HESSISCHER LANDTAG

7. Wahlperiode . Drucksache 7/1495

29. 03. 72

Vorlage des Datenschutzbeauftragten

betreffend den Ersten Tätigkeitsbericht

Mit Schreiben vom 29. März 1972 legt der Datenschutzbeauftragte gemäß § 14 Abs. 1 des Datenschutzgesetzes vom 7. Oktober 1970 (GVBl. I S. 625) dem Landtag folgenden Ersten Tätigkeitsbericht vor:

Eingegangen am 29. März 1972 . Ausgegeben am 12. April 1972

Druck: Carl Ritter & Co. Wiesbaden . Vertrieb: Verlag Dr. Hans Heger 53 Bonn-Bad Godesberg Goethestr. 54 Tel. 63551

Erster Tätigkeitsbericht

des

Hessischen Datenschutzbeauftragten

vorgelegt zum 31. März 1972

gemäß § 14 des Hessischen Datenschutzgesetzes vom 7. Oktober 1970

INHALTSVERZEICHNIS

1. VORBEMERKUNGEN

1.1 Einleitung

Der erste Datenschutzbeauftragte des Landes Hessen wurde auf Grund des Hessischen Datenschutzgesetzes vom 7. Oktober 1970 am 8. Juni 1971 vom Hessischen Landtag auf Vorschlag der Landesregierung gewählt. Er trat am gleichen Tag sein Amt an.

Die seitdem gemachten Erfahrungen ermöglichen noch keine umfassende Darstellung aller den Datenschutz berührenden Probleme, die sich aus der Einführung der maschinellen Datenverarbeitung in der öffentlichen Verwaltung ergeben. Einmal war die Zeit zu kurz, um ein so großes und komplexes Terrain zu erforschen. Zum anderen ist die Entwicklung der elektronischen Datenverarbeitung (EDV) noch alles andere als abgeschlossen.

Trotzdem haben die wenigen Monate der Tätigkeit des Datenschutzbeauftragten gezeigt, wie vielschichtig die Probleme des Datenschutzes und der Datensicherung sind. Die Notwendigkeit, diesen Problemkreis zu erkennen, zu analysieren, frühzeitig unerwünschte Tendenzen und Gefahrenherde festzustellen und Gegenmaßnahme anzuregen, hat sich bestätigt.

Am Anfang der Tätigkeit stand eine Bestandsaufnahme der maschinellen Datenverarbeitung in der öffentlichen Verwaltung des Landes Hessen. Sie war Ausgangsbasis für die Überlegungen, in welcher Form und mit welchen Mitteln der Datenschutzbeauftragte seine Überwachungsfunktion ausüben sollte. Für eine fundierte Beurteilung der hessischen Situation war es darüber hinaus unumgänglich, die Entwicklung von Automation und Datenverarbeitung auf einer möglichst breiten Ebene zu verfolgen und anderwärts gemachte Erfahrungen zu verwerten.

1.2 Vorgeschichte

1.2.1 Die elektronische Datenverarbeitung in der Verwaltung

Die rasche Fortentwicklung der modernen Industriegesellschaft macht in immer stärkerem Maße eine umfassende planerische Vorsorge notwendig. Diese Entwicklung führte zu einem sprunghaften Anwachsen der öffentlichen Aufgaben. Der traditionelle Obrigkeitsstaat war dieser Aufgabenflut nicht gewachsen. Er wurde vom modernen sozialen Leistungsstaat abgelöst.

Um die neuen Aufgaben sachgemäß und rechtzeitig erledigen zu können, mußte die Verwaltung ihre Struktur und ihre Arbeitsmethoden überprüfen und ökonomischer gestalten. Ihre Entscheidungen beeinflussen das Leben der Gemeinschaft und des einzelnen in erheblichem Maße. Um richtige Entscheidungen fällen zu können, benötigt die Verwaltung möglichst umfassende Informationen, d. h. die Qualität ihrer Entscheidungen ist in erster Linie abhängig von der Quantität und Qualität der verfügbaren Informationen. Das große Problem für jede Verwaltung ist deshalb der Informationsfluß, denn veraltete, unvollständige und fehlerhafte Informationen können zu Fehlentscheidungen mit unter Umständen katastrophalen Folgen führen.

Die herkömmliche Art und Weise, in der die Verwaltung sich die für ihre Arbeit erforderlichen Informationen beschafft, beruht auf der historisch gewachsenen — nicht immer sachgerecht begründeten — Aufteilung ihrer Arbeitsgebiete. Jedes Arbeitsgebiet besorgt sich seine speziellen Informationen, ohne sich dabei mit anderen Arbeitsgebieten abzustimmen. So werden zahlreiche Informationen vielfach erfragt und festgehalten. Die Grunddaten für jeden Bürger — wie Name, Anschrift, Geburtsdatum, Familienstand usw. — sind heute in weit über 100 verschiedenen Karteien enthalten. Diese Mehrarbeit wird künftig vermeidbar sein. Im Rahmen eines integrierten Informationssystems brauchen diese Angaben nur an einer Stelle gespeichert zu sein, von der jede berechtigte Behörde sie abrufen kann, um sie mit anderen Informationen zu kombinieren und zu verarbeiten.

Zur Erfassung, Speicherung und Verarbeitung von Informationen bedient sich die Verwaltung daher in zunehmendem Umfang der elektronischen Datenverarbeitung. Sie ermöglicht bei zweckentsprechender Organisation einen schnellen Fluß und eine umfassende, exakte und gezielte Auswertung der Informationen. Sie macht den Verwaltungsablauf sicherer, wirtschaftlicher und transparenter. Diese moderne Informationstechnik ist ein Hilfsmittel für die Verwaltung. Es gibt ihr die Möglichkeit zu schnellen und sachlich qualifizierten Entscheidungen für ihr operatives und planerisches Handeln. Beim operativen Handeln stehen die Aufgaben sowie die Mittel und Verfahren zu ihrer Erledigung fest; der Entscheidungsspielraum ist genau begrenzt.

Bei der Planung hingegen ist das Ziel bekannt, und es wird untersucht und darüber entschieden, wie dieses Ziel mit den verfügbaren Mitteln erreicht werden kann.

Es liegt im Interesse des einzelnen Bürgers wie der Gemeinschaft, daß der Verwaltung für ihre Entscheidungen möglichst umfassende Informationen zur Verfügung stehen. Gleichzeitig entstehen damit aber auch neue Probleme für das Verhältnis des Bürgers zum Staat:

Die Behörden, denen der Bürger im Interesse der Ordnung des Gemeinwesens oder als Voraussetzung für staatliche Leistungen Auskünfte über seine persönlichen Lebensverhältnisse gibt, waren seither auf den in der Regel überschaubaren lokalen oder regionalen Bezirk begrenzt. Dies ändert sich, wenn die Individualinformationen in Datenbanken oder integrierten Informationssystemen gespeichert werden. Dem Bürger bleibt es verborgen, wohin und für welche Zwecke seine Individualdaten weitergegeben werden. Außerdem bildete bisher die arbeitsteilige Aufgliederung in selbständige Ressorts eine Barriere gegen die „Allwissenheit" des Staates. Das integierte Informationssystem hebt diese Barrieren auf durch die Möglichkeiten des Vielfachzugriffs und der Datenübertragung über große Entfernungen hinweg.

Die Vorteile für Regierung und Verwaltung liegen auf der Hand. Andererseits bedroht diese Technik die freie und unkontrollierte Entfaltungsmöglichkeit des Menschen durch Einblicke in seine Privatsphäre und durch die Möglichkeiten der Manipulation mit den so gewonnenen Informationen. Wenn auch die Fähgikeiten eines noch so vollkommenen Informationssystems natürliche Grenzen haben und ein Wunderglaube an den Computer verfehlt wäre, so dürfen doch die Mißbrauchsmöglichkeiten eines derartigen technischen Systems nicht unterschätzt werden. Es ist auch ein Instrument staatlicher Machtausübung und birgt die Verlockung in sich, es so umfassend, wie die Technik es ermöglicht, zu gebrauchen. Dabei können leicht die Schranken überschritten werden, welche die Grundrechte und die demokratischen Prinzipien des Staates ziehen.

Gleichzeitig mit der Einführung und dem Ausbau der elektronischen Datenverarbeitung muß daher sorgfältig geprüft werden, ob die bestehenden Sicherheits- und Geheimhaltungsbestimmungen für die neuen Techniken noch ausreichen, ob neue Vorkehrungen erforderlich sind und welche Auswirkungen sich dabei für die bisher angewandten Bestimmungen ergeben.

1.2.2 Einführung der EDV in Hessen

In Hessen erkannte man schon sehr früh die Bedeutung der elektronischen Datenverarbeitung für die Rationalisierung der Verwaltung. Durch eine Reihe verwaltungsinterner Untersuchungen bereitete man den Boden vor für eine möglichst weitgehende Erfassung der diversen Verwaltungszweige durch ein integriertes Informationssystem.

Am 16. Dezember 1969 verabschiedete der Landtag das Gesetz über die Errichtung der Hessischen Zentrale für Datenverarbeitung (HZD) und Kommunaler Gebietsrechenzentren (KGRZ) (GVBl. I S. 304). Das Gesetz gab die rechtliche Grundlage für den Aufbau einer integrierten Datenverarbeitung für die staatliche und kommunale Verwaltung..

Ende 1971 wurden im Bereich der Landesverwaltung in Hessen mit Hilfe der EDV 157 Aufgaben voll und 87 teilweise erledigt, und zwar in den Bereichen Einwohnerwesen, Finanzwesen, Personalwesen, Gesundheitswesen, Sozialwesen, Bildungswesen, Öffentliche Sicherheit und Ordnung, Rechtswesen, Landwirtschaft und Forsten und Technik. Weitere rund 250 Angaben sollen später durch die Datenverarbeitung erfaßt werden. Die Übernahme anderer Bereiche der Landesverwaltung in die Datenverarbeitung befindet sich im Vorbereitungsstadium.

Diese schnelle Ausbreitung der elektronischen Datenverarbeitung ist um so bemerkenswerter, weil bisher nur Massen- und Routinearbeiten erfaßt wurden. Hier ist der Vorteil der elektronischen Datenverarbeitung unumstritten. Bei der Berechnung von Bezügen, von Renten oder von Steuerschulden, bei der Aufarbeitung statistischer Unterlagen oder im Einwohner- und Meldewesen, aber auch in anderen Sachbereichen hat sich gezeigt, daß die öffentliche Verwaltung ihre Aufgaben ohne die Automation nicht mehr bewältigen könnte. Dynamische Renten z. B. sind ohne Computer praktisch kaum noch berechenbar. Trotzdem ist die Leistungsfähigkeit der Anlagen noch keinesfalls voll ausgenutzt. Und die Integration, d. h. der Verbund verschiedener Dateien, Datenbanken und Informationssysteme untereinander, befindet sich erst im Anfangsstadium bzw. im Stadium der Vorbereitung. Aber schon heute kann festgestellt werden, daß die öffentliche Verwaltung in Zukunft immer mehr auf die maschinelle Datenverarbeitung angewiesen sein wird. Auf diese Entwicklung bezog sich Ministerpräsident Osswald im Vorwort zu „Hessen '80 — Datenverarbeitung" mit den Worten: „Regieren und Verwalten wird in Zukunft mit der Entwicklung von Informationssystemen und Datenbanken untrennbar verbunden sein. Diese Modernisierung der Verwaltung wird .... dem wachsenden Informationsbedürfnis von Legislative und Exekutive Rechnung tragen."

Die Landesregierung gab damit zu erkennen, daß sie bereits im damaligen Zeitpunkt die Notwendigkeit sah, ein Informationsgleichgewicht zwischen Legislative und Exekutive sicherzustellen, obwohl dieses Problem in der Auseinandersetzung über die Möglichkeiten und Problematik der elektronischen Datenverarbeitung erst in jüngster Zeit die ihm zukommende Bedeutung erhalten hat und auch im Gesetz über die Errichtung der Hessischen Zentrale für Datenverarbeitung (HZD) und Kommunaler Gebietsrechenzentren (KGRZ) vom 25. Juni 1970 noch nicht erwähnt worden ist.

1.2.3 Notwendigkeit und Problematik des Datenschutzes

Die maschinelle Datenverarbeitung liefert der öffentlichen Verwaltung nicht nur verbesserte

Informationen; sie schafft auch neue Möglichkeiten des Informationsmißbrauchs. Es muß deshalb sichergestellt sein, daß

1. das Persönlichkeitsrecht des Bürgers berücksichtigt und nur soviel Informationen über ihn gespeichert werden, wie die Verwaltung für ihre Entscheidungen benötigt,
2. die Datenbestände vor unberechtigten Zugriffen und Veränderungen geschützt sind und
3. die Parlamente aller Ebenen ein — allerdings auf nicht personenbezogene Daten begrenztes — Zugriffsrecht auf die Datenbestände erhalten.

Für Inhalt und Umfang des Schutzes des Persönlichkeitsrechts des Bürgers hat das Bundesverfassungsgericht in verschiedenen neueren Urteilen Maßstäbe entwickelt. Danach ist es mit der Menschenwürde nicht vereinbar,

> „wenn der Staat das Recht für sich in Anspruch nehmen könnte, den Menschen zwangsweise in seiner ganzen Persönlichkeit zu registrieren und zu katalogisieren, sei es auch in der Anonymität einer statistischen Erhebung, und ihn damit wie eine Sache zu behandeln, die einer Bestandsaufnahme in jeder Hinsicht zugänglich ist. . . . . Dem einzelnen (muß) um der freien und selbstverantwortlichen Erhaltung seiner Persönlichkeit willen ein ‚Innenraum' verbleiben . . . . ., in dem er ‚sich selbst' besitzt und ‚in den er sich zurückziehen kann, zu dem die Umwelt keinen Zutritt hat, in dem man in Ruhe gelassen wird und ein Recht auf Einsamkeit genießt' (Wintrich, Die Problematik der Grundrechte, 1957 S. 15 f.). . . . . In diesem Bereich kann der Staat . . . . bereits durch eine — wenn auch bewertungsneutrale — Einsichtnahme eingreifen, die die freie Entfaltung der Persönlichkeit durch psychischen Druck öffentlicher Anteilnahme zu hemmen vermag. . . . . "
>
> Andererseits muß jedermann „als gemeinschaftsbezogener und gemeinschaftsgebundener Bürger . . . . die Notwendigkeit statistischer Erhebungen über seiner Person in gewissem Umfang, wie z. B. bei einer Volkszählung, als Vorbedingung für die Planmäßigkeit staatlichen Handelns hinnehmen. . . . . .
>
> Eine statistische Befragung zur Person kann deshalb dort als entwürdigend und als Bedrohung des Selbstbestimmungsrechtes empfunden werden, wo sie den Bereich menschlichen Eigenlebens erfaßt, der von Natur aus Geheimnischarakter hat, und damit auch diesem inneren Bezirk zu statistisch erschließbarem und erschließungsbedürftigem Material erklärt. . . . . Wo dagegen die statistische Erhebung nur an das Verhalten des Menschen in der Außenwelt anknüpft, wird die menschliche Persönlichkeit in aller Regel noch nicht in ihrem unantastbaren Bereich privater Lebensgestaltung erfaßt." (Vgl. BVerfGE, Beschluß v. 16. 7. 1969)

An anderer Stelle sagt das Bundesverfassungsgericht:

> „Dem Schutz der Integrität der menschlichen Person in geistig-seelischer Beziehung ist ein besonders hoher Wert beizumessen." (Vgl. BVerfGE 27, 1 und 344)

Welche einzelnen personenbezogenen Daten zu diesem — auch Intimsphäre genannten — Bereich des Persönlichkeitsrechts gehören, kann nicht eindeutig bestimmt werden. Der Name, das Geschlecht, der Wohnsitz, das Geburtsdatum, der Familienstand, kurz Merkmale, die den einzelnen identifizieren, sind meistens offenkundig. Dagegen gehören Angaben über Krankheiten, über Aufenthalt in geschlossenen Anstalten, über die Zugehörigkeit oder Nichtzugehörigkeit zu einer Kirche, einer Religions- oder Weltanschauungsgemeinschaft, über Betriebsumsätze, gewerbliche Herstellungsverfahren, über Einkommen- und Vermögensverhältnisse zu der Kategorie von Merkmalen einer Person, die ihrer Natur nach Geheimnischarakter haben. Sie werden einem Dritten in der Regel nur offenbart, wenn die Diskretion auf Grund eines besonderen Vertrauensverhältnisses verbürgt ist, wie beim Arzt, Pfarrer, Rechtsberater, Fürsorger. Andererseits sind diese oder ähnliche Daten der Intimsphäre ohne Geheimnischarakter, wenn die Person, auf die sie sich beziehen, unbekannt bleibt und ihre Identifizierung auch nicht durch Rückschlüsse möglich ist. Dies trifft in der Regel für Tatbestände zu, die für statistische Zwecke erfaßt werden. Solche „harmlosen" Daten können jedoch ihre Qualität verändern, wenn sie mit Identifizierungsmerkmalen verbunden werden, weil dadurch persönliche Eigenschaften oder Verhaltensweisen des betroffenen Bürgers bloßgelegt werden. Die Gefahr der Zusammenführung von Daten aus dem „Bereich menschlichen Eigenlebens . . . ., der von Natur Geheimnischarakter hat", mit Identifizierungsmerkmalen des einzelnen Bürgers wächst mit dem Fortschreiten des Verbundes einzelner Dateien aus verschiedenen Aufgabenbereichen der öffentlichen Verwaltung zu Datenbanken und Informationssystemen.

In diesem Zusammenhang stellt sich die Frage, ob es Daten gibt, die wegen ihres Charakters von vornherein von der Datensammlung auszuschließen sind, so wie etwa unzulässig erworbene Beweise oder Beweismittel im Gerichtsverfahren unberücksichtigt bleiben müssen. Unter diesem Gesichtspunkt ist z. B. auch die Datenbank des Hessischen Landeskriminalamtes zu prüfen. Das Persönlichkeitsrecht des Bürgers wird beeinträchtigt, wenn in bezug auf seine Person Daten gesammelt werden, die keine ob-

jektiv nachgewiesenen, sondern nur vermutete Merkmale oder Verhaltensweisen seiner Person fixieren.

Das gleiche muß gelten, wenn unbestimmte, auf persönlich-subjektive Einschätzungen beruhende Urteile und Annahmen als Daten erfaßt werden. Denn hier geht es für den Betroffenen nicht nur darum, in bestimmtem Umfang unbeobachtet und unkontrolliert zu sein. Hinzu tritt die oft noch unerträglichere Gefahr, subjektiv oder objektiv von der Umwelt falsch eingeschätzt zu werden. Werden solche Daten auch nur beschränkt weitergegeben, so kann bereits eine einzige nachteilige Information die Entfaltungschancen des Betroffenen empfindlich beeinträchtigen. Denn der Empfänger wird die Information in der Regel nicht richtig einschätzen können, weil er die Bedingungen, unter denen sie zustande gekommen sind, nicht kennt.

Die sich hieraus ergebenden Bedenken sprächen für einen radikalen Verzicht auf die Verarbeitung und Speicherung solcher Daten. Dem stehen die spezifischen Informationsbedürfnisse vieler Bereiche der Verwaltung entgegen. Im Personalwesen und im Ausbildungssektor wird man ohne Leistungsbeurteilungen nicht auskommen. Ärztliche Diagnosen oder polizeilich-kriminalistische Aufzeichnungen sind unentbehrlich. Hier kommt den Beschränkungen und Kontrollen besonderes Gewicht zu. Die Verarbeitung und Verwertung solcher Daten muß ein interner Vorgang der zuständigen Verwaltung bleiben.

Die rechtliche Frage, inwieweit der Bürger wegen der vom Bundesverfassungsgericht angesprochenen Sozialbindung solche Maßnahmen der Verwaltung z. B. im Interesse einer wirksamen Verbrechensbekämpfung hinnehmen muß, ist vom Datenschutzbeauftragten nicht zu entscheiden. Auf die Problematik muß jedoch hingewiesen werden (siehe auch unter 4.113 c).

Zum Schutz der Privatsphäre gibt es bereits eine Reihe von Vorschriften im BGB und im StGB, im Gesetz über die Statistik für Bundeszwecke, in der Gewerbeordnung, in der Reichsabgabenordnung und in den Geheimhaltungs- und Verschwiegenheitsvorschriften für öffentliche Bedienstete. Aber diese Vorschriften entsprechen nicht mehr dem technischen Stand der elektronischen Datenverarbeitung und sind nicht umfassend genug. „Sämtliche zur Zeit existierende Schutzmaßnahmen sind auf eine ganz andere Informationsstruktur zugeschnitten. Gerade weil elektronische Anlagen eine neue Informationsqualität garantieren, bedarf es auch neuer, an den spezifischen Eigenschaften der elektronischen Datenverarbeitung ausgerichteten Regeln“ (Simitis in NJW 1971, S. 677).

Zur Regelung des Datenschutzes und der Datensicherung kommen berufsethisch-personelle, rechtliche, technische und organisatorische Maßnahmen in Betracht. Die Schutzmaßnahmen sollen die Datenverarbeitung nicht über Gebühr behindern, weil sonst der Nutzen der Automation in Frage gestellt würde. Außerdem müssen die Kosten der einzelnen Vorkehrungen in einem vertretbaren Verhältnis zu den Gesamtkosten der Datenverarbeitung stehen. Datenverarbeitung ohne wirksamen Datenschutz darf es jedoch nicht geben. Ist bei einzelnen Automationsprojekten eine wirtschaftliche Lösung der Datenschutzproblematik nicht möglich, so dürfen nicht etwa die Sicherheitsanforderungen herabgeschraubt werden. Vielmehr muß man die betreffenden Projekte zurückstellen. Damit wird nur die Konsequenz aus der Erkenntnis gezogen, daß eine freie, d. h. nur technisch und wirtschaftlich begrenzte Entwicklung der Automation nicht mehr den heutigen sozialen Bedürfnissen der Gesellschaft gerecht wird. Der Datenschutz ist eine der sozialen Grenzen, die die Gesellschaft dem technologischen Fortschritt stecken muß.

Die Bundesregierung hat als Diskussionsbasis den Plan für ein allgemeines Informationssystem vorgelegt, das sowohl den öffentlichen als auch den privaten Bereich umfaßt (Das Informationsbankensystem, Carl Heymanns Verlag KG 1971). In Rheinland-Pfalz ist bereits ein Einwohnerinformationssystem in Betrieb genommen worden, das die Datenfernverarbeitung verwendet. An ihm sind 16 staatliche und — versuchsweise — 3 kommunale Behörden beteiligt. Die Entwicklung der elektronischen Datenverarbeitung ist bereits so weit fortgeschritten, daß die damit verbundenen Gefahren klar erkennbar sind. Integrierte Informationssysteme sind in Vorbereitung und teilweise bereits in Ansätzen vorhanden.

In der wissenschaftlichen Literatur dominiert die Ansicht, daß die Rechtsordnung Gefahr laufe, „der Entwicklung hinterher zu hinken“ (Simitis; ähnlich Steinmüller, Kamlah). „Schutzmaßnahmen gegen die mißbräuchliche Verwendung elektronischer Anlagen dürfen niemals nur nachträgliche Reaktionen auf bittere Erfahrungen sein, sie müssen vielmehr den zwangsläufigen normativen Kontext jeder Einrichtung einer elektronischen Datenbank bilden“ (Simitis a.a.O. S. 677).

In Hessen wurde mit dem Datenschutzgesetz vom 7. Oktober 1970 der Versuch unternommen, diese Aufgabe zu lösen.

1.3 Das Hessische Datenschutzgesetz

1.3.1 „Vorstoß ins Neuland“

Die Hessische Landesregierung legte, in Ergänzung des Gesetzes über die Errichtung der Hessischen Zentrale für Datenverarbeitung (HZD) und Kommunaler Gebietsrechenzentren (KGRZ) vom 16. Dezember 1969, am 25. Juni 1970 den Entwurf für ein Datenschutzgesetz vor (Hessicher Landtag, 6. Wahlperiode, Drucks. Nr.

3065). Darin wurde neben dem Schutz der Privatsphäre auch ein Informationsrecht des Landtags und der kommunalen Vertretungsorgane festgelegt. In der Begründung zu dem Gesetz betonte die Landesregierung, „sie ergreife mit der Vorlage des Datenschutzgesetzes die Initiative, um nachteiligen Auswirkungen des Einsatzes der elektronischen Datenverarbeitung in Regierung und Verwaltung vorzubeugen".

Es gelte vor allem,

„die Privatsphäre des Bürgers zu sichern,

die Datenbestände vor unberechtigten Zugriffen zu schützen und

die Parlamente aller Ebenen, dem Landtag, den Kreistagen und den Gemeindevertretungen Zugang zu den gespeicherten Informationen zu gewähren."

Mit der Verabschiedung des Datenschutzgesetzes und der Einrichtung der Institutionen des Datenschutzbeauftragten betrat Hessen juristisches „Neuland". Es gibt keine vergleichbare Einrichtung. Parlament und Regierung waren sich dabei bewußt, daß es bei dem derzeitigen Stand der Entwicklung nicht möglich war, ein Gesetz vorzulegen, das viele Jahre oder gar Jahrzehnte unverändert gelten kann. Der Gesetzgeber hielt es aber für besser, bereits jetzt eine — wenn auch ergänzungsbedürftige — Regelung zu schaffen, anstatt eine perfekte Regelung verspätet zu verabschieden.

1.3.2 Bereich und Inhalt des Gesetzes

Das Hessische Datenschutzgesetz gilt nur im Bereich der öffentlichen Verwaltung des Landes. Es erfaßt in diesem Bereich alle Unterlagen, die für die Zwecke der maschinellen Datenverarbeitung hergestellt werden sowie alle gespeicherten Daten und die Ergebnisse ihrer Verarbeitung (§ 1). Das Gesetz mußte sich auf eine Regelung für die öffentliche Verwaltung beschränken, weil Regelungen im Bereich des Privatrechts unwirksam geblieben wären, sei es, daß sie mit geltendem Bundesrecht kollidieren, sei es, daß sie wegen der räumlichen Begrenzung auf das Land leicht umgangen werden können. Das Gesetz gilt daher nicht für die maschinelle Datenverarbeitung im privatrechtlichen Bereich, also nicht für den einzelnen Bürger, für Vereine oder Gesellschaften des bürgerlichen oder des Handelsrechts, welche DV-Anlagen für ihre persönlichen, beruflichen oder gewerblichen Zwecke einsetzen.

Der Datenschutz greift jedoch ein, wenn eine Behörde oder Stelle der öffentlichen Verwaltung im Sinne des § 1 einen Privatunternehmer beauftragt, Unterlagen oder Daten herzustellen bzw. zu verarbeiten. Es kommt darauf an, ob mit dem Einsatz der EDV eine kronkrete Aufgabe der öffentlichen Verwaltung erfüllt werden soll, nicht jedoch darauf, wo der technische Vorgang vollzogen wird.

1.4 Der Datenschutzbeauftragte

Die Schwierigkeiten einer Realisierung des Datenschutzes liegen weniger im Bereich der technischen Sicherung: wie z. B. Schutz der Datenträger vor Verlust, Beschädigung und gegen unbefugte Verwendung, als vielmehr im rechtspolitischen Bereich: Schutz vor Mißbrauch der Individualinformationen sowie im verfassungspolitischen Bereich: Machtbalance zwischen den Verfassungsorganen Parlament und Regierung auf der staatlichen und der kommunalen Ebene.

Das Datenschutzgesetz versucht den Datenschutz im umfassenden Sinne mit mehreren Maßnahmen in den Griff zu bekommen: Einerseits regelt es auf die herkömmliche Weise durch eine generelle Anweisung an die Verwaltung den Umgang mit Daten und mit Unterlagen für die maschinelle Datenverarbeitung unter dem beherrschenden Gesichtspunkt des Persönlichkeitsschutzes (§ 2 Datenschutzgesetz — Inhalt des Datenschutzes). Ergänzend kommt hinzu eine spezielle, subsidär geltende Verschwiegenheitspflicht der in der Datenverarbeitung tätigen Bediensteten. Die Bedeutung dieser Verschwiegenheitspflicht wird jedoch dadurch wesentlich eingeschränkt, daß der über die Unterlagen, Daten und Ergebnisse Verfügungsberechtigte das Schweigegebot aufheben kann (vgl. § 3 DSG, unter 1.3).

Andererseits schafft das Datenschutzgesetz eine neuartige Einrichtung mit umfassenden Kontrollaufgaben: den unabhängigen, von Weisungen freien Datenschutzbeauftragten.

1.4.1 Pflichten und Rechte

Der Datenschutzbeauftragte wird vom Landtag auf Vorschlag der Landesregierung für die Dauer einer Legislaturperiode gewählt. Er hat für die Einhaltung der Vorschriften des Datenschutzgesetzes und der übrigen Vorschriften, die dem Datenschutz dienen, zu sorgen (§ 10 Abs. 1). Er hat zu beobachten, ob die Auswirkungen der Datenverarbeitung zu Verschiebungen in der Gewaltenteilung zwischen den Verfassungsorganen des Landes, zwischen den Organen der kommunalen Selbstverwaltung und zwischen staatlicher und kommunaler Selbstverwaltung führen (§ 10 Abs. 2). Gegebenenfalls schlägt er Gegenmaßnahmen vor, meldet der zuständigen Aufsichtsbehörde festgestellte Verstöße gegen Schutzbestimmungen und regt Vorkehrungen zur Verbesserung des Datenschutzes an.

Der Datenschutzbeauftragte kann vom Bürger angerufen werden (§ 11). Der Landtag und die kommunalen Parlamente können ihn mit einer Untersuchung beauftragen, wenn nach ihrer Auffassung ihre „Auskunftsersuchen nicht oder nicht ausreichend beantwortet werden" (§ 12). Der Datenschutzbeauftragte hat ein Auskunftsrecht gegenüber allen vom Datenschutz erfaßten Behörden und Stellen (§ 13). Er verfügt aber — ähnlich wie die Rechnungshöfe des Bundes

und der Länder — nicht über Eingriffsbefugnisse.

1.4.2 Verhältnis zu Legislative und Exekutive

Die Einrichtung des Datenschutzbeauftragten als einer unabhängigen, weisungsfreien Aufsichts- und Beobachtungsinstanz trägt der Erkenntnis Rechnung, daß die maschinelle, insbesondere die elektronische Datenverarbeitung als Hilfsmittel der Verwaltung und der Regierung den Rahmen der herkömmlichen Methoden der Verwaltung und der Abwehr von Verwaltungsmißbrauch sprengt und neuartige Gefahrenquellen erschließt, denen mit spezifischen Mitteln begegnet werden muß. Daher hat das Datenschutzgesetz den Aufgabenbereich des Datenschutzbeauftragten (§ 10) umfassend definiert und für die Anpassung an die fortschreitende Automation der öffentlichen Verwaltung und die Fortentwicklung der Techniken der Datenverarbeitung offen gehalten. Von anderen Einrichtungen mit Kontrollfunktion gegenüber der Verwaltung unterscheidet sich der Datenschutzbeauftragte grundsätzlich dadurch, daß er in erster Linie präventiv tätig ist. Er soll Gefahren aufspüren und als Warner und Berater von Parlament und Regierung wirksam werden. Die Abwehr von Gefahren oder von Schäden, die auf dem Einsatz der elektronischen Datenverarbeitung in der öffentlichen Verwaltung beruhen, nicht ihre Beseitigung charakterisiert seinen Aufgabenbereich. Hieraus rechtfertigt es sich, dem Datenschutzbeauftragten keine Eingriffsbefugnisse zu verleihen, sondern seine Befugnisse auf Auskunfts- und Vorschlagsrechte zu beschränken. Dabei ist der Standort des Datenschutzbeauftragten im Organisationssystem des Staates näher dem Parlament in seiner Funktion als oberstes Kontrollorgan gegenüber der Regierung und Verwaltung angesiedelt als der Exekutive, zu der er zu rechnen ist, weil er weder legislatorisch noch rechtsprechend tätig ist und — anders als der Landesanwalt (öffentlicher Kläger beim Staatsgerichtshof — Art. 130 HV) — nicht als besonderes Verfassungsorgan in der Landesverfassung verankert ist. Mangels eines Verfassungsranges wäre der Datenschutzbeauftragte, wenn er mit Eingriffsbefugnissen gegenüber der Verwaltung ausgestattet wäre, ein Exekutivorgan. Er wäre dann notwendigerweise einer obersten Landesbehörde unterstellt, welche die parlamentarische Verantwortung für ihn trüge (Art. 102 HV). Der Kontrollierende würde jedoch damit ein Glied des von ihm kontrollierten Apparates. Diese Inkompatibilität wird richtigerweise vermieden.

In der wissenschaftlichen Kritik des Hessischen Datenschutzgesetzes ist geltend gemacht worden, die Tätigkeit des Datenschutzbeauftragten könne nicht die angestrebte Wirkung erreichen, wenn er keine Anordnungsbefugnisse gegenüber den kontrollierten Behörden habe. Diese Befürchtung wird nicht geteilt. Gegenteilige Erfahrungen, die diesen Einwand rechtfertigen könnten, liegen jedenfalls bisher nicht vor. Vielmehr hat sich mehrfach die Erwartung bestätigt, daß die obersten Landesbehörden Anregungen und Vorschläge des Datenschutzbeauftragten so bewerten, wie es der Absicht des Gesetzgebers entspricht. Die Tätigkeit des Datenschutzbeauftragten ist öffentlich. Eine der Funktionen des Berichts, den der Datenschutzbeauftragte nach § 14 DSG dem Landtag und dem Ministerpräsidenten zu erstatten hat, ist es, seine Amtsführung vor jedermann offenzulegen. Das geschieht einmal durch die Berichterstattung über festgestellte Verstöße gegen den Datenschutz oder über strukturelle Veränderungen im verfassungsmäßigen Kräfteausgleich aller Ebenen und zum anderen durch die Vorschläge, wie ihnen vorgebeugt oder entgegengewirkt werden sollte.

2. RECHTLICHE REGELUNGEN DES DATENSCHUTZES AUSSERHALB HESSENS

2.1 Andere Länder — Überblick

Die Bemühungen der Länder um eine gesetzliche Regelung des Datenschutzes unterscheiden sich erheblich, und zwar nach Inhalt, Reichweite und Entwicklungsstand. Vier Gruppen lassen sich unterscheiden:

- — Länder, in denen ein Datenschutzgesetz in Kraft ist (bislang nur Hessen),
- — Länder, in denen ein Datenschutzgesetz sich im Gesetzgebungsgang befindet (Rheinland-Pfalz, Hamburg, Nordrhein-Westfalen) oder doch geplant wird (Baden-Württemberg, Berlin),
- — Länder, die sich auf einzelne Datenschutzbestimmungen im Rahmen der EDV-Organisationsgesetze beschränkt haben (Baden-Württemberg, Bayern),
- — Länder, die eine gesetzliche Regelung des Datenschutzes z. Z. weder kennen noch anstreben (Bremen, Saarland, Niedersachsen, Schleswig-Holstein), z. T. jedoch verwaltungsinterne Regelungen besitzen (Niedersachsen, Schleswig-Holstein).

In chronologischer Reihenfolge ergibt sich für die Länder im einzelnen folgendes Bild:

2.1.1 Schleswig-Holstein

In Schleswig-Holstein hat die dortige Datenzentrale am 3. Februar 1970 für ihren Bereich eine Dienstanweisung über Datenschutz und Datengeheimnis erlassen.

Die Dienstanweisung verweist auf die allgemeinen Geheimhaltungsvorschriften, erklärt jedoch auch über deren Geltungsbereich hinaus alle Daten und Programme für besonders schutzbedürftig (Datengeheimnis). Entsprechend werden eine Reihe von allgemeinen Sorgfaltsvorschriften sowie Auskunfts-, Verwertungs- und Manipulationsverbote aufgestellt. Alle Mitarbeiter sind förmlich zu verpflichten und jährlich erneut zu belehren.

2.1.2 Bayern

Das bayerische EDV-Organisationsgesetz vom 12. Oktober 1970 (GVBl. S. 457) verpflichtet die mit der Datenverarbeitung befaßten Stellen, speziell auch dann für die Einhaltung der Amtsverschwiegenheit und der sonstigen Geheimhaltungspflichten zu sorgen, wenn andere Stellen in das Verfahren eingeschaltet sind (Art. 15). Art. 16 bedroht denjenigen mit Freiheitsstrafe bis zu einem Jahr und mit Geldstrafe, der im Zusammenhang mit der Datenverarbeitung sich ein fremdes Geheimnis unbefugt verschafft, es offenbart oder verwertet. Die Strafdrohung kommt jedoch nur dann zum Zuge, wenn kein anderes Strafgesetz eingreift und wenn der Verletzte Strafantrag gestellt hat.

Für die Information der gesetzgebenden Körperschaften gilt eine abgestufte Regelung. Landtag und Senat haben nach Art. 1 II Zugriff auf die gespeicherten Daten mit allgemeinem Informationsgehalt und planerischer Zielsetzung. Die zur näheren Ausgestaltung nach dem Gesetz erforderliche Rechtsverordnung ist noch nicht ergangen. Darüber hinaus besteht ein Anspruch des Landtags, seiner Fraktionen und des Senats gegenüber der Staatsregierung auf Auskunft auf Grund der gespeicherten Daten, soweit nicht Geheimhaltungsvorschriften entgegenstehen.

2.1.3 Rheinland-Pfalz

Der von der CDU-Fraktion des Landtags von Rheinland-Pfalz erstmals am 7. Oktober 1970 eingebrachte Entwurf (LT-Drucks. VI/2300) sieht vor, den Datenschutz durch ein eigenes Gesetz zu regeln. Wegen des Ablaufs der Legislaturperiode wurde der Entwurf am 15. September 1971 mit einigen Änderungen erneut eingebracht (LT-Drucks. 7/283). Die Hauptunterschiede gegenüber dem hessischen Modell sind folgende: Die Regelungen beziehen sich auf alle Daten, die der Amtsverschwiegenheit oder der Geheimhaltung unterliegen, insbesondere personenbezogene Daten. Bei selbständiger Datenübermittlung besteht eine Protokollpflicht (§ 2 III). Der Betroffene soll ein Auskunftsrecht erhalten. Verstöße gegen den Datenschutz sollen nicht nur mit einer Geldbuße, sondern mit Freiheitsstrafe bis zu zwei Jahren geahndet werden. Die fahrlässige Regelung wird jedoch nicht erfaßt (§ 14).

Die Überwachung soll durch einen gemischten Ausschuß aus drei Landtagsabgeordneten und zwei Beamten oder Richtern erfolgen (§ 6). Seine Aufgaben beschränken sich auf den Persönlichkeitsschutz (§ 7). Alle Behörden etc. haben dem Ausschuß detailliert über die EDV-Projekte zu berichten (§ 10 II). Untersuchungen zur Unterstützung der parlamentarischen Informationsrechte oder in bezug auf die Einflüsse der EDV auf die Gewaltenbalance zwischen den staatlichen Organen sind nicht vorgesehen.

2.1.4 Niedersachsen

In Niedersachsen wurde der Datenschutz für den Bereich der Rechenzentren der Landesverwaltung durch einen Runderlaß des Innenministers geregelt (RdErl. vom

9. November 1970 — I/2 — 118.055 — GütlL MdI 9/84 —, Nds. MinBl. Nr. 46/1970 S. 1326). Was die einzelnen Schutzvorkehrungen betrifft, handelt es sich um die bisher konkreteste Regelung. Im einzelnen wird zwischen Maßnahmen der Dienstaufsicht, der räumlichen und programmtechnischen Sicherung sowie Regelung und Kontrolle des Betriebsablaufverfahrens unterschieden. Für jedes Rechenzentrum ist ein sogenannter Datenschutzbeauftragter zu bestellen, der im Zusammenwirken mit dem Dienststellenleiter die Maßnahme des Datenschutzes und der Datensicherheit durchführt, überwacht und entsprechende Dienstanweisungen aufstellt. Nach Stellung und Aufgabe handelt es sich um einen eng betriebsbezogenen Sicherheitsbeauftragten, der mit dem hessischen Modell nicht vergleichbar ist.

2.1.5 Baden-Württemberg

Das Gesetz über die Datenzentrale Baden-Württemberg vom 17. November 1970 (GesBl. S. 492) bestimmt in § 13 I, daß die Rechenzentren über Datenbestände mit personenbezogenen Daten nur mit Zustimmung derjenigen Stellen verfügen dürfen, von welchen sie diese erhalten haben. Außerdem wird angeordnet, die Daten durch technische und organisatorische Vorkehrungen vor dem Zugriff Unbefugter zu schützen (§ 13 II). Diese Regelungen sind dem § 5 des HZD-Gesetzes entnommen.

Für den Landtag gibt es ein Recht, sich der Datenzentrale zu bedienen (§ 12 I), jedoch kein besonderes Informationsrecht. Nach Erlaß des Bundesdatenschutzgesetzes soll ein ergänzendes Landesdatenschutzgesetz ergehen. Auch das geplante integrierte Landesinformationssystem soll durch Gesetz geregelt werden (§ 2 I Ziff. 5).

2.1.6 Nordrhein-Westfalen

Dem rordrhein-westfälischen Landtag liegt ein von der CDU-Fraktion eingebrachter Entwurf eines Datenschutzgesetzes vor (LT-Drucks. 7/835 vom 11. Juni 1971).

Erstmals wird vorgesehen, daß sich der Datenschutz nicht nur auf die maschinelle, sondern auch auf die herkömmliche Datenverarbeitung erstrecken soll. Andererseits ist er auf die personenbezogenen Daten beschränkt (§ 1). Der Bürger soll ein Auskunftsrecht erhalten, darüber hinaus aber auch bei der Ersteingabe und danach jährlich über die ihn betreffenden Aufzeichnungen unterrichtet werden (§§ 5, 13). Die Regelung der Datenweitergabe (§§ 7 II, 12 I, II) entspricht derjenigen im Initiativentwurf für ein Bundesdatenschutzgesetz der Abgeordneten Hirsch, Dichgans, Kirst und Genossen vom 2. Dezember 1971, BT-Drucks. VI/2885 (vgl. unter 2.2.2).

Alle Dateien mit personenbezogenen Daten sind bei einem öffentlichen Datenbankregister anzumelden (§§ 9, 10). Bei maschinellen Datenbanken besteht eine umfassende Protokollpflicht (§ 11). Der Betroffene kann über die ihn betreffenden Vorgänge Auskunft aus dem Protokoll verlangen.

Zur Überwachung soll ein gemischter Ausschuß aus drei Landtagsabgeordneten, einem Vertreter des Rechnungshofes, einem Verwaltungsrichter und einem höheren Beamten aus der Praxis der Datenverarbeitung eingesetzt werden, von denen die letzteren drei ihre Tätigkeit hauptamtlich wahrnehmen sollen.

Der Ausschuß soll — abgesehen davon, daß Untersuchungen im Auftrag der Volksvertretungen und ihrer Gliederungen nicht vorgesehen sind — die gleichen Aufgaben haben wie der Hessische Datenschutzbeauftragte, darüber hinaus ist er mit der Führung des Datenbankregisters betraut. Seine Dienststelle soll der Landtagsverwaltung zugeordnet werden.

In begrenztem Umfang soll der Ausschuß auch materielle Eingriffsrechte besitzen. So kann er von der zuständigen Fachaufsichtsbehörde die Löschung oder anderweitige Korrekturen verlangen, wenn der Zweck einer Datenbank oder die Art von gesammelten Daten unzumutbar in das Persönlichkeitsrecht eingreift. Im Weigerungsfalle soll der Landtag unterrichtet werden (§ 17).

Der Entwurf enthält sowohl Straf- als auch Ordnungswidrigkeitsvorschriften (§§ 19, 20). Ein in Arbeit befindlicher Regierungsentwurf wurde mit Rücksicht auf die Absichten des Bundes zurückgestellt.

2.1.7 Hamburg

Auch der von der Hamburger CDU-Fraktion der Bürgerschaft vorgelegte Entwurf eines Datenschutzgesetzes (Drucks. VII/1460 vom 5. Oktober 1971) entspricht weithin den Vorstellungen des Entwurfs BT-Drucks. VI/2885 und enthält deshalb viele Parallelen zum nordrhein-westfälischen Entwurf. Anders als dieser enthält er jedoch keine Beschränkung auf personenbezogene Daten (§ 1). Eine periodische Benachrichtigung ist nicht vorgesehen, ebensowenig eine Protokollpflicht. Die Überwachung soll einem dem nordrhein-westfälischen Modell weitgehend nachgebildeten Ausschuß obliegen. Der Rechnungshof soll jedoch keinen Vertreter entsenden. Es fehlt die Beobachtungsfunktion in bezug auf die Gewaltenteilung.

2.1.8 Berlin, Bremen, Saarland

In den übrigen Ländern liegen noch keine Vorschriften oder Gesetzentwürfe vor. In Berlin ist jedoch beim Senat ein Datenschutzgesetz in Vorbereitung.

2.2 Gesetzgebungsstand im Bund

Auf Bundesebene bestehen drei Ansätze zur gesetzlichen Lösung der Datenschutzproblematik. Zunächst wird im Bundesinnenministerium ein Datenschutzgesetz vorbereitet. Der Entwurf

sollte ursprünglich im Jahre 1971 vorgelegt werden, läßt jedoch immer noch auf sich warten. Die Behandlung des schon genannten Entwurfs BT-Drucks. VI/2885 wurde im Plenum ausgesetzt, damit der erwartete Regierungsentwurf einbezogen werden kann. Im gleichen Sinne hat sich der Innenausschuß des Bundestages bezüglich des ihm vorliegenden Entwurfs des Bundesmeldegesetzes entschieden, der ebenfalls wichtige Datenschutzbestimmungen enthält.

2.2.1 Bundesmeldegesetz

Mit dem Entwurf eines Bundesmeldegesetzes (BT-Drucks. VI/2654) sollen die bundesrechtlichen Grundlagen für das geplante Einwohnerinformationssystem geschaffen werden. So werden eine Bürgernummer (Personenkennzeichen, „PK") eingeführt und eine Reihe vereinheitlichender und koordinierender Vorkehrungen getroffen.

Der Gesetzentwurf zielt auf die Erleichterung und Intensivierung des Austauschs von Einwohnerdaten. Um den damit verbundenen Gefahren und Mißbrauchsmöglichkeiten entgegenzutreten, werden auch einige spezielle für das Meldewesen geltende Datenschutzbestimmungen vorgesehen. So soll der Bürger einen Auskunfts- und Berichtigungsanspruch bezüglich der von der Meldebehörde über ihn gespeicherten Daten erhalten (§ 18). Die Übermittlung von Daten an andere Behörden soll nur insoweit zulässig sein, als die Angaben dort zur Aufgabenerfüllung benötigt werden (§ 16 I). Falls die Daten unmittelbar abrufbar sind, müssen entsprechende Sperren in das System eingebaut sein. Außerdem müssen in diesem Falle Zeitpunkt, Empfänger und Art der übermittelten Daten protokolliert werden (§ 16 II). Privatpersonen sollen nur noch Auskunft erhalten über Namen, Anschrift und Datum des Ein- oder Auszugs aus der Wohnung, bei berechtigtem Interesse auch über Personenkennzeichen, Geburtstag und -ort, frühere Namen und Wohnungen, Familienstand und Staatsangehörigkeit. Für den Betroffenen soll die Möglichkeit geschaffen werden, einen Teil seiner Daten gegenüber Privatauskünften sperren zu lassen (§ 19). Datenschutzverstöße von Angehörigen der Meldebehörden oder sonst an Meldewesen beteiligten Personen sollen mit Freiheitsstrafe bis zwei Jahren geahndet werden, wobei ein Strafantrag des Verletzten Voraussetzung ist.

2.2.2 Bundesdatenschutzgesetz — Entwurf der Abgeordneten Hirsch, Dichgans, Kirst und Genossen, BT-Drucks. VI/2885

Der am 2. Dezember 1971 eingebrachte Entwurf (BT-Drucks. VI/2885) ist das Ergebnis mehrjähriger Vorarbeiten im Rahmen der Interparlamentarischen Arbeitsgemeinschaft. Er trifft Regelungen sowohl für die Datenbanken des Bundes als auch für die von privaten Unternehmen.

Ebenso wie in den Fraktionsentwürfen in Hamburg und Nordrhein-Westfalen soll der Datenschutz auch dort gelten, wo keine maschinellen Verfahren eingesetzt werden (§ 1), fast alle Einzelvorschriften sind jedoch nur bei personenbezogenen Daten anzuwenden. Der Entwurf vereinigt nahezu alle in der bisherigen Diskussion herausgebildeten Forderungen. Zur Information der Betroffenen dient eine Mitteilungspflicht bei Ersteingabe (§§ 9 I, 17) sowie ein Auskunftsanspruch, der sich nicht nur auf die gespeicherten Daten (§§ 3 I, 9 II, 17), sondern auch auf das Protokoll bezieht (§§ 9 III, 17), das bei allen Auskunftserteilungen über Einzelangaben zu führen ist (§§ 7, 15). Bei Falschinformationen oder rechtswidrigen Informationsvorgängen kommen weitgehende Berichtigungs- und Schadensersatzansprüche zum Zuge (Gefährdungshaftung).

Die Weitergabe von Informationen soll grundsätzlich „verrechtlicht" werden. Datenbanken des Bundes sollen personenbezogene Daten nur noch demjenigen weitergeben, dem auf Grund einer Rechtsvorschrift ein Recht auf Kenntnisnahme zusteht (§ 8 I, II). Bei privaten Datenbanken soll auch ein sonstiger Rechtfertigungsgrund ausreichen (§ 16 I).

Ein noch zu bestimmender Bundesminister soll die Funktion einer Aufsichtsbehörde über die dem Gesetz unterstehenden Datenbanken erhalten. Er soll ein öffentliches Register führen, das insbesondere über die Art der Daten sowie über Zweck und Methode des Systems jeder einzelnen Datenbank Aufschluß gibt. Gegen private Datenbanken können bei Eingriffen in das Persönlichkeitsrecht besondere Maßnahmen getroffen werden, im öffentlichen Bereich werden die zuständige Fachaufsichtsbehörde unterrichtet und Abhilfemaßnahmen vorgeschlagen. Wie auch bei allen anderen vorgeschlagenen Überwachungsorganen vorgesehen, soll die Aufsichtsbehörde jährlich dem Parlament einen Tätigkeitsbericht vorlegen.

2.2.3 Bundesdatenschutzgesetz — Regierungsentwurf

Ein Referentenentwurf liegt dem Vernehmen nach im Bundesinnenministerium zwar bereits seit längerem vor. Er wird jedoch noch vertraulich behandelt. Lediglich einige, z. T. freilich noch vage Grundsätze wurden bereits publiziert (vgl. Auernhammer/Keller, Personenkennzeichen und Datenschutz, Beilage 19/71 zum BAnz. Nr. 142 vom 5. August 1971 S. 14 f.).

Die Schwerpunkte dieses Entwurfs sollen in folgenden Bereichen liegen:

Die Privatsphäre im öffentlichen und privaten Bereich soll gleichwertig geschützt werden, und zwar unabhängig von der Verarbeitungsmethodik. Welche Rechte der Betroffene haben soll,

ist noch nicht genau erkennbar. Grundsätzlich soll die Zulässigkeit der Ermittlung und Weitergabe von Daten im öffentlichen Bereich an der Aufgabenerfüllung der betreffenden Behörde orientiert werden. Im privaten Bereich soll sie aus einer Güter- und Interessenabwägung zwischen den Beteiligten folgen. Die Errichtung neuer Überwachungsorgane wird abgelehnt. Manipulationsverbote, Geheimhaltungs- und Strafvorschriften sind geplant.

2.2.4 Entwurf eines Einführungsgesetzes zum Strafgesetzbuch

Nach Art. 18 Ziffer 80 des Entwurfs eines Einführungsgesetzes zum Strafgesetzbuch (BR-Drs. 1/72 vom 3. Januar 1972) soll das StGB einen neuen 15. Abschnitt erhalten. Seine Vorschriften betreffen die Verletzung des persönlichen Lebens- und Geheimnisbereichs. §§ 203, 204 regeln u. a. die Verletzung von Privatgeheimnissen durch Amtsträger.

Der Entwurf hält diese Materie damit für abschließend geregelt und hebt deshalb die besonderen Vorschriften der Länder über die Verletzung der Geheimhaltung im Rahmen der Datenverarbeitung auf. Davon wird u. a. die Bußgeldvorschrift des § 16 DSG betroffen (vgl. 2.4.6).

2.3 Ausland

2.3.1 USA

In Kalifornien wurde im Jahre 1968 ein Gesetz erlassen, das die Publizität der Akten der öffentlichen Verwaltung aus Gründen des Persönlichkeitsschutzes einschränkt. Der Bürger hat jedoch weiterhin Einsicht in die ihn betreffenden Unterlagen. Ein weitergehender Gesetzentwurf, der eine Registrierung der Datenbanken der öffentlichen Verwaltung, einen Berichtigungsanspruch und ein Verbot der Herausgabe von Listen mit persönlichen Daten vorsah, ist nicht verabschiedet worden.

Der Bereich der Auskünfte über die Kreditwürdigkeit für Zwecke der Krediterteilung, des Versicherungsabschlusses und der Personalbeurteilung wurde 1970 auf Bundesebene durch den Fair Credit Reporting Act gesetzlich geregelt. Danach dürfen grundsätzlich keine Angaben über Ereignisse usw. weitergegeben werden, die weiter als sieben Jahre zurückliegen. Der Betroffene ist von der Einholung der Kreditauskunft unter Belehrung über seine Rechte zu unterrichten und auf Anfrage über Natur und Gegenstand der angeforderten Nachforschung aufzuklären. Der Betroffene kann außerdem jederzeit erfahren, welche Informationen über ihn gespeichert sind und an wen innerhalb der letzten sechs Monate — bei Personalbeurteilungen zwei Jahre — Auskünfte erteilt worden sind. Wird die Richtigkeit von Angaben bestritten, so ist die Auskunftei zu weiteren Nachforschungen verpflichtet. Bleibt die Meinungsverschiedenheit auch danach bestehen, so muß eine kurz gefaßte Gegendarstellung des Betroffenen aufgenommen werden. Führt eine Auskunft zu einer für den Betroffenen nachteiligen Entscheidung, so ist ihm dies unter Benennung der Auskunftei mitzuteilen. Bei schuldhaften Verstößen kann der Betroffene Schadensersatz verlangen.

2.3.2 Großbritannien, Kanada

In Großbritannien und in der kanadischen Provinz Ontario sind im Jahre 1969 inhaltsgleiche Gesetzentwürde eingebracht, jedoch nicht verabschiedet worden. Mit ihnen sollte die Datenschutzproblematik umfassend und weitgehend einheitlich für den öffentlichen und den privaten Bereich gelöst werden. Im einzelnen waren vorgesehen: Ein Datenbankregister, eine Protokollierungspflicht bei Abruf personenbezogener Daten sowie weitgehende Auskunfts- und Berichtigungsrechte des Betroffenen.

2.3.3 Frankreich

In Frankreich wurde Ende 1970 der Nationalversammlung durch die Initiative der unabhängigen Republikaner ein Gesetzesvorschlag unterbreitet. Hauptziel war die Einrichtung einer Datenüberwachungskommission (Comité de surveillance de l'informatique), deren 9 Mitglieder teils vom Parlament, teils von der Regierung bestimmt werden sollten. Die Kommission sollte sowohl die öffentliche als auch die private Datenverarbeitung kontrollieren. Hierzu waren die Einrichtung eines öffentlichen Registers und weitgehende Untersuchungsrechte vorgesehen. Im Falle von Beanstandungen sollte eine neue, besonders spezialisierte Abteilung des Verwaltungsgerichtshofes („tribunal de l'informatique") verbindlich entscheiden.

Der Entwurf ist nicht verabschiedet worden.

2.4 Tendenzen der Datenschutzgesetzgebung

Die allgemeine Lage ist durch eine Vielzahl von Gesetzentwürfen und Plänen gekennzeichnet, denen ein recht kleiner Bestand an in Kraft getretenen gesetzlichen Bestimmungen gegenübersteht. Auch im internationalen Rahmen ist das Hessische Datenschutzgesetz noch immer das einzige, zwar auf den öffentlichen Sektor beschränkte, hier aber umfassende Modell. Einige Bundesländer haben ihre Projekte bewußt einstweilen zurückgestellt, bis eine inhaltliche Koordinierung mit der Bundesdatenschutzgesetzgebung möglich wird. Eine Abstimmung wird vor allem dann unumgänglich, wenn der Geltungsbereich des Bundesgesetzes nicht auf die Bundesverwaltung beschränkt, sondern — wie beabsichtigt sein soll — allgemein auf die Durchführung von Bundesrecht erstreckt wird (vgl. die Beantwortung einer Kleinen Anfrage durch den Bundesinnenminister, BT-Drucks. VI/1223 S. 2). Außerdem besteht nach wie vor eine gewisse Unsicherheit in bezug auf die Konsequenzen ver-

schiedener Regelungen. Die Frage, ob gesetzlich Maßnahmen notwendig sind, ist jedoch — jedenfalls in der Bundesrepublik — mittlerweile eindeutig positiv entschieden. Um so wichtiger sind die Auseinandersetzungen um die einzelnen Regelungselemente.

2.4.1 Anwendungsbereich

Abgesehen von der Differenzierung nach privatem und öffentlichem Bereich und hier nach Bundes- sowie Landes- und Kommunalverwaltung, die sich aus der Aufteilung der Gesetzgebungskompetenzen ergeben, werden für den Anwendungsbereich der Datenschutzvorschriften noch drei weitere Unterscheidungen gemacht. Hinsichtlich des Informationsgegenstandes geht es um die Frage, ob nur personenbezogene oder grundsätzlich alle Daten (so Hessen, Hamburg) umfaßt werden sollen. Nach der Zwecksetzung der Datenbanken wird zwischen austauschorientierten und internen Systemen unterschieden (Initiativ-Entwurf BT-Drucks. VI/2885). Nach der Methodik der Informationsverarbeitung soll zur Zeit auch die „konventionelle Datenverarbeitung", d. h. auch der manuelle Übergang mit jeder Art von Aufzeichnungen, einbezogen werden (so der Initiativ-Entwurf BT-Drucks. VI/2885 und Referentenentwurf des Bundesinnenministeriums, CDU-Entwürfe in Nordrhein-Westfalen und Hamburg).

Diese Abgrenzung der Bereiche steht mit unterschiedlichen Zwecksetzungen in Zusammenhang. So scheinen die Befürworter einer nur dem Persönlichkeitsschutz verpflichteten Datenschutzregelung davon auszugehen, daß andere als personenbezogene Daten ohne Interesse seien. Nur intern benutzte Datenbanken werden zum Teil als unterhalb der Reizschwelle liegend angesehen. Auf der anderen Seite bemüht man sich, eine Umgehung der Schutzvorschriften dadurch zu verhindern, daß man auch konventionell geführte Verzeichnisse, Register etc. einbezieht. Sollen dagegen auch die mehr gesellschaftlichen Gefahren der neuen Informationstechnologien gemeistert werden, will man also die Informationsrechte der Parlamente und die Funktion der Gewaltenteilung unterstützen bzw. sichern, so kann die Überwachung vom Informationsgehalt her ebensowenig eingeschränkt werden wie vom Verwendungszweck der jeweiligen Informationseinrichtung.

Eine Erstreckung auf nicht automatisierte Informationsbereiche dürfte sich jedoch — unabhängig von den verfolgten Zwecken — nicht empfehlen. Denn die Gefahren, sowohl für den einzelnen als auch für den politischen Prozeß, haben erst durch die technisch bewirkte erhöhte Verfügbarkeit und Aussagekraft der Daten diejenige Intensität erreicht, die über die traditionellen Sicherungen hinaus besondere Maßnahmen erforderlich macht. Zudem führt eine derart weite Regelung zwangsläufig zu zahlreichen, im einzelnen noch nicht absehbaren Kollisionen. Die dadurch notwendigen vielfältigen Ausnahmen und Vorbehalte müßten die Effektivität des Gesetzes erheblich belasten, wenn nicht in Frage stellen. Umgehungen, die in der weiteren Entwicklung zu befürchten sind, kann mit Maßnahmen entgegengetreten werden, die auf die speziellen Probleme zugeschnitten sind.

2.4.2 Zielsetzung

Während das hessische Gesetz den Datenschutz noch komplex sieht und dem Persönlichkeitsschutz gleichrangige Maßnahmen zur Sicherung demokratisch-rechtsstaatlicher Informationsstrukturen zur Seite stellt, hat sich in der weiteren Entwicklung die Aufmerksamkeit mehr und mehr auf die Individualrechte verengt. Zwar sind parlamentarische Informationsrechte zum Teil noch vorgesehen (EDV-Gesetz Bayern, CDU-Entwürfe in Rheinland-Pfalz, Nordrhein-Westfalen). Eine institutionelle Unterstützung hierfür entsprechend der Regelung des § 12 Hessisches Datenschutzgesetz wird nicht mehr angeboten. Die Untersuchung, ob die Datenverarbeitung Veränderungen in der Arbeitsweise und den Entscheidungsbefugnissen verursacht, die das Prinzip der Gewaltenteilung und der kommunalen Selbstverwaltung tangieren (vgl. § 10 II Hessisches Datenschutzgesetz), ist als Aufgabe lediglich im nordrhein-westfälischen Entwurf enthalten.

Der Rückzug auf den Privatsphäre-Aspekt dürfte zum Teil darauf zurückzuführen sein, daß die Bedrohungen hier leichter greifbar sind. So spielt auch in der amerikanischen allgemeinen und populärwissenschaftlichen Publizistik das Privacy-Problem eine klar dominierende Rolle. Der tiefere Grund wird jedoch darin liegen, daß das politische Denken sich immer noch stark am konventionellen Modell des liberalen Rechtsstaates orientiert. Die Frage des rechtlichen Schutzes des Individuums vor staatlicher — allmählich auch vor gesellschaftlicher — Macht wird für wichtiger gehalten als das Problem der Erhaltung und des Ausbaues der demokratischen Strukturen. Diese Betrachtungsweise entspricht nicht mehr dem heutigen Staats- und Gesellschaftsverständnis, denn wenn der politische Entscheidungsprozeß seinen demokratischen Charakter verliert, geraten über kurz oder lang auch die Freiheitsrechte in Gefahr. Deshalb sollte eine Strategie der Freiheitssicherung unbedingt beide Aspekte verfolgen. In den USA, wo computerunterstützte Führungsinstrumente seit einigen Jahren in verschiedenen Bereichen der Verwaltung und Regierung eingesetzt werden, ist bereits eine umfangreiche wissenschaftliche Literatur über die damit zusammenhängenden politischen Fragen entstanden (vgl. insbesondere den Sammelband Information Technology in a Democracy, Herausgeber Alan F. Westin, Cambridge/Mass. 1971).

Die vorliegenden Arbeitsergebnisse lassen die Prognose zu, daß die Informationstechnologie auch in der Bundesrepublik in absehbarer Zeit Probleme für die Fortentwicklung der demokratischen Strukturen aufwirft, die intensiver Untersuchung bedürfen und möglichst frühzeitige Maßnahmen erfordern (vgl. unter 3.5.4). Außerdem ist die Erwartung nicht unberechtigt, daß sich aus der Analyse der gesellschaftlich-politischen Funktionen der EDV auch wertvolle neue Ansätze für die Lösung der Privatsphäre-problematik gewinnen lassen.

2.4.3 Datenbankregister

Die Forderung nach Schaffung eines öffentlichen Datenbankregisters wird zu Recht als eine Kernforderung der Datenschutzgesetzgebung betrachtet und ist in fast allen Entwürfen berücksichtigt. Je nach Detailliertheit gibt das Register einen groben bis feinen Überblick über das durch die Datenbanken über die Gesellschaft und ihren Lebensraum gezogene „Informationsnetz".

Das Register kann einerseits als erster Wegweiser zu gesuchten Informationen dienen. Andererseits macht es die bestehende Informationsstruktur für Bürger, politische Instanzen und Wissenschaften transparent und bildet insoweit die Voraussetzung für eine planmäßige, den Interessen der Gesellschaft entsprechende Fortentwicklung.

Diese Funktion kann freilich nur dann richtig zur Geltung kommen, wenn im Register alle Datenbanken, unabhängig vom (personen- oder sachbezogenen) Gegenstand erfaßt werden. Dies unterstreicht die Kritik, die (unter 2.4.2) an der einseitigen Zielsetzung geübt wurde.

Freilich ist zu bedenken, daß bisher nirgends ein derartiges Register verwirklicht ist, so daß Aufwand, Nutzen und optimale Gestaltung vorerst nur abgeschätzt werden können.

2.4.4 Protokollierung

Auch das Prinzip der Protokollierung ist in allen neueren Entwürfen vorgesehen. Eine bereits in Kraft befindliche Vorschrift besteht jedoch, soweit ersichtlich, nur in USA mit dem Fair Credit Reporting Act. Über praktische Erfahrungen ist noch nichts bekannt geworden. Ob der mitunter erhobene Einwand, der erforderliche technische Aufwand stehe in keinem Verhältnis zum Nutzen, zutrifft, ist auch unter Experten noch umstritten. Überall dort, wo ein direkter Zugriff auf fremde Informationsbestände an die Stelle eines Informationsersuchens tritt, entfällt künftig die Überprüfung der Berechtigung durch einen Bearbeiter. Die automatische Protokollierung ist dann das einzige Mittel, mit dem sich eine mißbräuchliche Datennutzung aufdecken läßt. Wo es um empfindliche Daten geht und ein Mißbrauch zu befürchten ist, ist die Protokollierung deshalb ein unverzichtbares Kontrollinstrument. Die nähere Ausgestaltung muß sich nach den Umständen des jeweiligen Projektes richten.

2.4.5 Rechte des Betroffenen

Lediglich Hessen kennt bereits einen besonderen Wiederherstellungs- und Unterlassungsanspruch. Ein Auskunftsanspruch besteht noch im amerikanischen Fair Credit Reporting Act. Im übrigen gibt es nur Gesetzentwürfe. Sie sehen durchweg Auskunfts- und Berichtigungsansprüche vor. Unterschiede bestehen beim Schadensersatzrecht sowie bei dem Anspruch auf Auskunft nach dem Protokoll und auf Versendung von Korrekturmitteilungen durch die Datenbank an frühere Empfänger beanstandeter Informationen.

Diese Differenzen beruhen zum Teil auf einer unterschiedlichen Einschätzung der Realisierbarkeit, vor allem wegen der zu erwartenden Anzahl von Auskunftsbegehren, Beanstandungen etc. Die Gesetzgeber stehen deshalb vor dem doppelten Risiko, entweder unerfüllbare Rechte zu gewähren oder vor einem vermeintlichen Aufwand zu kapitulieren. Diese Unsicherheit ließe sich jedoch durch demoskopische Umfragen, systematische Auswertung anderweitiger Erfahrungen und eine Studie über den technischen und organisatorischen Aufwand stark reduzieren. Solche Untersuchungen sollten deshalb nicht länger aufgeschoben werden.

2.4.6 Straf- und Bußgeldvorschriften

Besondere Straf- und Bußgeldvorschriften mit allerdings recht unterschiedlichen Tatbestands- und Rechtsfolgeregelungen sind in allen Datenschutzgesetzentwürfen enthalten. Die mit dem Entwurf eines Einführungsgesetzes zum Strafgesetzbuch (vgl. oben 2.2.4) vorgesehene Vereinheitlichung ist deshalb zwar grundsätzlich zu begrüßen. Der Entwurf nimmt jedoch die Grenze der Strafbarkeit erheblich zurück. So sollen fahrlässige Verstöße generell sanktionslos bleiben. Auch wer sich vorsätzlich unbefugt Informationen verschafft, hat nichts zu befürchten. Eine Verwertung der so erlangten Information wird nur bei Amtspersonen bestraft. Dem Ziel, einen möglichst lückenlosen Datenschutz aufzubauen, wäre mit der zur Zeit vorgesehenen Fassung nicht gedient.

2.4.7 Überwachung des Datenschutzes

Die Forderung nach einem unabhängigen Überwachungsorgan ist eines der Hauptergebnisse der deutschen und internationalen Datenschutzdiskussion. Fast alle Gesetzentwürfe wollen sie verwirklichen. Nur der Referentenentwurf des Bundesinnenministers scheint auf besondere Kontrollorgane verzichten zu wollen. Verwirklicht ist die Forderung bisher allein in Hessen. Wie das Überwachungsorgan eingerichtet sein

soll, wie es in den Staatsaufbau eingegliedert und welche Befugnisse es haben soll, ist noch lebhaft umstritten. Die wichtigsten bisher entwickelten Modelle sind folgende:

a) Die Aufgabe wird einem Bundesminister übertragen (Initiativentwurf BT-Drucks. VI/2885).

b) Ein besonderer Ausschuß, in dem Parlament und Regierung (Verwaltung) vertreten sind, wird geschaffen (Mehrzahl der in den Ländern vorliegenden Gesetzentwürfe).

c) Eine unabhängige Behörde wird errichtet (Vorschlag in der deutschen und ausländischen Literatur).

d) Ein Datenschutzgericht soll die Aufgabe erfüllen (Vorschlag in der Literatur, französischer Entwurf).

e) Eine einzelne Person wird als unabhängiger Datenschutzbeauftragter eingesetzt (Hess. Datenschutzgesetz; ein „information-ombudsman" wurde in den USA gefordert).

Zwar hat jedes Modell Vorzüge und Nachteile; sie sind jedoch nicht gleichwertig. Die Unabhängigkeit der Stellung eines Aufsichtsorgans wird zu Recht als zentrale Forderung angesehen. Der Vorschlag a) kann deshalb nicht befriedigen. Ein Bundesminister wird als Mitglied der Exekutive in Zweifelsfällen eher dazu neigen, dem Interesse der Regierung und der öffentlichen Verwaltung Vorrang vor dem Schutz des Persönlichkeitsrechts des Bürgers zu geben. Er untersteht ferner der Richtlinienkompetenz des Regierungschefs. Der Interessenkonflikt zwischen Bürgerintersse und Kabinettsloyalität wird geradezu herausgefordert. Unzuträglichkeiten im Verhältnis zu anderen Ministerien wären kaum zu vermeiden. Schließlich müßte der Minister sich zum Teil selbst kontrollieren.

Das Ausschußmodell (b) vermeidet zwar die Eingliederung in die Exekutive. Doch bringt seine Zusammensetzung andere Nachteile. Die Willensbildung wäre relativ umständlich und für die Öffentlichkeit undurchsichtig.

Der Vorschlag einer unabhängigen Behörde (c) hat seine Vorbilder vor allem in den Federal Commissions der USA. Diese haben weitgehende Regelungsbefugnisse. Außerdem unterscheiden sie sich von der hessischen Lösung des Datenschutzbeauftragten durch ihre kollegiale Verfassung.

Auch ein Datenschutzgericht (d) stellt keine befriedigende Lösung dar. Der Datenschutz ist keine Aufgabe der Rechtsprechung, d. h. der Streitentscheidung, sondern eine Verwaltungsaufgabe. Rechtsverletzungen sind seitens der Verwaltung durch Maßnahmen und Vorkehrungen zu verhindern, die der Verwaltung eigen sind.

Die Aufgabe, als „Datenschutzbeauftragter" oder als „Ombudsman für den Datenschutz" dem Bürger zur Seite zu stehen und seine Interessen gegenüber der Verwaltung zu vertreten, kann durch eine öffentliche Vertrauensperson, die jederzeit anrufbar und deren Handlungsweise transparent ist, besser erfüllt werden. Dies belegen die Erfahrungen mit dem Wehrbeauftragten und den skandinavischen Ombuds-Männern.

3. DIE DATENVERARBEITUNG IN DER ÖFFENTLICHEN VERWALTUNG DES LANDES HESSEN

Auf Anregung des Datenschutzbeauftragten hat die Landesregierung mit Beschluß vom 6. Juli 1971 als erste Maßnahme eine Bestandsaufnahme der Behörden und Stellen veranlaßt, die Unterlagen für die maschinelle Datenverarbeitung herstellen oder Daten speichern und verarbeiten. Gleichzeitig hat sie einen Bericht über die von diesen Behörden und Stellen angewandten personellen und technischen Vorkehrungen für den Datenschutz angefordert. Eine solche Bestandsaufnahme war notwendig, damit sich der Datenschutzbeauftragte einen Überblick darüber verschaffte, inwieweit die maschinelle, insbesondere die elektronische Datenverarbeitung bereits in die öffentliche Verwaltung des Landes Eingang gefunden hat. Erst aus diesem Überblick konnte sich ergeben, welchen Umfang seine Überwachungsaufgaben haben und voraussichtlich künftig annehmen werden.

Für die Beurteilung der Frage, in welchem Maße die beiden Rechtsgüter — Persönlichkeitsschutz und Informationsgleichgewicht — durch die Einführung der Automation in der öffentlichen Verwaltung beeinträchtigt werden oder welche künftigen Gefahren zu erwarten sind, muß die Bestandsaufnahme auch erkennen lassen, bis zu welchen Behördeninstanzen die maschinelle Datenverarbeitung eingeführt ist und ob — und ggf. wo — sich irgendwelche Schwerpunkte hinsichtlich der Anhäufung von technischen Einrichtungen gebildet oder Zusammenziehungen von verschiedenen Verwaltungsaufgaben stattgefunden haben. Ferner sollte festgestellt werden, inwieweit die Zusammenführung einzelner Dateien zu Datenbanken oder andere Formen der Integration bereits vorliegen. Schließlich sollte der Beschluß der Landesregierung einen Überblick über die personellen oder technischen Vorkehrungen geben, welche die Behörden bereits getroffen haben, um die Datenbestände wirksam gegen unbefugten Zugriff und vor Katastrophen zu schützen und welche Erfahrungen sie dabei sammeln konnten.

3.1 Bestandsaufnahme

Bis Februar 1972 haben 286 Behörden, Stellen und Körperschaften des öffentlichen Rechts über ihre Datenschutzvorkehrungen berichtet und teilweise Vordrucke (Erfassungsbögen) resp. Datenträger vorgelegt. Darunter befinden sich 216 der rund 1 200 Gemeinden des Landes Hessen. In den meisten Fällen bedient man sich zur Datenverarbeitung der Einrichtung der HZD oder eines der KGRZ. Es werden aber auch Privatfirmen oder Zentralen von Körperschaften des öffentlichen Rechts für Datenerfassung oder Datenverarbeitung in Anspruch genommen.

Insgesamt haben über 800 Erfassungsbögen, Lochkartenformulare und andere Datenträger vorgelegen. Mehr als 50% davon enthalten personenbezogene Daten mit rund 1 500 Informationen. Diese Angaben werden in den verschiedenen Aufgabenbereichen mehrfach benötigt, so daß es zu Doppel- und Vielfach-Erfassungen kommt. Der Familienname, der Vorname, das Geburtsdatum und die Wohnung werden z. B. insgesamt 30mal erfragt. Berücksichtigt man diese Mehrfach-Erfassungen, so verbleiben 300 verschiedene personenbezogene Einzelangaben, die in bestimmten Kombinationen schutzbedürftig sind. Dieses Schutzbedürfnis gilt ebenso für die übrigen sachbezogenen Daten, die zwar keine Identifikationsmerkmale aufweisen, die aber für den Datenschutz beachtlich werden, wenn man sie mit personenbezogenen Daten verbindet.

3.2 Beurteilung der Bestandsaufnahme

Die vorgelegten Berichte sind jedoch offensichtlich noch lückenhaft, so daß noch kein abgeschlossenes Bild gewonnen werden konnte. Aus Gründen der Verwaltungsvereinfachung war von Fehlanzeigen abgesehen worden, wenn keine Datenverarbeitungsanlagen bestehen und auch keine Unterlagen für die maschinelle Datenverarbeitung hergestellt werden. Deshalb kann der Datenschutzbeauftragte nicht feststellen, welche Lücken in der Berichterstellung noch vorhanden sind.

Von der Staatskanzlei und den ihr unmittelbar unterstehenden Behörden liegen die Meldungen vollständig vor. Die Meldungen der Ressorts scheinen dagegen von unterschiedlicher Dichte zu sein. Die Zahl der öffentlich-rechtlichen Körperschaften, Anstalten und Stiftungen, die Meldungen vorgelegt haben, ist auffallend niedrig. Es fehlen z. B. Meldungen von der Hessischen Landesbank — Girozentrale, der Nassauischen Sparkasse, den öffentlich-rechtlichen Brandversicherungsanstalten, den berufsständischen Kammern, die als öffentlich-rechtliche Körperschaften gebildet worden sind, u. a. mehr.

Das Fehlen dieser Meldungen ist möglicherweise durch eine mißverständliche Auffassung über den Bereich, den das Gesetz in § 1 umschreibt, verursacht (s. unter 4.1.3). So hatten z. B. die ärztlichen Körperschaften des öffentlichen Rechts die Vorstellung, daß das Aufsichtsrecht und Auskunftsrecht des Datenschutzbeauftragten mit dem ärztlichen Schweige-

gebot unvereinbar seien. Dieses Mißverständnis konnte bei einer persönlichen Aussprache aufgeklärt werden.

Auffallend ist auch die geringe Anzahl der Meldungen von Gemeinden und Gemeindeverbänden. Wenn auch mit Sicherheit angenommen werden kann, daß viele — insbesondere kleinere — Gemeinden über keine DV-Anlagen verfügen, so fehlen doch auch Meldungen von größeren Gemeinden und Städten, die aller Wahrscheinlichkeit nach DV-Anlagen betreiben oder doch Unterlagen für die maschinelle Datenverarbeitung in einzelnen Bereichen ihrer Verwaltungsaufgaben herstellen.

Offensichtlich wird das rechtliche Interesse des Datenschutzbeauftragten unterschätzt, einen Überblick über die Behörden und Stellen zu gewinnen, die — ohne selbst Daten zu verarbeiten — Unterlagen für die maschinelle Datenverarbeitung herstellen. Das Gesetz bezieht sich zwar nicht auf die herkömmliche oder manuelle Sammlung von Daten; der Datenschutz setzt jedoch bereits mit der Herstellung der Unterlagen für die maschinelle Datenverarbeitung ein. Aus diesem Grunde ist der Berichtspflicht auf Grund des Beschlusses der Landesregierung nicht allein dadurch genügt, daß, wie vielfach geschehen, nur darauf hingewiesen wurde, daß die Speicherung und Verarbeitung der im örtlichen Bereich gewonnenen Daten von dem zuständigen KGRZ oder von der HZD ausgeführt wird.

Auch von den Universitäten und Hochschulen liegen nur unvollständige Meldungen vor. Z. B. hat die Philipps-Universität in Marburg/L. keinen Bericht eingereicht, obwohl sie vom Kultusminister mehrfach dazu aufgefordert wurde. Gerade in diesem Bereich scheint aber der Datenschutz eine besondere Bedeutung zu gewinnen (s. unter 4.1.1.2).

Berücksichtigt man diese Einschränkungen, so kann auf Grund der vorliegenden Berichte festgestellt werden, daß die Automation der öffentlichen Verwaltung in Hessen weit fortgeschritten ist. Eine starke Konzentration der Datenverarbeitung ist bei der HZD und bei den KGRZ festzustellen. Letzteres ist für die Beurteilung der Datensicherung (vgl. 4.3) von Bedeutung, weil diese öffentlich-rechtlichen Körperschaften, welche die Datenverarbeitung als Dienstleistung betreiben, in dieser Hinsicht ein vorbildliches Modell bilden.

Für den Schutz des Persönlichkeitsrechts werden bisher nur die traditionellen organisatorischen und personellen Sicherheitsvorkehrungen getroffen. Dies braucht z. Z. nicht zu beunruhigen, weil die Bedrohung des Persönlichkeitsrechts des Bürgers und die Beeinflussung der Gewaltenbalance zwischen der Legislative und der Exekutive noch keine aktuelle Bedeutung hat. Trotz Einführung der Automation ist die Integrierung der Dateien der einzelnen Behörden, innerhalb der einzelnen Verwaltungsbereiche und der Verwaltungsbereiche untereinander, noch wenig entwickelt. Die herkömmlichen Kontrollverfahren der lokalen oder regionalen Behörden bieten daher noch einen einigermaßen ausreichenden Schutz gegen mißbräuchliche Verwendung der Daten.

Die Bestandsaufnahme zeigt jedoch, daß die Notwendigkeit des Datenschutzes für die bevorstehende Entwicklung noch nicht an allen Orten erkannt und anerkannt wird. Es bedarf weiterer Anstrengung, die Behörden und Stellen der öffentlichen Verwaltung des Landes hierüber aufzuklären und sie zu veranlassen, mit den in § 2 DSG vorgeschriebenen personellen und technischen Vorkehrungen nicht erst zu warten, bis ein erster Mißbrauch ein Alarmzeichen setzt.

4. AUFGABEN UND TÄTIGKEITEN DES DATENSCHUTZBEAUFTRAGTEN

Das Datenschutzgesetz führt in § 10 als Schutzobjekte des Datenschutzbeauftragten die Persönlichkeitsrechte des Bürgers und die verfassungsmäßige Gewaltenbalance auf.

4.1 Der Schutz des Persönlichkeitsrechts

An erster Stelle nennt das Gesetz (§ 10, Abs. 1) die Aufgabe des Datenschutzbeauftragten, darüber zu wachen, daß die Angaben der Bürger und die über die einzelnen Bürger vorhandenen Unterlagen bei der maschinellen Datenverarbeitung durch die Behörden und Stellen der öffentlichen Verwaltung des Landes vertraulich behandelt werden. Die Überprüfung der auf Grund des Beschlusses der Landesregierung vom 6. Juli 1971 eingegangenen Berichte sowie eigene Recherchen geben zu folgenden kritischen Bemerkungen Anlaß.

4.1.1 Der Umgang mit personenbezogenen Daten

Personenbezogene Daten und Datenbestände dürfen nach dem Grundsatz, der in § 5 Datenschutzgesetz seinen Ausdruck gefunden hat, nur weitergegeben werden, wenn sie keine Einzelangaben über natürliche oder juristische Personen enthalten und keine Rückschlüsse auf solche Einzelangaben zulassen; nur in den in § 5 Abs. 1 und Abs. 3 Datenschutzgesetz vorgesehenen Fällen ist auch die Weitergabe solcher Daten, die Identifizierungsmerkmale enthalten, zulässig. Dieser Grundsatz wird, wie im folgenden dargelegt wird, vielfach mißachtet.

4.1.1.1 Der Datenschutz (§ 2 DSG) setzt bereits mit der Erfassung der Daten für die Unterlagen ein, die für die maschinelle Datenverarbeitung erstellt werden. Die Vertraulichkeit der Angaben der Bürger sollte daher bereits bei der Erfassung der Daten, d. h. bei der Fixierung der Tatbestände in den Erfassungsbögen und Formularen berücksichtigt werden. Nur so ist die Gefahr des Vertrauensbruches oder des Mißbrauchs der Daten von vornherein weitestmöglich auszuschließen. An erster Stelle sollte stets geprüft werden, ob es für die Erfüllung der Aufgabe unverzichtbar ist, überhaupt Identifizierungsmerkmale des Bürgers in die Unterlagen für die maschinelle Datenverarbeitung aufzunehmen, oder auf welche dieser einzelnen Merkmale verzichtet werden kann. Die gleiche Prüfung sollte angestellt werden, bevor Unterlagen mit Identifizierungsmerkmalen weitergegeben werden. Die Mißbrauchsgefahr wird um so größer, je weiter die Integration der vielfach noch gesondert geführten Dateien oder Datenbanken kleineren Umfanges fortschreitet.

Die persönliche Verschwiegenheitspflicht der mit dem Umgang mit Daten befaßten Angehörigen des öffentlichen Dienstes (§ 3 DSG) gewährt keine hinreichende Sicherung des Persönlichkeitsrechts des Bürgers. Der personelle Umfang der staatlichen und kommunalen Leistungsverwaltung ist so groß, daß es für den Bürger unübersehbar ist, welche Bediensteten oder welche Verwaltungsabteilungen von seinen vertraulich zu behandelnden Daten Kenntnis haben oder Kenntnis erhalten; die Quelle von Indiskretionen ist meistens nicht auffindbar.

Zahlreiche Erhebungen personenbezogener Daten im Bereich der öffentlichen Verwaltung dienen statistischen Zwecken und beruhen auf Bundesgesetzen, die von den Ländern als eigene Angelegenheiten (Art. 83 GG) ausgeführt werden. Auf diesem Gebiet könnte der Bundesgesetzgeber einen wirksamen Beitrag zum Datenschutz dadurch leisten, daß er die Erhebung von Identifizierungsmerkmalen des Bürgers und ihre Weitergabe an andere Stellen auf das unabdingbar notwendige Maß beschränkt. Da voraussichtlich eine allgemeine bundesgesetzliche Regelung des Datenschutzes in absehbarer Zeit nicht zu erwarten ist, muß in den einzelnen Gesetzen des Bundes, auf Grund deren personenbezogene Daten der Bürger erfaßt und gesammelt werden, dem Mißbrauch von Individualinformationen durch entsprechende Regelungen entgegengewirkt werden. Die Dringlichkeit dieses Anliegens wird durch folgende Erwägungen verdeutlicht:

Der Bund bereitet ein umfassendes Informationsbankensystem vor. Mit dem Aufbau einer statistischen Datenbank, die ein Teil dieses Informationssystems bilden soll, ist schon 1969 begonnen worden. Ein unselbständiger Bestandteil dieser statistischen Datenbank soll die hochschulspezifische Datenbank sein, die auf Grund des § 18 Hochschulstatistikgesetz vom 31. August 1971 (BGBl. I S. 1473) errichtet wird. In der Begründung zu dem Entwurf dieser Vorschrift führt die Bundesregierung aus, daß Eingabe- und Ausgabemöglichkeiten geschaffen werden sollen, die im Wege der Fernübertragung den direkten Zugriff gestatten.

Das Statistische Bundesamt verweist ebenfalls in seiner Schrift „Das Arbeitsgebiet der Bundesstatistik" (Verlag Kohlhammer 1971 S. 11, 13, 30 ff.) auf den in Vorbereitung befindlichen Aufbau einer statistischen Datenbank als Teil eines automatisierten Informationssystems hin; es erfordert, daß in der Regel — aber eben nur in der Regel — statistische Ergebnisse (Summenangaben u. dgl.) und nicht das Urmaterial der Erfassung der statistischen Daten

in die statistische Datenbank aufgenommen werden sollen (S. 30/31).

Wenn aber sichergestellt werden soll, daß der Datenbank keine Individualdaten entnommen werden, darf die Regel keine Ausnahme haben.

4.1.1.2 Nach §§ 4 bis 14 des Hochschulstatistikgesetzes werden eine Reihe von Tatbeständen erhoben, welche personenbezogene Daten der Studenten, der Teilnehmer an Weiterbildungskursen, der Doktoranden, des wissenschaftlichen, künstlerischen Personals, von Schülern der Sekundarstufe II etc. umfassen. Unter anderem wird auch nach der Finanzierung des Promotionsstudiums und nach anderen individuellen Angaben für beurlaubte oder exmatrikulierte Studenten gefragt. Die Notwendigkeit, in eine hochschulspezifische Datenbank Identifizierungsmerkmale der statistisch erfaßten Personen aufzunehmen, muß in Frage gestellt werden.

Das Bundesausbildungsförderungsgesetz (BAföG) vom 26. August 1971 (BGBl. I S. 1409) sieht ebenfalls eine jährliche Bundesstatistik vor, die den Namen, das Geschlecht und das Geburtsdatum sowie weitere persönliche Daten, insbesondere auch Angaben über die Einkommens- und Vermögensverhältnisse sowohl des Auszubildenden als auch seines Ehegatten und seiner Eltern erfaßt. Das Ausbildungsförderungsgesetz wird von allen Bundesländern mit Hilfe elektronischer Datenverarbeitungsanlagen ausgeführt. Eine allgemeine Verwaltungsvorschrift legt das Programm zur Berechnung des Förderungsbetrages und das Verzeichnis der Individualdaten fest. Die Datenbanken der Länder haben die auf Grund dieses Gesetzes erhobenen Tatbestände dem Statistischen Bundesamt mitzuteilen, das eine jährliche Bundesstatistik zu erstellen hat.

Auch hier erhebt sich die Frage, ob die Weitergabe der Identifizierungsmerkmale der Betroffenen für die statistischen Zwecke unabdingbar ist.

Die gleiche Frage stellt sich auch bei dem Graduiertenförderungsgesetz (GFG) v. 2. September 1971 (BGBl. I S. 1465).

In beiden Gesetzen wird darüber hinaus der Grundsatz, daß die Angaben des Bürgers über seine Einkommens- und Vermögensverhältnisse von den Finanzämtern absolut vertraulich zu behandeln sind, durchbrochen:

Die Finanzbehörden haben den Ämtern für Ausbildungsförderung bzw. Hochschulen Auskünfte über Einkommens- und Vermögensverhältnisse des Auszubildenden bzw. Stipendiaten, seines Ehegatten und nach dem BAföG auch seiner Eltern zu geben. Ehegatten und Eltern sind daneben auch unmittelbar zur Auskunft gegenüber den Ämtern für Ausbildungsförderung bzw. der Hochschule, die das Stipendium gewährt, zur Auskunft verpflichtet, und zwar unabhängig davon, ob sie von dem Antrag des Auszubildenden oder des Stipendiaten überhaupt Kenntnis hatten oder ihm zustimmten.

Der Datenschutz ist insbesondere deswegen angesprochen, weil die Auskünfte der Finanzbehörden sowohl bei den Ämtern für Ausbildungsförderung als auch bei den Hochschulen statistisch erfaßt werden und in eine jährlich durchzuführende Bundesstatistik über Ausbildungsförderung bzw. in die Hochschulstatistik nach dem Hochschulstatistikgesetz eingehen. Beide Dateien werden Teile der Statistischen Datenbank werden, die beim Statistischen Bundesamt eingerichtet wird (vgl. unter 4.1.1.1). Keines dieser Gesetze enthält jedoch Regelungen gegen Mißbrauchsgefahren.

Auch in dem Entwurf eines Wohnungsstichprobengesetzes 1972 — BT-Drucks. VI/2543 — ist die Erfassung personenbezogener Daten vorgesehen, die tief in die Privatsphäre des Auskunftspflichtigen eindringen. Wenn auch der Name und die Anschrift des Auskunftspflichtigen nicht offen erhoben werden, so lassen doch Angaben über die Lage des Grundstücks Rückschlüsse auf die Einzelperson zu. Die Bedenken gegen dieses Verfahren werden dadurch verstärkt, daß diese Statistik vermutlich in die geplante Statistische Datenbank des Statistischen Bundesamtes eingehen wird, zumal da nach der amtlichen Begründung des Gesetzentwurfs die Ergebnisse dieser Statistik auch für die Familienberichte der Bundesregierung ausgewertet werden sollen.

Diese Beispiele aus der Bundesgesetzgebung der jüngsten Zeit erweisen, daß die Grundvorstellungen des Hessischen Datenschutzgesetzes über den Schutz des Bürgers vor Eingriffen in sein Persönlichkeitsrecht in der Bundesgesetzgebung nicht oder nicht genügend verwirklicht werden.

Hierdurch wird die Aufgabe des Datenschutzbeauftragten erheblich erschwert; denn die Bundesgesetze sind durch die Behörden und Stellen der Landesverwaltung auszuführen; sei es als eigene Angelegenheit, sei es im Auftrage des Bundes (Art. 83 ff. GG). Soweit die Landesverwaltung sich hierbei der Mittel der EDV bedient, unterliegt sie der Kontrolle des Datenschutzbeauftragten (§ 1 DSG). Andererseits enthalten die hierfür in Betracht kommenden Bundesgesetze in der Regel auch Vorschriften über das von den Landesbehörden einzuhaltende Verwaltungsverfahren. Diese nach Art. 84, 85 GG zulässigen Verwaltungsvorschriften sind für die Behörden des Landes verbindlich. Infolgedessen treten die Grundsätze des Hessischen Datenschutzgesetzes, soweit sie dem Bürger einen besonderen, durch den Einsatz der EDV veranlaßten Persönlichkeitsschutz gewähren, gegenüber abweichenden konkreten Regelungen des Bundes zurück. Insoweit kann daher das Hessische Datenschutzgesetz keine volle Wirksamkeit entfalten.

4.1.1.3 Im Bereich der Landesverwaltung besteht

a) bei der HZD und den KGRZ eine besondere Lage. HZD und KGRZ betreiben die Datenverarbeitung als Dienstleistung; sie ist der Zweck ihrer Einrichtung, nicht ein Hilfsmittel ihrer Tätigkeit. Daher ist der Datenschutz ein wesentlicher Bestandteil ihrer Verwaltungsaufgabe, und zwar sowohl hinsichtlich des Persönlichkeitsschutzes als auch in der Datensicherung (vgl. 4.3). Die Grundlage hierfür ist neben den Vorschriften des Datenschutzgesetzes die Bestimmung über den Zugriff auf Datenbestände in § 5 DVG. Danach haben lediglich die Mitglieder und die Auftraggeber ein Zugriffsrecht, und zwar nur auf die eigenen eingegebenen Daten. Ferner ist durch geeignete Vorkehrungen sicherzustellen, daß die Daten nicht durch Unbefugte abgerufen werden können. Neben den Vorkehrungen der Datensicherung dient dem Schutz des Persönlichkeitsrechts des Bürgers auch hier nur die allgemeine für den öffentlichen Dienst geltende Pflicht der Bediensteten zur Verschwiegenheit.

b) Auch im Statistischen Landesamt wird Datenverarbeitung in großem Umfange, jedoch als notwendiges Hilfsmittel für die Verwaltungsaufgabe betrieben. Gleichwohl begnügt man sich neben den Vorkehrungen der Datensicherung als Mittel zum Schutz des Persönlichkeitsrechts mit der allgemeinen Verschwiegenheitsverpflichtung der Bediensteten. Diese Situation ist nicht frei von Bedenken. Im Statistischen Landesamt fallen eine Fülle von personenbezogenen Daten oder Datensammlungen mit Identifizierungsmerkmalen der einzelnen Bürger an. Obwohl seither kein Fall eines Mißbrauchs der personenbezogenen Daten in Erscheinung getreten ist, wird man die Situation unter dem Gesichtspunkt des § 2 DSG erneut überdenken müssen.

c) Eines der aufwendigsten und für den Datenschutz wichtigsten EDV-Projekte innerhalb der Landesverwaltung ist das bereits im Aufbau befindliche polizeiliche Informationssystem des Landeskriminalamtes. Die erste Ausbaustufe, die 1973 in Betrieb gehen soll, sieht im wesentlichen ein personenbezogenes Auskunftssystem vor. Über etwa 30 Terminals, die über das Land verteilt werden sollen, wird das System auf Anfrage in wenigen Sekunden angeben, welche Erkenntnisse über eine bestimmte Person bekannt sind. Hierzu gehören neben persönlichen Daten, Angaben über Fahndungen und Aktenzeichen von Personenakten und erkennungsdienstlichen Unterlagen auch Angaben über Straftaten, die der Betreffende begangen hat oder deren er verdächtig ist, sowie Hinweise zur Charakterisierung seiner Persönlichkeit, wie z. B. „gewalttätig", „Ansteckungsgefahr", „geisteskrank", „Simulant" oder „süchtig". Hierbei handelt es sich nicht um eindeutige und objektiv feststehende Merkmale, sondern um Beurteilungen, die stark von subjektiven Faktoren abhängen. Welche Merkmale gespeichert werden und welche Straftaten dem Betreffenden durch entsprechende Verknüpfungen im System „angehängt" werden, entscheidet in der Regel allein der einzelne Polizeibeamte, der den Fall bearbeitet. Die sachliche Notwendigkeit, für die kriminalistische Tätigkeit auch Informationen über Fälle bloßen Verdachts, vermutete Eigenschaften und Verhaltensweisen bereitzustellen, soll nicht bestritten werden. Die von der Automation erhofften Vorteile einer aktuellen, gezielten Information sind ohne Berücksichtigung auch derartiger Daten nicht zu erzielen. Eine Kontrolle durch die Betroffenen wäre mit dem Zweck der Einrichtung unvereinbar. Andererseits greift dieses Informationssystem vom Inhalt der Daten her tief in das Persönlichkeitsrecht des Betroffenen ein, und zwar auch in den grundsätzlich unantastbaren Intimbereich (vgl. 1.2.3). Der Aufbau und die Unterhaltung eines solchen Systems ist aus höherwertigen Interessen des Gemeinwohls nur dann zu rechtfertigen, wenn Weitergabe und Verwendung der Informationen so eng wie möglich geregelt sind und optimal wirksame Sicherungen gegen unberechtigte Kenntnisnahme und Verwendung bestehen. Schon die geltenden Richtlinien bestimmen, daß die kriminalpolizeilichen Personenakten ausschließlich für den internen polizeilichen Gebrauch benutzt werden dürfen und untersagen jegliche Auskunft an Außenstehende. Wenn dagegen die polizeilichen Personenakten auch für Zwecke der Personalbeurteilung verwendet würden, ginge das über die Zwecke der Verbrechensbekämpfung und der polizeilichen Gefahrenabwehr hinaus. Diese Frage wird noch einer Überprüfung unterzogen werden müssen. Besonderer Aufmerksamkeit wird auch die Überwachung und Sicherung des Systems bedürfen. Die Maßnahmen liegen einerseits auf dem personellen Sektor. Hier gilt es, für verantwortungsvolle Positionen nur besonders zuverlässige Beamte einzusetzen. Alle Bediensteten müssen verstärkt auf die Bedeutung des Datenschutzes und die Folgen von Verstößen hingewiesen werden. Zum anderen bedarf es technischer und organisatorischer Maßnahmen, die die Mißbrauchsgefahr mindern. Zwar können unberechtigte Abfragen nicht unmöglich gemacht werden. Um so wichtiger ist es, Verstöße zu erkennen und Konsequenzen zu ziehen. Voraussetzung dafür ist eine lückenlose Aufzeichnung aller Zugriffe in der Weise, daß unberechtigte Abfragen rekonstruierbar sind.

Zusammen mit gelegentlichen stichprobeweisen Kontrollen wäre dadurch bereits ein hohes Maß an präventiver Sicherheit erreichbar.

d) Bemerkenswert ist schließlich, daß sich einige Verwaltungen zur Erfüllung ihrer Verwaltungsaufgabe der Hilfe privater Unternehmen bedienen. Die Staatskasse setzt als Kopfbank für die Auszahlung des Wohngeldes sowohl öffentlich-rechtliche Sparkassen als auch private Banken ein. Die Zentralen der Kreditinstitute erhalten die Datenträger, auf denen die Zahlungsempfänger und der auszuzahlende Betrag fixiert sind. Obwohl dieses von der HZD organisierte Verfahren sehr rationell ist, bleibt doch zu bedenken, daß die an die Privatbanken gegebenen Datenträger mit den personenbezogenen Daten zwar durch das privatrechtliche Bankgeheimnis abgesichert, aber dem behördlichen Datenschutz faktisch entzogen sind. Rechtlich bleiben die Daten und die Verarbeitungsergebnisse im Bereich des Datenschutzes im Sinne des § 1 DSG auch dann, wenn sich eine Behörde oder Stelle der öffentlichen Verwaltung eines Privatunternehmers bedient, um eine konkrete öffentliche Aufgabe zu erfüllen (vgl. 1.3.2). Eine vergleichbare Zusammenarbeit zwischen der öffentlichen Verwaltung und privatrechtlichen Unternehmungen findet auch im Bereich der Sozialversicherung statt, und zwar zwischen den Trägern der Sozialversicherung und den Arbeitgebern (vgl. die Verordnung über die Datenübermittlung in der gesetzlichen Rentenversicherung — DÜVO — vom 24. April 1971 — BGBl. I S. 362).

e) Das Hessische Landesamt für Landwirtschaft in Kassel erhebt zur Durchführung des Gasölverwendungsgesetzes — Landwirtschaft — bei der Antragstellung personenbezogene Daten, wie Name, Anschrift und Einzelheiten der Betriebsverhältnisse des Antragstellers. Als Datenschutz sind in dem Bericht des Landesamtes nur die allgemeinen Vorschriften über die Verschwiegenheitspflicht der Bediensteten aufgeführt. Die Anträge werden mit Hilfe der maschinellen Datenverarbeitung erledigt, und zwar in der Weise, daß die Datenverarbeitungsanlage auch die schriftliche Zahlungsanweisung ausdruckt. Aus diesem Grunde ist eine Anonymisierung des Antragstellers zur Wahrung der Vertraulichkeit seiner Angaben nicht möglich; andererseits macht, wie unterstellt werden kann, die volle Automatisierung des Verwaltungsvorganges bis zur schriftlichen Zahlungsanweisung den Einsatz der EDV erst rationell. Vereinfachung und Verbilligung des Verwaltungsverfahrens haben hier Vorrang vor dem Datenschutz.

Zugunsten der Verwaltung kann jedoch berücksichtigt werden, daß die Angaben über die Betriebsverhältnisse weitestgehend offenkundig sein werden und die spezifischen Gefahren der EDV für die Wahrung des Persönlichkeitsrechtes erst aktuell werden, wenn solche einzelnen Dateien zu einer Datenbank verbunden werden.

f) Der Schutz der Privatsphäre spielt auch im Verhältnis der Kirchen zum Staat eine Rolle. Unter Berufung auf das Hessische Kirchensteuergesetz (vgl. oben 1.3.2) haben kirchliche Organisationen von einer Gemeinde verlangt, ihnen die Veränderungen in der Einwohnerkartei auch bezüglich der Einwohner, die nicht Mitglieder der Kirchen sind, fortlaufend mitzuteilen. Ob diese Forderung berechtigt war, brauchte der Datenschutzbeauftragte nicht zu entscheiden, weil die Verwaltung sie abgelehnt hat. Zu diesem Ergebnis hätte auch die Anwendung der Datenschutzgrundsätze geführt. Zugehörigkeit und Nichtzugehörigkeit zu einer Kirche, einer Religions- oder einer Weltanschauungsgemeinschaft gehören wegen des Grundrechts der Bekenntnisfreiheit, das auch eine „negative" Bekenntnisfreiheit einschließt (Art. 4 GG, Art. 9 HV, vgl. StGH Urteil vom 27. Oktober 1965 P.St. 388 StAnz. 1965 S. 1394), zu dem Bereich menschlichen Eigenlebens, der Geheimnischarakter hat (vgl. oben 1.2.3). Der Zugriff auf Daten dieses Bereichs ist vom Datenschutz her nur zugelassen, wenn hierfür eine spezielle Befugnis durch Gesetz oder auf Grund eines Gesetzes begründet ist (vgl. auch unter 4.1.2).

4.1.2 Befugnis

Der Datenschutz ist nach § 2 DSG darauf gerichtet, daß Unbefugte weder Zugang zu den Unterlagen, Daten und Ergebnissen der maschinellen Datenverarbeitung noch Einwirkungsmöglichkeiten auf sie haben. Weder das Datenverarbeitungsgesetz noch das Datenschutzgesetz bestimmen, wer befugt oder wer unbefugt ist. Nach § 3 DSG ist, wer über Unterlagen, Daten und Ergebnisse verfügungsberechtigt ist, auch befugt, von der Schweigepflicht zu entbinden. Nach § 5 und § 23 DVG hat das Zugriffsrecht auf Datenbestände nur, wer Mitglied oder Auftraggeber der HZD bzw. eines KGRZ ist. Diese Regelung läßt folgende im Berichtszeitraum aufgetretenen Fragen offen:

a) Kann das Mitglied oder der Auftraggeber der HZD bzw. einem KGRZ kraft seines Zugriffsrechtes auf seine eigenen Datenbestände bestimmen, wer befugt ist, Einsicht in sie zu nehmen?

Diese Frage stellte sich bei dem Verlangen einer kirchlichen Organisation an eine Gemeindevertretung, das zuständige KGRZ zu beauftragen, ihr die vollständige Einwohnerdatei der Gemeinde zu übermitteln (vgl. unter 4.1.1.3).

b) Inwieweit sind die Behörden und Stellen der öffentlichen Verwaltung befugt, Einsicht in Datenbestände (durch Auskunft, durch Ausdruck oder auf sonstige Weise) im Wege der Amtshilfe zu gewähren?

Art. 35 GG gibt keine Antwort, weil er nach wohl einhelliger Auffassung in Literatur und Praxis eine Rahmenvorschrift darstellt, die zwar die allgemeine Pflicht zur gegenseitigen Amtshilfe begründet, deren Voraussetzungen, Umfang und Durchführung zu regeln jedoch dem einfachen Gesetzgeber überläßt.

Die nach herrschender Auffassung gültigen Regeln für die Amtshilfe sind im § 5 bis § 7 des Entwurfs der Bundesregierung für ein Verwaltungsverfahrensgesetz — BT-Drucks. VI/1173 — zusammengefaßt. Danach gilt u. a. für die Durchführung der Amtshilfe das für die ersuchte Behörde geltende Recht; sie ist für die Durchführung der Amtshilfe verantwortlich.

Diese Frage stellte sich in verschiedener Hinsicht, etwa bei der Verwaltungsübung der Statistischen Landesämter, Datenbestände miteinander auszutauschen, wenn dies die „funktionale Mitwirkung" anderer Landesämter erfordert; oder an Statistische Ämter der Gemeinden Datenbestände, soweit sie deren regionalen Bereich betreffen, „auszuleihen", wie es beispielsweise mit der Scheidungsstatistik geschieht, die auf Grund § 4 des Bevölkerungsstatistikgesetzes vom 4. Juli 1957 — BGBl. I S. 694 — erhoben wird und die Religionszugehörigkeit, den Wohnort der Prozeßparteien, die gesetzliche Vorschrift, auf welche die Scheidung gestützt wird (Scheidungsgrund), sowie das Aktenzeichen des Gerichts enthält.

Zur Rechtfertigung der Weitergabe personenbezogener Daten, die mehr oder weniger stark in die Intimsphäre des Bürgers Einblick gewähren, wird in der Regel auf die Verschwiegenheitspflicht der Bediensteten der empfangenden Stelle hingewiesen und der Vorgang offenbar als ein Internum einer durch die gleiche Schweigeverpflichtung verbundenen Gemeinschaft angesehen. Diese Betrachtungsweise widerspricht der Grundkonzeption des Datenschutzgesetzes. Sie berücksichtigt nicht die durch die EDV bewirkte Veränderung des Verwaltungsablaufs mit ihren neuartigen Gefahren mißbräuchlicher Verwendung der Auskünfte des Bürgers aus seinem Privatbereich. Sie verharmlost die Schweigepflicht des „abgebenden" Bediensteten, der die Erfüllung seines Gelöbnisses zur Verschwiegenheit einem anderen schweigepflichtigen Bediensteten überlassen zu können glaubt. Außerdem läßt die personale, auf den einzelnen Bediensteten abgestellte Schweigepflicht die Frage unberührt, nach welchen Grundsätzen die Behörde oder Stelle der öffentlichen Verwaltung Amtshilfe durch die Weitergabe vertraulicher Auskünfte des Bürgers leisten darf. Die „Amts"-pflicht zur Vertraulichkeit beruht auf den Grundsätzen der Gesetzmäßigkeit der Verwaltung und der Gewährleistung der Grundrechte des Bürgers. Demgemäß ist die Zulässigkeit der oben erörterten Amtshilfeverfahren am Maßstab der Zielsetzung des Gesetzes, den Persönlichkeitsschutz des Bürgers zu gewährleisten, zu messen. § 3 DSG gibt keinen hinreichenden Maßstab.

4.1.3 Bereich des Gesetzes

Bei der Bestandsaufnahme, mit welcher der Einsatz der EDV in der öffentlichen Verwaltung festgestellt werden sollte, hat sich ergeben, daß verschiedentlich Unklarheiten darüber bestehen, welche Behörden oder Stellen zum Bereich des Datenschutzes im Sinne des § 1 DSG gehören (vgl. oben 1.3.2).

4.1.3.1 Eine öffentlich-rechtliche Körperschaft vertrat die Auffassung, daß eine Überwachung des Datenschutzes in ihrem Betriebe unnötig, wenn nicht sogar unzulässig sei, weil sie ihren Betrieb auf privatrechtlicher Grundlage betreibe und der Inhalt ihrer Datensammlungen ohnehin dem Bankgeheimnis unterliege.

Der Datenschutzbeauftragte hat hierzu gegenüber dem Hessischen Ministerpräsidenten — Staatskanzlei — folgende Äußerung abgegeben:

> Das Datenschutzgesetz gilt für alle Unterlagen, die in der öffentlichen Verwaltung für Zwecke der maschinellen Datenverarbeitung hergestellt werden, sowie für alle in der öffentlichen Verwaltung gespeicherten Daten und für die Ergebnisse ihrer Bearbeitung.
>
> Zweck des Gesetzes ist es, den besonderen Gefahren, die aus der maschinellen, vor allem aus der elektronischen Datenverarbeitung erwachsen können, durch hierauf ausgerichtete Schutzmaßnahmen (Datenschutz — Datensicherung) entgegenzuwirken. Für die Ausführung des Datenschutzgesetzes ist es unerheblich, ob die Aufgaben der öffentlichen Verwaltung mit den Mitteln des öffentlichen Rechts oder mit denen des Privatrechts wahrgenommen werden. Denn der Datenschutz betrifft nur das technische Instrument, das bei der Erfüllung der Aufgabe benutzt wird, nicht dagegen den sachlichen Gehalt der Aufgabe, zu deren Erfüllung das Instrument benutzt wird. Daher unterliegt die maschinelle Datenverarbeitung — und die Herstellung der hierfür bestimmten Unterlagen — dem Datenschutz, unabhängig davon, ob die Daten, die gesammelt, gespeichert und verarbeitet werden, aus dem staatlichen oder kommunalen Aufgabenbereich oder aus den privatwirtschaftlichen Rechtsbeziehungen der öffentlich-rechtlichen Körperschaft stammen.
>
> Die Vorschriften des Hessischen Datenschutzgesetzes lassen die dem Privatrecht zugehörigen Vorgänge, die in den Daten verschlüsselt sind, völlig unberührt. Sie

dienen nur dem Schutz dieser Daten vor dem Zugriff und der Einsicht durch Unbefugte und sichern somit, im Hinblick . . . (auf die Aufgaben dieser öffentlich-rechtlichen Körperschaft), auch das Bankgeheimnis gegen die neuartigen Gefahren ab, die aus der elektronischen Datenverarbeitung erwachsen können.

In einem anderen Fall vertrat ein kommunales Unternehmen die Auffassung, „daß unsere ausschließlich kommerziell benutzte (EDV-)Anlage nicht unter das Datenschutzgesetz fällt". In der Anlage würden die „Persönlichkeit des Bürgers betreffende Daten nicht verarbeitet". Vielmehr sei sie einer Anlage gleichzusetzen, die bei Unternehmen in der Privatwirtschaft betrieben werden.

Der Datenschutzbeauftragte trat dieser Auffassung mit den bereits genannten Argumenten entgegen.

4.1.3.2 Eine oberste Landesbehörde hat die Frage aufgeworfen, ob sich das Datenschutzgesetz auch auf die Sammlung rein technischer Daten beziehe, die ihrer Natur nach nicht personenbezogen sind.

Hierzu vertritt der Datenschutzbeauftragte folgende, dem Hessischen Ministerpräsidenten — Staatskanzlei — mitgeteilte Auffassung:

> Das Datenschutzgesetz erstreckt sich sowohl auf personenbezogene als auch auf sachbezogene Daten und macht für Unterlagen und Daten, die ausschließlich technische Berechnungen betreffen, keine Ausnahme. Die Zielrichtung des Gesetzes würde verfehlt werden, wenn der Datenschutz in der öffentlichen Verwaltung nicht möglichst lückenlos geregelt wäre; denn die Entwicklung wird über kurz oder lang zur Integration der von den einzelnen Verwaltungen zunächst noch getrennt geführten Dateien führen, und in der integrierten Datenbank können sachbezogene Daten, wenn sie mit personenbezogenen kombiniert werden, unvorhergesehen eine neue Qualität erhalten, für die der Datenschutz erforderlich ist.

Diese unter dem Gesichtspunkt des Schutzes des Persönlichkeitsrechtes des Bürgers begründete Stellungnahme wird auch der weiteren Zielsetzung des Gesetzes gerecht, eine Verschiebung in der Gewaltenteilung zwischen den Verfassungsorganen des Landes zu Lasten der Legislative zu verhindern. Dieser Zweck des Gesetzes verbietet eine restriktive Auslegung des in § 1 DSG bewußt weit gefaßten Bereiches des Datenschutzes. Da der Datenschutzbeauftragte nach § 10 Abs. 2 DSG auch die verfassungspolitischen Auswirkungen des Einsatzes der EDV in der öffentlichen Verwaltung zu beobachten hat, muß er über den Einsatz der EDV in der öffentlichen Verwaltung umfassend und uneingeschränkt unterrichtet sein.

4.1.4 Anrufungsrecht des Bürgers

Von dem Anrufungsrecht nach § 11 DSG hat im Berichtszeitraum kein Bürger Gebrauch gemacht. Ebensowenig ist bekannt geworden, daß im Berichtszeitraum Ansprüche nach § 4 Abs. 2 auf Wiederherstellung des früheren Zustandes oder auf Unterlassung erhoben worden sind.

Daraus kann jedoch nicht gefolgert werden, daß alle von der öffentlichen Verwaltung gespeicherten Daten richtig seien und daß die Tatbestände des § 4 Abs. 2 DSG in keinem einzigen Falle objektiv erfüllt wären.

Vielmehr ist zu berücksichtigen, daß § 4 Abs. 1 DSG eine unvollständige Vorschrift ist, weil mangels einer gesetzlich begründeten Auskunftspflicht der öffentlichen Verwaltung der Bürger mehr oder weniger nur durch Zufall erfahren wird, ob über ihn gespeicherte Daten unrichtig sind. In den Entwürfen von Datenschutzgesetzen oder vergleichbaren gesetzlichen Regelungen sowohl des Bundes als auch anderer Länder ist eine Verpflichtung der Behörden vorgesehen, dem Bürger unter bestimmten Voraussetzungen von Amts wegen oder auch auf Antrag Auskünfte über die über ihn gespeicherten Daten zu erteilen.

Da die öffentliche Verwaltung des Landes nur an der Speicherung richtiger Daten interessiert sein kann, wird empfohlen, Auskunftsverlangen der Bürger über die gespeicherten Daten, die sie betreffen, nicht wegen des Fehlens einer ausdrücklichen gesetzlichen Regelung abzulehnen. Denn das Datenschutzgesetz verbietet der Verwaltung nicht, solche Auskünfte zu erteilen.

4.2 Erhaltung der Gewaltenteilung

§ 10 Abs. 2 des Datenschutzgesetzes stellt dem Datenschutzbeauftragten die Aufgabe, Auswirkungen der maschinellen Datenverarbeitung dahingehend zu beobachten, ob sie zu Verschiebungen der verfassungsmäßigen Gewaltenteilung führen und ggf. Gegenmaßnahmen anzuregen. Der Gesetzgeber hat damit berücksichtigt, daß die neuartigen Informationsinstrumente nicht nur das Verhältnis zwischen den Bürgern als den Betroffenen und den Behörden als den Inhabern verändert, sondern ebenso Auswirkungen auf das Verhältnis der staatlichen Organe zueinander haben kann. Dies beruht auf dem Umstand, daß die verschiedenen Teile der staatlichen Organisation in höchst unterschiedlicher Weise an der Datenverarbeitung partizipieren. Da sich der Einsatz neuer Methoden und Techniken im Außenverhalten der Institutionen bemerkbar macht, wird sich zwangsläufig auch ihr funktionelles Zusammenwirken verändern. Unserem Staatsaufbau liegt der Gedanke einer mehrfachen Gewaltenteilung, einer wechselseitigen Machtkontrolle und eines daraus resultierenden Gleichgewichts zugrunde. Deshalb führt jeder Funktionsverlust oder -zuwachs einer Teilgewalt unmittelbar zu der Frage, ob er das Gleichgewicht gefährdet und

mit welchen Gegenmaßnahmen es ggf. aufrechterhalten werden kann.

Gewaltenteilung besteht nicht nur zwischen den drei klassischen Staatsgewalten Legislative, Exekutive und Judikative. Sie realisiert sich auch im föderativen Staatsaufbau sowie im Prinzip der kommunalen Selbstverwaltung. Sie kommt zum Ausdruck in der Verteilung der Aufgaben und in einem komplizierten System wechselseitiger Beeinflussung und Abhängigkeit. Verschiebungen der Gewaltenteilung sind deshalb nicht ohne weiteres wahrnehmbar. Vielmehr kommt es darauf an, zunächst festzustellen, welche Veränderungen wahrscheinlich oder doch denkbar sind, die tatsächliche Entwicklung unter diesen Aspekten gezielt zu untersuchen und den Befund sodann zu bewerten. Da die für die Gewaltenteilung besonders wichtigen Planungs- und Entscheidungshilfen z. Z. praktisch noch keine Rolle spielen, darf hier noch nicht mit handgreiflichen Resultaten gerechnet werden. Es wird aber an der Aufstellung eines Programmes im dargelegten Sinne gearbeitet.

4.2.1 Parlament — Regierung

Das Verhältnis des Parlaments zur Exekutive wird durch den automatischen Vollzug von Massenarbeiten nicht tangiert. Hier handelt es sich um Gesetzesanwendung. Die Programmierung besitzt dabei inhaltlich keine weitergehenden Folgen als andere Formen der verwaltungsinternen Präzisierung von Gesetzen wie etwa Erlasse und Richtlinien. Dagegen betreffen Planungs- und Entscheidungshilfen den rechtlich grundsätzlich ungebundenen Bereich freier politischer Gestaltung. Hier liegt der Schwerpunkt der parlamentarischen Auseinandersetzung über politische Ziele und Programme. Wenn allein die Regierung in diesem Bereich modernste Managementtechniken anwendet, dann sind für die Handlungschancen des Parlaments Auswirkungen vor allem in folgenden Richtungen zu erwarten:

Die von der Regierung entwickelten Pläne werden dank besserer Informationssammlung und -verarbeitung genauer auf die sozialen, wirtschaftlichen und natürlichen Bedingungen zugeschnitten, d. h. realitätsgerechter sein, als dies bislang möglich war. Dies macht es für das Parlament zunehmend schwieriger, Kritik anzubringen oder Alternativen aufzubauen, die gegenüber Argumenten der Regierung Bestand haben. Die Regierung erhält in der „Sachargumentation" einen deutlichen Vorsprung.

Ein weiterer Faktor kann die Chancen der Volksvertretung, auf die Pläne der Regierung inhaltlich Einfluß zu nehmen, stark mindern: die durch systemanalytische Verfahren zu bewirkende Abstimmung zwischen den verschiedenen Einzelplänen (integrierte Planung). Sie hat zur Folge, daß jeder ändernde Eingriff wie eine Störung eines genau ausregulierten Systems wirkt, der weitreichende, im einzelnen gar nicht absehbare disharmonische Konsequenzen befürchten läßt.

Gegenüber einer mit modernsten Methoden und Techniken arbeitenden Planungsbürokratie könnte das Parlament leicht in die Rolle eines Störenfriedes geraten. Eine solche Entwicklung müßte die demokratische Glaubwürdigkeit auf die Dauer untergraben.

Besonders deutlich wird die Gefahr einer technokratischen Aushöhlung des Parlamentarismus, wenn die Regierung moderne Techniken nicht nur zur Sach- oder Aufgabenplanung, sondern auch zur Absicherung ihrer eigenen Machtstellung verwendet. Zwar ist bislang von einem „integrierten Planungs- und Machterhaltungssystem" nichts bekannt geworden. Ein solches Projekt läge aber durchaus in der Konsequenz eines (weit verbreiteten) Denkens, das moderne Planungs- und Entscheidungsmethoden ausschließlich unter dem Aspekt ihrer Verwendbarkeit für die Regierungen betrachtet.

Allerdings ist darauf hinzuweisen, daß es gegenwärtig noch keine ausreichenden Erfahrungen gibt, um die Auswirkungen moderner Managementtechniken auf den politischen Prozeß endgültig zu beurteilen. So ist z. B. noch nicht geklärt, ob systemanalytische Planungstechniken die politische Diskussion tatsächlich austrocknen, wie dies oben angedeutet wurde. Möglicherweise wird umgekehrt durch die in diesem Verfahren enthaltene Offenlegung der Planungsziele und ihrer Ableitung aus übergeordneten gesellschaftlichen Werten eine bisher nicht gekannte Transparenz hergestellt, die die politischen Diskussionen in Parlament und Öffentlichkeit außerordentlich befruchten und dadurch zu Rückwirkungen auf die Planziele führen könnte.

Unabhängig davon, welche Prognosen man im einzelnen für zutreffend hält, läßt sich doch insgesamt nicht verkennen, daß der Einsatz moderner Verfahren durch die Regierungen eine Herausforderung der Parlamente darstellt. Dies in mehrfacher Beziehung.

Minimalbedingung für eine Funktionserhaltung des Parlaments ist eine ausreichende Vertrautheit mit dem neuen Instrumentarium. Gegenüber einer Regierung, die sich auf die Objektivität ihrer Computerergebnisse beruft, könnte eine pauschale Kritik wenig bewirken. Vielmehr wird eine Kritik erst dann sinnvoll, wenn sie den Schein der Objektivität durchbricht, indem sie aufzeigt, auf Grund welcher Bedingungen und Entscheidungen die Computer zu diesen Ergebnissen gekommen sind. Um aber herauszufinden, ob ungenaue Daten, unzureichende Programme oder politische Entscheidungen in Form von Vorgaben oder Annahmen mit im Spiel sind, ist nicht nur eine gewisse Transparenz des Informationssystems erforderlich. Vor allem müssen die Kritiker über die entsprechende Kenntnis verfügen, damit sie die neuralgischen Punkte aufspüren und damit den Weg für Alternativen öffnen können.

Das Parlament muß sich aber nicht nur reaktiv auf eine Regierung einstellen, die neue Techniken verwendet; es muß vor allem auch seinen eigenen Standpunkt zu dieser neuen Technik entwickeln. Dies betrifft nicht nur die Frage, wie es den Gebrauch der Instrumente durch die Regierung beeinflussen möchte. Es geht vor allem darum, ob und ggf. wie das Parlament sich die neuen Methoden auch für die eigene Tätigkeit zunutze machen kann. Prinzipiell sind hier drei Lösungen denkbar: Enthaltsamkeit, der Aufbau eigener Systeme und die Partizipation an den Projekten der Exekutive.

Wollte das Parlament auf die Nutzung moderner Planungs- und Informationsmethoden verzichten, während die Regierung sie nutzt, so bedeutete das einen politischen Machtverlust. Dieser Weg sollte deshalb nicht ernstlich in Betracht gezogen werden.

Der Aufbau eines eigenen parlamentarischen Informationssystems würde zwar dem Modell der Gewaltenteilung am ehesten entsprechen. Als längerfristige Möglichkeit darf er auch keineswegs ausgeschlossen werden. Andererseits dürfte aber die Entwicklung und Unterhaltung eines völlig selbständigen Systems kaum in Betracht kommen. Dies würde den Aufbau eine „Gegenverwaltung" voraussetzen und doch weitgehend nur zu einem Ebenbild der von der Regierung betriebenen Systeme führen. Sowohl verfassungsrechtliche als auch wirtschaftliche Argumente stünden einer solchen Lösung entgegen.

Als drittes Modell bleibt die Teilnahme des Parlaments an den Systemen der Regierung, wie sie im Hessischen Datenschutzgesetz sowie einigen anderen Gesetzen und Entwürfen in Form besonderer parlamentarischer Informationsrechte auch bereits angedeutet ist. Hier dürfte eine durchaus praktikable mittelfristige Perspektive liegen. Allerdings wird dieses Modell nur dann einen etwa einigermaßen gleichwertigen Ersatz für eigene Systeme darstellen, wenn die Beteiligung nicht auf die bloße Benutzung eines von der Exekutive bestimmten Angebots beschränkt bleibt. Es muß vielmehr ein wesentlich weitergehender Einfluß der parlamentarischen Instanzen gesichert sein. Zwar fehlen bislang noch eingehendere Untersuchungen über den Informationsbedarf der Parlamente. Man wird aber nicht ohne weiteres davon ausgehen können, daß sich der Informationsbedarf der Parlamente ausschließlich innerhalb des Bereichs bewegt, den die Exekutive für ihre eigenen Zwecke benötigt. Soll auch der darüber hinausgehende Bedarf berücksichtigt werden, so wird es einer Beteiligung des Parlaments schon in der Phase der Systemplanung bedürfen. Hierfür müßten zunächst geeignete Kooperationsformen gefunden werden.

Naturgemäß ergeben sich aus dem Kooperationsmodell einige besondere Schwierigkeiten. Zwar wird wegen des weitgehend öffentlichen Charakters der Parlamentstätigkeit eine Geheimhaltung von „parlamentarischen" Datenbereichen gegenüber der Regierung kaum in Betracht kommen. Dagegen sollte die Art und Weise der Benutzung des Systems grundsätzlich der Geheimhaltung unterliegen. Denn wenn ein Benutzer vorbereitende Untersuchungen, Planspiele oder andere gedankliche Experimente durchführt, so wird er Wert darauf legen, dies unbeobachtet und ohne die Befürchtung tun zu können, daß andere Interessierte schon in diesem Stadium Kenntnis von seinen Vorhaben erlangen. Dieses Bedürfnis ist legitim. Denn nur so ist es möglich, auch unorthodoxe Modelle durchzuspielen und damit ggf. eine umfassende Neuorientierung vorzubereiten.

In der Praxis würde eine solche Geheimhaltung allerdings auf Schwierigkeiten stoßen, wenn die Rechenzentren organisatorisch voll dem Regierungsapparat eingegliedert wären. Dagegen bietet die in Hessen gewählte Organisationsform besonderer öffentlich-rechtlicher Körperschaften, in deren Leitungsgremien auch Parlamentsabgeordnete vertreten sind, die institutionellen Voraussetzungen, um auch den parlamentarischen Bedürfnissen gerecht zu werden.

Eine parlamentarische Beteiligung gibt auch der — bisher nur in Baden-Württemberg positiv entschiedenen (vgl. oben 2.1.5) — Frage neue Aktualität, ob und wieweit die Informationssysteme einer gesetzlichen Grundlage bedürfen.

4.2.2 Land — Kommunen

Das Verhältnis zwischen dem Land und den Kommunen kann durch die Datenverarbeitung in zweifacher Weise betroffen werden: durch die Aufbauorganisation der DV, insbesondere der Rechenzentren, und durch die Ausgestaltung der Informationssysteme.

Die mit dem HZD-Gesetz gewählte Organisationsstruktur eines Verbundmodells wurde, vor allem von Kritikern außerhalb des Landes, als eine zentralistische Lösung bezeichnet, die den Interessen der Kommunen nicht gerecht werde. Diese Kritik ist durch Erfahrungen des Datenschutzbeauftragten in der Berichtszeit nicht bestätigt worden. Ein Zwang zur Nutzung der EDV und zu kooperativer Lösung der organisatorischen Probleme folgt aus der Natur der Sache, nicht aus einem speziellen Organisationskonzept. Durch die Struktur der Leitungsorgane im hessischen Modell sind die kommunalen Interessen gewahrt. Die Vorteile einer institutionalisierten Koordination zwischen Landes- und Kommunalbereich, vor allem im Hinblick auf vertikal integrierte Systeme, sind mittlerweile allgemein anerkannt, was sich in vielen Ländern in der Einrichtung besonderer Koordinierungsgremien niedergeschlagen hat. Auch die Finanzierung der Kommunalen Gebietsrechenzentren durch das Land wird man nicht als Beeinträchtigung der kommunalen Selbstverwaltung bezeichnen können. Im Gegenteil liegt hier eine wichtige Voraussetzung für den zügigen Aus-

bau der Datenverarbeitung auch auf der kommunalen Seite.

Die Erhöhung der Verwaltungskraft der Kommunen sollte synchron mit der Entwicklung bei der Landesverwaltung verlaufen. Eine technologische Rückständigkeit, die den Tendenzen zur Einschränkung der kommunalen Selbstverwaltung Vorschub leisten würde, darf nicht eintreten. Dies gilt nicht nur für den Vollzugssektor, sondern gerade auch für den Bereich der Entscheidungshilfen. Hier wird es darauf ankommen, mit den Projekten des Landes gleichauf zu bleiben, damit sichergestellt wird, daß die wechselseitigen Verbindungen von vornherein entsprechend den Bedürfnissen beider Seiten mit einbezogen werden. Bezüglich des Zuganges zu den Daten ist im Grundsatz eine weitgehende wechselseitige Offenheit wünschenswert, um eine inhaltliche Abstimmung der Planungen zu fördern. Andererseits wird es möglicherweise aber auch besonderer Sicherungen bedürfen, um Daten, welche die Verfügungsberechtigten geheimhalten wollen, abzuschirmen.

Der Datenverarbeitung wird oft eine Tendenz zur Zentralisierung zugeschrieben. Diese Annahme hat sich bisher nur sehr beschränkt bestätigt. Die Anforderungen, die die Datenverarbeitung an die Organisation stellt, wurden bisher im wesentlichen nicht durch eine Zentralisierung von Befugnissen oder einen Zusammenschluß zu größeren Einheiten erfüllt, sonden konnten mit den Mitteln der Koordination und Kooperation aufgefangen werden. So erlauben die Kommunalen Gebietsrechenzentren eine dezentrale Nutzung der Datenverarbeitung, wobei allerdings eine weitgehende Angleichung der Arbeitsmethoden und Verfahrensabläufe erforderlich ist.

4.2.3 Parlamentarische Informationsrechte

§ 6 des Datenschutzgesetzes gibt dem Landtag und den kommunalen Vertretungsorganen ein besonderes Informationsrecht gegenüber den Rechenzentren und Behörden, die Datenverarbeitungsanlagen betreiben. Die praktische Ausübung dieses Rechts setzt voraus, daß die Berechtigten wissen, welche Datenbestände ihnen offenstehen und welche Auswertungsprogramme vorhanden sind. Diese Voraussetzungen sind bisher im Bereich der Statistik gegeben, nicht dagegen im Verwaltungsvollzug. Hier ist die Gewinnung von Entscheidungshilfen als eine Art Nebenprodukt zwar auch möglich, zuvor müssen jedoch die Dateien aufbereitet und spezielle Programme geschrieben werden. Einen systematischen Ansatz hierzu stellt das Projekt „Hessisches Planungsinformations- und Analyse-System" (HEPAS) dar, das unter 4.2.4 behandelt wird. Erst mit dem Fortschreiten dieses Vorhabens werden die Informationsrechte des § 6 DSG größere praktische Bedeutung erlangen.

Von der Möglichkeit, wegen mangelhafter Beantwortung eines Auskunftsersuchens den Datenschutzbeauftragten mit der Untersuchung der Ursachen zu betrauen (§ 12 DSG), ist im Berichtszeitraum nicht Gebrauch gemacht worden.

4.2.4 Hessisches Planungsinformations- und Analyse-System (HEPAS)

Ein erster Schritt in Richtung auf die Realisierung planungs- und entscheidungsorientierter Informationssysteme wurde vor kurzem von der Hessischen Zentrale für Datenverarbeitung mit der Vorlage einer ersten Konzeption für ein „Hessisches Planungsinformations- und Analyse-System" (HEPAS) vollzogen. Die HZD folgt damit ihrem Satzungsauftrag, Informationssysteme zu errichten (§ 3 Nr. 3 der von der Landesregierung genehmigten Satzung). HEPAS will die Informationsgrundlage für Planungen und Entscheidungen von Grund auf verbessern. Die relevanten Daten sollen hauptsächlich aus den Dateien des automatisierten Verwaltungsvollzugs gewonnen werden, darüber hinaus auch aus der Statistik und aus Erhebungen. Zur Aufbereitung, Analyse und Darstellung sollen Programme entwickelt werden, die großenteils auf sozialwissenschaftlichen Methoden aufbauen. HEPAS soll nicht nur über die zurückliegende Entwicklung und den gegenwärtigen Stand der wichtigsten Bereiche informieren, sondern mit Prognose- und Simulationsmodellen auch künftige Trends und die zu erwartenden Auswirkungen verschiedener Alternativpläne deutlich machen. Dagegen bleiben die Entscheidungen selbst den zuständigen Stellen vorbehalten.

Die Studie versteht sich als Diskussionsgrundlage, die noch der Abstimmung mit der Verwaltung bedarf. Die Realisierung des HEPAS soll stufenweise erfolgen, wobei z. B. die Gemeindedatei relativ kurzfristig und die Einwohner-Planungsdatei mittelfristig (4 bis 5 Jahre) aufgebaut werden können. Für die anderen Bestandteile werden längere Zeiträume veranschlagt.

Für die weitere Entwicklungsarbeit hat der Planungsausschuß der Landesregierung die Bildung der Arbeitsgruppen „Datenbasis" und „Methodenbasis" beschlossen, in denen Verwaltung und HZD zusammenarbeiten. Ihre Aufgabe ist es, den Informationsbedarf näher zu analysieren, detaillierte Sollvorstellungen über die benötigten Dateien und Programme zu erarbeiten und Prioritäten für das weitere Vorgehen festzulegen. Beide Arbeitsgruppen haben ihre Tätigkeit inzwischen aufgenommen.

Ein besonderes Entscheidungsverfahren zur Steuerung des Aufbaues des HEPAS ist derzeit noch nicht vorgesehen. Das für Automationsvorhaben aus dem Bereich des Verwaltungsvollzuges geltende Verfahren, bei welchem der Ar-

beitsausschuß für die Automation von Aufgaben der Landesverwaltung über die sachliche Ausgestaltung und der Koordinierungsausschuß über den Zeitpunkt der Übernahme jedes Projekts entscheiden, kommt hier nicht zur Anwendung. Auch aus dem bereits erwähnten § 3 Nr. 3 der Satzung der HZD sind keine eindeutigen Folgerungen für die weitere Prozedur abzuleiten.

Im Hinblick auf die unter 4.2.1 angestellten Überlegungen ist festzustellen, daß sich die Planungen für das HEPAS noch im ersten Anfangsstadium befinden. Das weitere Verfahren ist noch in jeder Beziehung offen. Andererseits liegt aber eine bereits relativ konkrete Diskussionsgrundlage vor, und die Detailplanungen sind angelaufen. Insofern wäre der gegenwärtige Zeitpunkt geeignet, die Interessen des Parlaments in die weitere Arbeit einzubringen.

4.3 Datensicherung

Unter dem umfassenden Begriff Datenschutz versteht das Hessische Datenschutzgesetz

a) den Schutz der natürlichen oder juristischen Personen und Personengruppen, über die Daten erfaßt, gespeichert und verarbeitet werden, vor Eingriffen in die Privat- und Geheimsphäre durch unbefugten Zugriff, unbefugte Änderung, Weitergabe, Unterdrückung oder Vernichtung ihrer personenbezogenen Daten;

b) die Erhaltung der Gewaltenteilung zwischen Parlament, Regierung und Gemeinden einmal durch Sicherung eines Informationsrechtes des Landtags und der kommunalen Vertretungsorgane und zum anderen durch Aufstellen von Grundsätzen, die bei der Weiterentwicklung der Informations- und Kommunikationsstrukturen beachtet werden müssen, sowie

c) die Sicherung der Daten und Datenbestände durch personelle, organisatorische und technische Vorkehrungen gegen unbefugten Zugriff, Diebstahl oder Zerstörung.

Dieser dritte Bereich, in dessen Vordergrund nicht die Person, sondern die Daten stehen, wird als Datensicherung bezeichnet.

Dabei handelt es sich demnach um konkrete Schutzmaßnahmen, die den störungsfreien Ablauf der automatisierten Verfahren gewährleisten, Daten, Dateien und Programme vor Verfälschung, Entwertung und unberechtigten Zugriff schützen und Beschädigungen und Beeinträchtigungen der EDV-Anlage sowie der Hilfseinrichtungen abwehren. Hierzu dienen eine Vielzahl von Einzelmaßnahmen, die auf verschiedenen Ebenen ansetzen können. Neben personellen und rechtlichen Vorkehrungen sind programm- und maschinentechnische, bauliche und organisatorische zu nennen.

Wichtige Teilaufgaben der Datensicherung sind z. B. die Abschirmung des Maschinensaals gegen unbefugten Zutritt, die geschützte Aufbewahrung und der sichere Transport von Datenträgern sowie eine klare, arbeitsteilige Organisation mit genau abgegrenzten Verantwortlichkeiten im Rechenzentrum. Die Einzelmaßnahmen müssen aufeinander abgestimmt sein und in ihrem Zusammenwirken ein lückenloses Sicherheitssystem ergeben.

Während in der ersten Aufbauphase der Datenverarbeitung die Sicherheitsprobleme wenig beachtet wurden, wird ihnen in jüngster Zeit sowohl in der EDV-Wirtschaft als auch bei den Anwendern besondere Aufmerksamkeit gewidmet. Man versucht, die entstandene Sicherheitslücke möglichst rasch zu schließen.

Im Vergleich zu den privaten EDV-Anwendern ist die Situation innerhalb der öffentlichen Verwaltung relativ günstig. Hier war das Sicherheitsdenken niemals völlig dem Effizienzdenken untergeordnet. Auch die geringere Personalfluktuation macht sich positiv bemerkbar. Systematische Bemühungen um die Lösung des Sicherheitsproblems sind jedoch auch hier relativ neuen Datums.

4.3.1 HZD und KGRZ

Der Koordinierungsausschuß des hessischen Datenverarbeitungs-Verbundes hat 1970 eine Arbeitsgruppe mit dem Auftrag eingesetzt, ein für alle Rechenzentren anwendbares Sicherheitskonzept zu erarbeiten. Dieses Projekt ist noch nicht abgeschlossen. In mehreren Zwischenberichten wurden jedoch Teilergebnisse vorgelegt, u. a. ein nach Ablaufphasen und Gefahren gegliederter Katalog der empfehlenswerten Sicherheitsmaßnahmen.

Soweit Gestaltung und technische Ausrüstung der Baulichkeiten berührt sind, werden die Empfehlungen bei den laufenden Bauvorhaben berücksichtigt, wie sich bei einer Reihe von Gesprächen und Besichtigungen ergeben hat. Z. B. wurde der Zugang zum Maschinensaal und zum Datenträgerarchiv so gestaltet, daß Unbefugten der Zutritt zu diesen Räumen nicht möglich ist. Die Lagerräume für die Datenträger wurden gegen Feuer- und Einbruchsgefahr besonders abgesichert. In anderen Bereichen steht die Realisierung der Empfehlungen noch aus. An der Ausarbeitung von Dienstanweisungen, die die Grundlage der organisatorischen Sicherheit bilden sollen, wird zur Zeit gearbeitet.

4.3.2 Außerhalb des Datenverarbeitungs-Verbundes

Außerhalb des hessischen Datenverarbeitungs-Verbundes wird der Datensicherung noch nicht überall die gebührende Aufmerksamkeit gewidmet. Manche Stellen haben noch keine besonderen Maßnahmen ergriffen oder haben sich mit einer Belehrung bzw. Verpflichtung der Be-

diensteten auf das Datenschutzgesetz begnügt (s. unter 3.2). Die Datenträger sind nicht überall ausreichend gegen Entwendung oder unberechtigten Einblick geschützt. Dies gilt sowohl für die Aufbewahrung als auch für den Transport zwischen Verwaltung und Rechenzentrum oder Erfassungsstelle. Zum Teil ließe sich das Risiko dadurch mindern, daß man Unterlagen vernichtet, sobald sie nicht mehr benötigt werden. So sollten z. B. Lochkarten vernichtet werden, sobald ihre Daten auf Magnetband oder -platte überspielt sind.

Im Zusammenhang mit dem geplanten Personenkennzeichen gewinnen die Sicherungsvorkehrungen bei der Datenerfassung und -verarbeitung im Einwohnerwesen besondere Bedeutung. Unter Anleitung der HZD haben einige Gemeinden einen Modell-Versuch in der Ersterfassung im Einwohnerwesen unternommen. Der Datenschutzbeauftragte hat sich in den Gemeinden Geisenheim und Eltville über die veranlaßten Sicherungsmaßnahmen in Verbindung mit der Datenerfassung, dem Datentransport und der bestehenden Organisation an Ort und Stelle eingehend informiert. Die zu diesem Zeitpunkt erforderlichen Schutzmaßnahmen waren ausreichend und wurden beachtet.

Trotz der noch bestehenden Mängel sind keine konkreten Verstöße gegen Mißbrauchsfälle bekannt geworden. Die Computerkriminalität, die privaten EDV-Anwendern zunehmend Sorge bereitet, konnte in der öffentlichen Verwaltung noch nicht Fuß fassen. Obwohl die Täter meist nur den eigenen Vorteil anstreben und deshalb die Rechte der Bürger im allgemeinen nicht unmittelbar bedroht sind, ist die Computerkriminalität auch für den Datenschutz von großem Interesse. Die bekannt gewordenen Fälle zeigen die Schwachstellen im Sicherheitssystem, die auch potentielle Gefahren für die Geheimhaltung darstellen. Eine Analyse dieser Fälle kann deshalb wertvolle Hinweise für die Verbesserung des Sicherheitssystems ergeben, was auch dem Datenschutz zugute käme.

5. ANREGUNGEN

Wie die vorstehenden Abschnitte 1. bis 4. des Berichts zeigen, hat der Datenschutzbeauftragte bei seiner bisherigen Tätigkeit keine direkten Verstöße gegen die Datenschutzbestimmungen feststellen können. Ihm wurden jedoch eine Reihe von Tatsachen bekannt, die den Grundsätzen des Datenschutzes widersprechen. Berichte aus dem In- und Ausland zeigen darüber hinaus, daß bei den Vorausplanungen für integrierte Informationssysteme der Datenschutz oft unbeachtet bleibt oder als störender Faktor angesehen wird, der die Weiterentwicklung nur hemmen kann. Den Grundsatz „Datenschutz kommt vor Datenfluß" möchte man gern umkehren.

Auf Grund seiner Feststellungen und Überlegungen trägt der Datenschutzbeauftragte folgende Anregungen vor:

5.1 Verzicht auf Identifizierungsmerkmale

Um die unberechtigte Identifizierung des einzelnen aus Daten zu verhindern oder zu erschweren, sollte sowohl der Gesetzgeber als auch die Verwaltung bei der Sammlung von Daten von vornherein prüfen, ob auf Identifizierungsmerkmale, Name, Geburtsdatum, Wohnort u. a., verzichtet werden kann oder, wenn dies nicht möglich ist, ob die Identifizierung des einzelnen durch eine Verschlüsselung oder Anonymisierung der über ihn gesammelten Daten erschwert werden kann (vgl. unter 4.1.1).

5.2 Getrennte Aufbewahrung

Bei besonders empfindlichen Informationen sollten die Identifizierungsmerkmale schon bei der Erfassung von den übrigen Daten getrennt gespeichert und unter besonderem Verschluß aufbewahrt werden. An andere Behörden oder Stellen sollten sie nur weitergegeben werden, wenn dies aus sachlichen Gründen zwingend geboten ist. Im Interesse des Persönlichkeitsschutzes muß in Kauf genommen werden, daß durch dieses Verfahren bestimmte Rationalisierungseffekte wegfallen.

5.3 Statistik ohne Individualdaten

Für statistische Zwecke sollten grundsätzlich keine Individualdaten gespeichert werden, sondern nur statistische Ergebnisse (vgl. unter 4.1.1).

5.4 Regelung des Zugriffs

Wie die Erfahrungen zeigen (vgl. unter 4.1.2), ist die Frage, wer Zugriff auf Daten hat, weder im Datenschutzgesetz noch im Datenverarbeitungsgesetz befriedigend geregelt. Die Frage gewinnt, wenn es sich um Daten aus dem Intimbereich handelt, besondere Bedeutung. Die Schwierigkeit, den Kreis der Befugten im Sinne des § 2 DSG zu bestimmen, wird nicht verkannt. Eine gesetzliche Regelung oder eine Regelung durch Rechtsverordnung kann auf Grund der bisher vorliegenden Erfahrungen nicht empfohlen werden. Dagegen könnte durch Verwaltungsanordnungen sichergestellt werden, daß über die Weitergabe von Daten, die zum Intimbereich eines Bürgers gehören, der Leiter der abgebenden Behörde oder ein anderer besonders verpflichteter Bediensteter entscheidet.

5.5 Zusammenarbeit mit privaten Stellen

Soweit Unterlagen, auf die das Datenschutzgesetz Anwendung findet, im Rahmen einer Zusammenarbeit zwischen Verwaltungen oder Rechenzentren und privaten Stellen — im Rahmen des rechtlich Zulässigen — weitergegeben oder doch dem Zugriff Außenstehender ausgesetzt werden, sind besondere Sicherungsmaßnahmen notwendig. Durch entsprechende Auflagen muß ein gleichwertiger Schutz gewährleistet werden. Ihre Einhaltung ist zu kontrollieren.

5.6 Verantwortlichkeit der Verwaltungen

Entgegen manchen Äußerungen und Erwartungen ist daran zu erinnern, daß die volle Verantwortung für die Durchführung des Datenschutzes den Behörden und Stellen obliegt, die mit der maschinellen Datenverarbeitung befaßt sind. Die besondere Überwachungsfunktion des Datenschutzbeauftragten soll diese Verantwortung nicht schmälern, sondern stärken.

5.7 Aus- und Fortbildung

Die Verwirklichung des Datenschutzes ist nicht nur eine Frage entsprechender Gesetze und technischer Vorkehrungen, sondern hängt stark von den Einstellungen der Menschen ab, denen der Datenschutz in der Praxis anvertraut ist. Deshalb sollte der Datenschutz einen festen Standort in der Aus- und Fortbildung der Bediensteten der öffentlichen Hand erhalten.

Auch außerhalb des öffentlichen Dienstes läßt sich im Rahmen der politischen Bildungsarbeit am Beispiel des Datenschutzes gut exemplifizieren, welche Chancen und Gefahren die moderne Technologie für Individuum und Demokratie mit sich bringt und wie die Gesellschaft diese Probleme angeht.

5.8 Datensicherung

Wie unter 4.3.1 dargestellt, weist bei vielen mit der Datenverarbeitung befaßten Stellen das Sicherheitssystem noch Lücken auf; zum Teil ist es erst in Ansätzen vorhanden. Ein Nachholbedarf besteht insbesondere in folgenden Punkten:

— Aufbewahrung und Transport von Datenträgern,

— planmäßige Vernichtung obsoleter Datenbestände,

— Organisation in den Maschinensälen.

In der näheren Zukunft wirft die Datenfernverarbeitung, die z. B. im Einwohnerwesen und von der Polizei eingesetzt werden soll, zusätzliche Datensicherungsprobleme auf. Ihnen muß schon in der laufenden Planung besondere Beachtung geschenkt werden.

5.9 Parlamente und Informationssysteme

Wie unter 4.2.1 im einzelnen erörtert, stellt die künftig zu erwartende Verwendung EDV-gestützter Entscheidungshilfen durch Regierung und Verwaltung für das Parlament eine zweifache Herausforderung dar. Zum einen erfordert seine Kontrollfunktion, daß es die von der Exekutive benutzten Instrumente kennt. Zum anderen geht es darum, die Datenverarbeitung auch zur Verbesserung der parlamentarischen Information heranzuziehen. Die tatsächlichen Voraussetzungen für die Wahrnehmung der Informationsrechte des § 6 DSG müssen geschaffen werden (vgl. 4.2.3). Darüber hinaus stellt sich für den Landtag die Frage, ob und in welcher Weise er seine speziellen Informationsbedürfnisse schon bei der Entwicklung von Informationssystemen zur Geltung bringen sollte. Besonders aktuell ist dieser Punkt bei dem von der HZD geplanten „Hessischen Planungsinformations- und Analyse-System" (HEPAS, vgl. 4.2.4).

5.10 Auskunftsverlangen des Bürgers

Zwar besteht nach dem Datenschutzgesetz keine Auskunftspflicht der Verwaltung gegenüber dem Bürger. Da die Verwaltung aber nur an der Speicherung richtiger Daten interessiert sein kann, sollte die Landesregierung die Verwaltung anweisen, dem Auskunftsverlangen des Bürgers über die ihn betreffenden Daten nach Möglichkeit zu entsprechen (vgl. unter 4.1.4).

5.11 Gesetzgebung des Bundes und Bundesdatenschutzgesetz

Die Analyse neuerer Gesetze des Bundes hat ergeben, daß den Belangen des Datenschutzes nicht immer ausreichend Rechnung getragen wird (vgl. unter 4.1.1). Um hier eine bessere Koordination zu ermöglichen, sollten die Grundsätze des geplanten Bundesdatenschutzgesetzes bald veröffentlicht werden, damit sie für andere Gesetzesvorhaben als Maßstab dienen können.

5.12 Forschungsaufträge

Die Verzögerung in der Datenschutzgesetzgebung beruht zum Teil darauf, daß die wirtschaftlichen Konsequenzen bestimmter vorgeschlagener Regelungen nicht abschätzbar sind. So weiß man nicht, mit welcher Häufigkeit die Bürger von Auskunfts- und Berichtigungsrechten Gebrauch machen werden (vgl. 2.4.5 und 5.10). Ebenso fehlt es an Berechnungen des Kosten- und Arbeitsaufwands für die automatische Protokollierung (vgl. 2.4.4). Um die Entscheidung der Gesetzgeber auf eine sichere Grundlage zu stellen, sollten bald entsprechende Forschungsaufträge an demoskopische Institute vergeben und Kosten-Nutzen-Studien bezüglich verschiedener Modelle veranlaßt werden. Für die Durchführung der Untersuchungen könnte der Datenschutzbeauftragte die Verantwortung übernehmen, um möglichst objektive Ergebnisse zu erreichen.

5.13 Wissenschaftsförderung

Das Verhältnis von Informationstechnologie und Demokratie wird in den industriell fortgeschrittenen Ländern rasch zu einer der Kernfragen der politisch-gesellschaftlichen Fortentwicklung werden. Wenn zukunftsweisende Antworten gefunden werden sollen, ist zunächst eine umfassende wissenschaftliche Aufhellung des Problemkreises erforderlich. Die staatliche Förderung der Informationstechnologie darf deshalb nicht bei EDV-Technik und -Anwendung stehenbleiben (EDV-Förderungsprogramme des Bundes), sondern sollte möglichst bald auch die sozialwissenschaftliche Seite mit einbeziehen. Dabei könnte auf die Erfahrungen amerikanischer Forschungsprojekte zurückgegriffen werden.

6. SCHLUSSBEMERKUNGEN

Der vorliegende Erste Tätigkeitsbericht des Hessischen Datenschutzbeauftragten versucht, auf dem Hintergrund des gegenwärtigen Entwicklungsstandes von Automation und Datenverarbeitung in der hessischen öffentlichen Verwaltung die Probleme des Datenschutzes und der Datensicherung darzustellen. Er untersucht die Rückwirkungen auf den Schutz der Privatsphäre und auf die verfassungsmäßige Gewaltenteilung und gibt Anregungen, wie man diesen Gefahren begegnen könnte.

*

In vielen Fällen konnten nur Probleme und Tendenzen aufgezeigt, aber keine Lösungen angeboten werden. Die von der maschinellen Datenverarbeitung initiierten Wandlungen in den Verfahrensweisen der öffentlichen Verwaltung und im Verhältnis der Staatsorgane zueinander sind äußerst komplex. Viele Probleme wurden aufgeworfen. Ihre Lösung sollte von Wissenschaft, Legislative, Exekutive und Judikative gemeinsam angestrebt werden.

*

Zu diesem Problemkreis gehört auch die Frage, wie die für die Überwachung des Datenschutzes verantwortliche Institution organisiert und wie sie in das staatliche Gefüge eingegliedert werden soll (vgl. unter 2.4.7). Nach den vorliegenden Erfahrungen kann gesagt werden, daß sich die hessische Lösung bewährt.

Damit dieses System funktioniert, müssen dem Datenschutzbeauftragten die notwendigen Hilfskräfte nach § 15 DSG zur Verfügung stehen.

Es war richtig, daß die Dienststelle anfangs sehr klein gehalten wurde. Zunächst mußten Erfahrungen darüber gesammelt werden, in welcher Form und mit welchen Mitteln — aber ohne jeden unnötigen Aufwand — die Aufgabe des Datenschutzes wirksam wahrgenommen werden konnte.

In § 15 Abs. 1 des Datenschutzgesetzes ist bestimmt, daß dem Datenschutzbeauftragten bei Bedarf zur Erfüllung seiner Aufgaben Hilfskräfte von der Staatskanzlei zur Verfügung gestellt werden können. Dementsprechend waren für die Haushaltsjahre 1971 und 1972 im Einzelplan der Staatskanzlei eine Amtmannstelle und eine Stelle für eine Schreibkraft vorgesehen. Außerdem bietet der § 15 Abs. 2 DSG die Möglichkeit, für bestimmte Einzelfragen Dritte zur Mitarbeit heranzuziehen.

Im Verhältnis zur Aufgabenstellung erwies sich diese Ausstattung der Dienststelle als unzureichend. Die Anfangsschwierigkeiten konnten gemeistert werden, da es gelang, einen erfahrenen Juristen und einen mit Fragen der elektronischen Datenverarbeitung vertrauten jüngeren Wissenschaftler für eine beratende Mitarbeit zu gewinnen. Außerdem wurden von zwei verschiedenen Ressorts ein technischer Amtsrat und ein Beamter des höheren Dienstes ab 15. Oktober 1971 bzw. 1. Januar 1972 zur Staatskanzlei abgeordnet und dem Datenschutzbeauftragten zur Verfügung gestellt. Die Amtmannstelle wurde nicht in Anspruch genommen.

Es erscheint unumgänglich notwendig, die haushaltsmäßigen Voraussetzungen für eine bessere Ausstattung zu schaffen. Sie sollte, soweit es um die Personalstellen geht, mindestens vier Stellen des höheren bzw. des gehobenen Dienstes umfassen, und zwar eine Stelle für einen Mitarbeiter mit Erfahrung in Parlaments- und Regierungsarbeit, eine Stelle für einen qualifizierten Juristen, eine Stelle für einen Mitarbeiter mit rechts- bzw. sozialwissenschaftlichen Kenntnissen und eine Stelle für einen erfahrenen EDV-Fachmann sowie zwei Stellen für Schreibkräfte. Außerdem wären ausreichende Sachmittel bereitzustellen, die es gestatten würden, die wissenschaftliche Literatur zu verfolgen und eine zusätzliche Beratung durch die Vergabe von Gutachten usw. sicherzustellen.

Die voraussichtlichen Ansätze im Landeshaushalt für die integrierte Datenverarbeitung (Landes- und Kommunalverwaltung) werden in den kommenden Jahren in einer Größenordnung von 80 Millionen DM jährlich liegen. Die hier vorgeschlagenen Aufwendungen für die Dienststelle des Datenschutzbeauftragten machen nur einen Bruchteil von einem Prozent dieses Betrages aus. Berücksichtigt man, daß man im privaten Anwendungsbereich von EDV-Anlagen damit rechnet, daß die Datenschutzmaßnahmen heute etwa 5% der Investitionen ausmachen und sich dieser Prozentsatz in naher Zukunft noch wesentlich erhöhen wird, so erscheinen die mit der vorgeschlagenen Ausstattung der Dienststelle des Datenschutzbeauftragten verbundenen Kosten durchaus vertretbar.

*

Zahlreiche Gespräche haben gezeigt, daß beim Bürger und selbst bei den Repräsentanten größerer Institutionen und Verbände Mißverständnisse über die Stellung und die Aufgaben des Datenschutzbeauftragten bestehen. Oft wird er mit der Hessischen Zentrale für Datenverarbeitung verwechselt oder als Teil von ihr angesehen.

Andererseits haben andere Verbände und Institutionen, selbst wenn sie nicht in den Bereich des Datenschutzgesetzes fallen, Kontakt mit dem Datenschutzbeauftragten aufgenommen.

Nachdem sie festgestellt hatten, daß mit dem Vordringen der EDV ein verstärkter Datenschutz immer notwendiger wird, suchten sie den Erfahrungsaustausch mit dem Datenschutzbeauftragten, um dabei die Erkenntnisse zu vertiefen und für gemeinsame Probleme auch gemeinsame Lösungen anzustreben.

*

Diese Informationsgespräche waren auch für den Datenschutzbeauftragten wertvoll. Sie bestätigen ihm, daß im Kreis der Verarbeiter und Benutzer der maschinellen Datenverarbeitung zwei Richtungen miteinander konkurrieren: Die einen neigen dazu, dem Rausch der nahezu unbegrenzten Möglichkeiten des Computers zu erliegen und wollen sie auch voll ausschöpfen, ohne die damit zusammenhängende Problematik zu erkennen. Die anderen sehen zwar ebenfalls die Chance, die der Computer bei der Rationalisierung der Verwaltung und der Steigerung ihrer Effektivität bietet, sie erkennen aber klar, welche Gefahren diese neue Informationstechnik für die Individualsphäre und die demokratische Staatsstruktur in sich birgt.

Beide Problemkreise, der Schutz der Würde des Bürgers und die Erhaltung der verfassungsmäßigen Machtbalance, sind in dem Bericht getrennt behandelt. Zweifellos sind sie aber eng miteinander verbunden, weil das Eindringen in die Individualsphäre des einzelnen nicht nur die menschliche Würde verletzt, sondern auch der Verwaltung eine Art von Allwissenheit vermittelt, was ihre Macht verstärkt und die demokratische Struktur erschüttert. Ebenso gefährdet auch ein Informationsvorsprung von Regierung und Verwaltung gegenüber dem Parlament das Gleichgewicht zwischen den Verfassungsorganen und damit letztlich auch die Freiheit des Bürgers.

*

In der wissenschaftlichen Diskussion werden diese Probleme lebhaft diskutiert. Eine Reihe von Gesetzesentwürfen liegen, wie berichtet, auf der Ebene des Bundes und der Länder sowie im Ausland vor. Diese intensiven Versuche der Parlamente, die EDV-Entwicklung unter Kontrolle zu bringen und an demokratische und freiheitliche Mindestnormen zu binden, sind zu begrüßen. Aber nach wie vor ist Hessen das einzige Land, wo es gelungen ist, durch Gesetz ein handlungsfähiges, unabhängiges und weisungsfreies Überwachungsorgan zu schaffen. Erst die gesetzliche Verpflichtung, die Einhaltung der Datenschutz-Vorschriften zu überwachen, erzwingt aber die Herausarbeitung klarer Richtlinien und Abgrenzungen für die Arbeit der EDV.

So wertvoll ohne Zweifel der hessische Vorstoß auf dem Gebiet des Datenschutzes ist, so sind doch die Wirkungsmöglichkeiten eines auf ein Land beschränkten Modells notwendigerweise begrenzt. Die Gesetzgebungskompetenz des Landes erlaubte nicht, die Datenverarbeitung im privaten Bereich dem Datenschutzgesetz zu unterstellen. Die Abhängigkeit des Landes Hessen von der Bundesgesetzgebung und die enge Kooperation der Länder begrenzen die Wirkungsmöglichkeiten des Datenschutzbeauftragten im eigenen Lande. Dieser Zustand wird sich erst ändern, wenn auch anderwärts Überwachungsorgane ins Leben gerufen worden sind. Die Zusammenarbeit mit solchen Partnern, die vor den gleichen Problemen stehen wie der Datenschutzbeauftragte in Hessen, ist für die Weiterentwicklung des Datenschutzes notwendig. Denn die Probleme erhalten in der Praxis doch oft ein anderes Gesicht als in der wissenschaftlichen Diskussion, so wichtig und unersetzlich diese auch für die Analyse und Entwicklung von Modellvorstellungen ist.

Die Zeit drängt. Die weitverbreitete Ansicht, man solle die Weiterentwicklung der EDV-Systeme abwarten, bevor man Gesetze erläßt, ist bedenklich. Jeder weitere Aufschub verstärkt die Gefahr, daß nicht mehr die Gesetze die Entwicklung der Datenverarbeitung bestimmen, sondern daß sie dem Stand der Datenverarbeitung angepaßt werden. Denn wenn man die EDV-Anlagen erst einmal mit hohem finanziellem Aufwand installiert und die Arbeitsstruktur entsprechend umgestellt hat, dann sind Sachzwänge entstanden, die den Entscheidungsspielraum der Legislative einengen. Die nachträgliche Berücksichtigung der für den Datenschutz notwendigen Maßnahmen wäre mit hohem Aufwand verbunden oder gar nicht mehr durchführbar.

*

Es gibt keine — oder bestenfalls nur eine für jeweils kurze Zeit geltende — perfekte Lösung für den Datenschutz. Denn die Entwicklung steht nicht still. Neue Techniken werden vielleicht schon morgen neue Wege zum Fortschritt und zum Wohl des Menschen erschließen; aber sie werden auch neue, unbekannte Gefahren für den einzelnen und für die freiheitliche Struktur von Staat und Gesellschaft in sich bergen. Diesen Gefahren muß rechtzeitig und wirksam entgegengetreten werden. Stete Wachsamkeit ist notwendig. Auch die Gesellschaft wird ihre Strukturen wandeln. Neue Bedürfnisse und Auffassungen werden auch Fragen des Datenschutzes berühren. Datenschutz ist deshalb keine einmalige, sondern eine permanente Aufgabe, die jeden Tag aufs neue gestellt wird und die es gilt, jeden Tag neu zu überdenken.

Anlage

Datenschutzgesetz
Vom 7. Oktober 1970

ERSTER ABSCHNITT
Datenschutz

§ 1
Bereich des Datenschutzes

Der Datenschutz erfaßt alle für Zwecke der maschinellen Datenverarbeitung erstellten Unterlagen sowie alle gespeicherten Daten und die Ergebnisse ihrer Verarbeitung im Bereich der Behörden des Landes und der der Aufsicht des Landes unterstehenden Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts.

§ 2
Inhalt des Datenschutzes

Die vom Datenschutz erfaßten Unterlagen, Daten und Ergebnisse sind so zu ermitteln, weiterzuleiten und aufzubewahren, daß sie nicht durch Unbefugte eingesehen, verändert, abgerufen oder vernichtet werden können. Dies ist durch geeignete personelle und technische Vorkehrungen sicherzustellen.

§ 3
Datengeheimnis

(1) Den mit der Datenerfassung, dem Datentransport, der Datenspeicherung oder der maschinellen Datenverarbeitung betrauten Personen ist untersagt,

> die dabei erlangten Kenntnisse über Unterlagen, Daten und Ergebnisse anderen mitzuteilen oder anderen zu gestatten oder andere dabei zu fördern, derartige Kenntnisse zu erlangen,

soweit sich nicht eine Befugnis aus Rechtsvorschriften oder aus der Zustimmung derjenigen ergibt, die über die Unterlagen, Daten und Ergebnisse verfügungsberechtigt sind.

(2) Das Verbot des Abs. 1 gilt nicht, wenn die dort bezeichneten Handlungen zur verwaltungsmäßigen oder technischen Durchführung der Datenverarbeitung erforderlich sind.

(3) Die Pflicht zur Geheimhaltung besteht auch nach der Beendigung der in Abs. 1 bezeichneten Tätigkeiten.

(4) Gesetzliche Auskunftspflichten bleiben unberührt.

§ 4
Anspruch auf Datenschutz

(1) Sind gespeicherte Daten unrichtig, so kann der Betroffene Berichtigung verlangen.

(2) Wer durch eine widerrechtliche Einsicht, Änderung oder Vernichtung oder durch einen widerrechtlichen Abruf (§ 2 Satz 1) in seinen Rechten verletzt wird, kann Wiederherstellung des früheren Zustandes und bei Gefahr weiterer Verletzungen Unterlassung verlangen.

(3) Der Anspruch jeder natürlichen oder juristischen Person auf Auskunft nach den bestehenden Gesetzen wird durch dieses Gesetz nicht berührt.

§ 5

Datenbanken und Informationssysteme

(1) Für den Aufbau von Datenbanken und Informationssystemen sowie für statistische Zwecke der in § 1 genannten Stellen können Unterlagen, Daten und Ergebnisse weitergegeben werden.

(2) Bei Datenbanken und Informationssystemen ist zu gewährleisten, daß keine Stellen Unterlagen, Daten und Ergebnisse einsehen oder abrufen können, die nicht auf Grund ihrer Zuständigkeiten hierzu befugt sind.

(3) Daten und Datenbestände, die keine Einzelangaben über natürliche oder juristische Personen enthalten und keine Rückschlüsse auf solche Einzelangaben zulassen, können weitergegeben und veröffentlicht werden, wenn nicht ein gesetzliches Verbot oder ein wichtiges öffentliches Interesse entgegensteht. Dem Auskunftsrecht des Landtags (§ 6 Abs. 1) steht ein öffentliches Interesse in der Regel nicht entgegen.

§ 6

Informationsrecht des Landtags und der kommunalen Vertretungsorgane

(1) Die Hessische Zentrale für Datenverarbeitung, die Kommunalen Gebietsrechenzentren und die Landesbehörden, die Datenverarbeitungsanlagen betreiben, sind verpflichtet, dem Landtag, dem Präsidenten des Landtags und den Fraktionen des Landtags die von diesen im Rahmen ihrer Zuständigkeiten verlangten Auskünfte auf Grund der gespeicherten Daten zu geben, soweit die Voraussetzungen des § 5 Abs. 3 vorliegen und Programme zur Auswertung vorhanden sind.

(2) Das Auskunftsrecht des Abs. 1 steht im Rahmen ihrer Zuständigkeiten den Gemeindevertretungen und den Kreistagen sowie deren Fraktionen und den entsprechenden Organen anderer in § 1 genannten Körperschaften und Anstalten gegenüber der Hessischen Zentrale für Datenverarbeitung, dem zuständigen Kommunalen Gebietsrechenzentrum sowie den sonstigen von Gemeinden und Landkreisen betriebenen Datenverarbeitungsanlagen zu. Der Antrag der Fraktionen ist über den Gemeindevorstand bzw. den Kreisausschuß zu leiten.

(3) Im Zweifelsfalle entscheidet die Aufsichtsbehörde.

ZWEITER ABSCHNITT

Datenschutzbeauftragter

§ 7

Rechtsstellung

(1) Der Landtag wählt auf Vorschlag der Landesregierung einen Datenschutzbeauftragten.

(2) Der Datenschutzbeauftragte steht nach Maßgabe dieses Gesetzes in einem öffentlich-rechtlichen Amtsverhältnis. Das Amt kann auch einem Beamten im Nebenamt, einem beurlaubten Beamten oder einem Ruhestandsbeamten übertragen werden.

(3) Der Datenschutzbeauftragte wird für die Dauer der jeweiligen Wahlperiode des Landtags gewählt; nach dem Ende der Wahlperiode bleibt er bis zur Neuwahl im Amt. Die Wiederwahl ist zulässig. Vor Ablauf der Amtszeit kann er nur abberufen werden, wenn Tatsachen vorliegen, die bei einem Beamten die Entlassung aus dem Dienst rechtfertigen. Er kann jederzeit von seinem Amt zurücktreten.

(4) Die Vergütung des Datenschutzbeauftragten ist durch Vertrag zu regeln.

§ 8

Weisungsfreiheit

Der Datenschutzbeauftragte ist unbeschadet seiner Verpflichtungen aus den §§ 10 und 12 frei von Weisungen.

§ 9

Verschwiegenheitspflicht

Der Datenschutzbeauftragte ist auch nach Beendigung seines Amtsverhältnisses verpflichtet, über die ihm bei seiner amtlichen Tätigkeit bekannt gewordenen Angelegenheiten Verschwiegenheit zu bewahren. Dies gilt nicht für Mitteilungen im dienstlichen Verkehr oder über Tatsachen, die offenkundig sind oder ihrer Bedeutung nach keiner Geheimhaltung bedürfen. Er darf über die der Verschwiegenheitspflicht unterliegenden Angelegenheiten ohne Genehmigung weder vor Gericht noch außergerichtlich aussagen. Die Genehmigung erteilt der Ministerpräsident.

§ 10

Aufgaben

(1) Der Datenschutzbeauftragte überwacht die Einhaltung der Vorschriften dieses Gesetzes und der übrigen Vorschriften über die vertrauliche Behandlung der Angaben der Bürger und der über die einzelnen Bürger vorhandenen Unterlagen bei der maschinellen Datenverarbeitung durch die in § 1 genannten Stellen. Er unterrichtet die zuständige Aufsichtsbehörde über festgestellte Verstöße und regt Vorkehrungen zu Verbesserungen des Datenschutzes an.

(2) Der Datenschutzbeauftragte beobachtet die Auswirkungen der maschinellen Datenverarbeitung auf die Arbeitsweise und die Entscheidungsbefugnisse der in § 1 genannten Stellen dahingehend, ob sie zu einer Verschiebung in der Gewaltenteilung zwischen den Verfassungsorganen des Landes, zwischen den Organen der kommunalen Selbstverwaltung und zwischen der staatlichen und der kommunalen Selbstverwaltung führen. Er kann Maßnahmen anregen, die ihm geeignet erscheinen, derartige Auswirkungen zu verhindern.

§ 11

Anrufungsrecht

Jedermann hat das Recht, sich an den Datenschutzbeauftragten zu wenden, wenn er annimmt, durch die maschinelle Datenverarbeitung der in § 1 genannten Stellen in seinen Rechten verletzt zu werden.

§ 12

Untersuchungen für den Landtag und die kommunalen Vertretungsorgane

Der Landtag, der Präsident des Landtags, die Fraktionen des Landtags und die in § 6 Abs. 2 genannten Vertretungsorgane können verlangen, daß der Datenschutzbeauftragte untersucht, aus welchen Gründen Auskunftsersuchen nicht oder nicht ausreichend beantwortet wurden.

§ 13

Auskunftsrecht

Alle in § 1 genannten Stellen haben dem Datenschutzbeauftragten die ihm für die Erfüllung seiner Aufgaben notwendigen Auskünfte zu erteilen.

§ 14

Jahresbericht

(1) Bis zum 31. März jeden Jahres, erstmalig zum 31. März 1972, hat der Datenschutzbeauftragte dem Landtag und dem Ministerpräsidenten einen Bericht über das Ergebnis seiner Tätigkeit vorzulegen.

(2) Der Ministerpräsident führt eine Stellungnahme der Landesregierung zu dem Bericht herbei und legt diese dem Landtag vor.

(3) Zwischenberichte sind zulässig. Sie sind nach Abs. 2 zu behandeln.

§ 15

Hilfskräfte

(1) Dem Datenschutzbeauftragten können bei Bedarf zur Erfüllung seiner Aufgaben Hilfskräfte von der Staatskanzlei zur Verfügung gestellt werden. Sie unterstehen insoweit seinen Weisungen.

(2) Für bestimmte Einzelfragen kann der Datenschutzbeauftragte auch Dritte zur Mitarbeit heranziehen.

DRITTER ABSCHNITT

Schlußvorschriften

§ 16

Ordnungswidrigkeit

Ordnungswidrig handelt, wer entgegen § 3 vorsätzlich oder fahrlässig daran mitwirkt, Unbefugten dem Datenschutz unterliegende Kenntnisse zu verschaffen.

§ 17

Inkrafttreten

Dieses Gesetz tritt am Tage nach seiner Verkündung in Kraft.

Die verfassungsmäßigen Rechte der Landesregierung sind gewahrt.

Das vorstehende Gesetz wird hiermit verkündet.

Wiesbaden, den 7. Oktober 1970

Der Hessische Ministerpräsident
Osswald