkmalen (Datenfeld, regionaler Bereich, Größenklassen usw.) programmieren läßt. Auf diese Weise werden lediglich die Außengrenzen eines Bereichs festgelegt, den ein Systembenutzer jedenfalls nicht überschreiten darf. Das heißt aber nicht, daß eine materielle Berechtigung zum jederzeitigen Abruf aller innerhalb dieser Grenzen liegenden Daten besteht. So würde der Bedienstete eines Sozialamtes etwa programmgesteuert Zugriff auf die Wohngelddaten seiner Gemeinde erhalten — und umgekehrt der des Wohnungsamtes auf bestimmte Sozialleistungsdaten —, damit er im Bewilligungsverfahren die entsprechenden Leistungen berücksichtigen kann.

Eine materielle Abrufberechtigung steht dem Bediensteten aber nicht bezüglich aller Wohngeld- bzw. Sozialhilfeempfänger zu, sondern nur bezüglich solcher Personen, die Antrag auf Sozialhilfe bzw. Wohngeld gestellt haben. Die Prüfung dieser Voraussetzung ist nicht programmierbar. Ihre Beachtung läßt sich nur auf dem Wege über die Protokollierung der Datenabrufe kontrollieren. Auch beim Erkennen und Aufklären von manipulativen Versuchen der Umgehung oder Änderung der Berechtigungsprüfungsprogramme spielt die Protokollierung eine entscheidende Rolle.

Ob diese Gesichtspunkte den Protokollierungsaufwand rechtfertigen, läßt sich nicht allgemein entscheiden. Maßgeblich sind Umfang und Schwere der Mißbrauchsgefahren, die sich vorwiegend aus dem Charakter der betroffenen Daten, aus den jeweiligen Möglichkeiten der programmgesteuerten Berechtigungszuweisung und -prüfung und aus dem potentiellen Mißbrauchsinteresse ergeben.

2.4.6 und 2.4.7 Keine neuen Entwicklungen

3. DIE DATENVERARBEITUNG IN DER ÖFFENTLICHEN VERWALTUNG DES LANDES HESSEN

3.1 Bestandsaufnahme

Die aufgrund des Kabinettsbeschlusses vom 6. 7. 1971 veranlaßte Bestandsaufnahme wurde durch den Eingang der Meldungen der Ressorts und sonstigen Stellen bis Februar 1973 fortgeschrieben.

Während es im Februar 1972 noch rund 1 200 Gemeinden gab, reduzierte sich ihre Zahl bis Februar 1973 auf 874. Von den 1 200 Gemeinden des Jahres 1972 hatten 216 über elektronische Datenverarbeitung berichtet. 1973 sind es, trotz der gesunkenen Gesamtzahl der Gemeinden, 306, wobei festzustellen ist, daß es sich in erster Linie um Gemeinden mit einer größeren Einwohnerzahl handelt. 1972 hatten neben den Gemeinden noch weitere 70 Stellen und Körperschaften des öffentlichen Rechts Meldungen vorgelegt; 1973 waren es 124 sonstige Stellen, so daß — zusammen mit den 306 Gemeinden — 430 Meldungen vorliegen.

Für diese 430 Stellen werden z. B. im Einwohner-, Finanz-, Personal-, Gesundheits-, Sozial- und Bildungswesen z. Z. 160 Aufgaben der EDV zugeführt. Fast alle Stellen nehmen die EDV im Einwohnerwesen, Finanzwesen oder Personalwesen in Anspruch. Es gibt aber auch größere Gemeinden, die alle hier genannten und weitere Aufgaben bereits durch die elektronische Datenverarbeitung erledigen.

Im Einwohnerwesen sind heute schon die maschinelle Auswertung für statistische Zwecke und die Fortschreibung des Bevölkerungsstandes möglich. Außerdem sind der Aufbau einer Einwohnerdatenbank, die maschinelle Erstellung der Lohnsteuerkarten, die Wehrerfassung, die Erstellung der Wahlverzeichnisse u. a. mehr vorgesehen.

Von den vorliegenden rund 1 000 Erfassungsbögen, Lochkarten und anderen Datenträgern, enthalten nach wie vor etwa 50 % personenbezogene Daten. Von den übrigen Daten wird im Falle einer Integration ein großer Teil durch Verbindung mit personenbezogenen Daten, so z. B. mit Daten im Einwohner-, Finanz-, Gesundheits-, Sozial- und Bildungswesen, besonders schutzbedürftig.

3.2 Beurteilung der Bestandsaufnahme

Die vorgelegten Berichte sind nach wie vor lückenhaft. Dies dürfte in erster Linie darauf zurückzuführen sein, daß den beteiligten Stellen nicht klar ist, wie weit der Anwendungsbereich des Datenschutzes reicht.

Der Wirkungsradius ist weniger in den formellen Abgrenzungskriterien der §§ 2 und 3, als vielmehr in der Aufgabenbeschreibung in § 10 festgelegt (vgl. 4.1.2.1).

Die Bestandsaufnahme hat nicht die statistische Erfassung zum Ziel, sondern soll einen Überblick über die Ausbreitung der maschinellen Datenverarbeitung in Hessen geben und aufzeigen, wo, in welchen Verwaltungsbereichen und welchen Zeiträumen sich die schon erkennbare Entwicklung zur Integration der Datenverarbeitung vollzieht. Nur auf dieser Grundlage kann der Datenschutzbeauftragte präventiv wirken.

So ist z. B. dem Datenschutzbeauftragten durch die Auswertungen der Meldungen bekannt geworden, daß eine Kriminalpolizeibehörde ein Service-Unternehmen für die Ablochung kriminalpolizeilicher Daten in Anspruch nimmt. Wegen der hiergegen bestehenden Bedenken vgl. 4.1.1.3 d.

Eine Zeitungsmeldung über den Brand der EDV-Anlage einer Universitätsklinik veranlaßte den Datenschutzbeauftragten, sich an Ort und Stelle zu informieren. Die zur Leistungsabrechnung (Krankenhausaufenthalt und Krankenhausbehandlung) benutzte Anlage war ihm bis zu diesem Zeitpunkt nicht gemeldet.

Von Betriebskrankenkassen liegen bis heute keine Meldungen vor, obwohl inzwischen bekannt ist, daß einige dieser Stellen Datenerfassung oder Datenübermittlung durch EDV erledigen. Die Bestandsaufnahme kann erst abschließend behandelt werden, wenn alle Unterlagen der Stellen vorliegen, die nach § 1 DSG zur Meldung verpflichtet sind.

4. AUFGABEN UND TÄTIGKEITEN DES DATENSCHUTZBEAUFTRAGTEN

4.1 Der Schutz des Persönlichkeitsrechts

Die im Ersten Tätigkeitsbericht erörterten Probleme standen im Berichtszeitraum weiterhin im Mittelpunkt. Erkenntnisse und Erfahrungen aus der Gesetzgebung und aus der Verwaltung haben neue Blickpunkte für die Beurteilung der Problematik eröffnet.

4.1.1 Der Umgang mit personenbezogenen Daten

Die maschinelle Datenverarbeitung kann das Persönlichkeitsrecht des Bürgers besonders dann gefährden, wenn personenbezogene Daten oder die Ergebnisse ihrer Verarbeitung von der datenermittelnden Behörde an andere Behörden, Stellen oder Datenbanken weitergegeben oder in Informationssysteme eingebracht werden. Daher ist der Grundsatz allgemein anerkannt, daß personenbezogene Daten — mit Ausnahme der öffentlich-bekannten —, die den Betroffenen identifizieren oder die in der Zusammensetzung mit anderen Daten die Rückidentifizierung des Betroffenen ermöglichen, nicht oder nur mit seinem Einverständnis oder Kraft gesetzlicher Vorschrift weitergegeben werden dürfen.

Dieser Grundsatz hat sich auch in dem Entwurf eines Bundesdatenschutzgesetzes, der im Bundesinnenministerium erstellt worden ist — §§ 7, 18, 23, 24 —, niedergeschlagen. Das Datenschutzgesetz trägt diesem Grundsatz in §§ 2 und 5 Rechnung.

Die offenbar zu knappe Darstellung in 4.1.1 des Ersten Tätigkeitsberichtes hat zu Mißverständnissen geführt (vgl. die Stellungnahme der Landesregierung in LT-Drucks. 7/1705 unter III, 7 Abs. 2). Deswegen und wegen der grundlegenden Bedeutung des § 5 DSG ist es geboten, den Inhalt dieser Vorschrift klarzustellen.

1. **§ 5 Abs. 1** gestattet, Unterlagen, Daten und Ergebnisse an Datenbanken und Informationssysteme sowie für statistische Zwecke ohne Rücksicht auf ihren Inhalt weiterzugeben. Diese Regelung ergänzt einerseits § 2, wonach Einsicht, Abruf, Änderung oder Vernichtung der Unterlagen, Daten und Ergebnisse nur dem „Befugten" gestattet werden dürfen;

   andererseits § 5 DVG, wonach der „Zugriff" auf Datenbestände, die in der HZD oder in den KGRZ gespeichert sind, nur demjenigen Mitglied oder dem Auftraggeber gewährt werden darf, von welchem die Datenbestände stammen.

   Auch diese Vorschrift für den Aufbau von Datenbanken und Informationssystemen steht unter dem — nicht ausdrücklich genannten — Vorbehalt, daß nicht höherrangige Normen die Weitergabe verbieten.

2. **§ 5 Abs. 3** stellt — anders als Abs. 1 — auf den Inhalt der Daten und Datenbestände ab, nämlich auf deren Identifikationsqualitäten.

   Unter den in Abs. 3 genannten Voraussetzungen können Datenbestände auch an Empfänger außerhalb der in § 1 DSG genannten Stellen weitergegeben oder auch veröffentlicht werden.

   Diese Vorschrift beruht auf dem für den Datenschutz allgemein gültigen Grundsatz, daß Daten und Datenbestände, die Einzelangaben über natürliche oder juristische Personen enthalten oder Rückschlüsse auf solche Einzelangaben zulassen (Identifizierung oder Rückidentifizierung) grundsätzlich weder veröffentlicht noch weitergegeben werden dürfen. § 5 Abs. 3 gilt nicht nur, wie die Überschrift der Vorschrift vermuten läßt, für Datenbanken und Informationssysteme.

4.1.1.1 Verschwiegenheitspflicht und EDV

Die potentielle Bedrohung des Persönlichkeitsrechts durch die maschinelle Datenverarbeitung darf weder übertrieben noch unterschätzt werden. „Der Computer ist nicht die Wurzel der persönlichkeitsrechtlichen Datenschutzprobleme, sondern er trägt zur Verschlimmerung des status quo bei"*). Untersucht man den Ablauf der maschinellen Datenverarbeitung unter dem Blickpunkt möglicher Gefährdungen, so wird deutlich, daß es anderer als der herkömmlichen Mittel der öffentlichen Verwaltung bedarf, damit der Bürger vor dem Mißbrauch der über ihn gesammelten Informationen den gleichen — oder einen besseren — Schutz erhält, als ihn das Amtsgeheimnis und die Verschwiegenheitspflicht der Bediensteten gewähren:

a) Der Beamte ist nach § 75 HBG verpflichtet, „über die ihm bei seiner amtlichen Tätigkeit bekannt gewordenen Angelegenheiten Verschwiegenheit zu bewahren"**). Diese Vorschrift geht von der herkömmlichen Arbeitsmethode aus, wonach der Beamte seine vertraulich zu behandelnden Kenntnisse durch Übermittlung in der natürlichen Sprache erwirbt, in dieser Weise in Akten oder Karteien sammelt, verarbeitet und mündlich oder schriftlich weitergibt. Wer die natürliche Sprache beherrscht und auf die Sammlungen in Akten oder Karteien zugreifen kann, ist befähigt, sich die darin enthaltenen Informationen zu eigen zu machen. Die maschinelle Datenverarbeitung schafft einen grundsätzlich anderen Sachverhalt: In Datenträger „Einblick" zu nehmen und Informationen daraus zu gewinnen, erfordert andere Voraussetzungen als die Informationsvermittlung herkömmlicher Art: Nur wer den Lochcode versteht, mit welchem die Daten auf den Lochkarten oder Lochstreifen erfaßt sind, erhält die darauf festgehaltene Information. Die

*) L. Baskir, zitiert nach Seidel in ÖVD 5/72, S. 216 f.

**) Für die Angestellten im öffentlichen Dienst gilt nach § 9 BAT in etwa das Gleiche.

natürliche Sprache wird nur für die Unterlagen, die für die Zwecke der maschinellen Datenverarbeitung hergestellt werden, benutzt, sofern nicht auch hier schon selbstregistrierende Datenverarbeitungseinrichtungen verwendet werden. Sind die Informationen an die Speicher der Datenverarbeitungsanlagen abgegeben, dann hat Zugang zu den Informationen nur, wer das Programm für die Speicherung und für den Arbeitsablauf der Maschine kennt und beeinflussen kann. Der Beamte erlangt daher während wesentlicher Abläufe der maschinellen Datenverarbeitung keine Kenntnis von dem gedanklichen Inhalt der erfaßten, gespeicherten oder verarbeiteten Daten. Demnach wird dieser Sachverhalt von der Pflicht zur Verschwiegenheit gar nicht erfaßt.

b) Darüber hinaus ist die Verschwiegenheitspflicht in § 75 HBG so eng eingegrenzt, daß für den Persönlichkeitsschutz wesentliche Bereiche herausfallen. Die Verschwiegenheitspflicht gilt nicht „für Mitteilungen im dienstlichen Verkehr oder über Tatsachen, die offenkundig sind oder ihrer Bedeutung nach keiner Geheimhaltung bedürfen". Die Aufhebung der Verschwiegenheitspflicht zugunsten des dienstlichen Verkehrs verlagert die Problematik auf die Frage, inwieweit der Persönlichkeitsschutz die Amtshilfe einschränkt (vgl. I 4.1.2 b). Die Amtshilfe, zu der Art. 35 Abs. 1 GG die Behörden des Bundes und der Länder untereinander verpflichtet, wird als eine gegenseitige Hilfeleistung verstanden, durch welche die ersuchende Behörde in den Stand versetzt wird, die ihr obliegende Aufgabe zu erfüllen. Eine ins Einzelne gehende Definition des Begriffs der Amtshilfe umgeht auch — aus verfassungsrechtlichen Gründen — der Entwurf eines Verwaltungsverfahrensgesetzes (BR-Drucks. 227/73). Die Frage, welche Voraussetzungen für ein Ersuchen um Amtshilfe gegeben sein müssen oder welche Umstände einem Rechtshilfeersuchen entgegenstehen können, wird nur unter verfahrensrechtlichen und verwaltungsbezogenen Gesichtspunkten beantwortet. Die Auswirkungen der Amtshilfe auf den „betroffenen" Bürger bleiben im genannten Entwurf unberücksichtigt*), obwohl es bereits erste Ansätze dafür gibt, das Persönlichkeitsrecht des Bürgers in die Prüfung, ob ein Amtshilfe-(Rechtshilfe-)ersuchen rechtmäßig ist, einzubeziehen: So ist die Überlassung gerichtlicher Ehescheidungsakten an den Untersuchungsführer in einem Disziplinarverfahren als Eingriff in das Persönlichkeitsrecht der Ehegatten gewertet worden, weil Ehescheidungsakten im Hinblick auf ihren Inhalt der Geheimhaltung nach Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG unterliegen und beide Ehepartner gemeinsam Anspruch auf diesen Schutz haben**). Dieser Fall illustriert, wie schon im herkömmlichen Verfahren der Rechts- und Amtshilfe die Zusammenführung von Informationen aus verschiedenen Lebensbereichen Konflikte mit der Verpflichtung der staatlichen Gewalt, die Würde des Menschen zu achten (Art. 1 Abs. 1 GG), herbeiführen kann. In außerordentlich verstärktem Maße gilt dies für die elektronische Datenverarbeitung.

Hieraus ergibt sich, daß in einer automatisierten Verwaltung die beamtenrechtliche Verschwiegenheitspflicht wegen der Ausnahme für „Mitteilungen im dienstlichen Verkehr" den beabsichtigten Zweck verfehlt, den Bürger davor zu schützen, daß die behördlichen Informationen über seine Person zweckentfremdet oder sonst mißbräuchlich verwendet werden.

Gleiches gilt für die weitere Ausnahme von der Verschwiegenheitspflicht hinsichtlich der Tatsachen, die ihrer Bedeutung nach keiner Geheimhaltung bedürfen. Dies zu beurteilen kann einem Bediensteten nur zugemutet oder überlassen werden, wenn und soweit die Tatsache (das Datum) eine Einzelinformation bleibt und bekannt ist, für welche Zwecke sie verwendet wird. Beim Fernabruf gespeicherter Daten und bei ihrer Auswertung zu verschiedenen Zwecken kann jedoch eine Information über eine einzelne Tatsache vom Blickpunkt des Persönlichkeitsschutzes aus die Qualität einer „geheimhaltungsbedürftigen" Information erhalten, z. B. wenn medizinisch-diagnostische Individualdaten durch Fernabruf Personen bekannt werden, für die sie nicht bestimmt sind oder vor denen sie geheimgehalten werden sollten; oder wenn Daten über die Zugehörigkeit zu einer Kirche oder zu einer Weltanschauungsgemeinschaft mit Daten einer Sozialdatenbank (etwa der Datenbank der Bundesanstalt für Arbeit) zusammengeführt werden und dadurch ermöglicht wird, diese Daten für oder gegen bestimmte Bevölkerungsgruppen oder auch Einzelpersonen auszuwerten.

c) Der Vergleich der herkömmlichen Verwaltungstätigkeit mit der automatisierten Verwaltung zeigt, daß der Mensch hier als Träger der Verschwiegenheitspflicht weitgehend ausgeschaltet ist. Daher kann die Vertraulichkeit von Informationen mit dem Mittel der Amtsverschwiegenheit nur bei der Datenermittlung und bei der Weitergabe der durch die Datenverarbeitung gewonnenen Ergebnisse geschützt werden. Bei den anderen, wesentlichen Phasen der Datenverarbeitung versagt die Verschwiegenheitspflicht; dies gilt auch für die Weitergabe, wenn sie nicht manuell, d. h. durch Übergabe der ausgedruckten Ergebnisse, an einen anderen, sondern durch Fernabruf erfolgt. Insofern bietet zwar die maschinelle Datenverarbeitung gegenüber der herkömmlichen Sammlung von Informationen in Karteien, Akten und dgl. einen erhöhten Schutz der Vertraulichkeit, weil die Informationen wie in einem Safe verschlossen sind, zu dem nur Zugang hat, wer die Maschinensprache beherrscht und über die Maschine verfügt. Andererseits eröffnet der Computer neue Gefahrenquellen, vor allem den Mißbrauch der Informationen durch die

*) Ähnlich Podlech, Verfassungsrechtliche Probleme öffentlicher Informationssysteme in Datenverarbeitung im Recht Band I, Heft 2—3, S. 155
und Seidel, Datenbanken und Persönlichkeitsrecht, S. 155.

**) BVerfGE 27, 344; Leibholz/Rinck Art. 2 GG Anmerkung 9 q.

unerlaubte Beeinflussung des Verarbeitungsablaufs. Neben der Gefahr des Vertrauensbruchs durch Mitteilung personenbezogener Informationen an Unbefugte tritt die Gefahr der mißbräuchlichen Verwendung der Informationen, die entweder der Bürger für bestimmte und für ihn erkennbare Zwecke aus seinem persönlichen Lebensbereich der Verwaltung gegeben hat, oder die aus dem Verwaltungsvollzug für bestimmte gesetzlich festgelegte Zwecke anfallen. Datenschutz bedeutet daher in diesem Zusammenhang, den rechtmäßig programmierten Ablauf des Datenverarbeitungsvorgangs sichern und einer „Zweckentfremdung" der Daten vorbeugen. Es muß verhindert werden, daß Bedienstete, die für den Ablauf des Datenverarbeitungsvorganges verantwortlich sind, ihn willkürlich verändern. Dazu dienen sowohl technische Sicherungen und Kontrollen als auch personelle und organisatorische Maßnahmen.

Die Gefährdung des Persönlichkeitsrechts ist um so größer, je mehr individualisierende Daten in den Verarbeitungsvorgang eingebracht werden und je weiter die Verbindung von Dateien verschiedener Lebensbereiche zu einer Datenbank oder zu einem Informationssystem fortschreitet. Die Gefährdung wird am wirksamsten verringert, wenn man ihre Quellen verstopft. Im Hinblick auf den Schutz des Persönlichkeitsrechtes bedeutet dies eine sorgfältige Auswahl der personenbezogenen Daten schon bei der Datenermittlung, um alle überflüssigen Daten, die für den Zweck der Datenverarbeitung, d. h. für die Verwaltungsaufgabe nicht benötigt werden, von vornherein auszuschalten.

Insoweit hat sich die Problematik, die im Hinblick auf die Bundesgesetzgebung unter 4.1.1.1 und 4.1.1.2 im Ersten Tätigkeitsbericht dargestellt ist, nicht verändert, allenfalls verschärft. Denn die Bemühungen der Bundesregierung, die Leistungsmöglichkeiten der öffentlichen Verwaltung dadurch zu steigern, „daß in zunehmendem Maße auf Unterlagen zurückgegriffen werden kann, die bereits für andere Verwaltungszwecke oder für wissenschaftliche Aufgaben auf Datenträgern gespeichert sind"*), werden sich verstärken. Der technische und organisatorische Weg hierzu führt zur Errichtung umfassender Datenbanken, die zur Benutzung für die vielfältigen Zwecke der Verwaltung bereitgehalten werden.

An einem Modell aus dem Landesbereich kann das Prinzip der integrierten Datenverarbeitung erläutert werden: Während bisher anfallende Daten über den Verlust oder die Aberkennung des Wahlrechts einzelner Einwohner in einer besonderen Kartei beim Wahlamt der Gemeinde geführt werden, wird künftig mit der Automation der Verwaltungsaufgaben im Einwohnerwesen diese Wahlrechtskartei mit den Karteien anderer Ämter, etwa des Einwohnermeldeamtes, der Lohnsteuerkartenstelle und dgl., zu einer Gesamtdatei (Datenbank) zusammengeführt. Werden keine technischen oder organisatorischen Schutzmaßnahmen getroffen, so könnte jeder, der befugt ist, bestimmte einzelne Informationen über einen Bürger abzufragen, automatisch dessen sämtliche Daten (ein Persönlichkeitsprofil) aus der Gesamtdatei erhalten, also auch — um in dem gewählten Beispiel zu bleiben — erfahren, daß der Betroffene von der Wahl zu den Parlamenten (Bundestag, Landtag, Gemeindevertretung) ausgeschlossen ist und daß er die Fähigkeit zur Bekleidung öffentlicher Ämter verloren hat.

Hiermit soll nicht die Zweckmäßigkeit und die Notwendigkeit dieser Entwicklung in Frage gestellt, sondern nur verdeutlicht werden, wie notwendig es ist, die zunehmende Automation der Verwaltung mit Maßnahmen zu flankieren, die geeignet sind, den Persönlichkeitsschutz des Bürgers zu gewährleisten. Nur auf diese Weise können Konfliktsituationen, die eine ungezügelte technische Entwicklung auslösen kann, rechtzeitig vermieden werden. Das hessische Datenschutzgesetz macht den Versuch, die in der Wissenschaft weltweit diskutierten rechtlichen und gesellschaftspolitischen Probleme der elektronischen Datenverarbeitung in der öffentlichen Verwaltung und im Verhältnis Parlament - Regierung in praktikable Maßnahmen aufzulösen. Dieser Versuch darf jedoch nicht auf ein Land begrenzt bleiben. Wegen der weitgehenden Verflechtung der öffentlichen Verwaltungen der Länder und des Bundes untereinander, z. B. im Beamten- und Angestelltenrecht, in der Frage der Amtshilfe, muß der erste Schritt, den Hessen getan hat, von den anderen Ländern nachvollzogen und weitergeführt werden, wenn nicht der Bundesgesetzgeber dazu imstande ist.

4.1.1.2 Bundesrechtliche Regelungen

Für die Bereiche der Krankenversicherung, der Rentenversicherung und für die Bundesanstalt für Arbeit hat der Bundesgesetzgeber die rechtliche Voraussetzung dafür geschaffen, daß deren Informationsbedürfnis mit der Abgabe nur einer Meldung befriedigt werden kann*). Dies wird erreicht durch die Vergabe einer Versicherungsnummer, durch die Einführung der maschinell lesbaren Versicherungskarte, durch die Zulassung maschinell verwertbarer Datenträger und durch die Verpflichtung der Sozialversicherungsträger, die Daten untereinander auszutauschen.

Nach der DEVO sind von den auf Vordrucken zu erstattenden Meldungen der Arbeitgeber u. a. folgende individuelle Daten auf maschinell ver-

*) Bundesminister Genscher in seiner Ansprache zur Festveranstaltung am 14. 11. 1972 anläßlich der 100-jährigen Wiederkehr der Errichtung eines zentralen statistischen Amtes in Deutschland — Sonderdruck des Statsitischen Bundesamts, Wiesbaden, S. 5.

*) Drittes Rentenversicherungsänderungsgesetz vom 28. 7. 1969 (BGBl. I S. 956),

Gesetz zur Weiterentwicklung des Rechtes der gesetzlichen Krankenversicherung vom 10. 8. 1972 (BGBl. I S. 1433),

Datenerfassungs-Verordnung (DEVO) vom 24. 11. 1972 (BGBl. I S. 2159),

Datenübermittlungs-Verordnung (DÜVO) vom 15. 12. 1972 (BGBl. I S. 2482).

wertbaren Datenträgern aufzunehmen (§ 14 a.a.O.):

Die Versicherungsnummer, die der Arbeitnehmer erhalten hat,

seine Staatsangehörigkeit, sein Familienstand, die Anzahl der Kinder, der Beginn der Beschäftigung, die Beitragsgruppe,

verschlüsselte Angaben über die Beschäftigung oder Tätigkeit, über die Stellung im Beruf, über die Ausbildung,

das beitragspflichtige Brutto-Arbeitsentgelt, die Betriebsnummer.

Gegenüber dem herkömmlichen Verfahren begründet die Einführung der elektronischen Datenverarbeitung neuartige Mißbrauchsgefahren sowohl im Bereich der Arbeitgeber als auch bei den Trägern der Sozialversicherung (vgl. 4.1.1.3 d und I 1.2.3). Jeder Mißbrauch der Individualdaten gefährdet das Persönlichkeitsrecht des Versicherten. Die bundesrechtliche Regelung läßt jedoch einen hinreichenden Datenschutz vermissen. Die Datenerfassungs-Verordnung beschränkt sich in § 14 darauf, den Träger der gesetzlichen Rentenversicherung zu verpflichten, „die Daten entsprechend dem jeweiligen Stand der Technik zu sichern und vor unberechtigtem Zugriff zu schützen". Der Verpflichtung, den grundrechtlichen Schutz des Persönlichkeitsrechts zu gewährleisten, kann sich der Bundesgesetzgeber nicht dadurch entledigen, daß er die Verpflichtung den Sozialversicherungsträgern auferlegt; vielmehr hätte er selbst Mindestmaßnahmen vorschreiben müssen, etwa die Anonymisierung der Individualdaten, ihre getrennte Verwahrung oder andere Maßnahmen, die verhindern, daß Unbefugte Kenntnis vom „Versicherungsverlauf" des einzelnen Versicherten erhalten; er hätte den Sozialversicherungsträgern nur die weitere Ausgestaltung überlassen dürfen. Es fehlen auch Vorschriften, die den Versicherten davor schützen, daß der Arbeitgeber die auf maschinenlesbaren Datenträgern gespeicherten Individualdaten seiner Arbeitnehmer mißbräuchlich verwendet.

Die Vorschriften der Datenübermittlungs-Verordnung über „Datensicherung durch den Arbeitgeber" (§ 10) und „Datensicherung bei den Trägern der Krankenversicherung" (§ 14) bezwecken ebenfalls keinen Datenschutz. Durch sie soll lediglich die Richtigkeit der Daten und der für die Übermittlung der Daten bestimmten Programme gewährleistet und der Verlust von Versicherungsunterlagen verhindert werden.

Die beiden Verordnungen berücksichtigen nicht die vorangegangene Entschließung des Deutschen Bundestages vom 21. 6. 1972 (Umdruck Nr. 300), in der die Bundesregierung ersucht wird,

> „sicherzustellen, daß bei der Verwendung von Versicherungsnummern in der Sozialversicherung die Privatsphäre der Versicherten und der mitversicherten Familienangehörigen nicht beeinträchtigt wird. Dabei ist bei personenbezogenen Informationen über gesundheitliche Verhältnisse von der Notwendigkeit eines erhöhten Datenschutzes auszugehen, damit eine mißbräuchliche Verwendung ausgeschlossen wird."

Dies ist ein weiteres Beispiel dafür, daß in der Bundesgesetzgebung die Grundvorstellung des Datenschutzes als eine Einrichtung zum Schutz des Bürgers vor Eingriffen in sein Persönlichkeitsrecht nicht oder nicht genügend verwirklicht wird. An diesem Beispiel eines umfassenden Datenaustauschsystems erweist sich erneut die Notwendigkeit, den Datenschutz auch bundesgesetzlich zu regeln.

4.1.1.3 Aus dem Bereich der Landesverwaltung:

a) Die vom Koordinierungsausschuß eingesetzte Arbeitsgruppe Datenschutz hat im Berichtszeitraum **„Richtlinien zur Gewährleistung des Datenschutzes und der Datensicherheit im Datenverbund (DASCH)"** ausgearbeitet (vgl. I 4.3.1). Die darin empfohlenen Maßnahmen und Anweisungen dienen vornehmlich der Datensicherung (vgl. 4.3). Sie werden für die Teilnehmer am hessischen Datenverbund, die Hessische Zentrale für Datenverarbeitung und die kommunalen Gebietsrechenzentren verbindlich, sobald der Koordinierungsausschuß, ein Organ des Datenverbundes, sie gebilligt hat. Der Datenschutzbeauftragte hat sich an den Beratungen dieser Arbeitsanleitung beteiligt und dabei Anregungen gegeben, die unter dem Blickpunkt seiner Aufgaben als wichtig erschienen.

b) Zeitnahe statistische Ergebnisse über wirtschaftliche oder gesellschaftspolitische Veränderungen und Entwicklungstendenzen sind ein wertvolles und für eine fortschrittliche Regierungspolitik unverzichtbares Instrument geworden. Die traditionellen Programme für die Sammlung statistischer Informationen und deren sich über Jahre erstreckende Auswertung genügen nicht mehr den berechtigten Forderungen nach Vermittlung eines aktuellen Wissens über die für die Gesetzgebung und Regierung wichtigen Tatsachen und Entwicklungstendenzen. Die Technik ermöglicht es, das Leistungsvermögen der statistischen Ämter zu steigern und den veränderten Anforderungen anzupassen. Mit Bezug auf ihre Nutzbarmachung beim Statistischen Bundesamt hat der Bundesinnenminister in der oben erwähnten Ansprache (vgl. 4.1.1.1 c) ausgeführt: „Das Prinzip der gesetzlichen Verankerung jeder einzelnen statistischen Erhebung sollte dabei auf jeden Fall aufrechterhalten werden, da es dem Schutze des einzelnen Befragten dient und vor einem Übermaß staatlich angeordneter Erhebungen bewahrt". Im hessischen Landesrecht gilt dieses Prinzip nicht. Das **Statistische Landesamt** ist aufgrund einer Anordnung der damaligen Militärverwaltung im Jahre 1946*) errichtet und später als eine obere Landesbehörde, die dem Ministerpräsidenten untersteht, fortgeführt worden. Weder die Aufgaben des Statistischen Landesamtes noch die Voraussetzungen seiner Tätigkeiten sind landesgesetzlich geregelt. Die Landesregierung kann daher — wenn sie darauf verzichtet, den Bürger zu Auskünften zu verpflichten — statistische Erhebungen ohne Mitwirkung des Landtages durchführen lassen und über deren Verwendung und die Frage ihrer Veröffentlichung frei entscheiden. Bei

*) Direktive Nr. 15 der US-Militärregierung für Groß-Hessen vom 14. 1. 1946.

dieser Rechtslage und wegen der wachsenden Bedeutung statistischer Erhebungen für die politische Planung werden der Datenschutz und die Einschaltung des Datenschutzbeauftragten immer wichtiger nicht nur wegen des Schutzes des Bürgers vor dem Mißbrauch seiner Individualdaten, sondern auch unter dem Gesichtspunkt des Informationsgleichgewichts zwischen Legislative und Exekutive (vgl. 4.2.1).

Einen begrenzten Einfluß auf die Datenermittlung und auf die Aufbereitung des Erhebungsmaterials für Statistiken des Landes kann nur der Hessische Statistische Koordinierungsausschuß*) im Rahmen seiner Zuständigkeit „für alle grundsätzlichen Fragen auf statistischem Gebiet" durch Vorschläge an die Landesregierung ausüben.

Der Datenschutzbeauftragte hat angeregt, ihn als ständiges Mitglied in diesen Ausschuß aufzunehmen, damit die Forderungen des Datenschutzes ausreichend berücksichtigt werden.

c) Die Überprüfung des Informationssystems des **Landeskriminalamtes** hat folgendes ergeben.

Die kriminalpolizeilichen Personenakten werden seither nach den „Richtlinien für die Führung der kriminalpolizeilichen Personenakten"**) geführt. Danach sind die Personenakten ausschließlich für den innerdienstlichen Gebrauch der Kriminalpolizei bestimmt. Die Angaben in den Personenakten werden laufend ergänzt. Stirbt die erfaßte Person oder erreicht sie das 80. Lebensjahr, dann werden die über sie angelegten Akten ausgesondert und in einem Archiv oder einer Sammlung ausgeschiedener Akten aufbewahrt.

Nach der Auskunft des Landeskriminalamtes werden diese Richtlinien, die zunächst für die herkömmliche Aktenführung der Personenakten bestimmt waren, auch für das automatische Informationssystem sinngemäß angewandt. Es muß jedoch zweifelhaft erscheinen, ob sie den an ein EDV-System zu stellenden höheren Anforderungen an Geheimnisschutz genügen. Für Änderungen und Ergänzungen wäre der Zeitpunkt gekommen. Denn nach der Auskunft des Landeskriminalamtes steht die erste Aufbaustufe der Datenverarbeitungsanlage kurz vor der Fertigstellung. Am 1. 11. 1973 sollen an die Zentralanlage des Amtes 6 Datenstationen für den Dialogverkehr angeschlossen werden. Bis Ende 1974 wird die Anlage mit 24 solcher Terminals verbunden sein, die in den einzelnen Kriminalkommissariaten stehen. Schon jetzt ist das Landeskriminalamt mit der Zentrale des Bundeskriminalamtes durch ein Terminal verbunden, das für Fahndungsaufgaben zur Verfügung steht. Eine volle Integration mit dem polizeilichen Informationssystem des Bundes soll bis Ende 1974 abgeschlossen sein. Zwischen dem Bundeskriminalamt und den Landesämtern werden künftig die Datensätze untereinander ausgetauscht, so daß jedes Amt den gleichen Grunddatensatz besitzt. Dieses Informationssystem erfordert nach den Grundsätzen des Datenschutzgesetzes einen erhöhten Geheimnisschutz, damit das Persönlichkeitsrecht des Bürgers nicht verletzt wird. Das System muß so eingerichtet sein, daß „Unbefugte" keinen Zugriff zu den gespeicherten Daten haben (§ 2 DSG). Dies ist nach der Forderung des Datenschutzgesetzes durch personelle und technische Vorkehrungen sicherzustellen. Organisatorische Maßnahmen können dies unterstützen. Nach Auskunft des Landeskriminalamtes sind für das Informationssystem entsprechende Vorkehrungen vorgesehen. So sollen nur ausgewählte Beamte berechtigt sein, die Datenstationen zu bedienen. Die Zugriffsberechtigung soll nach verschiedenen Gesichtspunkten abgestuft werden. Auf diese Weise soll die Vertraulichkeit der Daten gewahrt und zugleich gewährleistet werden, daß das System nur für innerdienstliche Zwecke benutzt wird. Die Abfragen werden protokolliert und kontrolliert. Die Kontrolle erfolgt bei Direktabfragen nachträglich, bei Auskunftsersuchen mittels Fernschreibens oder Briefes vor Weiterleitung der Auskunft. Das Protokoll erfaßt den Namen des Anfragenden, die anfragende Stelle sowie den Zeitpunkt und den Inhalt der Anfrage und hält fest, ob die Auskunft gegeben oder verweigert worden ist.

Ungeregelt bleibt hierbei die Frage, wie lange die über den Einzelnen gesammelten Informationen aufbewahrt und erhalten bleiben. Die seitherige Regelung, wonach die Personenakten auszusondern sind, wenn die erfaßte Person verstorben ist oder das 80. Lebensjahr erreicht hat, sind auf das neue System nicht unmittelbar übertragbar. Die zeitlich unbegrenzte Archivierung ist nicht generell notwendig. Sofern nicht ganz besondere Umstände vorliegen, müßte vielmehr erwartet werden, daß die personenbezogenen Daten, mindestens die Identifikationskennzeichen, nach Ablauf bestimmter Fristen oder nach dem Tode getilgt, d. h. physisch vernichtet werden. Maßstäbe für eine solche Regelung könnten die Vorschriften des Bundeszentralregistergesetzes über Auskünfte und Tilgung geben. Dabei wird jedoch nicht verkannt, daß die verschiedenen Zweckbestimmungen dieses Registers und des kriminalpolizeilichen Informationssystems Unterschiede erfordern. Andererseits darf der Schutzzweck, den das Gesetz über das Bundeszentralregister verfolgt, nicht durch weitergehende Auskunftsmöglichkeiten des polizeilichen Informationssystems unterlaufen werden.

Der Vergleich mit dem Bundeszentralregister wirft die weitere Frage auf, ob es genügt, die Organisation und die Benutzung des kriminalpolizeilichen Informationssystems lediglich durch verwaltungsinterne Anordnungen zu regeln. Richtlinien und Verwaltungsanweisungen legen den Beamten und Angestellten zwar dienstrechtliche Pflichten auf; daraus erwachsen jedoch für den einzelnen Bürger keine eigenständigen Rechte. Der Schutz des Persönlichkeitsrechts der Bürger erfordert wegen der besonderen Empflindlichkeit der polizeilichen Daten eine gesetzliche Regelung.

*) Erlaß des Hessischen Ministerpräsidenten vom 6. 1. 1970 — StAnz. S. 130 —.

**) Kriminalpolizeiliche Vorschriftensammlung für die hessische Polizei nach dem HOSG (hsgg. vom LKA Hessen).

Die Verrechtlichung der Richtlinien für den Aufbau und die Benutzung des Informationssystems ist auch aus einem weiteren Grund wünschenswert: Die Bestimmung, daß die Personenakten ausschließlich für den innerdienstlichen Gebrauch der Kriminalpolizei bestimmt sind, gilt nicht uneingeschränkt. Aus Gründen des Allgemeinwohls nehmen die Aufsichtsbehörde und andere oberste Landesbehörden ein Auskunftsrecht in Anspruch, z. B. für Sicherheitsüberprüfungen bei der Einstellung von Personen in verantwortlichen Stellungen des öffentlichen Dienstes. Die Grenzen dieser Befugnis sollten gesetzlich bestimmt werden. Das Vertrauen in die Verwaltung würde gestärkt, wenn die bisher geübte Selbstbeschränkung der obersten Landesbehörde, welche die Dienstaufsicht über das Landeskriminalamt führt, in Rechtsnormen festgelegt würde, auf die der Bürger sich berufen kann.

d) Die Probleme, die sich für den Datenschutz aus der **Zusammenarbeit** von Behörden und Stellen der öffentlichen Verwaltung **mit privaten Unternehmen** ergeben, gewinnen stetig an Bedeutung. Entweder ist es aus wirtschaftlicher Erwägung geboten, Datenerfassung und Datenverarbeitung für öffentliche Aufgaben durch private Rechenzentren oder ähnliche Unternehmen ausführen zu lassen, oder die öffentliche Aufgabe erfordert das Zusammenwirken der Behörden mit privaten Unternehmen.

Hierfür ist die Einführung der elektronischen Datenverarbeitung in der Sozialversicherung ein Beispiel (vgl. 4.1.1.2 — die unter I 4.1.1.3 d genannte DÜVO vom 24. 4. 1971 ist aufgehoben worden). Überläßt die öffentliche Verwaltung personenbezogene Daten privaten Unternehmen zur Erfassung oder zur Verarbeitung oder tauscht sie Daten im Zusammenwirken mit privaten Unternehmen aus, so stellt sich die Frage sowohl nach dem Schutz des Bürgers als auch nach der Überwachung durch den Datenschutzbeauftragten.

Die Behörde bleibt für den Datenschutz verantwortlich, wenn sie die Erfassung oder Verarbeitung von Daten an Service-Unternehmen abgibt (vgl. I 1.3.2). Die Möglichkeiten der Behörde, den Persönlichkeitsschutz in diesen Fällen zu gewährleisten, sind jedoch begrenzt. Sie können in der Regel nur durch privatrechtliche Vereinbarung geschaffen werden. Der Datenschutzbeauftragte hat ein Auskunftsrecht nur gegenüber den Behörden und Stellen der öffentlichen Verwaltung (§ 13 DSG). Daher kann er die Einhaltung der Vorschriften über die vertrauliche Behandlung der Daten (§ 10 Abs. 1 DSG) bei dem privaten Unternehmen nicht überwachen. Er kann nur darauf hinwirken, daß die öffentliche Verwaltung die nötigen und möglichen Vereinbarungen zum Schutze der Vertraulichkeit der Daten trifft und deren Erfüllung überwacht. Diese Rechtslage ist unbefriedigend. Deswegen sollten Sammlungen personenbezogener Daten zwecks Erfassung oder Verarbeitung nur dann außer Haus gegeben werden, wenn zwingende Gründe es gebieten und wenn die Dateien keine „empfindliche" Daten enthalten. Bei der Auswahl des Service-Unternehmens sind neben der Prüfung seiner Zuverlässigkeit folgende Gesichtspunkte zu beachten: Von den Unternehmen muß gefordert werden, daß sie ihre Arbeitskräfte zu besonderer Geheimhaltung verpflichten, die Datenträger unter besonderem Verschluß aufbewahren und der auftraggebenden Behörde die Befugnis einräumen, Kontrollen an Ort und Stelle vorzunehmen. Die Einhaltung dieser Vereinbarungen sollte durch Konventionalstrafen abgesichert werden. Die Daten von mittlerer oder höherer Empfindlichkeit, deren Weitergabe unvermeidbar ist, sollten vorher anonymisiert werden. Dabei besteht die Möglichkeit, die Datensätze in der Weise aufzuteilen, daß die zur Identifizierung der Person geeigneten Daten und die sonstigen Daten getrennt und von verschiedenen Firmen erfaßt oder verarbeitet werden. Wenn je nach dem Gegenstand und der Struktur der Daten trotz Anonymisierung die Möglichkeit einer Rückidentifizierung mittels bestimmter Merkmalskombinationen nicht ausgeschlossen werden kann, wird die Vergabe nur zu verantworten sein, wenn das Risiko der Verletzung des Persönlichkeitsrechts durch die gebotenen Sicherheitsvorkehrungen auf ein dem Bürger zumutbares Minimum eingegrenzt ist.

Vor allem sind die Behörden der kommunalen Selbstverwaltung auf ihre erhöhte Verantwortung hinzuweisen, wenn sie personenbezogene Daten zur Erfassung oder Verarbeitung an private Unternehmen weitergeben, z. B. im Personal- und im Einwohnerwesen. Der Hessische Gemeindetag hat der grundsätzlichen Forderung, die Weitergabe personenbezogener Daten aus dem Verwaltungsvollzug an private Datenerfassungs- oder -verarbeitungsunternehmen zu verbieten, zugestimmt.

Der Datenschutzbeauftragte hat beanstandet, daß die erkennungsdienstlichen Unterlagen einer kommunalen Kriminalpolizeibehörde zur Erfassung auf Lochkarten an ein privates Rechenzentrum weitergegeben werden. Die Unterlagen (Ablochbelege) enthalten u. a. offene Angaben über Name, Geburtsdatum und Anschrift, über den Familienstand, den Beruf oder die ausgeübte Tätigkeit, auch Daten über polizeiliche oder kriminalistische Merkmale (Polizeiaufsicht, Führerscheinentzug, Landstreicher, Geistesgestörter), über persönliche Kennzeichen (Größe, Haarfarbe, Mundart u. ä.); ferner Daten über die aufzuklärende Straftat und die Tatumstände (Fahrzeug, Schußwaffe, Alkoholeinfluß, Vorstrafen u. ä.), die nur zum Teil verschlüsselt dargestellt sind. Bei einigen der verschlüsselten Daten ist außerdem der Schlüssel aus dem Ablochformular zu entnehmen. Erschwerend kam hinzu, daß dasselbe Rechenzentrum auch die Daten aus dem Aufgabengebiet „Personalwesen" im Auftrag derselben Gemeinde erfaßt. Die Konzentrierung personenbezogener Daten aus ein und demselben Personenkreis bei einem Rechenzentrum, statt der Aufteilung auf verschiedene Unternehmen, erhöht die Möglichkeit mißbräuchlicher Verwendung selbst anonymisierter Daten.

Aufgrund der Beanstandung hat das Landeskriminalamt angeordnet, daß polizeiliche Da-

ten vom 15. 3. 1973 an nicht mehr an private Unternehmen zur Erfassung (Ablochung) weitergegeben werden dürfen.

e) Das Nachrichtendienstliche Informationssystem (NADIS) dürfte dasjenige der öffentlichen Verwaltungen in der Bundesrepublik sein, dessen Aufbau am weitesten fortgeschritten ist. Gleichzeitig besitzen die in diesem System gespeicherten Daten einen besonders hohen Grad an Empfindlichkeit, weil sie Informationen über Lebensweise, Umgang und Neigungen enthalten, die zum Intimbereich des Menschen gehören. Diesem Informationssystem sind oder werden demnächst alle bundesdeutschen Nachrichtendienste — das Bundesamt und die Landesämter für Verfassungsschutz, der Militärische Abschirmdienst und der Bundesnachrichtendienst — angeschlossen. Die zentrale Fundstelle des NADIS sitzt in Köln. Sie gibt Querverweise auf die Zentraldateien der verschiedenen Ämter. Das **Hessische Landesamt für Verfassungsschutz** wird ab 1. 6. 1973 mit Köln und den anderen Landesämtern durch eine eigene Leitung verbunden sein.

Aus der besonderen Aufgabenstellung des Landesamtes für Verfassungsschutz ergibt sich, daß es selbst an der strikten Geheimhaltung dieser Informationen interessiert ist. Ein Informationsfluß findet grundsätzlich nur innerhalb des Verbundes statt. Eine Weitergabe von Daten nach außen erfolgt lediglich, wenn die Erkenntnisse aus den Informationen, d. h. aus der Verarbeitung der Daten, den Verdacht begründet erscheinen lassen, daß die überwachte Person an staatsfeindlichen oder staatsgefährdenden Umtrieben beteiligt ist.

Zweck und Aufgabe des Verfassungsschutzamtes rechtfertigen diese Weitergabe auch der empfindlichen Daten über den Einzelnen, wenn und solange der Kreis der empfangsberechtigten Personen und Stellen eng gezogen ist. Dies ist nur dann gewährleistet, wenn sichergestellt ist, daß nur die Stellen diese Daten erhalten, die die Verantwortung für die Sicherheit des Staates tragen.

Diese Voraussetzungen erfüllt die derzeitige Praxis des Landesamtes für Verfassungsschutz. Auskünfte aus seinen Erkenntnissen gibt es nur an oberste Landesbehörden ab. Über die im Rahmen der Tätigkeit der Verfassungsschutzorgane anfallenden Erkenntnisse unterrichtet das Landesamt den Innenminister, dem es direkt untersteht. Dieser entscheidet im eigenen Ermessen, ob, an wen und welche Informationen er weitergibt.

Diese Praxis ist jedoch durch keine Rechtsvorschrift abgesichert. Sie bedarf der Verrechtlichung.

Für die Löschung von Daten gibt es im Landesamt für Verfassungsschutz keine Vorschriften. Da dieses Problem auch bei den anderen Nachrichtendiensten nicht oder nicht ausreichend geregelt zu sein scheint, wird z. Z. auf Bundesebene für die Löschung von Daten des Nachrichtendienstlichen Informationssystems eine einheitliche Regelung in Form einer Verwaltungsanweisung angestrebt. Dabei könnten auch die im Rahmen der hessischen Datenschutzgesetzgebung gewonnenen Erfahrungen und die hier entwickelten Grundsätze als hessischer Beitrag in diese Diskussion eingebracht werden.

Diese Regelung allein genügt aber nicht. Verwaltungsanweisungen legen den Bediensteten der Behörden zwar dienstrechtliche Pflichten auf, sie begründen jedoch für den Bürger keine eigenständigen Rechte. Ebenso wie beim polizeilichen Informationssystem (vgl. 4.1.1.3 c) ist es daher wegen der besonderen Empfindlichkeit der im nachrichtendienstlichen Informationssystem gespeicherten Daten erforderlich, daß die Verpflichtung zur Löschung bestimmter Daten und die Befugnisse des Landesamtes für Verfassungsschutz zur Weitergabe von Daten nach außen rechtlich geregelt werden, um dem Bürger hinreichenden Schutz gegen eine mißbräuchliche Verwendung der über ihn gesammelten Informationen zu gewähren.

f) In Vertragsverhandlungen zwischen dem Land und den **evangelischen Kirchen und den katholischen Bistümern** in Hessen sind auch im Berichtszeitraum unterschiedliche Auffassungen über Erfordernisse des Datenschutzes hervorgetreten, und zwar wegen der Weitergabe maschinell aufbereiteter Besteuerungsgrundlagen der Finanzämter an kirchliche Stellen (vgl. 2.2.1).

Nach § 8 des Kirchensteuergesetzes*) sind den Kirchen (Kirchengemeinden) von den zuständigen Staats- und Gemeindebehörden auf Anforderung die Unterlagen mitzuteilen, deren sie für die Besteuerung bedürfen. Wird die Kirchensteuer als Zuschlag zu einer staatlichen Steuer (Einkommen oder Lohn) erhoben, so berechtigt und verpflichtet dies die Finanzämter, den Kirchen die rechtskräftig festgesetzte Steuer, oder die steuerpflichtigen Einkünfte mitzuteilen. Die Kirchen fordern jedoch einen „umfassenden Überblick über die Besteuerungsgrundlagen", d. h. die Einsicht in die einzelnen Elemente der individuellen Steuerveranlagung (die einzelnen Einkommensarten, Sonderausgaben, Abschreibungen und dgl.).

Sie begründen dies auf verschiedene Weise: Im Hinblick auf das Kirchgeld in glaubensverschiedenen Ehen (§ 2 Abs. 1 Nr. 5 a.a.O.) wird geltend gemacht, daß dieses „besondere Kirchgeld seiner Höhe nach an das gemeinsame Einkommen der Ehegatten nach § 32 EStG anknüpft". Diese Auffassung ist nicht grundgesetzkonform. Der Halbteilungsgrundsatz, nach dem in glaubensverschiedenen Ehen die Kirchensteuer des einer steuerberechtigten Religionsgesellschaft angehörenden Ehegatten nach der Hälfte der zusammengerechneten Einkommensteuer beider Ehegatten erhoben wird, verstößt gegen Art. 2 Abs. 1 GG. „Bei der Wahl des Besteuerungsmaßstabes darf die Kirche nur an Merkmale anknüpfen, die in der Person des ihr angehörenden Ehegatten gegeben sind." Wählt sie das Einkommen im Sinne des Einkommensteuerrechts als Maßstab, so kann es nur das des kirchenangehörigen Ehegatten sein**).

*) In der Fassung vom 25. 9. 1968 — GVBl. I S. 268.

**) BVerfGE 19, 274; Leibholz/Rinck Art. 140 GG Anm. 11.

Im Hinblick auf die Kirchensteuer, die als Zuschlag zur Einkommensteuer (Lohnsteuer) erhoben wird, wird darauf verwiesen, daß das Recht, die Kirchensteuer zu stunden, ganz oder teilweise zu erlassen oder niederzuschlagen (§ 11 Abs. 2 a.a.O.), ohne Einsicht in die einzelnen Elemente der Steuerveranlagung nicht ausgeübt werden könne. Diese Begründung kann nicht anerkannt werden: Das Recht der kirchlichen Behörden, die Kirchensteuer zu stunden, zu erlassen oder niederzuschlagen, das neben dem Stundungsrecht des Finanzamts besteht (§ 11 Abs. 1 a.a.O.), bleibt von der Regelung des Kirchensteuergesetzes unberührt, wie der Wortlaut des § 11 Abs. 2 besagt. Das Stundungsrecht fließt nicht aus dem Besteuerungsrecht, das Art. 137 Abs. 6 WRV den Religionsgesellschaften verleiht. Es gehört vielmehr zu den Angelegenheiten der Kirchen, die diese nach Art. 137 Abs. 3 WRV selbständig innerhalb der Schranken des für alle geltenden Gesetzes ordnet und verwaltet. Für die Ausübung dieses Rechtes gelten die allgemeinen Schranken, die das grundrechtlich geschützte Persönlichkeitsrecht des Bürgers setzt. Die Finanzämter dürfen Einsicht in die Besteuerungsunterlagen des Einzelnen nur gewähren, wenn der Steuerpflichtige zustimmt. Das Erfordernis der Zustimmung haben die staatlichen Behörden zu beachten, wenn sie den Kirchen Amtshilfe leisten.

Ferner wird geltend gemacht, daß der umfassende Überblick über die Besteuerungsgrundlagen der einzelnen Kirchenmitglieder für die Durchführung eines Finanzausgleiches zwischen Wohnsitzdiözesen und Betriebsstättendiözesen notwendig sei. Hierfür ist es jedoch unerheblich, wie die Lohnsteuer des einzelnen Arbeitnehmers berechnet wird. Vielmehr kommt es auf das Gesamtaufkommen der Lohnsteuer in den zum Ausgleich verpflichteten Diözesen an. Schließlich ist die Kenntnis der individuellen Besteuerungsgrundlagen der einzelnen Mitglieder der Kirche auch entbehrlich, wenn die Kirchensteuer auf Grund besonderer Steuertarife anstatt als Zuschlag zur Einkommensteuer erhoben wird (§ 2 Abs. 2 a.a.O.). Denn Steuertarife werden nach allgemeinen Maßstäben aufgestellt, für welche die Einkommensarten des einzelnen Steuerpflichtigen und die Veranlagungselemente ohne Belang sind. Gleiches gilt für die Erhebung eines gestaffelten Kirchengeldes. Welche Anknüpfungspunkte für die Besteuerung auch immer die Kirchen wählen, stets muß sich die vom Staat geforderte Amtshilfe im Rahmen der allgemeinen Rechtsordnung halten.

Die kirchenrechtlichen Bestimmungen der Weimarer Reichsverfassung bilden mit dem Grundgesetz zusammen ein organisches Ganzes. Sie sind nach dem Sinn und dem Geist der grundgesetzlichen Wertordnung auszulegen. Daher müssen die staatlichen Kirchensteuergesetze, die den Religionsgesellschaften das Recht der Steuererhebung verleihen (Art. 137 Abs. 6 WRV), im Einklang mit den Verfassungsgrundsätzen, namentlich den Grundrechten, stehen*). Der Datenschutz gewährleistet die grundrechtlich verbürgte Rechtsstellung des Bürgers im Bereich der maschinellen Datenverarbeitung (§§ 1, 2 DSG). Das Kirchensteuergesetz gestattet keine Eingriffe in die Grundrechte; es muß verfassungskonform ausgelegt und angewandt werden. Vor den Verwaltungsbedürfnissen der Kirchen hat das Persönlichkeitsrecht des Bürgers uneingeschränkt Vorrang. Man kann dem auch nicht entgegenhalten, daß in der Vergangenheit die erwähnten Auskünfte in vielen Fällen gegeben worden sind. Abgesehen von der Frage, ob sich die staatlichen Stellen dabei immer im Rahmen des geltenden Rechts bewegt haben, muß hier darauf hingewiesen werden, daß mit der Einführung der EDV eine grundlegende Veränderung bewirkt wird. Konnte früher bestenfalls die eine oder andere Unterlage eingesehen werden oder eine zusätzliche Auskunft erfolgen, so würde durch die neue Technik eine jederzeitige systematische und lükkenlose Durchleuchtung der Steuerunterlagen durch nichtstaatliche Stellen ermöglicht. Vom Standpunkt des Datenschutzes aus kann daher nicht gebilligt werden, daß die Kirchen in das System der Amtshilfe der staatlichen Behörden vorbehaltlos eingegliedert werden, wie es in den Entwürfen eines Bundesmeldegesetzes und eines Bundesdatenschutzgesetzes vorgesehen ist (vgl. 2.2.1).

*) BVerfGE 19, 236; Leibholz/Rinck Art. 140 GG Anm. 11.

g) Ein umfangreicher Austausch personenbezogener Daten findet zwischen der Deutschen Bundespost und bestimmten Landesbehörden in dem sogenannten **Rentenauskunftsverfahren** statt. Die Höhe der Rente aus der Sozialversicherung ist dafür bestimmend, ob andere Sozialleistungen beansprucht werden können und in welcher Höhe, z. B. Leistungen nach dem Bundessozialhilfegesetz, aufgrund der Kriegsopferfürsorge, nach dem Jugendwohlfahrtsgesetz, nach dem Ausbildungsförderungsgesetz und dgl. Beantragt ein Rentenempfänger eine der vorgenannten Sozialleistungen, so erhält die hierfür zuständige Behörde von der Deutschen Bundespost Auskunft über die Höhe der Rente, die der Antragsteller bezieht, und über die Rentenberechnungsmerkmale. Der Austausch der Daten findet zwischen der Deutschen Bundespost und einer für das Land bestimmten Kopfstelle — für Hessen ist es die HZD — statt. Die Auskunftsersuchen werden von den Sozialämtern über das zuständige KGRZ an die HZD und von dort an die Rentenrechnungsstelle der Deutschen Bundespost in Hannover geleitet. Die Deutsche Bundespost übermittelt der HZD einmal monatlich auf Magnetbändern die Auftragsbestätigungen und die Auskünfte. Die Auskünfte enthalten den Namen und die Anschrift des Sozialleistungsempfängers, die Höhe der Rente und die Rentenberechnungsmerkmale.

Dieser Datenaustausch erspart dem Sozialleistungsempfänger die mehrfache Befragung nach den Rentenberechnungsmerkmalen und der Höhe seiner Rente und vereinfacht das Verfahren für die Träger der Rentenversicherung und der Sozialhilfeleistungen. Das Verfahren ist in einem Anwendungshandbuch, welches das KGRZ Kassel ausgearbeitet hat, verbindlich festgelegt.

Auf Anregung des Datenschutzbeauftragten wird der Sozialleistungsempfänger, der eine Rente bezieht, auf dem Bewilligungsbescheid darüber unterrichtet, daß die Höhe der berücksichtigten Renteneinkünfte von der Deutschen Bundespost im Rentenauskunftsverfahren mitgeteilt worden ist. Hierdurch erfährt der Empfänger von Sozialleistungen, auf welchem Wege die Behörde Kenntnis über seine Rente ohne seine Beteiligung erhalten hat.

4.1.2 Befugnis

4.1.2.1 Konkretisierung der Generalklausel

Nach § 2 DSG ist „Inhalt des Datenschutzes" die verfahrensmäßige Regelung, mit welcher die Verwaltung Unbefugte daran hindert, Daten „einzusehen" oder über sie durch Abruf oder Vernichtung zu verfügen. Wer befugt ist und auf welcher Rechtsgrundlage die Befugnis beruhen muß, ist nicht bestimmt. Demgegenüber besteht die Aufgabe des Datenschutzbeauftragten nach § 10 Abs. 1 DSG im Schutz eines materiellen Rechtsgutes, des Persönlichkeitsrechts des Bürgers. Die vertrauliche Behandlung der Angaben der Bürger und der über die einzelnen Bürger vorhandenen Unterlagen ist zu gewährleisten. Diese Umschreibung der Aufgabe des Datenschutzbeauftragten definiert zugleich den materiellen Inhalt des Datenschutzes. Dabei bleibt wiederum ungeregelt, welche Daten vertraulich zu behandeln sind und wem gegenüber die Vertraulichkeit zu wahren ist. Diese Fragen haben sich auch im Berichtszeitraum immer wieder gestellt; sie gewinnen mit fortschreitender Integration an praktischer Bedeutung. Dies hat sich beispielsweise gezeigt bei dem Datenverbund im Krankenhauswesen, den § 13 des Hessischen Krankenhausgesetzes*) vorsieht, und bei den Vertragsverhandlungen mit den Kirchen über den Umfang der Daten, welche die Finanzämter als Besteuerungsunterlage für Kirchensteuer und Kirchengeld zur Verfügung stellen sollen (vgl. 4.1.1.3 f und 4.1.2.3).

Mit der sogenannten Sphärentheorie, deren sich das Bundesverfassungsgericht für die Abgrenzung des Persönlichkeitsrechtsschutzes bedient (vgl. I 1.2.3), läßt sich dieses Problem praktisch nicht lösen. Vielmehr wird es nach den Erfahrungen im Berichtszeitraum künftig unvermeidlich sein, die Generalklausel des § 2 DSG für die einzelnen automatisierten Aufgaben der öffentlichen Verwaltung zu konkretisieren, d. h., zu bestimmen, welche Daten innerhalb eines Aufgabenbereiches als sensitiv oder empfindlich zu gelten haben und an wen die Behörde, für deren Aufgabe die Daten erfaßt und gespeichert werden, sie weitergeben darf. Für bestimmte Bereiche der öffentlichen Verwaltung ist es notwendig, rechtlich verbindlich festzulegen, wer von den bei einer Behörde oder Stelle der öffentlichen Verwaltung gespeicherten oder verarbeiteten Informationen Kenntnis erhalten darf. Dies gilt mit Sicherheit für die medizinischen Daten im Bereich des Gesundheitswesens, für die Daten aus dem Bereich des Landeskriminalamtes und des Landesamtes für Verfassungsschutz.

*) v. 4. 4. 73 GVBl. I S. 145.

4.1.2.2 Interpretation der Privatsphäre

Im wissenschaftlichen Schrifttum ist die Auffassung vorherrschend, daß es nicht möglich ist, die Privat- oder Intimssphäre des Bürgers genau abzugrenzen, etwa indem man eine Liste der Daten verbindlich aufstellt, die von der Erfassung und Speicherung in Datenverarbeitungsanlagen ihrer Art nach ausgeschlossen sind, weil sie zur Privat- oder Intimssphäre gehören. In der Sicht einer rollentheoretischen Interpretation der Privatsphäre informiert der Einzelne die Umwelt über sich jeweils in dem Umfange, wie ihm zur Ausfüllung der Rolle, die er in der jeweiligen Lebenssituation spielt oder spielen will, notwendig erscheint. Die Vertraulichkeit hängt weitgehend davon ab, ob und inwieweit der Einzelne bereit ist, Informationen über sich anderen mitzuteilen und zu billigen, daß sie weitergegeben werden. Letztlich bestimmt der Einzelne in seinem Verhalten zur Umwelt, welche Information und wem gegenüber sie vertraulich ist. Privatsphäre sind bei dieser Betrachtung die Lebensbereiche, in denen die Individuen „agieren können, ohne daß eine für sie dysfunktionale Informationsweitergabe an andere erfolgt, bzw. erfolgen kann*)."

4.1.2.3 Schutz medizinischer Daten

Auch in der Praxis zeichnet sich immer deutlicher ab, daß man den Bedürfnissen weder des Bürgers noch der Verwaltung gerecht wird, wenn man die Empfindlichkeit der einzelnen personenbezogenen Daten nach vermeintlich objektiven Maßstäben bewertet und danach bestimmt, welche Daten gespeichert und welche weitergegeben werden dürfen. Ein in Hessen aktuelles Beispiel hierfür bot der Entwurf eines Hessischen Krankenhausgesetzes (LT-Drucks. 7/2505). Ein Verbundsystem der Datenverarbeitung im Krankenhauswesen soll wirtschaftliche und medizinische Daten der Patienten speichern und unter bestimmten Umständen weitergeben. Hierzu soll die Landesregierung durch Rechtsverordnung bestimmen, welche medizinischen Daten „unter Wahrung der ärztlichen Schweigepflicht" weiterzuleiten sind.

Der Datenschutzbeauftragte hat in einem Schreiben an den Landtagspräsidenten und an den Ministerpräsidenten auf die Problematik dieser Konzeption hingewiesen (vgl. Stenogr. Bericht 7/53 vom 29. 2. 1972 S. 2965 ff.). Zweifellos gehören medizinische, also diagnostische und therapeutische Daten zu der Intimssphäre des Einzelnen, d. h. zu dem Bereich des Persönlichkeitsrechts, das gegen Eingriffe von außen zu schützen ist. Deshalb bedroht das Bundesrecht den Arzt wegen Bruchs der Schweigepflicht mit Strafe, wenn er die Vertraulichkeit der Information über seinen Patienten verletzt. Ebenso zweifelsfrei ist der Arzt aber befugt, unter Umständen sogar verpflichtet, die Information über seinen Patienten weiterzugeben, sei es, daß dieser zustimmt oder daß dessen Interesse oder das höherwertige Interesse, Gefahren von der Allgemeinheit abzuwenden, z. B. Seuchengefahren, die Weitergabe gebietet. Die Vertraulichkeit einer Information läßt sich in der Regel nur in bezug auf den in Aussicht genommenen Empfänger der Information bestimmen. Von dessen Beziehung

*) Paul J. Müller in ÖVD 2/73 S. 61 ff.

zum Informanten hängt es ab, ob dieser zustimmt, daß eine ihn betreffende Information an einen Dritten weitergegeben wird. Diese Beziehungen sind im Leben so vielfältig, daß der Gesetzgeber sie weder vollständig erfassen noch für den einzelnen Fall zutreffend regeln kann. Besonders im medizinischen Bereich kommt es daher weniger darauf an, welche Daten der Erstinformierte, also der behandelnde Arzt, über seinen Patienten speichert, als vielmehr darauf sicherzustellen, daß diese Daten nicht oder nur mit Billigung der Patienten weitergegeben werden, es sei denn, daß die Weitergabe gesetzlich vorgeschrieben ist.

Dieser Schutz der Vertraulichkeit kann bei der maschinellen Datenverarbeitung durch verschiedene — organisatorische, technische und auch personelle — Maßnahmen gewährt werden, z. B. durch Zugriffssperren, Verschlüsselungen, Einschaltung von Vertrauenspersonen, die über die Weitergabe entscheiden. Grundsätzlich sollten medizinische Individualdaten aus dem Verfügungsbereich des Arztes, der als erster die Information empfangen hat, nur so verschlüsselt hinausgelangen, daß nur ihm die Rückidentifizierung des Patienten möglich ist.

Die Aufgabe des Datenschutzes liegt mit ihrem Schwergewicht in der Abschirmung des gespeicherten Datenprofils gegen den unbefugten „Einblick" in diejenigen Datenarten, welche es ermöglichen, das Individuum, das sie darstellen (profilieren), zu erkennen. Der Datenschutzbeauftragte hat versucht, diese Grundsätze so zu formulieren, daß sie in den Entwurf des Krankenhausgesetzes eingefügt werden könnten. Diese „Formulierungshilfe" ist dem Vorsitzenden des zuständigen Ausschusses des Landtages zugeleitet worden und ist diesem Bericht als Anlage beigefügt*).

4.1.3 Bereich des Gesetzes

Im Berichtszeitraum ist mehrfach deutlich geworden, daß der Aufgabenbereich des Datenschutzbeauftragten in § 10 Abs. 1 DSG die Praxis der öffentlichen Verwaltung nicht vollkommen abdeckt. Nach dem Wortlaut der Vorschrift hat der Datenschutzbeauftragte zu überwachen, ob die in § 1 DSG genannten Behörden und Stellen der öffentlichen Verwaltung die Vorschriften über die vertrauliche Behandlung der Angaben der Bürger und der über die einzelnen Bürger vorhandenen Unterlagen einhalten.

Findet die für die öffentliche Aufgabe eingesetzte maschinelle Datenverarbeitung nicht bei den in § 1 DSG genannten Stellen statt (Beteiligung von privaten Service-Unternehmen), oder wird die öffentliche Aufgabe von anderen Einrichtungen als den in § 1 DSG genannten erfüllt (Ausgliederung der Aufgabenerfüllung aus der öffentlichen Verwaltung), dann laufen die Kontrollbefugnisse des Datenschutzbeauftragten leer.

4.1.3.1 Service-Unternehmen

Ein Fall der erstgenannten Art ist in 4.1.1.3 d erwähnt. Läßt eine Behörde oder Stelle der öffentlichen Verwaltung ihre Daten von einem privaten Unternehmen erfassen oder verarbeiten, so ist dem Datenschutzbeauftragten eine unmittelbare Überwachung verwehrt. Er kann lediglich auf die Verwaltung einwirken, vor der Weitergabe der Daten die erforderlichen Maßnahmen des Datenschutzes i. S. des § 2 DSG zu treffen und das private Unternehmen zur vertraulichen Behandlung der Daten besonders vertraglich zu verpflichten.

4.1.3.2 Privatrechtliche Organisationen der öffentlichen Hand

Bei der anderen Fallgruppe gibt es zwei Erscheinungsformen: Entweder wird eine öffentliche Aufgabe in vollem Umfange von Organisationen des Privatrechts (Handelsgesellschaften oder dgl.) statt von den in § 1 DSG genannten Behörden oder Stellen wahrgenommen, oder dieselbe Aufgabe wird teils von der öffentlichen Verwaltung, teils von privaten Einrichtungen erfüllt.

Ein Beispiel der erstgenannten Art sind die kommunalen Energieversorgungs- oder Verkehrs-Gesellschaften des Handelsrechts (Verkehrsbetriebe, Stadtwerke und dgl.). Auf sie erstrecken sich die Kontrollbefugnisse des Datenschutzgesetzes nicht, obwohl sie die gleichen personenbezogenen Daten maschinell verarbeiten wie Energieversorgungs- und Verkehrsbetriebe, die als Eigenbetriebe oder als Zweckverbände der Kommunen errichtet worden sind. Ob der Bürger den vollen gesetzlichen Datenschutz genießt, hängt davon ab, ob die öffentliche Aufgabe, für welche der Bürger seine Daten hergibt, von Institutionen des öffentlichen oder des privaten Rechts erfüllt wird.

Dies ist unbefriedigend. Einerseits trägt die öffentliche Verwaltung die Verantwortung für die Aufgabe, gleichgültig in welcher Rechtsform sie erfüllt wird. Andererseits hat der Bürger wegen der Monopolstellung der kommunalen Unternehmen keine Ausweichmöglichkeit.

Ein Beispiel der zweiten Art ist das Verbundsystem der Datenverarbeitung, welches das Hessische Krankenhausgesetz vorsieht (vgl. 4.1.2.3). Die Krankenhausversorgung der Bevölkerung sicherzustellen ist eine öffentliche Aufgabe (§ 1 KHG), die sowohl von den Gebietskörperschaften (Land, Landkreise, Gemeinden) und dem Landeswohlfahrtsverband, als auch in freigemeinnütziger und privater Trägerschaft erfüllt wird (§ 1 a.a.O.). Die Träger der privaten und der gemeinnützigen Krankenhäuser fallen jedoch nicht unter das Datenschutzgesetz. Der Datenschutzbeauftragte hat in seiner Stellungnahme zu dem Entwurf des Hessischen Krankenhausgesetzes auf diese Rechtslage hingewiesen und angeregt, in einer Vorschrift klarzustellen, daß das Datenschutzgesetz für das Verbundsystem der Datenverarbeitung unabhängig davon gilt, ob die Krankenhausversorgung in öffentlicher oder in privater Trägerschaft gewährt wird. Aufgrund dieser Anregung hat der Landtag den Regierungsentwurf zwar durch materielle Datenschutzvorschriften ergänzt, jedoch unterlassen oder übersehen, die Befugnisse des DSB (§ 10 Abs. 1, § 13 DSG) auf die privaten oder gemeinnützigen Krankenhäuser zu erstrecken.

Das gleiche Problem, wenn auch von geringerer Bedeutung für den Persönlichkeitsschutz des Bürgers, wirft Art. 1 Nr. 4 (§ 111) des Entwurfs eines Gesetzes zur Änderung des Gemeindewirt-

*) Siehe Anlage 2.

schaftsrechtes und anderer kommunalrechtlicher Vorschriften auf (LT-Drucks. 7/2659). Läßt die Gemeinde ihre Kassengeschäfte ganz oder teilweise von einer Stelle außerhalb der Gemeindeverwaltung, also von einem privaten Unternehmen, unter Einsatz der elektronischen Datenverarbeitungsanlagen erledigen, so ist der Datenschutzbeauftragte zu einer unmittelbaren Überwachung im Sinne des § 10 Abs. 1 und Abs. 2 DSG nicht befugt.

4.1.4 Anrufungsrecht des Bürgers

Im Berichtszeitraum hat der Datenschutzbeauftragte einige Zuschriften von Bürgern erhalten, die nur zum geringsten Teil als Anrufungen im Sinne des § 11 DSG behandelt werden konnten. Einzelne dieser Petitionen betrafen Vorgänge außerhalb Hessens oder Datenverarbeitungen in der privaten Wirtschaft; in den anderen wurde die Verletzung oder Mißachtung von Rechten geltend gemacht, die durch die EDV weder verursacht war, noch im Zusammenhang mit ihr stand. In einem weiteren Fall ist der Datenschutzbeauftragte neben zwei Ressorts nur am Rande beteiligt. Zusammenfassend ist festzustellen, daß der Bürger von den Rechtsbehelfen, die die §§ 4, 11 DSG zur Verfügung stellen, auch in diesem Berichtszeitraum so gut wie keinen Gebrauch gemacht hat.

Es wäre vorschnell, diese Erscheinung allein dadurch zu erklären, daß sich der Bürger in voller Übereinstimmung mit der Erledigung seiner Angelegenheiten durch die Verwaltung des Landes, der Kommunen und der öffentlich-rechtlichen Körperschaften und Anstalten befände. Seine Enthaltsamkeit hat vermutlich andere Gründe: Im allgemeinen wird es daran liegen, daß dem Bürger in der Bundesrepublik die elektronische Datenverarbeitung mit ihren komplexen Problemen weitgehend unbekannt oder undurchschaubar geblieben ist.

Außerdem spielt der Umstand eine Rolle, daß im Bereich der öffentlichen Verwaltung die meisten durch die Datenverarbeitung laufenden Informationen von den Betroffenen selbst stammen, daß die Mehrzahl der Daten für sich betrachtet offenkundig oder relativ unempfindlich sind und die Integration der verschiedenen in der öffentlichen Verwaltung geführten Dateien noch nicht durchgeführt ist.

Dazu kommt die Schwierigkeit, die Gefährlichkeit eines erst in der Entwicklung begriffenen Instrumentes, nämlich der integrierten Datenverarbeitung, mehr oder weniger vorausschauend zu erkennen und sich zu vorbeugenden Abwehrmaßnahmen bereitzufinden. In diesem Zusammenhang ist es auch von Bedeutung, daß das hessische Datenschutzgesetz dem Bürger kein Auskunftsrecht darüber gewährt, welche Daten über ihn gespeichert werden und wohin sie weitergegeben werden.

Zur Realisierung der Rechte, die das Datenschutzgesetz den Bürgern in den §§ 4 und 11 gibt, bedarf es daher neben den Funktionen des Datenschutzbeauftragten weiterer geeigneter Maßnahmen, damit der Bürger einen größeren Einblick in Informationssysteme der Verwaltung erhält und transparent wird, was die öffentliche Verwaltung mit den personenbezogenen Daten unternimmt (vgl. 2.4.3—5).

4.2 Erhaltung der Gewaltenteilung

4.2.1 Keine neuen Entwicklungen

4.2.2 Kommunale Selbstverwaltung

Aktuelle Gefährdungen der kommunalen Selbstverwaltung durch die maschinelle Datenverarbeitung hat der Datenschutzbeauftragte wiederum nicht festgestellt.

Die in der Anfangsphase der Datenverarbeitung aufgestellte Voraussage, der EDV-Einsatz werde eine grundsätzliche Revision des Verwaltungsaufbaus unter zentralistischen Vorzeichen auslösen, ist heute im wesentlichen widerlegt.

Weder in Hessen noch anderswo hat sich das Bild der Verwaltung grundlegend geändert, nur ist zu der herkömmlichen Verwaltung eine mehr oder weniger selbständige EDV-Verwaltung, bestehend aus einem oder mehreren Rechenzentren, hinzugetreten. Zu einer Zentralisierung in der Aufgabenerledigung hat dies nur in einem sehr eingeschränkten Sinne geführt. Lediglich die Arbeitsabschnitte der Datenerfassung- und -verarbeitung und in zunehmendem Umfang auch der Speicherung werden zwecks optimaler Nutzung der Maschinenkapazitäten zentral in Datenerfassungs- und Datenverarbeitungszentralen abgewickelt. Dabei handelt es sich allein um die technische Durchführung vorgezeichneter Abläufe, die das Verfahren inhaltlich unberührt läßt. Ein qualitativer Funktionsverlust für die Aufgabenträger tritt nicht ein. Die eigentliche Sachbearbeitung hat zwar teilweise eine neue Ablaufstruktur erhalten, die durch eine exakte Trennung in manuelle und maschinelle Arbeitsphasen gekennzeichnet ist. Außerdem ist eine Entlastung von Routineaufgaben eingetreten, soweit diese jetzt maschinell erledigt werden. Daraus resultierende Organisationsanpassungen erfolgen jedoch im allgemeinen auf einer relativ niedrigen Ebene und haben auf die Behördenstruktur im ganzen keinen nennenswerten Einfluß.

Soweit echte Zentralisierungen zur Diskussion stehen, wie z. B. die Einrichtung eines zentralen Amtes für die Bearbeitung von Verkehrsordnungswidrigkeiten, handelt es sich um Rationalisierungsprojekte, deren Zweck und Begründung (gleichmäßigere und arbeitsökonomischere Abwicklung) relativ unabhängig vom Arbeitsmittel (ADV) ist.

Von der Aufgabenerledigung ist die Verfahrensentwicklung zu trennen. Da dieser Arbeitsbereich in der nichtautomatisierten Verwaltung kein direktes Pendant hat — die Organisation (als Aufgabe) entspricht ihm noch am ehesten — kann die Frage nicht nach Funktions**verlagerungen** gestellt werden, sondern danach, wem diese neue Funktion zugewachsen ist und wie sie ausgeübt wird. Die Programmierung im engeren Sinn ist — in Hessen wie auch sonst üblich — bei den Datenzentralen angesiedelt und wird damit zentral erledigt. Die der Programmierung vorgeordnete und für die sachliche Ausgestaltung der Verfahren entscheidende Aufgabe des Verfahrensentwurfs (Ist- und Soll-Analyse) liegt dagegen bei den sachlich zuständigen Verwaltungen. Daß diese hierbei meist in Form gemeinsamer Arbeitsausschüsse zusammenarbeiten, wird man ebensowenig als einflußmindernde

Zentralisierung werten können wie den Umstand, daß die kommunalen Gebietskörperschaften hierbei weitgehend durch ihre Spitzenverbände handeln. Allerdings darf nicht übersehen werden, daß in der Praxis die Datenzentralen oft auch im Bereich des Verfahrensentwurfs über großen sachlichen Einfluß verfügen. Hierfür gibt es mehrere Ursachen. Soweit die Übernahme von Programmen in Betracht kommt, die von Herstellern oder anderen Verwaltungen entwickelt wurden, liegt der zur Beurteilung notwendige technische Sachverstand meist einseitig bei den Datenzentralen. Aber auch bei Eigenentwicklungen scheint der dominierende Einfluß auf seiten der Vertreter der Rechenzentren zu liegen. Symptomatisch dafür ist, daß der für die Verfahrensentwicklung zuständige Arbeitsausschuß für die Automation von Aufgaben der Gemeinden und Landkreise in seinen Richtlinien bestimmt hat, daß der Vorsitz in den mit der eigentlichen Entwicklungsarbeit betrauten Unterausschüssen stets bei einem Vertreter eines **Rechenzentrums** liegen muß.

Aus dieser Konstellation haben sich zwar bisher keine Konflikte ergeben. Es dürfte sich aber empfehlen, die weitere Entwicklung unter dem Gesichtspunkt kritisch zu verfolgen, ob die sich aus der Verwaltungsaufgabe ergebenden Belange, die nicht zuletzt die Interessen der jeweils betroffenen Bürger mit umfassen, gegenüber den datentechnischen Erfordernissen den ihnen gebührenden Vorrang behalten. Um Fehlentwicklungen in dieser Richtung zu vermeiden, muß die Verwaltungsseite darauf hinwirken, daß sie in der datentechnischen Fachbeurteilung nicht in eine Abhängigkeit von den Datenzentralen gerät. Dies ist vor allem eine Ausbildungsfrage. Nachdem die Städte ihre Rechenzentren samt Personal an den EDV-Verbund übergeleitet haben, ist vorübergehend zwangsläufig ein gewisses Vakuum entstanden. Dieses muß jedoch allmählich wieder aufgefüllt werden. Für eigene EDV-Experten wird allerdings die Personalstruktur vor allem bei mittleren und kleineren Gemeinden keinen Raum lassen. Deshalb wäre zu überlegen, ob nicht die kommunalen Spitzenverbände ihren Mitgliedern verstärkt EDV-Sachverstand zur Verfügung stellen könnten. Die Funktion der Rechenzentren als zentrale Fachverwaltung für Datenverarbeitung wird damit keineswegs in Frage gestellt. Denn die Rechenzentren sind im Gegenteil selbst stark daran interessiert, in der Verwaltung mehr und fachkundigere Kooperationspartner zu finden. Worum es allein geht, ist das frühzeitige Erkennen und Meistern der Gefahr, daß die Rechenzentren aus der ihnen zugedachten technischen Servicefunktion herauswachsen und dominierenden Einfluß auf die allein von der Verwaltung zu be- und verantwortenden Sachfragen der spezifischen Verwaltungsaufgaben gewinnen.

(Die unter I 4.2.2 angesprochenen Probleme des Aufbaues planungs- und entscheidungsorientierter Informationssysteme und ihrer Auswirkungen auf die kommunale Selbstverwaltung werden unter 4.2.4 behandelt.)

Die Datenverarbeitung verursacht nicht nur Probleme, die die Träger der kommunalen Selbstverwaltung insgesamt in ihrem Verhältnis zur Landesverwaltung und zu den Rechenzentren betreffen, sondern sie schafft auch gewisse Spannungen zwischen einzelnen Teilgruppen des kommunalen Sektors. So resultiert im Bereich der Massenarbeiten eine gewisse Bevorzugung größerer Verwaltungsträger daraus, daß die Vorteile und Ersparnisse mit den Fallzahlen wachsen. Diese Asymmetrie wird durch das Prinzip der kostenfreien Verarbeitung — nur die Erfassungskosten sind nach dem EDV-Gesetz von den Benutzern der Kommunalen Gebietsrechenzentren selbst zu tragen — noch verstärkt. Man kann jedoch davon ausgehen, daß mit dem Abschluß der Gebietsreform alle Gemeinden eine Größenordnung ereicht haben, die eine rationelle EDV-Nutzung erlaubt. Die verbleibenden Unterschiede in den Nutzungsmöglichkeiten geben keinen Anlaß zu verfassungspolitischer Besorgnis.

Die unterschiedlichen Aufgaben und Problemstellungen bei großen und kleinen Kommunen können sich auch in einer unterschiedlichen Prioritätensetzung bei der Verfahrensentwicklung niederschlagen. Statistiken, Planungsunterlagen und Entscheidungshilfen beispielsweise haben für Großstädte enorme Bedeutung, während bei kleinen und mittleren Gemeinden hierfür weniger Bedarf besteht. Auch die Automation von Aufgaben aus dem Vollzugsbereich hat für die Gemeinden je nach Größe und sozio-ökonomischer Struktur sehr unterschiedliche Vorteile. Trotzdem ist es bisher bei der Setzung von Prioritäten zwischen den verschiedenen Entwicklungsprojekten nicht zu größeren Spannungen gekommen. Dies mag allerdings damit zusammenhängen, daß sich ein Großteil der Gemeinden bisher nur als Konsument eines vorgegebenen Angebots von Service-Leistungen versteht. In dem Maße, wie bei den Kommunen das Bewußtsein wächst, daß sie selbst eine Automationspolitik nach ihren Bedürfnissen betreiben können und müssen, können sich bisher latente Interessengegensätze aktualisieren. Für ihre Austragung dürfte die bestehende EDV-Organisation auf der Grundlage des HZD-Gesetzes durchaus einen günstigen Rahmen abgeben, so daß man eine solche Entwicklung nicht zu fürchten braucht. Ein stärkeres Ringen um Prioritäten dürfte jedoch bei der weiteren EDV-Entwicklung zu einer verstärkten Beachtung verwaltungspolitischer Faktoren führen und insofern durchaus auch positive Aspekte haben.

4.2.3 Parlamentarische Informationsrechte

Auch im zweiten Berichtsjahr hat die mit dem Datenschutzgesetz den parlamentarischen Gremien eröffnete Möglichkeit, unmittelbar von den Datenzentralen oder anderen datenverarbeitenden Stellen der Verwaltung Informationen anzufordern (§ 6 DSG), noch keine praktische Bedeutung erlangt. Dies ist angesichts des bis jetzt erreichten Standes der technischen Entwicklung nicht verwunderlich. Die im Verwaltungsvollzug anfallenden Daten sind nach Gegenstand und Struktur nur begrenzt für politisch-planerische Zwecke verwendbar. Bei vielen Vollzugsaufgaben erhalten die Rechenzentren die Daten nur für eine einmalige Verarbeitung und geben anschließend sämtliche Unterlagen an die auftraggebende Verwaltung zurück. Bei anderen Verfahren existieren jeweils nur die sogenannten Stammdaten, d. h. die auf den Stand des letzten maschinellen Verarbeitungslaufes ge-

brachten Grunddaten. Gerade über die für Planungszwecke besonders interessierende Entwicklung über die Zeit sind deshalb keine Aufschlüsse zu gewinnen. Diese Situation läßt sich auch nicht dadurch kurzfristig verändern, daß man Vollzugsdateien in regelmäßigen Abständen kopiert und dadurch historische Bestände aufbaut. Denn erst eine gründliche methodische und datentechnische Aufbereitung macht das Rohmaterial zu einem aussagekräftigen und technisch handhabbaren Datenbestand. Diese Leistungen gehören zum Programm des Hessischen Planungsinformations- und Analyse-Systems (HEPAS), in dessen Rahmen Instrumente der Entscheidungshilfe in einen systematischen und koordinierten Gesamtansatz, freilich auch in entsprechender zeitlicher Dimension, aufgebaut werden (vgl. 4.2.4). Nur in beschränktem Umfang wird es möglich und sinnvoll sein, Vollzugsdaten schon vorab, d. h. vor dem Aufbau der eigentlichen Planungsdateien, zur Gewinnung von Entscheidungshilfen zu benutzen. So waren die Wohngelddaten das Ausgangsmaterial für Berechnungen im Rahmen des Mietberichts 1972 des Bundesministers für Städtebau und Wohnungswesen und für Untersuchungen zur Strukturplanung der Stadt Frankfurt/Main. Vergleichbare Fragestellungen können auch in der parlamentarischen Arbeit auf der Landes- wie auf der kommunalen Ebene auftreten. Ihre volle Bedeutung werden die parlamentarischen Informationsrechte aber erst im Zuge des Ausbaues des HEPAS entfalten.

4.2.4 Hessisches Planungsinformations- und Analyse-System (HEPAS)

Die Entwicklungsarbeiten am HEPAS sind entsprechend der im Ersten Tätigkeitsbericht erwähnten Konzeption in Gang gekommen. Verfahrensvorschläge für den Aufbau einer Gemeindeplanungsdatei und einer Planungsdatei für soziale Infrastruktureinrichtungen liegen vor; für die kulturelle Infrastruktur ist ein Vorschlag in Arbeit. Ein Standardpaket mit sozialwissenschaftlichen Auswertungs-, Analyse- und Darstellungsprogrammen (SPSS) wurde bei der HZD installiert.

Mit gut einjährigem Abstand auf das HEPAS-Konzept der HZD, das speziell auf die Planungsbedürfnisse des Landes zugeschnitten ist, hat das im Verbund für kommunale Entwicklungsplanung federführende KGRZ Starkenburg kürzlich einen in Zusammenarbeit mit der HZD erstellen komplementären Entwurf für den kommunalen Bereich vorgelegt. Im Titel „HEPAS-KOMMUNAL, Konzeption für den Aufbau des Hessischen Planungsinformations- und Analyse-Systems im kommunalen Bereich" wie auch in den Vorbemerkungen kommt der Wunsch zum Ausdruck, nicht nur Kompatibilität mit dem Landesprojekt herzustellen, sondern HEPAS als einheitliches System mit kommunalen und Landes**komponenten** zu errichten. Dazu sollen Daten- und Methodenbasis nach einheitlichen Grundsätzen aufgebaut werden. In die Entwicklung der Methodenbasis sollen sich HZD und KGRZ Starkenburg teilen.

Der praktische Einsatz von HEPAS-KOMMUNAL soll bei den Kommunalen Gebietsrechenzentren liegen.

Ohne Zweifel ist eine genaue Abstimmung zwischen landes- und kommunalen Systemteilen schon von den ersten Planungsschritten ab unumgänglich, wenn ihre Bestandteile und Ergebnisse untereinander austauschbar bzw. vergleichbar sein sollen. Allerdings bedeutet Abstimmung immer zugleich auch den Zwang zu Kompromissen in der Sache, wenn die natürlichen Interessen den Planer aus dem kommunalen und dem Landesbereich sich nicht von vornherein decken.

Wie weit das der Fall sein wird, ist zur Zeit noch nicht genau festzustellen, weil sowohl auf der kommunalen als auch auf der Landesebene die Ermittlung und detaillierte Beschreibung der Interessen an Planungsinformationen auf Schwierigkeiten stoßen. Die Gefahr einer einseitigen Entwicklung in bestimmter Richtung ist deshalb zur Zeit nicht absehbar. Eine ausgewogene Gesamtlösung wird aber nur erreicht werden, wenn beide Seiten mit etwa gleicher Intensität am Systemaufbau arbeiten. Für die kommunale Seite ist es deshalb wichtig, den Erfahrensvorsprung des Landes möglichst rasch aufzuholen, damit sie bei der weiteren Entwicklung nicht nur als gleichberechtigter, sondern auch als gleich sachkompetenter Partner agieren kann. Schwierigkeiten bei der Bestimmung geeigneter Organisationsformen, in denen alle mit kommunaler Planung befaßten Instanzen angemessen vertreten sind, sollten deshalb die Aufnahme der konkreten Projektarbeit nicht verzögern.

Die Frage einer parlamentarischen Beteiligung beim Aufbau des HEPAS ist nach wie vor offen. Eine organisatorische Schwierigkeit besteht darin, daß die Aufgabe in keines der Tätigkeitsfelder der bestehenden Landtagsausschüsse zwanglos einzugliedern ist. Die Bildung eines besonderen EDV-Ausschusses, wie sie etwa in der erwähnten amerikanischen Studie dem Kongreß vorgeschlagen worden ist (vgl. 2.3.1), stellt eine von mehreren Möglichkeiten dar. Der Schwierigkeit der Materie würde sie wohl am ehesten gerecht. Diese Überlegungen, an denen der Datenschutzbeauftragte teilnimmt, sind noch nicht abgeschlossen.

Die Landtagsverwaltung hat die Stelle eines EDV-Referenten eingerichtet und rüstet sich damit für die Unterstützung einer intensiveren Tätigkeit der Abgeordneten auf dem EDV-Sektor (vgl. 4.2.3).

Auch auf der kommunalen Ebene werden sich die Volksvertreter den Problemen der EDV stellen müssen, wenn sie künftig deren Möglichkeiten kennenlernen und nutzen wollen. Der Gegensatz zwischen Volksvertretung und ausführendem Organ ist zwar in der Kommunalverfassung weniger ausgeprägt als im Verfassungsaufbau des Landes. Die Informationsinteressen von Gemeindevertretern und Stadtverordneten werden sich mit denen von Bürgermeistern und Magistratsmitgliedern weitgehend decken. Daraus folgt aber nicht, daß sie diesen das Feld der maschinellen Datenverarbeitung einfach überlassen könnten. Denn auch die kommunalen Volksvertretungen werden ihre Initiativ- und Kontrollfunktionen schon in wenigen Jahren nur noch unter Zuhilfenahme EDV-unterstützter Informationen zeitgemäß ausfüllen können.

Bereits die erste Version des „Regionaldatenatlas Odenwaldkreis", die kürzlich als Teil des

HEPAS erschienen ist, läßt Richtung und Ausmaß der Veränderungen erkennen, die die Praxis der politischen Planungsinformation in den nächsten Jahren durchlaufen wird. Für die gesamte Planung wichtige Trends, wie der in dieser Form unerwartete Rückgang der Geburtenzahlen, hätten auf der Grundlage eines bereits ausgebauten HEPAS wesentlich früher von den verantwortlichen Instanzen erkannt, nach Ursachen und Tragweite näher analysiert und in die politische Entscheidungspraxis eingebracht werden können.

4.3 Datensicherung

4.3.1 HZD und KGRZ

Der Rechnungshof für das Land Hessen hatte bereits im Mai 1967 im Einvernehmen mit der Landesregierung Mindestanforderungen und Empfehlungen für die Verfahrenssicherheit bei Verwendung elektronischer Datenverarbeitungsanlagen in der Landesverwaltung erlassen. Schon darin wurde die verfahrensmäßige Trennung von Programmierung, Datenerfassung, maschineller Verarbeitung und Verwertung der Ergebnisse und die abgestufte Verteilung der Verantwortlichkeiten und Zuständigkeiten auf verschiedene Mitarbeiter gefordert. Schutzbedürftige Aufgaben sollen nicht von einer Person allein durchgeführt werden.

Ungeachtet der Verschiedenheit der Aufgaben haben der Datenschutzbeauftragte und der Rechnungshof gemeinsame Anliegen gegenüber den datenverarbeitenden Behörden und Stellen der öffentlichen Verwaltung. Deshalb ist auf Vorschlag des Datenschutzbeauftragten mit dem Präsidenten des Rechnungshofes vereinbart worden, einen unmittelbaren Gedankenaustausch aufzunehmen und zu pflegen.

Die vom Koordinierungsausschuß eingesetzte Arbeitsgruppe Datenschutz hat, ausgehend von einer Bestandsaufnahme aller erkennbaren Gefahren, einen Katalog wirkungsvoller und praktikabler Maßnahmen (DASCH) entwickelt (vgl. 4.1.1.3 a). Er enthält die Mindestanforderungen für Datenschutz und Datensicherung nach dem heutigen Stand der Datenverarbeitung im Verbund. Wegen der raschen technischen Entwicklung muß er regelmäßig überarbeitet werden. Der Entwurf verlangt für die innere Organisation der HZD und KGRZ die Funktionstrennung von Anwendungsplanung und -programmierung einerseits und Arbeitsausführung andererseits. Er fordert bestimmte bauliche und räumliche Maßnahmen sowie Alarm- und Katastrophenpläne und trifft Zutrittsregelungen für die einzelnen Sicherheitsbereiche. Weitere Sicherheitsregelungen betreffen die Programmfreigabe, den Datentransport, die Dateneingabe und -ausgabe und die anderen Phasen der maschinellen Datenverarbeitung. Jeder Bedienstete des EDV-Verbundes hat sich besonders zu verpflichten, das Datengeheimnis nach § 3 DSG zu wahren.

Die erfolgreiche Durchführung der Sicherheitsmaßnahmen hängt nicht zuletzt von den einzelnen Mitarbeitern ab. Ausbildung und Unterrichtung der Mitarbeiter müssen deshalb das Ziel haben, jeden einzelnen davon zu überzeugen, daß die Sicherheit gerade von seinem Verhalten abhängt.

4.3.2 Außerhalb des Datenverarbeitungsverbundes

Der Datenschutzbeauftragte hat sich auch bei den Rechenzentren außerhalb des Datenverarbeitungsverbundes über Schutzmaßnahmen informiert.

Mit Einführung des Datenaustausches zwischen Arbeitgebern und Stellen der öffentlichen Verwaltung gewinnen die Schutzmaßnahmen immer mehr an Bedeutung. Bei allen Stellen, die die Daten austauschen, ist man daran interessiert, die Erfahrungen des Datenverbundes auf dem Gebiet des Datenschutzes und der Datensicherheit auszuwerten.

5. ANREGUNGEN

Die im ersten Bericht (I 5.1—5.13) gegebenen Anregungen sind zum großen Teil noch aktuell, so z. B. die Forderungen

- Daten soweit möglich in Formen zu speichern, die Rückschlüsse auf den einzelnen nicht zulassen (Anonymisierung, Verschlüsselung, getrennte Aufbewahrung der Identifizierungsmerkmale),
- die Berechtigung zum Zugriff auf Daten näher zu regeln,
- das Verständnis für Datenschutz durch Aus- und Fortbildungsmaßnahmen zu stärken,
- die Maßnahmen der Datensicherheit weiter zu verbessern,
- die Informationsbedürfnisse des Parlaments in die Entwicklung des Hessischen Planungsinformations- und Analyse-Systems mit einzubringen,
- wissenschaftliche Untersuchungen über Entwicklung und Konsequenzen der Datenverarbeitung und Probleme des Datenschutzes zu fördern.

Aus den Erfahrungen der letzten Berichtsperiode ergeben sich darüber hinaus die folgenden Anregungen:

5.1 Unterausschuß für Datenverarbeitung

Gemäß § 14 Abs. 2 der Geschäftsordnung des Hessischen Landtags vom 31. 1. 1973 sollte ein ständiger Unterausschuß für Fragen der maschinellen Datenverarbeitung in der öffentlichen Verwaltung eingesetzt werden.

Die Tätigkeitsberichte des Datenschutzbeauftragten sollen dem Landtag Erkenntnisse und Erfahrungen vermitteln, die sich aus der Datenverarbeitung in der öffentlichen Verwaltung ergeben. Der Landtag benötigt jedoch ein besonderes Organ, um diese Erkenntnisse und Erfahrungen für seine Funktionen nutzbar machen zu können. Denn wie die parlamentarische Behandlung des Ersten Tätigkeitsberichts gezeigt hat, sind die nach § 14 Abs. 1 GOHLT eingesetzten Fachausschüsse hierauf nicht eingerichtet. Nur ein Organ, das die Fortschritte in der Automatisierung der Verwaltung sowie in der Verbesserung und Entwicklung der technischen Methoden unmittelbar kontinuierlich überwacht, ist in der Lage, selbständig zu beurteilen, welche Konsequenzen sich jeweils für den Landtag oder die Opposition ergeben.

5.2 Zusammenarbeit mit privaten Unternehmen

Den Behörden und Stellen der öffentlichen Verwaltung (Land und Kommunen) sollte untersagt werden, empfindliche Daten und Datenermittlungs-Unterlagen zur Erfassung (z. B. Ablochen) oder zur Verarbeitung an private Unternehmen weiterzugeben. Ausnahmen sollten nur zulässig sein, wenn Rückschlüsse auf den einzelnen nicht möglich sind (vgl. 4.1.1.3 d).

Für diese Ausnahmefälle sollten die Behörden und Stellen das jeweilige private Unternehmen vertraglich verpflichten, dem Datenschutzbeauftragten Auskünfte im Sinne des § 13 DSG zu geben und ihm Zutritt zu den Datenerfassungs- oder -verarbeitungsanlagen, den hierfür gelieferten Unterlagen und den Verarbeitungsergebnissen zu gewähren.

5.3 Verrechtlichung von Verwaltungsanordnungen

Die Auskunfts- und Abrufsberechtigung sowie die Löschung von Daten sollten für Informationssysteme des Landeskriminalamtes und des Landesamtes für Verfassungschutz in Rechtsnormen festgelegt werden.

Verwaltungsanordnungen reichen zum Schutz des Bürgers vor mißbräulicher oder zweckentfremdeter Verwendung der über ihn gespeicherten Informationen nicht aus, wenn es sich um empfindliche, der Intimssphäre zuzurechnende Daten handelt (vgl. 4.1.1.3 c und 4.1.1.3 e).

5.4 Richtlinien für Datensicherheit

Die von den Rechenzentren des Hessischen Datenverbundes erarbeiteten Richtlinien über Datenschutz und Datensicherung (DASCH) sollten möglichst bald verbindlich gemacht werden. Die in ihnen enthaltenen Grundsätze sollen soweit möglich auch bei allen anderen Stellen der hessischen Verwaltung, die elektronische Datenverarbeitung betreiben, angewendet werden.

6. SCHLUSSBEMERKUNGEN

Die Dienststelle des Datenschutzbeauftragten konnte in der Berichtszeit weiter ausgebaut werden. Im Haushalt für die Jahre 1973/74 wurde ihre Ausstattung verbessert. Es stehen jetzt Stellen für drei Mitarbeiter des höheren und des gehobenen Dienstes sowie für zwei Schreibkräfte zur Verfügung. Mit Ausnahme dieser Personalkosten ist für die Aufwendungen der Dienststelle auf Vorschlag des Haushaltsausschusses eine eigene Titelgruppe im Einzelplan 02 der Staatskanzlei ausgebracht worden.

*

Der vorliegende Zweite Tätigkeitsbericht bemüht sich aufgrund weiterer einjähriger Erfahrung, den Politikern, den politisch interessierten Kreisen und der Öffentlichkeit die Datenschutzprobleme vor Augen zu führen, die mit der Einführung der EDV in der Landes- und Kommunalverwaltung in Hessen und in der Bundesverwaltung auftreten. Die Tätigkeitsberichte des Datenschutzbeauftragten sind weder Selbstdarstellung noch bloße Rechenschaftslegung. Ihr Sinn und Zweck liegt darin, offene Fragen aus dem Problembereich Datenverarbeitung / Grundrechte / politische Struktur frühzeitig zu erkennen und sie in das Wahrnehmungsfeld der politisch Verantwortlichen und der Öffentlichkeit zu rücken. Wo immer möglich, bemüht sich der Datenschutzbeauftragte, mit eigenen Vorschlägen zur Problemlösung beizutragen; vielfach zwingen ihn seine gesetzliche Stellung und seine Aufgaben, sich auf Hinweise und Anstöße zu beschränken.

Der Datenschutzbeauftragte ist in besonderem Maße darauf angewiesen, Resonanz nicht nur im Lande Hessen, sondern auch in einer weiten Öffentlichkeit zu finden, da er noch immer die einzige unabhängige Einrichtung repräsentiert.

Gesprächspartner mit vergleichbarer Aufgabenstellung gibt es nicht. Vor ähnlichen Problemen, wie die im Bericht angesprochenen, stehen auch die anderen Länder der Bundesrepublik und der Bund. Sie werden dort meist nur verwaltungsintern behandelt. Die breite Öffentlichkeit, Presse und Rundfunk konnten daran keinen Anteil nehmen. Auch die parlamentarischen Organe vermeiden es offenbar, die Materie aufzugreifen. Datenschutzfragen sind zwar oft zu kompliziert, als daß man auf den fachlichen Rat von System- und Verwaltungsexperten verzichten könnte; sie sind aber zu ernst und politisch zu folgenreich, um diesen auch die Entscheidungen zu überlassen.

Anlage I

Diskussionsbeitrag des Hessischen Datenschutzbeauftragten zum Hearing des Bundesinnenministeriums über den Referentenentwurf eines Bundesdatenschutzgesetzes vom 7. bis 9. 11. 1972 in Bonn.

I 1. Datenschutz ist eine der vielfältigen Erscheinungsformen des vom Schrifttum und von der Rechtssprechung anerkannten allgemeinen Persönlichkeitsrechts. Es beruht auf der nach Art 1 GG unantastbaren Würde des Menschen und dem Grundrecht der freien Entfaltung der Persönlichkeit nach Art. 2 GG.

Auch der Entwurf (§ 1) versteht unter Datenschutz nicht nur den Schutz der Daten, die Datensicherung; jedoch erschöpft sich der Datenschutz nicht in einer mehr oder weniger willkürlichen Zusammenfassung von Maßnahmen, die Beeinträchtigungen des Persönlichkeitsrechts verhindern sollen.

Datenschutz ist vielmehr eine der vielfachen Ausstrahlungen des Persönlichkeitsrechts in Richtung auf eine besondere, durch die Computertechnik geschaffene Lage, in welcher Beeinträchtigungen der Würde des Menschen und seiner freien Entfaltungsmöglichkeit greifbar nahe gerückt sind.

2. Aus dieser Ortsbestimmung des Datenschutzes ergibt sich sein Geltungsbereich; nämlich die Gewährleistung des allgemeinen Persönlichkeitsrechts gegenüber der automatischen Verarbeitung von Informationen, die über den einzelnen Bürger oder in bezug auf seine Lebensverhältnisse von der öffentlichen Verwaltung und von der privaten Wirtschaft gesammelt werden.

Das heißt einerseits,
daß der Datenschutz sich auf die automatische oder maschinelle Erfassung, Speicherung, Weitergabe und Veränderung oder Löschung von personenbezogenen Daten sowie auf ihre Verarbeitung und auf die Verarbeitungsergebnisse erstreckt;

andererseits,
daß der Datenschutz auf die sich aus der ADV ergebenden Mißbrauchsgefahren für das Persönlichkeitsrecht begrenzt ist.

3. Der vorliegende Entwurf eines Bundesdatenschutzgesetzes sollte sich daher auf die Abwehr derjenigen Mißbrauchsgefahren beschränken, die für die automatische Datenverarbeitung spezifisch sind.

Die Argumente der Gleichbehandlung und der Verhinderung von Gesetzesumgehungen schlagen nicht durch. Denn manuell geführte Bücher, Listen und Karteien und die automatische Datenverarbeitung sind in bezug auf die Gefährdung des Persönlichkeitsrechts ungleiche Tatbestände. Gesetzesumgehungen sind nicht zu befürchten, weil mit dem „Ausweichen" auf manuell geführte Sammlungen auch die spezifischen Gefahren der Automation schwinden, so daß die herkömmlichen Maßnahmen der Schweigepflicht und des Amtsgeheimnisses wieder relevant werden.

4. Die Abgrenzung der automatischen Datenverarbeitung von der manuellen Sammlung und Auswertung wirft keine besonderen Probleme auf.

Die Regelung in § 1 DSG hat sich als praktikabel erwiesen; der Datenschutz beginnt mit der Herstellung von Unterlagen, die der maschinellen Datenverarbeitung dienen.

II Ein weiteres grundsätzliches Problem ist, wie der Datenschutz realisiert werden kann. Schutzobjekt ist, wie dargelegt, das Persönlichkeitsrecht des Bürgers, sind nicht dagegen, wie die Formulierung in § 4 des Entwurfs vermuten ließe, die Daten.

1. Die Schwierigkeiten bestehen darin, daß der zu schützende Bereich der Privatsphäre des Bürgers nicht absolut, für jeden Fall gültig bestimmt werden kann. Die Informationen über den Einzelnen, die durch den Datensatz oder durch Verknüpfung verschiedener Datensätze vermittelt werden, besitzen oder beanspruchen einen verschiedenen Geheimcharakter je nach dem Zweck ihrer Verwendung und dem Kreis der Informationsempfänger. Deshalb spricht man von der „Relativität der Privatsphäre".
Objektive Maßstäbe, nach denen eindeutig bestimmt werden könnte, welche Datenermittlung oder welche Datenweitergabe das Persönlichkeitsrecht unzulässig beeinträchtigt, gibt es nicht.
Da die Grenzen der Befugnis, in die Privatsphäre einzudringen, nicht materiell bestimmt werden können, müssen formale Lösungen gesucht werden, um eine mißbräuchliche Verwendung von Daten soweit wie möglich auszuschließen.

2. Dafür stehen neben den technischen Zugriffssperren und ähnlichen Vorkehrungen auch organisatorische Maßnahmen zur Verfügung, wie dezentrale Verarbeitungsanlagen, der Ausschluß bestimmter Informationssysteme von der Verknüpfung mit anderen Datenbanken und dgl. Maßstab hierfür ist die „Empfindlichkeit" bestimmter Daten oder Datenverbindungen.

   Beispiele für solche „Empfindlichkeiten" sind die rechtlich geordneten Tatbestände, die z. B. zur Verweigerung des Zeugnisses vor Gericht zum Schutz eines Vertrauensverhältnisses berechtigen.
   Besondere Empfindlichkeit haben daher z. B. die medizinisch-diagnostischen und therapeutischen Daten, wenn das System die Identität des Patienten festzustellen ermöglicht.

   Ähnlich liegt es bei den Informationssystemen der Kriminalpolizei und der Verfassungsschutzämter.

   Vergleichbare Regelungen außerhalb des Datenschutzes sind etwa die Vorschriften, die den Einblick in das Bundeszentralregister beschränken oder die Tilgung von Eintragungen vorschreiben.
   Das Problem spitzt sich auf die Frage zu,

   a) ob bestimmte Merkmale oder Sachverhalte von der Aufnahme in die ADV von vornherein ausgeschlossen werden können — dies möchte ich verneinen —;

   b) ob hinreichend konkretisiert werden kann, wer oder welche Stelle befugt ist, bestimmte Informationen weiterzugeben oder zu empfangen.

3. Aufgabe des Gesetzgebers ist es, zumindest Maßstäbe oder Richtlinien zu geben, welche bestimmte Grenzen setzen, innerhalb derer die Behörden und die nicht öffentlichen Stellen Daten speichern, austauschen oder weitergeben dürfen.

   Die „rechtmäßige Erfüllung der in die Zuständigkeit fallende Aufgabe" (§ 6 d. E.) ist kein hinreichendes Kriterium. Denn ob die Aufgabe rechtmäßig erfüllt wird, hängt gerade auch davon ab, ob der Datenschutz gewährleistet ist, d. h., ob das Persönlichkeitsrecht des Betroffenen nicht beeinträchtigt wird.

   Die andere Formel: „Soweit überwiegende berechtigte Interessen nicht entgegenstehen" (§§ 17, 18, 19, 24, 25) gibt ebenfalls keine konkreten Anhaltspunkte.

   Bei diesen Regelungen bliebe es daher weitestgehend dem Ermessen der Behörde oder der nicht öffentlichen Stelle überlassen, selbst zu bestimmen, ob sie rechtmäßig Daten speichern, austauschen oder weitergeben.

   In diesem Zusammenhang gewinnt die Vorschrift in § 4 Abs. 1 Satz 2 besondere Bedeutung, wonach Datenschutzmaßnahmen nur erforderlich seien, „deren Schutzwirkung in einem angemessenen Verhältnis zu dem Aufwand steht, den sie verursachen". Das würde bedeuten, daß es von den Kosten der Datenschutzmaßnahmen abhinge, ob sie angeordnet werden. Nach dem Grundsatz der Verhältnismäßigkeit von Mittel und Zweck könnte ein Vergleich nur zwischen dem Aufwand für die Schutzmaßnahmen und der Schwere des abzuwendenden Eingriffs zugelassen werden.

III Ein drittes grundsätzliches Problem ist die Sicherstellung und Überwachung des Datenschutzes.

1. Um zutreffend zu beurteilen, welche Maßnahmen in Betracht kommen und notwendig sind, bedarf es zunächst einer Analyse der möglichen Gefahrenquellen.

   Bei der herkömmlichen Sammlung personenbezogener Daten in Büchern, Listen oder Karteien liegt die Gefahr vor allem darin, daß die Sammlung von Unbefugten eingesehen oder daß der sachliche Inhalt der Sammlung von demjenigen, der Zutritt zu ihr hat, Unbefugten ganz oder teilweise mitgeteilt wird. Davor schützt die in verschiedenen Rechtsvorschriften normierte Schweigepflicht.

   Die ADV verändert die Lage:

   Man kann eine Datensammlung auf Datenträgern nicht unmittelbar einsehen; man kann sie nur ausdrucken oder auf einem Bildschirm sichtbar machen. Das vollzieht sich nach einem der Maschine vorgegebenen Programm. Man kann aber die Arbeitsphasen der Maschine beeinflussen. Dazu bedarf es technischer Eingriffe in das Programm. Die Schweigepflicht entspricht dieser neuartigen Situation nicht. Vielmehr muß sichergestellt werden, daß das Maschinen-Programm nicht verändert und daß die Maschine nicht zu programmwidrigen Zwecken benutzt wird.

2. Programmierer und Operateur sind die „weichen Stellen" der automatischen Datenverarbeitung, wie auch die bekanntgewordenen Fälle der Computer-Kriminalität beweisen.

   Diesem Sachverhalt entsprechen die Vorschriften des Entwurfs nicht genügend:

   a) Die Strafvorschrift (§ 32) erfaßt nur den Tatbestand der unbefugten Weitergabe und Veränderung von Daten, nicht die Änderung oder Verfälschung des Programms.
   b) Die Aufsichtsbehörde (§ 31) überwacht nur die in Abschnitt IV des Entwurfs genannten nicht öffentlichen Stellen.
   c) Im öffentlichen Bereich und bei den in Abschnitt III d. E. genannten nicht öffentlichen Stellen begnügt sich der Entwurf mit der Selbstkontrolle.

   Die Kontrolle hat aber als Schutzmaßnahme gegen Datenmißbrauch bei der ADV besondere Bedeutung, weil, wie dargelegt, die Grenzen des Umganges mit privatbezogenen Daten nicht durch allgemeingültige Definitionen des unantastbaren Bereiches der Privatsphäre abgesteckt werden können, sondern weitgehend nur durch organisatorische und technische, also formale Maßnahmen. Eine der möglichen organisatorischen Maßnahmen ist die Kontrolle.

   Die Kontrolle ist um so wirksamer, je unabhängiger die Kontrollinstanz ist. Daher sind Inkompatibilitäten und Interessenkollisionen zu vermeiden.

   Die im Entwurf vorgesehene Selbstkontrolle in der Bundesverwaltung entspricht diesen Grundsätzen nicht.

Anlage II

Vorschlag des Datenschutzbeauftragten zum Entwurf des Krankenhausgesetzes

§ 13

Datenverarbeitung im Krankenhauswesen

(1) Die Krankenhausträger sind verpflichtet,

1. die der Auskunftspflicht nach § 28 des Gesetzes zur wirtschaftlichen Sicherung der Krankenhäuser und zur Regelung der Krankenhauspflegesätze — KHG — vom 29. 6. 1972 (BGBl. I S. 1009) unterliegenden Informationen (Daten) und
2. die wirtschaftlichen und die für die gegenwärtige ärztliche und pflegerische Betreuung des Patienten maßgeblichen medizinischen (diagnostischen und therapeutischen) Daten, auch soweit sie für eine künftige ärztliche Betreuung bedeutsam werden können,

in ein Verbundsystem der Datenverarbeitung einzubringen (Anschlußzwang).

(2) Die Daten nach Abs. 1 Nr. 1 und Nr. 2 sind voneinander getrennt zu speichern. In das Verbundsystem nach Abs. 1 Nr. 2 dürfen die Daten über den einzelnen Patienten nur in verschlüsselter Form eingegeben werden, die eine Rückidentifizierung außer durch einen verantwortlichen Arzt des eingebenden Krankenhauses ausschließt, es sei denn, der Patient stimmt einer offenen Weitergabe der ihn betreffenden Daten zu.

(3) Der Patient ist bei der Aufnahme in das Krankenhaus oder wenn sein Zustand dies nicht gestattet, zu dem frühestmöglichen Zeitpunkt über die Verwendung der ihn betreffenden Daten nach Abs. 1 und 2 zu unterrichten.

(4) Der Patient hat ein Recht auf Auskunft darüber, welche medizinischen Daten über ihn gespeichert und an welche Stellen sie weitergegeben worden sind. Die Auskunft kann verkürzt werden, wenn es aus gesundheitlichen Gründen im Interesse des Patienten geboten ist.

(5) Die Landesregierung wird ermächtigt, das Nähere durch Rechtsverordnung zu regeln, insbesondere

1. die Mitwirkung der Krankenhausträger im Verbundsystem der Datenverarbeitung,
2. die Abgeltung der Kosten durch die Krankenhausträger für die Inanspruchnahme des Verbundsystems,
3. den Beginn und den Umfang des Anschlußzwanges sowie die Ausnahme vom Anschlußzwang,
4. wie die Trennung der in Abs. 1 Nr. 1 und Nr. 2 genannten Daten durchzuführen und wie die Daten im Falle der Weitergabe zu verschlüsseln sind,
5. in welcher Weise der nach Abs. 2 verantwortliche Arzt zu bestimmen ist,
6. wie die Auskunft nach Abs. 4 erteilt wird und wer darüber bestimmt, ob und wie eine Auskunft zu verkürzen ist,
7. weitere Maßnahmen des Datenschutzes und der Datensicherung.

§ 13 a

Weitergabe von Daten an Datenbanken und Informationssysteme

Daten aus dem Verbundsystem nach § 13 sind für den Aufbau von Datenbanken und Informationssystemen der öffentlichen Verwaltung sowie für amtliche Statistiken weiterzugeben. Die Krankenhausträger haben sicherzustellen, daß Rückschlüsse auf Einzelpersonen ausgeschlossen sind. Das Nähere bestimmt die Landesregierung durch Rechtsverordnung.

§ 13 b

Überwachung des Datenschutzes

Die Rechte und Pflichten des Datenschutzbeauftragten nach dem Datenschutzgesetz vom 7. 10. 1970 (GVBl. I S. 625) erstrecken sich auch auf die freigemeinnützigen und die privaten Krankenhausträger sowie deren Einrichtungen, soweit sie an dem Verbundsystem der Datenverarbeitung nach § 13 teilnehmen.

Begründung

1. Das DSG gilt nur für die Behörden und Stellen der öffentlichen Verwaltung (§ 1). Die Datenverarbeitung im Krankenhauswesen erfaßt auch freigemeinnützige und private Krankenhausträger und deren Einrichtungen. Daher muß der Datenschutz auch hierauf erstreckt werden. Eine allgemeine Verweisung auf das Datenschutzgesetz genügt aber nicht. Denn das Datenschutzgesetz enthält nur Generalklauseln, die insbesondere im Krankenhauswesen einer Konkretisierung bedürfen.

2. Das vom Gesetzgeber konzipierte zweistufige Datenverbundsystem wird zweckmäßigerweise in zwei Vorschriften getrennt geregelt. Für beide Systeme gelten unterschiedliche Grundsätze.

   In § 13 wird das Verbundsystem im Bereich des Krankenhauswesens,

   in § 13 a wird die Integrierung des Verbundsystems des Krankenhauswesens mit Datenbanken oder Informationssystemen der öffentlichen Verwaltung (vgl. § 5 Abs. 1 und 2 DSG) geregelt.

3. In § 13 Abs. 2, 3 und 4 werden die hauptsächlichen Grundsätze zum Schutze der „empfindlichen" Individualdaten aus dem medizinischen Bereich festgelegt.

   Der Gesetzgeber muß dem Verordnungsgeber seine Maßstäbe für den Datenschutz vorgeben. Keine Blankoermächtigung für die Landesregierung. Weil das DSG nur Generalklauseln enthält, müssen für die einzelnen Lebensbereiche je nach dem Empfindlichkeitsgrad der gespeicherten Individualdaten konkrete Datenschutzmaßnahmen vorgeschrieben werden.

4. § 13 Abs. 5 Nr. 4, 5 und 6 bezeichnet die wesentlichen Gegenstände, die der Regelung durch die Landesregierung noch bedürfen und durch Rechtsverordnung — nicht Verwaltungsanordnung — zu regeln sind.

5. § 13 a behandelt die Integrierung des Verbundsystems nach § 13 in allgemeine Datenverarbeitungssysteme der öffentlichen Verwaltung und ihre Auswertung für statistische Zwecke in Anlehnung an § 5 Abs. 1 DSG. Das DSG ist sozusagen das Grundgesetz für den Datenschutz in der öffentlichen Verwaltung. Daher ist es notwendig, Gesetze, welche die Grundsätze des DSG in bestimmten Bereichen der öffentlichen Verwaltung verwirklichen, mit den Vorschriften des DSG zu koordinieren.

6. § 13 b erstreckt die Rechte und Pflichten des Datenschutzbeauftragten (§§ 10, 13) auch auf die freigemeinnützigen und privaten Krankenhausträger und deren Einrichtungen. Dies ist mindestens zur Klarstellung nötig, weil §§ 10 und 13 DSG ausdrücklich auf die Behörden und Stellen verweisen, die in § 1 genannt sind, und aus dem Anschlußzwang an das Datenverbundsystem des Krankenhauswesens nicht ohne weiteres zu folgern ist, daß die privaten und freigemeinnützigen Krankenhäuser damit auch der Überwachung durch den Datenschutzbeauftragten unterliegen und ihm auch auskunftspflichtig sind.

SACHWÖRTERVERZEICHNIS

(I und II bezeichnen den Ersten bzw. den Zweiten Tätigkeitsbericht, die arabischen Ziffern die Abschnitte der Berichte.)