



HESSISCHER LANDTAG

18. 12. 78

Siebenter Tätigkeitsbericht des Hessischen Datenschutzbeauftragten

Mit Schreiben vom 18. Dezember 1978 legt der Datenschutzbeauftragte gemäß § 29 des Hessischen Datenschutzgesetzes vom 31. Januar 1978 dem Landtag den folgenden Tätigkeitsbericht vor:

Eingegangen am 18. Dezember 1978 · Ausgegeben am 9. Februar 1979

Druck: Carl Ritter & Co., Wiesbaden · Auslieferung: Kanzlei des Hessischen Landtags · Postfach 3240 · 6200 Wiesbaden 1

INHALTSVERZEICHNIS

	Seite
1. Einleitung	5
1.1 Zur Situation	5
1.2 Zusammenarbeit der Kontrollorgane	9
1.3 Datenschutz und Bürger	10
2. Stand der Datenschutzgesetzgebung in den Ländern	12
3. Gesetzgebung im Ausland	16
3.1 Frankreich	16
3.2 Großbritannien	17
3.3 Österreich	18
3.4 Schweden	23
3.5 Europarat	25
4. Einwohnerwesen	26
4.1 Novellierung des Hessischen Meldegesetzes	26
4.2 Auskunft aus dem Melderegister	27
4.3 Einsicht der Polizei in das Melderegister	27
4.4 Überwachung des Datenschutzes im Meldewesen	28
4.5 Übermittlung von Daten durch das Kraftfahrt-Bundesamt	29
4.6 Verkauf von Adrema-Platteien	29
5. Datenschutz im Sicherheitsbereich	31
5.1 HEPOLIS und Kriminalakten	31
5.2 Verfassungsschutz und Bibliotheksdaten	34
6. Bildungswesen	35
6.1 Datenschutz bei Schülerbefragungen	35
6.2 Wissenschaftliche Untersuchungen im Schulbereich	36
6.3 Angaben über Schüler gegenüber Außenstehenden	37
6.4 Hochschulstatistik	37
6.5 Datenschutz im Bereich der Volkshochschulen	38
7. Personalwesen	40
7.1 Unbefugte Übermittlung der Adressen von Lehramtskandidaten und Referendaren	40
7.2 Datenschutz bei Eignungsprüfungen	40
7.3 Speicherung und Abrechnung von Telefongesprächen	40
8. Gesundheitswesen	42
8.1 Schulsportärztlicher Untersuchungsbogen	42
8.2 Vorsorgeuntersuchung bei der Einschulung	42
8.3 Auskunftsrecht des Patienten	43
8.4 Krebsregister	43
9. Sozialwesen	44
9.1 Projekt einer „Heimkinderdatei“	44
9.2 Zuschußgewährung an Behinderten-Clubs	44
10. Kommunen	46
10.1 Probleme bei der Anwendung des neuen HDSG	46
10.2 Öffentlich-rechtliche Wettbewerbsunternehmungen	46

	Seite
11. Datenübermittlung an öffentlich-rechtliche Religionsgesellschaften	48
12. Datensicherung	51
12.1 Realisierungsmöglichkeiten	51
12.2 Auswirkungen des HDSG auf den DV-Verbund	52
12.3 Datensicherungsmaßnahmen im DV-Verbund	52
Anlage zu Abschnitt 1 (Stellungnahme zum Entwurf eines Bundesmeldegesetzes im Rahmen der Anhörung am 20./21. November 1978)	54

Bei den Hinweisen (Fußnoten) bezeichnen I, II, III, IV, V und VI den Ersten (LT-Drucks. 7/1495), Zweiten (LT-Drucks. 7/3137), Dritten (LT-Drucks. 7/5146), Vierten (LT-Drucks. 8/438), Fünften (LT-Drucks. 8/2475 bzw. Sechsten (LT-Drucks. 8/3962) Tätigkeitsbericht, die arabischen Ziffern die angesprochenen Abschnitte in dem Bericht; Z 1 und Z 2 bezeichnen den Ersten Zwischenbericht vom 9. 2. 1976 (LT-Drucks. 8/2239) und den Zweiten Zwischenbericht vom 7. 6. 1978 (LT-Drucks. 8/6189).

1. EINLEITUNG

1. Einleitung

1.1 Zur Situation

Anfang 1978 hat der Hessische Landtag das zweite Hessische Datenschutzgesetz (HDSG) verabschiedet. Der Gesetzgeber leitete damit einen neuen, wichtigen Abschnitt in der Geschichte des Datenschutzes ein. Nicht nur, weil sich Inhalt und Anwendungsbereich der Datenschutzregeln an entscheidenden Punkten verändert haben: Man braucht nur an die Einbeziehung der manuellen Verarbeitung personenbezogener Daten zu denken; mindestens ebenso schwer wiegt vielmehr, daß Grundsätze, die lange Zeit mehr oder weniger als hessische Spezialregelung galten, mittlerweile für die Datenverarbeitung im gesamten Bundesgebiet maßgeblich geworden sind. Was der Bundesgesetzgeber 1976 mit dem Bundesdatenschutzgesetz bekräftigte, haben in der Zwischenzeit nahezu sämtliche Länder nicht minder nachdrücklich bestätigt: Wer personenbezogene Daten verarbeiten will, darf es nur tun, wenn er sich auf eine Rechtsnorm oder auf das Einverständnis des Betroffenen berufen kann. Mit anderen Worten: Die öffentliche Verwaltung handelt — nicht anders als private Unternehmen — nur solange rechtmäßig, wie sie sich strikt an diese vom Gesetzgeber ausdrücklich und unmißverständlich formulierte Bedingung (§ 7 HDSG) hält.

Trotzdem: Der Datenschutz ist nicht deshalb garantiert, weil Bund und Länder nunmehr über Datenschutzgesetze verfügen. Jedes dieser Gesetze formuliert in Wirklichkeit nicht mehr als die allgemeinen Voraussetzungen, unter denen personenbezogene Daten verarbeitet werden dürfen. Daraus folgt die vor allem in der Diskussion über das Bundesdatenschutzgesetz immer wieder hervorgehobene und auch nicht bestrittene Notwendigkeit einer konsequenten Weiterentwicklung des Datenschutzes. Sicher haben die Landesgesetze bereits manche wichtige Verbesserung mit sich gebracht. Dennoch sind sie letztlich ebenfalls nur ein erster Schritt in Richtung auf eine gesetzliche Regelung, die mehr und mehr an konkrete Problembereiche knüpft und deshalb präzise Regelungen zu genau eingegrenzten — für den Bürger wichtigen — Aspekten der Verarbeitung personenbezogener Daten bringt. Anders ausgedrückt: Ein aus der Perspektive des Bürgers zufriedenstellender Schutz ist erst dann erreicht, wenn exakt formulierte bereichsspezifische Regelungen den allgemeinen Datenschutzgrundsätzen das im Inter-

esse des Bürgers unerläßliche Maß an Konkretheit verleihen. Drei Beispiele aus der gegenwärtigen Diskussion über die Weiterentwicklung des Datenschutzes mögen dies verdeutlichen:

- 1.1 a) Hinzuweisen ist zunächst auf die verschiedenen Versuche, den Datenschutz im Rahmen des Melderechts zu verbessern. Der neue § 16 a des Hessischen Meldegesetzes (HMG) ist bezeichnend dafür. Zum einen, weil er versucht, berechtigten Informationswünschen Rechnung zu tragen, den Datenschutz also nicht zu einer unverständlichen und im Interesse des Bürgers auch nicht mehr erforderlichen Informationssperre werden zu lassen; zum anderen, weil er zum ersten Mal das Recht des Bürgers anerkennt, die Übermittlung seiner der öffentlichen Verwaltung überlassenen Daten an Außenstehende zu sperren. Der hessische Gesetzgeber hat insoweit für das Melderecht einen Grundsatz bestätigt, der — genaugenommen — im Interesse eines wirksamen Datenschutzes weit über diesen einen Bereich hinaus gelten müßte. Die Diskussion über das Hessische Datenschutzgesetz¹⁾ ist dafür ebenso bezeichnend wie die Tatsache, daß sich ein halbes Jahr später der Berliner Gesetzgeber für eine allgemeine Auskunftssperre entschieden (§ 7 Nr. 5 BlnDSG) hat.

So wenig sich die Bedeutung der vom Hessischen Gesetzgeber in § 16 a HMG getroffenen Entscheidung bestreiten läßt, so sehr gilt es, nicht zu übersehen, daß die Erwartungen an eine bereichsspezifische, den Datenschutz überzeugend konkretisierende Regelung des Melderechts damit keineswegs erfüllt sind. Nicht von ungefähr haben die verschiedenen Entwürfe für ein Bundesmeldegesetz (BMG) zu einer langen und intensiven Auseinandersetzung geführt. Sicher ist sie nicht zuletzt durch die zunächst beabsichtigte Einführung eines Personenkennzeichens und den gleichzeitig mit dem jüngsten Entwurf publizierten Datenkatalog besonders angereizt worden. In Wirklichkeit geht es freilich um viel mehr: Ein Meldegesetz-Entwurf ist unter Datenschutzgesichtspunkten erst annehmbar, wenn der Gesetzgeber die mit der Verarbeitung personenbezogener Daten verfolgten Ziele klar und verbindlich formuliert. Nur dann kann es gelingen, überzeugend festzustellen, welche Angaben zu welchen Zwecken effektiv gebraucht werden. Nur dann ist es aber auch möglich, die Speicherung und die Übermittlung an

¹⁾ Vgl. VI, 2.7, § 9 des Modellentwurfs.

Bedingungen zu binden, die sich an diesen Zielen orientieren, und jeden aus der Perspektive des Bürgers bedenklichen, wenn nicht sogar gefährlichen Spielraum von vornherein ausschließen.

Es genügt, an das Beispiel der Wahlausschlußgründe zu erinnern: Ohne jeden Zweifel muß der für die Führung des Wahlregisters Verantwortliche wissen, ob jemand nicht wählen darf. Keineswegs ist es aber in diesem Zusammenhang erforderlich, auch darüber informiert zu sein, warum der betreffende Bürger von der Wahl ausgeschlossen ist. Die Kenntnis so sensibler Daten wie etwa einer Geisteskrankheit muß von Anfang an auf wenige gesetzlich dazu berechnete Stellen beschränkt bleiben. Das Melderecht bedarf also einer Regelung, die sorgfältig zwischen der allein erforderlichen Information über den Wahlausschluß und die Kenntnis des Wahlausschlußgrundes unterscheidet. Noch einmal: Eine solche Regelung ist erst möglich, wenn die Aufgaben der Meldebehörde vom Gesetzgeber definiert worden sind, und damit auch das Maß der wirklich erforderlichen Daten überschaubar und kontrollierbar wird. Bund und Ländern fällt insoweit vor allen anderen die Aufgabe zu, sich über die Funktion der Meldebehörden und der im Zusammenhang damit tatsächlich notwendigen Informationen zu verständigen, um dann beides im Interesse des Bürgers gesetzlich festzuschreiben.

Am Beispiel des Melderechts wird freilich zugleich noch mehr deutlich: Um die Verarbeitung bestimmter Daten zu rechtfertigen, genügt es nicht, auf vorhandene gesetzliche Regelungen zu verweisen. Die Datenschutzgesetzgebung verpflichtet vielmehr die öffentliche Verwaltung zu einer permanenten Inventarisierung der Datenarten. Die öffentliche Verwaltung sollte sich daher ständig mit der Frage auseinandersetzen, inwieweit die ihr zur Verfügung stehenden Daten auch wirklich gebraucht werden. Dies gilt umso mehr, als manche gesetzliche Regelung, die zur Verarbeitung ermächtigt, aus einer Zeit stammt, in der die Notwendigkeit des Datenschutzes vom Gesetzgeber noch nicht ausdrücklich anerkannt worden war. Der Datenschutz zwingt zur Zurückhaltung bei der Verarbeitung personenbezogener Daten. Er verlangt deshalb mehr als nur den Hinweis auf eine gesetzliche Regelung. Seinen Anforderungen ist erst Rechnung getragen, wenn die angeforderte Information von der Aufgabe der jeweiligen Behörde her ständig überprüft und auf das von dieser Aufgabe her noch vertretbare Mindestmaß reduziert wird²⁾.

²⁾ Vgl. auch meine als Anl. beigefügten Ausführungen zum Entwurf eines Bundesmeldegesetzes im Rahmen der Anhörung des Bundesministers des Innern am 20. und 21. November 1978.

1.1 b) Nicht anders ist die Situation im Polizeirecht. Auch hier bietet die hessische Praxis Ansatzpunkte, die es im Hinblick auf die dringend erforderliche bereichsspezifische Regelung zu nutzen gilt. Anhand der „Vorläufigen Richtlinien für Auskünfte aus Kriminalakten“, auf die ich bereits in einem früheren Tätigkeitsbericht hingewiesen hatte³⁾, läßt sich zeigen, daß es auch im polizeilichen Bereich durchaus denkbar und möglich ist, dem Betroffenen ein Auskunftsrecht zuzugestehen. Wiederum kommt es darauf an, sorgfältig zwischen den einzelnen Aufgaben der Polizei zu unterscheiden und von dort aus die Frage zu stellen, in welchem Umfang die ansonsten dem Betroffenen im Rahmen der Datenschutzgesetzgebung garantierten Rechte hier ebenfalls ausgeübt werden können. Ganz in diesem Sinn hat das Bayerische Datenschutzgesetz mittlerweile bestimmt, daß der Auskunftsanspruch des Betroffenen der Polizei gegenüber nur entfallt, „soweit sie strafverfolgend oder zur Aufrechterhaltung der öffentlichen Sicherheit und Ordnung tätig wird“ (Art. 8 Nr. 3). Sicher eine immer noch sehr allgemein gehaltene Formulierung, die aber deutlich zu erkennen gibt, daß jeder Versuch, das Auskunftsrecht des Betroffenen generell auszuschließen, mit den Anforderungen eines ernst genommenen Datenschutzes unvereinbar ist.

Ähnliches gilt für die Löschung von Daten: Wiederum ist es im Interesse des Betroffenen unerlässlich, darüber Gewißheit zu gewinnen, ob und unter welchen Umständen vorhandene, sich auf seine Person beziehende Unterlagen vernichtet werden müssen. Deshalb bestimmt § 163 c Abs. 4 der Strafprozeßordnung (StPO) nunmehr ausdrücklich, daß die bei der Identitätsfeststellung einer Person angefallenen Unterlagen dann zu vernichten sind, wenn die Identität feststeht. In dieselbe Richtung zielt auch die vorgeschlagene Neufassung des § 81 StPO⁴⁾. Sie soll sicherstellen, daß die bei der Strafverfolgung angefallenen erkennungsdienstlichen Unterlagen grundsätzlich dann vernichtet werden, wenn das Strafverfahren rechtskräftig abgeschlossen und — bei einer Verurteilung — die Strafe vollstreckt ist.

Mehr als Fragmente einer im Interesse eines wirklichen Datenschutzes erforderlichen Regelung sind aber damit nicht angesprochen. Dies insbesondere, weil manche der beabsichtigten Regelungen widersprüchlich sind. So leuchtet es beispielsweise nicht ein, weshalb die Vernichtung von Unterlagen im Falle der Gefahrenabwehr⁵⁾ vom Ver-

³⁾ Vgl. V, 4.7.

⁴⁾ Begründung zum Musterentwurf für ein einheitliches Polizeigesetz des Bundes und der Länder, den die Innenministerkonferenz am 25. 11. 1977 beschlossen hat.

⁵⁾ § 10 Abs. 2 des Musterentwurfs.

langen des Betroffenen abhängen, bei der Strafverfolgung hingegen obligatorisch sein soll. Sowohl das Hessische als auch das Bundesdatenschutzgesetz geben deutlich zu erkennen: Es gibt keinen Bereich der öffentlichen Verwaltung, der von der Verpflichtung ausgenommen ist, dem vom Gesetzgeber geforderten Respekt vor der persönlichen Integrität des von der Datenverarbeitung Betroffenen Rechnung zu tragen. Nicht von ungefähr hat das Bundesverwaltungsgericht⁶⁾ gerade im Hinblick auf die Aktivitäten der Polizei die Grenzen einer Verarbeitung personenbezogener Daten deutlich betont.

Auch und gerade im Interesse einer überzeugenden Verwirklichung der polizeilichen Aufgaben kommt es deshalb in ganz besonderem Maße darauf an, möglichst bald Regelungen zu formulieren, die Voraussetzungen und Grenzen der Verarbeitung personenbezogener Daten verbindlich festlegen. Eine bereichsspezifische, die Aufgaben der Polizei und die Situation des Betroffenen berücksichtigende Regelung tut hier in hohem Maße not. Nirgendwo anders entsteht beim Bürger der Eindruck so leicht, daß es, entgegen allen Behauptungen, doch Bereiche gibt, für die der Datenschutz keine Rolle spielt. Nirgendwo anders ist es daher wahrscheinlich so dringlich, unmißverständlich klarzustellen, wie der Schutz des Bürgers konkret aussieht. Die Glaubwürdigkeit des Datenschutzes hängt davon ebenso ab, wie die Überzeugungskraft der staatlichen Aktivität im polizeilichen Bereich.

Noch einmal: Die Ansatzpunkte für eine bereichsspezifische Regelung des Datenschutzes sind, wie die Praxis der hessischen Polizeibehörden und Art. 8 Nr. 3 BayDSG zeigen, durchaus vorhanden. Am Anlaß für eine gesetzliche Regelung fehlt es ebenfalls nicht: Das gegenwärtig diskutierte einheitliche Polizeigesetz des Bundes und der Länder wäre der richtige Ort zu demonstrieren, wie sehr der Gesetzgeber bereit ist, die Ziele der polizeilichen Aufgaben mit den Anforderungen des Datenschutzes zu verbinden. Beides, die Erfahrungen aus der Praxis und die Gelegenheit einer legislativen Entscheidung, gilt es so schnell wie möglich zu nutzen.

- 1.1 c) Hinzuweisen ist schließlich auf die Schwierigkeiten, die sich offensichtlich in zunehmendem Maße bei der Übermittlung personenbezogener Daten für wissenschaftliche Untersuchungen ergeben. Sie sind nicht zuletzt ein untrügliches Zeichen für das durch die ständig steigenden Informationsanforderungen verursachte Unbehagen der Bürger.

Die Betroffenen sind eben nicht mehr bereit, eine nur scheinbar nicht einzudämmende Flut von Fragebogen unbesehen hinzunehmen, ganz gleich im übrigen, ob sie von einem Hochschulinstitut oder von einem einzelnen Wissenschaftler, etwa im Rahmen seiner Diplomarbeit formuliert werden. Der vorliegende Tätigkeitsbericht enthält — genauso wie die früheren Berichte — nur einige Beispiele dafür, wie allergisch die Bürger reagieren. Insofern verwundert auch die Zurückhaltung der Behörden nicht. Der Bürger erwartet, daß der ansonsten immer wieder betonte Grundsatz, er könne und dürfe nicht zum uneingeschränkt nutzbaren Informationsobjekt degradiert werden, auch von den verschiedenen wissenschaftlichen Institutionen zur Kenntnis genommen wird, und zwar mit all den sich daraus für den Schutz des Betroffenen ergebenden Konsequenzen.

So verständlich solche Reaktionen auch sind, so wenig dürfen sie dazu führen, den Datenschutz in ein Instrument der Zensur wissenschaftlicher Forschung zu verwandeln. Landesgesetzgeber (§ 3 Abs. 3 HDSG) und Bundesgesetzgeber (§ 1 Abs. 3 BDSG) haben sich bei der Verarbeitung personenbezogener Daten für pressenspezifische Aufgaben ausdrücklich für eine Regelung ausgesprochen, die vom allgemeinen Datenschutz abweicht. Sie haben damit ausdrücklich dem möglichen Konflikt zwischen Datenschutz und der verfassungsrechtlich garantierten Freiheit der Presse Rechnung getragen. Die Hessische Verfassung (Art. 10 und 13) und das Grundgesetz (Art. 5) sprechen sich aber nicht minder nachdrücklich für die Freiheit der Wissenschaft aus. Ebenso wie bei der Presse darf deshalb der Datenschutz kein Vorwand sein, in die wissenschaftliche Forschung steuernd einzugreifen, mißliebige oder sonst unangenehme Forschungsvorhaben durch Verwehrung des Zugangs zu den notwendigen Daten zu unterbinden.

Der hessische Gesetzgeber hat diese Gefahr deutlich gesehen. § 15 HDSG erleichtert deshalb gezielt die Datenverarbeitung zugunsten der wissenschaftlichen Forschung. Der Gesetzgeber leugnet zwar keineswegs die Notwendigkeit, den Datenschutz auch gegenüber der Wissenschaft zu garantieren. Der Grundsatz, daß es keine Datenschutzimmunität geben darf, ist im wissenschaftlichen Bereich genauso wie anderswo gültig. Nur gilt es, Mittel und Wege zu finden, die in Kenntnis der Situation des Betroffenen und der Verpflichtung, ihn zu schützen, eine Versorgung der wissenschaftlichen Forschung mit den von ihr benötigten Angaben ermöglichen.

Die Verwirklichung dieses Zieles ist freilich in der Praxis nicht zuletzt deshalb auf Schwierigkeiten gestoßen, weil das Verhältnis zwischen § 15

⁶⁾ BVerwGE 26, 169 (170 f.).

HDSG einerseits und § 16 a HMG andererseits offensichtlich immer wieder zu Mißverständnissen Anlaß gibt. Welche Komplikationen entstehen können, zeigt folgender Fall: Eine Doktorandin einer hessischen Universität trat an den Magistrat einer hessischen Stadt mit der Bitte heran, ihr die Grunddaten der über 60jährigen Frauen zu überlassen. Sie beabsichtigte, diese Angaben im Zusammenhang mit einer Untersuchung über die altersbedingte Veränderung der Lebenssituation zu verwenden, für eine Arbeit also, die sich als Beitrag zu der in den letzten Jahren an Bedeutung gewinnenden Geriatrieforschung verstand. Ich habe den Magistrat ausdrücklich auf § 15 hingewiesen, zugleich aber betonen müssen, daß die Sonderregelung des § 16 a HMG die Übermittlung vom „öffentlichen Interesse“ abhängig macht. Der Magistrat hat dann die Übermittlung mit der Begründung abgelehnt, daß ein „öffentliches Interesse“ nicht gegeben sei.

Unstreitig hat der Gesetzgeber mit dem Hinweis auf das „öffentliche Interesse“ eine Barriere gegen Übermittlungen errichten wollen. Die Daten sollen eben nur in besonderen Fällen zur Verfügung gestellt werden, in denen auch die Allgemeinheit ein Interesse an ihrer Verarbeitung hat. Und ebenso unstreitig ist es, daß der Verwaltung die Aufgabe zufällt, selbst zu bestimmen, ob im konkreten Fall das „öffentliche Interesse“ bejaht werden kann. Dennoch darf nicht übersehen werden, daß die Interpretation des § 16 a HMG auf dem Hintergrund des § 15 HDSG und der verfassungsrechtlich garantierten Wissenschaftsfreiheit erfolgen muß. Das „öffentliche Interesse“ ist mit anderen Worten kein taugliches Instrument, um unter dem Mantel des Datenschutzes inhaltliche Kritik an wissenschaftlicher Forschung zu vollziehen.

Diese Gefahr wird sich allerdings solange nicht vermeiden lassen, wie es über § 15 HDSG hinaus an einer spezifischen, an den Besonderheiten der wissenschaftlichen Forschung ausgerichteten Regelung fehlt. Die vor allem in jüngster Zeit besonders nachdrücklich propagierten „ethical codes“ machen eine solche Regelung nicht überflüssig. Standesethische Grundsätze dokumentieren zwar die gute Absicht der jeweils beteiligten Wissenschaftler, sie bringen aber nicht die aus der Perspektive des Betroffenen unerläßliche Sicherheit. „Ethical codes“ können insofern letztlich nur die Funktion haben, die im Einzelfall auf dem Hintergrund einer bereits bestehenden gesetzlichen Regelung erforderlichen Präzisierungen zu bringen. Sie erhöhen das für die Wirksamkeit jeder Regelung notwendige Maß an Konkretheit, ohne aber den Gesetzgeber von seiner Verpflichtung zu befreien, die Bedingungen, unter denen personenbezogene Daten der wissenschaftlichen Forschung

zugänglich gemacht werden dürfen, festzulegen.

Im Hinblick auf eine solche Regelung gilt es festzuhalten: Die Bereitstellung von Daten durch die öffentliche Verwaltung muß grundsätzlich auf die Fälle beschränkt bleiben, in denen es nicht möglich ist, die gewünschten Angaben von den Betroffenen selbst zu bekommen. Bloße Praktikabilitätsüberlegungen reichen nicht aus, um den Betroffenen zu übergehen. Seine Daten stehen auf dem Spiel; es muß daher prinzipiell auch seiner Entscheidung überlassen bleiben, ob und in welchem Umfang sie verwendet werden dürfen. Ferner: Der Bürger darf genauso wie im Zusammenhang mit jedem anderen Fragebogen nicht überrumpelt werden. Er muß — mit anderen Worten — sich nicht nur über die Freiwilligkeit seiner Beteiligung an der Fragebogenaktion im klaren sein, sondern er muß auch über das Ziel der Untersuchung und den Zweck der Fragen hinreichend unterrichtet werden. Solange dies nicht geschieht, mobilisiert die wissenschaftliche Forschung allzuleicht Affekte und zementiert letztlich Vorurteile, die sich nachteilig auf ihre eigenen Arbeitsmöglichkeiten auswirken. Schließlich: Daten, die um der wissenschaftlichen Forschung willen zur Verfügung gestellt werden, dürfen auch nur in ihrem Rahmen verwendet werden. Die strenge Zweckbindung ist Grundvoraussetzung eines erleichterten Zugangs. Gerade im Hinblick auf diese letzte Bedingung macht sich freilich die Notwendigkeit einer technischen und organisatorischen Infrastruktur bemerkbar, ohne die sich eine im Interesse der Betroffenen unabdingbare Sicherung der verwendeten Daten nicht verwirklichen läßt.

Wiederum bietet die Praxis Ansätze für eine solche Regelung. Zu erinnern ist beispielsweise an die in Zusammenarbeit mit dem Hessischen Kultusminister und den hessischen Universitäten entwickelten ersten Datenschutzvorkehrungen. Auch hier handelt es sich aber lediglich um Ansatzpunkte. Sie deuten an, daß eine umfassende bereichsspezifische Regelung durchaus möglich ist. Bis zu einer solchen Regelung erscheint es jedoch auf jeden Fall erforderlich, möglichen, mit der Interpretation des „öffentlichen Interesses“ im Rahmen des § 16 a HMG zusammenhängenden Fehlentwicklungen vorzubeugen. Die Meldebehörden müßten darauf hingewiesen werden, daß die in § 15 HMG formulierte Grundentscheidung des Gesetzgebers bei der Auslegung des „öffentlichen Interesses“ zu berücksichtigen ist. Nur: Ein erleichterter Zugang der wissenschaftlichen Forschung zu den Daten rechtfertigt sich lediglich solange, wie Zweifel an der Existenz der jeweils im Interesse des Betroffenen notwendigen Schutzvorkehrungen nicht bestehen.

1.2 Zusammenarbeit der Kontrollorgane

Eine wirksame Kontrolle des Datenschutzes läßt sich ohne eigens dafür verantwortliche Instanzen nicht durchführen. Landesgesetzgeber und Bundesgesetzgeber haben dem Rechnung getragen. Den Beauftragten der Länder und des Bundes sowie den in den §§ 30, 40 BDSG vorgesehenen Aufsichtsbehörden obliegt die Aufgabe, die Verwirklichung der Datenschutzgrundsätze jeweils in ihren sachlichen und örtlichen Zuständigkeitsbereichen zu überwachen. So notwendig freilich die sorgfältige Aufspaltung und Aufteilung der Kontrollfunktionen sein mag, so wenig darf sie dem Bürger zum Nachteil gereichen. Es ist ohnehin schwierig genug, die Kompetenzverteilung dem Bürger verständlich zu machen. Er will sich gegen Fragen, die ihm unzulässig vorkommen, zur Wehr setzen oder sich über den Umfang der Verarbeitung seiner Daten vergewissern, ohne Gefahr zu laufen, sich von Kontrollinstanz zu Kontrollinstanz verweisen zu lassen. Er ist deshalb auch nicht ohne weiteres bereit einzusehen, daß die Kontrolle Aufgabe verschiedener Stellen ist. Je deutlicher er aber mit unterschiedlichen Kompetenzen konfrontiert wird, desto nachhaltiger beginnt er, am Datenschutz zu zweifeln.

Wohlgemerkt: Es geht keineswegs darum, die Notwendigkeit einer Kompetenzabgrenzung in Frage zu stellen. Zur Debatte steht einzig und allein die Einsicht in die Tatsache, daß in voller Kenntnis der unterschiedlichen Kompetenzen im Interesse des Bürgers Kooperationsformen gefunden werden müssen, die eine fortlaufende gegenseitige Unterrichtung ebenso garantieren wie sie Zuständigkeitskonflikte rechtzeitig eliminieren. Der Datenschutz ist kein taugliches Objekt für Kompetenzstreitigkeiten, sondern ein Instrument, das um des Bürgers willen entwickelt worden ist und daher auch immer in voller Beachtung seiner Interessen gehandhabt werden muß. Deshalb haben Landesgesetzgeber (§ 23 Abs. 3 HDStG) und Bundesgesetzgeber (§ 19 Abs. 5 BDSG) die Kooperationsverpflichtung ausdrücklich hervorgehoben.

Ganz in diesem Sinn haben sich die nach den §§ 30 und 40 für die Verarbeitung im privaten Bereich zuständigen Aufsichtsbehörden zu mehr als nur zu einem regelmäßigen Meinungsaustausch entschlossen. Die gemeinsam erarbeiteten vorläufigen Verwaltungsvorschriften⁷⁾ dokumentieren den Wunsch, eine einheitliche Auslegung des BDSG anzustreben und sich dabei kontinuierlich auf die Erfahrungen aller Aufsichtsbehörden zu stützen.

In diese Richtung zielt auch meine Initiative, eine Ständige Konferenz der Länderbeauftragten für den Datenschutz und des Bundesbeauftragten für den Datenschutz zu konstituieren. Wie sehr es auf einen ständigen Informationsaustausch ankommt, hat gerade die Erfahrung der letzten Zeit gezeigt. Probleme, wie etwa die Übermittlung personenbezogener Daten an öffentlich-rechtliche Religionsgesellschaften oder die Bereitstellung von Angaben für Zwecke der wissenschaftlichen Forschung müssen im Interesse des Betroffenen möglichst einheitlich gelöst werden. Zudem helfen gerade die in den Ländern gewonnenen unterschiedlichen Erfahrungen, die einzelnen Fragen besser zu erkennen und damit auch differenzierter zu behandeln.

Ebenso wichtig ist schließlich eine kontinuierliche Abstimmung zwischen dem Landesbeauftragten und den Aufsichtsbehörden nach den §§ 30 und 40 BDSG. Schon deshalb, weil es eine ganze Reihe von Fällen gibt, die sich ohne eine intensive Kooperation nicht zufriedenstellend behandeln lassen. Die Übermittlung von personenbezogenen Daten aus der öffentlichen Verwaltung an eine politische Partei, die Informationen über potentielle Wähler bekommen möchte, unterliegt der Kontrolle des Datenschutzbeauftragten des jeweiligen Landes. Es genügt insoweit, an meinen Zwischenbericht vom 7. 6. 1978 und die dadurch veranlaßte Reform des § 16 a HMG zu erinnern. Sobald aber eine politische Partei Informationen über ihre Mitglieder speichert, unterliegt die Zulässigkeit der Datenverarbeitung der Kontrolle durch die gem. § 30 BDSG „nach Landesrecht zuständigen Aufsichtsbehörde“. Es versteht sich von selbst, daß beide Kontrollinstanzen nicht unabhängig voneinander operieren dürfen, sondern bestrebt sein müssen, ihre Erfahrungen im Interesse der Einheitlichkeit des Datenschutzes gemeinsam zu nutzen.

Die Zusammenarbeit zwischen dem Hessischen Innenminister sowie den Regierungspräsidenten in Darmstadt und Kassel als den zuständigen Aufsichtsbehörden nach den §§ 30 und 40 BDSG einerseits und meinem Amt andererseits ist deshalb von Anfang an besonders intensiv gewesen. Es ist die gemeinsame Überzeugung aller Beteiligten, daß diese Kooperation aufrechterhalten und weiter ausgebaut werden muß, wenn der vom Gesetzgeber beabsichtigte Schutz des Betroffenen vor dem Mißbrauch seiner Daten bei ihrer Verarbeitung nicht an Kompetenzschwierigkeiten scheitern soll. Der Datenschutz darf zu keinem Zeitpunkt durch eine Datenschutzbürokratie gefährdet werden, die aus Sorge um die eigenen Zuständigkeiten, die Verpflichtung hintanstellt, sich ohne Rücksicht auf alle Kompetenzfragen für

⁷⁾ StAnz. 12/1978, 587.

einen wirksamen Schutz des Betroffenen einzusetzen.

1.3 Datenschutz und Bürger

Bereits in früheren Berichten hatte ich mehrfach davor gewarnt, den Datenschutz einzig und allein als Forderung nach einer gesetzlichen Regelung zu sehen. Die zweifelsohne unentbehrlichen gesetzlichen Schutzvorkehrungen müssen von der Bereitschaft der Bürger und der Behörden begleitet werden, die Verarbeitung personenbezogener Daten nicht einfach hinzunehmen, sondern in Frage zu stellen und deshalb auch von den im Gesetz garantierten Kontrollrechten aktiv Gebrauch zu machen. Sonst ist der Datenschutz letztlich mehr oder weniger Wunschvorstellung, nämlich nichts weiter als eine begrüßenswerte legislative Intention, nicht aber eine gesellschaftliche Realität.

Deshalb gilt es, die wachsende Anteilnahme der Bürger an der Verwirklichung des Datenschutzes ganz besonders hervorzuheben. 1978 erreichten mich mehr als 1 000 Anfragen zu konkreten Problemen des Datenschutzes, die bislang weitaus höchste Anzahl. Sicher, gemessen daran ist der Anteil an begründeten Beschwerden — insgesamt 59 — relativ gering. Doch welche Bedeutung diesen 59 Beschwerden wirklich zukommt, ergibt sich erst, wenn man bedenkt, daß sich die Zahl der Beschwerden im Vergleich zum Vorjahr nahezu verdoppelt hat. Überhaupt läßt sich feststellen: Mit der Verabschiedung des Bundesdatenschutzgesetzes und des zweiten Hessischen Datenschutzgesetzes tritt auch in der Einstellung der Bürger eine Wende ein. Sie ergreifen mehr und mehr selbst die Initiative, wollen genau über ihre Rechte Bescheid wissen, verlangen exakte Informationen über speichernde Stellen und verwahren sich zunehmend gegen Informationsanforderungen, die ihnen zweifelhaft erscheinen. Der Datenschutzbeauftragte wird für sie zur Schaltstelle für die Verwirklichung ihrer Rechte, von ihm erwarten sie die notwendigen Orientierungshinweise und an ihn knüpfen sie die Hoffnung, fehlgelaufene Informationsverarbeitung noch korrigieren zu können.

Nicht minder bedeutsam ist die zunehmende Sensibilisierung der Behörden. Auch für sie ist der Datenschutzbeauftragte eine immer häufiger genutzte Informationsstelle. Und auch sie sind keinesfalls durchweg bereit, eine Datenverarbeitung unter allen Umständen durchzuführen. Mehr und mehr werden Verarbeitungserwartungen auf mögliche Konflikte mit dem Datenschutz hin überprüft. Mehr und mehr läßt sich deshalb sagen, daß ein großer Teil der von mir bearbeiteten Fälle auf die Initiative der Behörden selbst zurückzuführen ist.

Für diese Sensibilisierung spricht aber auch die Bereitschaft etwa der Großstädte, eigene Datenschutzbeauftragte zu bestellen. In die gleiche Richtung deutet der von den Kommunen angeregte Meinungsaustausch zwischen kommunaler Selbstverwaltung und Datenschutzbeauftragten, der es ermöglichen soll, Zweifel, die mit der Anwendung des Datenschutzgesetzes verbunden sind, rechtzeitig auszuräumen, also nicht erst, wenn die Bürger bereits darunter zu leiden haben.

Wohlgemerkt, nach wie vor ist der Anteil der Fälle, die auf Initiative des Datenschutzbeauftragten hin aufgegriffen und verfolgt werden, überproportional groß, solange man ihn mit der Zahl jener Fälle vergleicht, deren Untersuchung auf Anregungen von Bürgern zurückzuführen ist. Nach wie vor wird die vom Gesetz geforderte Kontrolle also in der Hauptsache durch den Datenschutzbeauftragten selbst ausgelöst. Trotzdem ist die langsame Verschiebung der Gewichte nicht zu übersehen. Die Aktivität der Bürger gewinnt zunehmend an Bedeutung, ja noch mehr, der Zeitpunkt zeichnet sich bereits ab, zu dem Bürger und Behörden durch ihre Zweifel und durch ihre Beschwerden in etwa der Hälfte aller Fälle den Anlaß für meine Untersuchungen geben werden.

Mindestens ebenso wichtig wie die Sensibilisierung der Bürger und der öffentlichen Verwaltung ist die Bereitschaft der Behörden, den Bürger auch und gerade im Zusammenhang mit der Verarbeitung seiner Daten als Gesprächspartner zu sehen. Die Intervention des Datenschutzbeauftragten wird in einer Vielzahl von Fällen dann überflüssig, wenn die Behörden von sich aus alles tun, um ihr Verhalten und ihre Erwartungen verständlich zu machen. Wer beispielsweise einen gesetzlich abgesicherten Fragebogen verteilt, darf sich nicht mit dem abstrakten Hinweis auf die einschlägigen gesetzlichen Bestimmungen zufriedengeben. Er muß vielmehr seine Verpflichtung, auf die gesetzliche Grundlage der Datenerhebung aufmerksam zu machen, als Aufforderung verstehen, dem Bürger Inhalt und Zweck der gesetzlichen Regelung und damit zugleich der eigenen Aktivität mitzuteilen.

Deshalb reicht auch die gesetzliche Anerkennung der Auskunftssperre in § 16 a HMG nicht aus. Vielmehr kommt es darauf an, den Bürger bei seinen ersten, zögernden Versuchen zu unterstützen, eine Übersicht über die gespeicherten Daten zu gewinnen, und ihn zugleich auf seine Rechte aufmerksam zu machen. Auf meine Initiative hin haben sich die Behörden konsequenterweise bereitgefunden, dem Bürger auch bei ungenügender Genauigkeit seiner Anfrage eine möglichst vollständige Antwort zu geben, anstatt ihn mit der

Forderung zu entmutigen, zunächst seine allgemein gehaltene Anfrage zu präzisieren. Aus dem gleichen Grund setzt sich mehr und mehr die Überzeugung durch, daß Informationsinstrumente entwickelt werden müssen, um den Bürger regelmäßig auf sein Recht hinzuweisen, die Auskunft über seine Daten sperren zu lassen, mit anderen Worten: die gesetzliche Regelung als ein effektives Mittel der Mitwirkung des Bürgers am Datenschutz zu gebrauchen.

Eine demokratische Gesellschaft lebt von der Bereitschaft der Bürger, sie mitzutragen, d. h., an der Verwirklichung der gemeinschaftlichen Ziele mitzuwirken oder teilzunehmen. Diese Bereitschaft setzt voraus, daß die öffentliche Verwaltung dem Bürger die Beweggründe ihres Handelns erkennbar macht, damit er beurteilen kann, warum sie so handelt, wie sie jeweils vorgeht. Insofern erweist sich Datenschutz als Prüfstein des Selbstverständnisses einer demokratischen Gesellschaft.

2. STAND DER DATENSCHUTZGESETZGEBUNG IN DEN LÄNDERN

2. Stand der Datenschutzgesetzgebung in den Ländern

Bei Abschluß dieses Berichts hatten sieben von elf Bundesländern Datenschutzgesetze erlassen; und zwar⁸⁾:

- Hessisches Datenschutzgesetz (HDSG) vom 31. 1. 1978 (GVBl. I S. 96),
- Bayerisches Gesetz zum Schutz vor Mißbrauch personenbezogener Daten bei der Datenverarbeitung (Bayerisches Datenschutzgesetz — BayDSG) vom 2. 5. 1978 (GVBl. S. 165),
- Gesetz über den Datenschutz in der Berliner Verwaltung (Berliner Datenschutzgesetz — BlnDSG) vom 21. 6. 1978 (GVBl. S. 1317),
- Gesetz zum Schutz vor Mißbrauch personenbezogener Daten bei der Datenverarbeitung (Bremisches Datenschutzgesetz — BrDSG) vom 23. 12. 1977 (GVBl. S. 393),
- Niedersächsisches Datenschutzgesetz (NDSG) vom 26. 5. 1978 (GVBl. S. 421),
- Saarländisches Gesetz zum Schutz vor Mißbrauch personenbezogener Daten bei der Datenverarbeitung (Saarländisches Datenschutzgesetz — SDSG) vom 17. 5. 1978 (AmtsBl. S. 581),
- Schleswig-Holsteinisches Gesetz zum Schutz vor Mißbrauch personenbezogener Daten bei der Datenverarbeitung (Landesdatenschutzgesetz — LDSG) vom 1. 6. 1978 (GVBl. S. 156).

In diesen Gesetzen ist eine Reihe von Anregungen aus meinem Entwurf für ein Hessisches Datenschutzgesetz⁹⁾, der als Modell für die Datenschutzgesetze der Länder gedacht war, von den einzelnen Landesgesetzgebern berücksichtigt worden. Die Befürchtung, daß dadurch die Rechtseinheit gefährdet werde, hat sich jedoch nicht bestätigt.

In den Rechtsgrundsätzen und wichtigsten Bestimmungen sind die Länder dem BDSG gefolgt.

⁸⁾ Das Datenschutzgesetz von Rheinland-Pfalz i.d.F. vom 24. 2. 1975 (GVBl. S. 84) wird nicht berücksichtigt, da eine Novellierung zur Anpassung an das BDSG vorgesehen ist.

⁹⁾ Vgl. VI, Anl. zu Abschn. 2.

Wo einzelne Regelungen vom BDSG abweichen, werden die Länder künftig ihre unterschiedlichen Erfahrungen in den gemeinsamen Diskussionsprozeß einbringen und so zur Weiterentwicklung des Datenschutzrechts beitragen.

Im einzelnen sind folgende wichtige Abweichungen vom BDSG in den vorliegenden Datenschutzgesetzen der Länder festzustellen:

- Während das BDSG nur den Schutz des Betroffenen vor Mißbrauch seiner Daten zum Gegenstand hat, hält Hessen daran fest, auch das sog. Informationsgleichgewicht zwischen Exekutive und Parlament als Aufgabe des Datenschutzes zu regeln; es folgt den Regelungen des ersten Datenschutzgesetzes von 1970 und gibt ihnen ein verstärktes Gewicht. In den Datenschutzgesetzen von Bremen und Berlin finden sich vergleichbare Bestimmungen. Bayern und Nordrhein-Westfalen haben ein parlamentarisches Auskunftsrecht im Rahmen ihrer ADV-Organisationsgesetze eingeführt.
- Bayern läßt die Verarbeitung für Daten nur für solche Aufgaben zu, die durch Gesetz, Satzung oder Rechtsverordnung geregelt sind. Nicht nur die Datenverarbeitung, auch die Aufgabe, zu deren Erfüllung sie erforderlich ist, muß durch eine Rechtsnorm zugewiesen sein.
- Bayern und das Saarland stellen ausdrücklich klar, daß die Vorschriften der Datenübermittlung auch für die Übermittlung zwischen Teilen einer Behörde oder öffentlichen Stelle gelten, sofern die empfangende Stelle andere Aufgaben wahrnimmt als die abgebende Stelle, oder wenn sie räumlich von ihr getrennt ist.
- Berlin räumt dem Bürger das Recht ein, die über ihn in der öffentlichen Verwaltung gespeicherten Daten für die Übermittlung an nichtöffentliche Stellen sperren zu lassen. In Hessen und Niedersachsen gilt ein solches Recht auf Auskunftssperre nur bei Meldebehörden.
- Hessen, Bayern und das Saarland legen für die Übermittlung an Stellen außerhalb des öffentlichen Bereichs fest, daß der Empfänger die Daten nur zu dem Zweck verwenden darf, zu dem die Behörde sie ihm überläßt.

- In Bayern und im Saarland untersagen die Datenschutzgesetze, wenn dem Betroffenen gegenüber der speichernden Stelle kein Auskunftsrecht zusteht, eine Datenübermittlung an nicht-öffentliche Stellen, es sei denn, daß das öffentliche Interesse es erfordert.
 - Im Saarland kann die Behörde die Übermittlung von Daten an Private mit Auflagen verbinden, um den Datenschutz sicherzustellen.
 - Nach dem Bayerischen Datenschutzgesetz bedarf die Einwilligung des Betroffenen zur Verarbeitung der über seine Person erhobenen Daten nicht nur der Schriftform; darüber hinaus muß er über die Auswirkung seiner Einwilligungserklärung unterrichtet werden.
 - In Bayern und im Saarland ersetzt das vom Landesbeauftragten geführte Datenschutzregister, das von jedermann eingesehen werden kann, die in den anderen Ländern geltende Verpflichtung der Behörden, die Art der von ihnen gespeicherten und regelmäßig übermittelten Daten, die Aufgaben, für die sie gebraucht werden, und den betroffenen Personenkreis in Veröffentlichungen bekanntzugeben.
 - Das Bayerische Datenschutzgesetz beschränkt das Auskunftsrecht des Betroffenen gegenüber der Polizei nicht allgemein, sondern nur für die Fälle, in denen die Polizei strafverfolgend oder zur Aufrechterhaltung der öffentlichen Sicherheit und Ordnung tätig wird¹⁰⁾.
 - Bayern, Berlin, Bremen und das Saarland verpflichten in ihren Datenschutzgesetzen die Behörden, die Berichtigung, Sperrung oder Löschung von Daten regelmäßig den Datenempfängern mitzuteilen.
 - Bremen gewährt dem Betroffenen einen Anspruch auf Löschung — statt auf Sperrung — der Daten zu seiner Person, wenn die Behörde weder die Richtigkeit noch Unrichtigkeit des Datensatzes beweisen kann.
 - In Hessen, Niedersachsen und Bayern kann der Bürger Schadenersatz verlangen, ohne ein Verschulden der datenverarbeitenden Stelle nachweisen zu müssen, wenn bei einer unzulässigen Datenverarbeitung seine schutzwürdigen Belange beeinträchtigt worden sind.
 - In Hessen und Berlin sind die Landesdatenschutzbeauftragten dem Präsidenten des Landtags bzw. des Abgeordnetenhauses zugeordnet; durch diese organisatorische Anbindung wird ihre Weisungsfreiheit und Unabhängigkeit betont. Niedersachsen verzichtet auf jede parlamentarische Beteiligung bei der Bestellung des Datenschutzbeauftragten.
- Einzelne Gesetze haben für bestimmte Bereiche Sonderregelungen getroffen:
- Hessen hat die Datenübermittlung zum Zwecke wissenschaftlicher Forschung besonders geregelt¹¹⁾.
 - Bayern weitet das Kontrollrecht des Datenschutzbeauftragten auf die öffentlich-rechtlichen Religionsgesellschaften aus, soweit ihnen personenbezogene Daten aus dem öffentlichen Bereich übermittelt werden.
- In der folgenden Übersicht werden die wichtigsten Abweichungen vom BDSG tabellarisch dargestellt und ihre Fundstellen genannt:

¹⁰⁾ Vgl. auch VII, 1.1 b.

¹¹⁾ Vgl. VII, 1.

Abweichungen der Datenschutzgesetze der Länder vom BDSG — Überblick

(arabische Ziffern: § oder Artikel, römische Ziffern: Absatz)

Stand: November 1978

	Hessen	Bayern	Berlin	Bremen	Niedersachsen	Saarland	Schleswig-Holstein
1. Aufgabenerweiterung							
— Schutz des Informationsgleichgewichts/der Gewaltenteilung	1 I Nr. 2, 23 II	—	21 II	20 II	—	—	—
2. Erhöhte Anforderungen an die Zulässigkeit der Datenverarbeitung							
2.1 Die Aufgabe, zu deren Erfüllung die Verarbeitung von Daten erforderlich ist, muß der Stelle durch eine Rechtsnorm zugewiesen sein	—	16 I, 17 I, 18 1	—	—	—	—	—

	Hessen	Bayern	Berlin	Bremen	Nieder- sachsen	Saarland	Schleswig- Holstein
2.2 Die Übermittlungsregelung gilt auch zwischen Teilen einer Stelle, die verschiedene Aufgaben wahrnehmen oder räumlich getrennt sind	—	17 III	—	—	—	14 III	—
2.3 Zweckbindung bei Übermittlung an Private	16 II	18 V	—	—	—	16 VI	—
2.4 Keine Übermittlung an Private bei Sperrung durch den Betroffenen	—	—	11, 7	—	—	—	—
2.5 Keine Übermittlung an Private, wenn an den Betroffenen keine Auskunft erteilt wird	—	18 IV (eingeschr.)	—	—	—	16 IV, V	—
2.6 Möglichkeit zu Datenschutzaufgaben bei Übermittlung an Private	—	—	—	—	—	16 VII	—
3. Besondere Durchführungsmaßnahmen							
3.1 Genehmigungspflicht des EDV-Einsatzes durch die oberste Dienstbehörde	—	26 II	—	—	—	18 II	—
3.2 Veröffentlichung gespeicherter Daten	17	—	12	14	12	—	13
3.3 Benachrichtigung des Empfängers nach erfolgter Berichtigung (sowie Löschung oder Sperrung)	—	16 III	14 IV	16 IV	—	10 III	—
4. Weitergehende Rechte des Betroffenen							
4.1 Anspruch auf Sperrung bei berechtigtem Interesse	—	10	—	—	—	10 I	—
4.2 Keine Übermittlung an Private bei Sperrung durch den Betroffenen	—	—	11, 7	—	—	—	—
4.3 Anspruch auf Löschung, wenn die Richtigkeit der gespeicherten Daten von der speichernden Stelle nicht bewiesen werden kann	—	—	—	4 IV, 16 III	—	—	—
4.4 Belehrung über die Bedeutung der Einwilligung	—	4 II	—	—	—	—	—
4.5 Gefährdungs-/verschuldensunabhängige Haftung	8 II	13 (eingeschr.)	15 I	—	4 II	—	—
5. Parlamentarisches Auskunftsrecht dazu Untersuchungen durch den Datenschutzbeauftragten (DSB)	13 14	— —	17 —	12 24	— —	15 —	— —
6. Verstärkte Kontrollrechte des DSB							
6.1 Organisatorische Zuordnung des DSB zur Legislative	30	—	19, II	—	—	—	—
6.2 Zusätzlicher Ausschuß/Beirat	—	29	—	28	—	—	—
6.3 Private Auftragnehmer öffentlicher Stellen unterliegen der Kontrolle des DSB	4 I Nr. 3	—	—	7 I Nr. 3	—	5 III	—
6.4 Öffentlich-rechtliche Wettbewerbsunternehmen unterliegen der Kontrolle des DSB	—	—	—	—	—	—	5
6.5 Religionsgesellschaften unterliegen der Kontrolle des DSB, soweit sie vom Staat erhaltene Daten verarbeiten	—	25 II	—	—	—	—	—

	Hessen	Bayern	Berlin	Bremen	Nieder- sachsen	Saarland	Schleswig- Holstein
6.6 Register des DSB enthält auch manuell geführte Dateien	25	—	—	21	—	—	—
7. Sonderregelungen							
7.1 Kein Rundfunkprivileg	—	—	—	—	1 III	—	3 III
7.2 Anwendung der §§ 23—27 BDSG auf dienst- und arbeitsrechtliche Rechtsverhältnisse	3 IV	—	1 IV	1 IV	7 II	—	—
7.3 DV für wissenschaftliche Zwecke	15	—	—	—	—	—	—
7.4 DV für statistische Zwecke	—	23	—	—	—	24	—
7.5 Auskunftssperre im Melderegister auf Antrag	16 a IV HMG	—	—	—	25	—	—
8. Straf- und Bußgeldvorschriften							
8.1 Weitergehende Strafvorschriften	—	—	—	30	21 I, II	—	23
8.2 Strafantragsrecht des DSB	—	—	—	—	21 III	27 III	—
8.3 Sanktion bei Zweckentfremdung übermittelter Daten	33 II	—	—	—	—	—	—
8.4 Sanktion bei Datenschleicherung	—	—	—	—	—	28 I	—

3. GESETZGEBUNG IM AUSLAND

3. Gesetzgebung im Ausland

3.1 Frankreich

Am 6. Januar 1978 hat der Präsident der Französischen Republik das neue Datenschutzgesetz „Loi relative à l'informatique, aux fichiers et aux libertés“¹²⁾ ausgefertigt, das die Nationalversammlung und der Senat in ihren Sitzungen am 21. Dezember 1977 verabschiedet hatten.

Das neue Gesetz enthält im Vergleich zu dem in meinem letzten Bericht kurz dargestellten Gesetzentwurf von 1976¹³⁾ eine ganze Reihe bedeutsamer Veränderungen zur Verbesserung des Datenschutzes. Dabei ist es im Umfang kaum gewachsen und enthält mit 48 Artikeln etwa die gleiche Zahl wie das Bundesdatenschutzgesetz (47). Die Veränderungen betreffen vor allem die Abschnitte über die Grundsätze für die Datenverarbeitung (I), die Stellung der Kommission (II) und die Einzelvorschriften für die Datenverarbeitung (IV).

Der auch bisher schon schärfer als im BDSG formulierte Schutzzweck des Gesetzes ist in Art. 1 noch weiter präzisiert worden: „Die Datenverarbeitung muß allen Bürgern dienen. Ihre Entwicklung muß sich im Rahmen der internationalen Zusammenarbeit vollziehen. Sie darf weder die menschliche Identität, noch die Grundrechte, noch das Privatleben, noch die individuellen und kollektiven Freiheitsrechte beeinträchtigen.“

In das Verbot einer — allein auf automatische Datenverarbeitung gestützten — Wertung menschlichen Verhaltens (Art. 2) wurden neben Gerichts- und Verwaltungsentscheidungen nun auch private Entscheidungen einbezogen.

Der — auch bisher schon verwendete — Begriff der „Verarbeitung personenbezogener Informationen“ erhielt in dem neu eingefügten Art. 5 eine Definition, die den Rahmen der darunter fallenden Tätigkeiten sehr weit zieht: „Als Verarbeitung personenbezogener Informationen im Sinne dieses Gesetzes wird bezeichnet die Gesamtheit aller durch automatische Mittel vorgenommener Handlungen bezüglich der Sammlung, Erfassung, Ausarbeitung, Speicherung, Veränderung und Löschung personenbezogener Informationen sowie

die Gesamtheit aller Handlungen gleicher Art, die sich auf die Auswertung von Akten, Dateien und insbesondere die Verknüpfung, Zusammenstellung, Abfrage oder Übermittlung personenbezogener Informationen beziehen.“

Die Stellung der Nationalen Datenschutzkommission, die im Entwurf noch eine starke Bindung an die Regierung erkennen ließ, wurde erheblich verbessert: Art. 8 gibt ihr den Status einer unabhängigen Verwaltungsbehörde („autorité administrative indépendante“), deren Mitglieder keinerlei Weisungen unterworfen (Art. 13 Abs. 1) und — abgesehen von eintretender Inkompatibilität — nicht absetzbar sind (Art. 8 letzter Abs.). Die nunmehr 17 — bisher 12 — Mitglieder der Kommission werden nicht, wie nach dem Entwurf, von der Regierung ernannt, sondern in ihrer Mehrzahl von der „assemblée générale“ der sie entsendenden Gremien (Nationalversammlung, Senat, Wirtschafts- und Sozialrat, Staatsrat, Kassationshof, Rechnungshof) gewählt. Die Nationale Datenschutzkommission setzt sich wie folgt zusammen: 2 Abgeordnete der Nationalversammlung und 2 Senatoren, 2 Mitglieder des Wirtschafts- und Sozialrats, 2 Mitglieder oder frühere Mitglieder des Staatsrats — einer davon mindestens im Range eines „Conseiller“ —, 2 Mitglieder oder frühere Mitglieder des Kassationshofes — einer davon mindestens im Range eines „Conseiller“, 2 Mitglieder oder frühere Mitglieder des Rechnungshofes — einer davon mindestens im Range eines „Conseiller-maitre“ —; schließlich 2 vom Präsidenten der Nationalversammlung oder des Senats ernannte Persönlichkeiten, die durch ihre Kenntnis der Anwendung der automatischen Datenverarbeitung qualifiziert sind, und 3 aufgrund ihrer Autorität und ihres Sachverstands durch Kabinetts-erlaß ernannte Persönlichkeiten (Art. 8). Der — aus den Reihen der Datenschutzkommission auf 5 Jahre gewählt — Präsident oder der damit betraute Vizepräsident ernannt die für die Kommission tätigen Beamten (Art. 10 Abs. 3). Darüber hinaus kann die Kommission die Ersten Präsidenten des Appellationsgerichts und der Oberverwaltungsgerichte ersuchen, Richter aus ihrem Bereich zur Durchführung von Untersuchungs- und Kontrollaufgaben zur Verfügung zu stellen (Art. 11). Zusätzlich zu den — bereits in Art. 18 des Entwurfs enthaltenen — bisherigen Kontrollaufgaben der Kommission hat sie die Aufgabe erhalten, sich über industrielle Vorhaben zur Verwirklichung der Datenverarbeitung auf dem laufenden zu hal-

¹²⁾ Loi no. 78-17 vom 6. Januar 1978, Journal Officiel de la République Française vom 7. 1. 1978, S. 227-231.

¹³⁾ Vgl. VI, 3.2.1, S. 13-15.

ten (Art. 21 Ziffer 7). Keine Person oder Stelle — weder Minister, noch öffentliche Behörden, öffentliche oder private Unternehmen, oder irgend jemand anders — hat das Recht, die Kommission an ihrer Tätigkeit zu hindern; sie sind im Gegenteil durch das Gesetz verpflichtet, alles zu tun, um dieser ihre Aufgabe zu erleichtern (Art. 21, letzter Abs.). Alle Entscheidungen, Gutachten und Empfehlungen der Kommission, deren Kenntnis für die Anwendung oder Auslegung des Datenschutzgesetzes nützlich ist, stehen der Öffentlichkeit zur Verfügung (Art. 22, letzter Abs.). Der jährliche Tätigkeitsbericht muß nunmehr nicht nur dem Präsidenten der Republik, sondern auch dem Parlament vorgelegt werden und wird dann veröffentlicht. Der Bericht hat zusätzlich die Funktion erhalten, durch Beschreibung der von der Kommission angewandten Verfahren und Arbeitsmethoden die Arbeit der Kommission für den Bürger transparent zu machen.

Bei den Einzelschriften über die Datenverarbeitung, die Rechte des Bürgers und den Anwendungsbereich des Gesetzes sind folgende Neuerungen gegenüber dem Entwurf hervorzuheben:

Vorangestellt ist das Verbot der Datensammlung „mit Hilfe jeglicher betrügerischer, gesetzwidriger oder unerlaubter Mittel“ (Art. 25) und das Recht jeder natürlichen Person, „sich aus rechtlich zulässigen Gründen gegen die Verarbeitung sie betreffender personenbezogener Daten zu wenden“ (Art. 26).

Art. 29 schreibt vor, daß jeder, der die Verarbeitung personenbezogener Informationen anordnet oder durchführt, gegenüber den davon Betroffenen verpflichtet ist, „alle Vorsichtsmaßnahmen zum Schutz der Sicherheit dieser Informationen zu ergreifen und insbesondere zu verhindern, daß sie verändert, beschädigt oder an unberechtigte Dritte übermittelt werden.“

Das Auskunftsrecht des Bürgers ist durch eine neue Bestimmung verstärkt worden: Befürchtet er die Verheimlichung oder Entfernung ihn betreffender personenbezogener Informationen, so kann er den zuständigen Richter um die Anordnung entsprechender Sicherungsmaßnahmen — entsprechend unserem Erlaß einer einstweiligen Verfügung oder Anordnung — anrufen, bevor er den Klageweg beschreitet (Art. 35, letzter Abs.). Auch die in den Artikeln 36—38 enthaltenen Vorschriften über die Rückzahlung der Auskunftsgebühr nach Berichtigung unrichtiger Informationen, die Berichtigung von Amts wegen und die Benachrichtigung Dritter von der Berichtigung sind neu in das Gesetz aufgenommen worden.

Wie schon aus dem Gesetzentwurf von 1976 erkennbar war, hat der französische Gesetzgeber

dem Postulat des Schutzes der individuellen und kollektiven Freiheitsrechte des Bürgers klaren Vorzug gegeben vor dem Ziel einer Rationalisierung und Verbesserung der Effizienz der Verwaltung. Die „klare Sprache“ (Klartext), in der die gegenüber dem Bürger zu erteilende Auskunft über seine personenbezogenen Daten abgefaßt sein soll (Art. 35 Abs. 1), hat der französische Gesetzgeber auch mit Erfolg in seinem Datenschutzgesetz verwendet, so daß es sich im Vergleich der Europäischen Gesetze als besonders bürgerfreundlich darstellt.

3.2 Großbritannien

Der ausführliche Bericht des britischen Data-Protection Committee¹⁴⁾ sollte nach den Parlamentsferien im Herbst 1980 dem Unterhaus zusammen mit einem mit den einzelnen Ressorts bereits abgestimmten Entwurf für ein Datenschutzgesetz vorgelegt werden. In diesen Planungen ist offenbar eine Verzögerung aufgetreten, so daß erst im Laufe des Jahres 1979 mit der Vorlage des Entwurfs gerechnet werden kann.

Bei meinem Erfahrungsaustausch über Datenschutzprobleme im Bereich des Gesundheitswesens in Großbritannien ist mir eine interessante praktische Lösung für den Datenschutz in der Medizin bekannt geworden. Es hat sich bisher als schwierig erwiesen, für die elektronische Datenverarbeitung in der Medizin Datenschutzvorschriften zu entwickeln, die für alle der einzelnen Bereiche (z. B. Krankenhäuser, öffentlicher Gesundheitsdienst, Privatpraxen, Sozialversicherungsträger, Forschung) anwendbar sind und den sehr verschiedenen dort auftretenden Datenschutzproblemen gleichermaßen Rechnung tragen. Deshalb — und bei der in Großbritannien ausgeprägten Neigung, neue Probleme zunächst einmal pragmatisch anzugehen — überrascht es nicht, hier eine Lösung vorzufinden, die eine elastische Antwort auf Datenschutzfragen ermöglicht und sich bereits bei der Bewältigung anderer Zweifelsfragen der modernen Medizin bewährt hat: die Einrichtung der „Ethical Committees“. Es sind Kommissionen für Fragen der ärztlichen Berufsethik; sie werden bei Krankenhausträgern, dem Ärztenverband, dem staatlichen Gesundheitsrat und ähnlichen Stellen eingerichtet, die über Datenschutz im Gesundheitswesen zu entscheiden haben. Das jeweilige Ethical Committee besteht nicht nur aus ärztlichen Fachleuten, sondern auch aus Vertretern beispielsweise des Krankenhausträgers, des Personals, der Gesundheitsverwaltung oder anderer beteiligter Körperschaften. Da die Zusammensetzung — nach meinen Informatio-

¹⁴⁾ Vgl. VI, 3.2.2; V, 3.2.

nen — nicht gesetzlich geregelt ist, kann sie von Fall zu Fall variieren. Wie der Name schon zum Ausdruck bringt, handelt es sich bei den Ethical Committees um eine Art Selbsthilfeeinrichtung der Ärzte, die vorwiegend beratende Funktion hat. Ist z. B. in einem Fall die Entscheidung darüber zu treffen, ob in einer Universitätsklinik vorhandene Patientendaten für ein Forschungsprojekt zur Verfügung gestellt werden können, so wird die Angelegenheit dem Ethical Committee vorgelegt.

Bei der Beurteilung des jeweils notwendigen Datenschutzes kann es neben den Überlegungen über die Einhaltung der ärztlichen Schweigepflicht und das Einverständnis des Patienten auch andere Aspekte berücksichtigen, wie „handelt es sich um seriöse medizinische Forschung (oder um Werbeer Interessen der Pharmaindustrie)?“, „bietet der Antragsteller als Wissenschaftler persönliche Gewähr für die Einhaltung des Datenschutzes?“, „bleiben die Daten in der gleichen Klinik, oder müssen sie an ein anderes Institut übermittelt werden?“, „rechtfertigt die Abwägung zwischen dem wissenschaftlichen Wert des Forschungsprojekts und einer möglichen Gefährdung des Datenschutzes von Patienten eine Datenübermittlung ohne Zustimmung der — nicht mehr erreichbaren — Patienten?“. Das Committee kann also bei seiner Beurteilung des jeweiligen Falles sehr viel mehr Aspekte berücksichtigen und in seiner Antwort sehr viel flexibler auf den Einzelfall eingehen, als dies jeder gesetzlichen Regelung möglich ist. Auch wenn die Entscheidung nicht bei ihm, sondern bei dem für die EDV in der betreffenden Institution verantwortlichen Arzt liegt, so wird dieser es doch kaum riskieren, bei einer negativen Antwort des Ethical Committee trotzdem der Datenanforderung zuzustimmen, denn er würde riskieren, standesrechtlich zur Verantwortung gezogen zu werden. Bei dem hohen Ansehen, welches die „profession“ (vor allem Ärzte und Juristen) auch heute noch in Großbritannien genießen, kann man davon ausgehen, daß durch die Einrichtung der Ethical Committees eine sehr wesentliche Voraussetzung für die Gewährleistung des Datenschutzes im medizinischen Bereich geschaffen ist.

Den Einwand, daß eine solche Lösung die Einheitlichkeit der Rechtsanwendung beeinträchtigen kann und daß für Außenstehende — insbesondere auch für Patienten — die Handhabung des Datenschutzes im medizinischen Bereich dabei nicht genügend transparent werde, halte ich nicht für unberechtigt. Natürlich ist das Ethical Committee als ärztliche Selbsthilfeeinrichtung kein Ersatz für eine gesetzliche Datenschutzregelung. Doch ist nicht zu verkennen, daß für eine Übergangszeit, bis genügend praktische Erfahrungen auf dem Ge-

biete des Datenschutzes im Medizinbereich vorliegen, die englische Lösung gute Möglichkeiten bietet, sogenannte bereichsspezifische gesetzliche Regelungen vorzubereiten. Gerade für das Auskunftsrecht des Patienten könnte die Einschaltung eines Ethical Committee in Zweifelsfällen eine große Hilfe sein.

3.3 Österreich

Nach jahrelangen Vorarbeiten, die zur Vorlage verschiedener Entwürfe eines Datenschutzgesetzes führten¹⁵⁾, hat der Nationalrat der Republik Österreich am 18. Oktober 1978 einstimmig ein von der Presse als „Jahrhundertgesetz“¹⁶⁾ bezeichnetes Datenschutzgesetz¹⁷⁾ beschlossen. Bemerkenswert ist in der Tat, daß das österreichische Gesetz dem Datenschutz Verfassungsrang bestätigt, indem es dem Bürger ein „Grundrecht auf Datenschutz“ garantiert:

„§ 1 (1) Jedermann hat Anspruch auf Geheimhaltung der ihn betreffenden personenbezogenen Daten, soweit er daran ein schutzwürdiges Interesse, insbesondere im Hinblick auf Achtung seines Privat- und Familienlebens, hat.“

Wenn es auch bisher schon Ansätze für eine solche Betrachtungsweise, z. B. in Kanada¹⁸⁾ gegeben hat, und auch in der Bundesrepublik aufgrund der Anregung von Innenminister Hirsch (Nordrhein-Westfalen) die Forderung eines Grundrechts auf Datenschutz diskutiert wird, so ist Österreich doch das erste Land der Welt, das diese Forderung erfüllt hat. Es hat damit die in Art. 8 der Europäischen Menschenrechtskonvention enthaltenen Grundsätze fortgeführt und in Richtung auf ein Informationsrecht des Betroffenen über seine Daten erweitert¹⁹⁾. Wie der Bericht des Verfassungsausschusses ausführt, soll dem Einsatz der modernen Informationstechnologie „rechtlich ein Gegengewicht in Form des Datenschutzes gegeben werden. Ein wesentliches Bemühen war es dabei, einen Ausgleich zwischen den schutzwürdigen Interessen des einzelnen an einem wirksamen Datenschutz und den legitimen Interessen an der Informationsbeschaffung und Datenverarbeitung herbeizuführen“²⁰⁾.

¹⁵⁾ Vgl. V, 3.2.

¹⁶⁾ „Die Presse“, Wien, vom 19. Oktober 1978.

¹⁷⁾ „Bundesgesetz vom 18. Oktober 1978 über den Schutz personenbezogener Daten (Datenschutzgesetz — DSG)“, BGBl. f. d. Rep. Österreich, Nov. 78.

¹⁸⁾ Vgl. VI, 3.2.6.

¹⁹⁾ Vgl. Bericht des Verfassungsausschusses in Nr. 1024 der Beilagen zu den Stenographischen Protokollen des Nationalrates, XIV. GP, Ziff. 3.

²⁰⁾ Bericht des Verfassungsausschusses a.a.O. Ziff. 2.

Dabei geht das Gesetz davon aus, „daß im Zweifelsfall der Geheimhaltung der Vorzug zu geben ist, daß also das private Interesse gegenüber einem öffentlichen überwiegen soll“. Die Hervorhebung des Schutzes des Familienlebens neben dem Schutz des Privatlebens in § 1 ist ein Akzent des österreichischen Datenschutzgesetzes, der besondere Beachtung verdient. In der bisherigen Datenschutzgesetzgebung und -diskussion war der Schutz des Familienlebens mehr in eine Randposition gedrängt, insbesondere im Zusammenhang mit dem Datenschutz bei Minderjährigen²¹⁾. Mit der Einbeziehung der Achtung des Familienlebens in das Grundrecht auf Datenschutz hat das österreichische Datenschutzgesetz diesem Aspekt eine zentrale Bedeutung gegeben.

Ebenso wie das französische Datenschutzgesetz vom 6. 1. 1978²²⁾ erstreckt das österreichische den Datenschutz auch auf juristische Personen (§ 3 Ziff. 1) — eine Konzeption, die der deutschen Datenschutzgesetzgebung fremd ist.

Das österreichische Datenschutzgesetz umfaßt 59 Paragraphen (HDSG: 39 §§, BDSG: 47 §§, schwedisches Datengesetz 26 §§, französisches Datenschutzgesetz: 48 Artikel), von denen außer § 1 fünf weitere Paragraphen Verfassungsbestimmungen enthalten. Das Gesetz gliedert sich in sieben Abschnitte: Allgemeine Bestimmungen, Bestimmungen für den öffentlichen Bereich, Bestimmungen für den privaten Bereich, internationaler Datenverkehr, Kontrolle des Datenschutzes, Strafbestimmungen, Schlußbestimmungen. Als Hauptdatum des Inkrafttretens bestimmt das Gesetz den 1. Januar 1980; für einige Bestimmungen sind Sonderregelungen getroffen, die sich bis zum 1. Januar 1981 bzw. bis zum 1. Januar 1982 erstrecken. Die aufgrund des Gesetzes zu erlassenden Durchführungsbestimmungen müssen ein halbes Jahr nach Inkrafttreten, also bis zum 1. Juli 1980, ergangen sein.

Der österreichische Gesetzgeber ging, ebenso wie der deutsche, von der Vorstellung aus, daß die möglichen Gefährdungen des Persönlichkeitsrechts des Bürgers durch die elektronische Datenverarbeitung im öffentlichen wie im privaten Bereich gleich hoch zu veranschlagen sind. Das österreichische Gesetz ist daher von der Tendenz bestimmt, „möglichst gleiche Regelungen für den öffentlichen wie für den privaten Bereich vorzusehen“²³⁾. Damit hat sich die in zwei europäischen

Nachbarländern erkennbare Tendenz, entweder im öffentlichen Bereich (Frankreich)²⁴⁾ oder im privaten Bereich (Großbritannien)²⁵⁾ eine größere Gefährdung der schutzwürdigen Belange des Bürgers durch die EDV zu sehen, nicht fortgesetzt.

Ein aus der Sicht des betroffenen Bürgers sicherlich sehr wichtiges Merkmal des österreichischen Datenschutzgesetzes ist, daß es den Datenschutz einheitlich regelt. Dies gilt nicht nur für die Bereiche Privatwirtschaft und öffentliche Verwaltung, sondern auch für alle Verwaltungsebenen, unabhängig davon, „ob die Verarbeitung der personenbezogenen Daten in Behörden oder sonstigen Einrichtungen des Bundes, der Länder, der Gemeinden oder anderer Selbstverwaltungskörper erfolgt“²⁶⁾. Diese — auch in Österreich nicht selbstverständliche — einheitliche Bundeskompetenz für den Datenschutz wird damit begründet, daß „die Vereinheitlichung des Rechtsschutzes, die Verminderung des Kostenaufwandes und die Verhinderung der Aufblähung des Rechtsschutzapparates“ es ratsam erscheinen lasse, „den eigentlichen Datenschutz einer zentralen Bundesbehörde anzuvertrauen“²⁷⁾. Die Interessen der österreichischen Bundesländer sollen dadurch gewährleistet werden, daß sie Mitglieder ihrer Wahl in die Kontrollgremien für Datenschutz entsenden und das Recht erhalten, im Landesbereich in Datenschutzangelegenheiten Durchführungsverordnungen zu erlassen. § 9 des Gesetzes bestimmt demgemäß, daß die obersten Organe des Bundes und der Länder sowie die Selbstverwaltungskörper zum Erlaß von Datenschutzverordnungen aufgrund dieses Gesetzes verpflichtet sind; diese sollen „je nach Art der zu verarbeitenden Daten die Grundsätze für deren Ermittlung, Verarbeitung, Benützung und Übermittlung bei möglichstem Schutz der personenbezogenen Daten festlegen“. Das österreichische System des Datenschutzes überläßt also die Festlegung aller wesentlichen Grundsätze des Datenschutzes dem Bundesgesetzgeber, während es den Ländern und Gemeinden den Erlaß bereichsspezifischer Regelungen für ihre Verwaltungsaufgaben zuweist. Hinsichtlich der Gemeinden bestimmt § 57, daß „von der Gemeinde nach diesem Bundesgesetz durchzuführende Aufgaben solche des eigenen Wirkungsbereiches sind“. Diese Regelung zielt offenbar auf die Garantie der kommunalen Selbstverwaltung.

²¹⁾ Vgl. insbesondere das amerikanische Gesetz über Elternrecht und Datenschutz (Family Educational Rights and Privacy Act of 1974, sog. „Buckley-Amendment“); siehe auch IV, 4.7.3.

²²⁾ Vgl. Art. 4.

²³⁾ Bericht des Verfassungsausschusses a.a.O. Ziff. 5.

²⁴⁾ Vgl. VI, 3.2.1: „Die Regelung der Datenverarbeitung“.

²⁵⁾ Vgl. VI, 3.2.2, vorletzter Absatz.

²⁶⁾ Bericht des Verfassungsausschusses a.a.O., Ziff. 4.

²⁷⁾ Bericht des Verfassungsausschusses a.a.O., Ziff. 4.

Auch für die Kontrolle des Datenschutzes sieht das österreichische Gesetz eine neuartige Lösung vor: Als Kontrollorgan für den öffentlichen Bereich wird eine Datenschutzkommission eingerichtet, die durch einen Datenschutzrat unterstützt wird (§ 35 Abs. 1).

Die Zusammensetzung sowie die Befugnisse und die Arbeitsweise der Datenschutzkommission sind in den §§ 35 bis 41 des Gesetzes geregelt. Die Datenschutzkommission besteht aus vier – auf dem Gebiete des Datenschutzes erfahrenen – Mitgliedern, von denen eines „dem Richterstand angehören“ muß. Die Mitglieder der Kommission werden auf Vorschlag der Bundesregierung vom Bundespräsidenten für die Dauer von fünf Jahren bestellt und können wiederbestellt werden. Bei Vorbereitung des Vorschlags der Bundesregierung hat der Bundeskanzler zwei Mitglieder von den Bundesländern zu berücksichtigen, eins aus dem Kreise der rechtskundigen Bundesbeamten und für das richterliche Mitglied den Vorschlag des Präsidenten des obersten Gerichtshofes. Regierungsmitglieder auf Bundes- und Landesebene sowie Staatssekretäre und Personen, die mit der Verarbeitung von Daten „unmittelbar befaßt sind“ und solche, die zum Nationalrat nicht wählbar sind, können der Datenschutzkommission nicht angehören (§ 38 Abs. 1 bis 5). Den Vorsitz in der Datenschutzkommission führt das richterliche Mitglied; dessen Stellvertreter wird von der Kommission gewählt (§ 39 Abs. 1). Die Mitglieder der Datenschutzkommission sind in Ausübung ihres Amtes unabhängig und an keine Weisungen gebunden (§ 40).

Die Geschäftsführung der Datenschutzkommission obliegt dem Bundeskanzleramt, das auch das notwendige Personal zur Verfügung zu stellen hat (§ 35 Abs. 2). Die Kommission, die „neben den Gerichten“²⁸⁾ und dem Datenschutzrat zur Prüfung der Einhaltung der Bestimmungen des Datenschutzgesetzes berufen ist, hat – im Gegensatz zur bisher überwiegenden Regelung bei Datenschutz-Kontrollorganen – eigene Exekutivbefugnisse. So hat sie „nicht nur die Aufgabe, Bescheide aufgrund von Beschwerden einzelner zu erlassen; ihr kommen auch Befugnisse genereller Art (z. B. Zustimmung zu Betriebsordnungen und in Verfahren vor anderen Behörden zu: Strafantragsrecht)“²⁹⁾. Da die Kommission anderen Behörden gegenüber Anweisungen erteilen kann (z. B. § 15 Abs. 2, § 37 Abs. 1 und 2, § 50 Abs. 5), unterliegen ihre Entscheidungen der gerichtlichen Kontrolle.

Gegen sie ist die Beschwerde an den Verwaltungsgerichtshof zulässig (§ 36 Abs. 4).

Einen Tätigkeitsbericht verfaßt die Datenschutzkommission „jedes zweite Jahr“ (§ 46 Abs. 1) und übermittelt ihn dem Bundeskanzler. Dieser legt ihn „mit einer Stellungnahme der Bundesregierung und des Datenschutzrates“ (§ 46 Abs. 2) dem Nationalrat vor.

Der Datenschutzrat ist als „politisches Beobachtungsorgan“ gedacht, „das die Verwaltung, den Gesetzgeber und die Öffentlichkeit aufmerksam machen soll auf weitere Gefährdungen der Privatsphäre und auf die Notwendigkeit der Ergänzung des Rechtsschutzes“³⁰⁾. Insbesondere hat der Datenschutzrat die Aufgabe, Auskünfte und Berichte über Fragen des Datenschutzes bei der Datenverarbeitung im öffentlichen Bereich von den zuständigen Organen zu verlangen, die Auswirkungen der EDV „insbesondere auf Achtung des Privat- und Familienlebens“ zu beobachten, Anregungen zur Verbesserung des Datenschutzes zu geben und auf Anregung eines Vertreters der politischen Parteien „Fragen von grundsätzlicher Bedeutung für den Datenschutz in Beratung zu ziehen“ (§ 42). Dem Datenschutzrat gehören an: Vertreter der politischen Parteien, je ein Vertreter des Gemeindebundes und des Städtebundes, ein vom Bundeskanzler zu ernennender Vertreter des Bundes. Die Mitglieder des Datenschutzrates sind ehrenamtlich tätig (§ 43). Der Datenschutzrat faßt seine Beschlüsse mit einfacher Mehrheit der abgegebenen Stimmen, wobei die Beifügung von Minderheitenvoten zulässig ist. Die Mitglieder der Datenschutzkommission können den Sitzungen des Datenschutzrates ohne Stimmrecht beiwohnen (§ 44).

Für den privaten Bereich soll „das dem Betroffenen nächste Landesgericht“³¹⁾ entscheiden, ob dieser, „unbeschadet etwaiger Ansprüche auf Schadenersatz, Anspruch auf Unterlassung und Beseitigung des diesem Bundesgesetz oder den aufgrund dieses Bundesgesetzes erlassenen Durchführungsbestimmungen widerstreitenden Zustandes“ hat (§ 28 Ziff. 2). Eine Begünstigung seiner prozessualen Stellung wird dem Betroffenen durch eine Bestimmung in § 29 eingeräumt. Danach hat die Datenschutzkommission, wenn es „zur Wahrung der nach diesem Bundesgesetz geschützten Interessen des Datenschutzes und einer größeren Zahl von Betroffenen geboten ist, auf Verlangen eines der Betroffenen dem Rechtsstreit auf seiten der Betroffenen als Nebenintervenient (§§ 17 ff. ZPO) beizutreten“ (§ 29 Abs. 3).

²⁸⁾ Bericht des Verfassungsausschusses a.a.O. zum 5. Abschnitt.

²⁹⁾ Bericht des Verfassungsausschusses a.a.O. zum 5. Abschnitt.

³⁰⁾ Bericht des Verfassungsausschusses a.a.O., Ziff. 7.

³¹⁾ Bericht des Verfassungsausschusses a.a.O., Ziff. 9.

Es wird sich zu erweisen haben, ob diese Regelung der Datenschutzkontrolle im privatwirtschaftlichen Bereich der Forderung des Datenschutzgesetzes Rechnung trägt, das Persönlichkeitsrecht des Bürgers im öffentlichen wie im privaten Bereich gleich wirksam zu schützen³²⁾. Auch die Frage, ob die erleichterte Erlangung einer einstweiligen Verfügung (§ 30) der Notwendigkeit eines präventiven Datenschutzes genügen kann, läßt sich heute noch nicht beantworten. Wegen der großen Bedeutung der Präventivfunktion des Datenschutzes ist die Übertragung der Datenschutzkontrolle an die Gerichte eine Frage, die seit Beginn der Datenschutzdiskussion kontrovers diskutiert wird.

Der Anwendungsbereich des Gesetzes umfaßt jegliche Form der „automationsunterstützten Verarbeitung personenbezogener Daten“, wobei es ausreicht, daß Daten „im oder für den automationsunterstützten Datenverkehr“ verarbeitet werden (§ 3 Ziff. 6). Entsprechend der bei der Datenverarbeitung häufig gegebenen Arbeitsteilung zwischen dem „Auftraggeber“³³⁾ und dem „Verarbeiter“³⁴⁾ trennt das Gesetz die Verantwortlichkeit in der Weise, daß der Schwerpunkt der Verantwortung des Auftraggebers bei der rechtlichen Zulässigkeit der einzelnen Phasen der Verarbeitung, also im Bereich des eigentlichen Datenschutzes liegt³⁵⁾, beim Verarbeiter (Rechenzentrum) hingegen auf dem Gebiet der Datensicherung.

Um die für den Bürger notwendige Transparenz zu erreichen, erlegt das Gesetz dem Auftraggeber verschiedene Pflichten auf, je nachdem, ob er dem öffentlichen oder dem privaten Bereich angehört. Sie beginnen „vor Aufnahme der Echtverarbeitung“³⁶⁾, also nach Abschluß von Prüfläufen mit fingierten Daten. Der öffentliche Auftraggeber hat gemäß § 8 dem Datenverarbeitungsregister eine schriftliche Meldung zu erstatten, in der „die Rechtsgrundlage, der Zweck der Ermittlung, der Verarbeitung und der Übermittlung der Daten, die Art der Daten und der Kreis der Betroffenen anzugeben“ (§ 8 Abs. 2) sind. Im privaten Bereich wird – ähnlich wie im BDSG – unterschieden nach Verarbeitung für eigene oder fremde Zwecke. Wer

für eigene Zwecke Daten von Personen verarbeitet, „die mit dem Auftraggeber dieser Verarbeitung in einem Vertragsverhältnis stehen oder gestanden sind“, hat den Betroffenen „darüber ausdrücklich deutlich lesbar zu informieren; dasselbe gilt für Vereine hinsichtlich der Daten ihrer Mitglieder“ (§ 22 Abs. 1). Auftraggeber, die ohne eine solche Vertragsbeziehung (§ 22) Daten verarbeiten wollen, haben beim Datenverarbeitungsregister vor der Aufnahme der Echtverarbeitung von Daten „die Registrierung zu beantragen“ (§ 23 Abs. 1). Schließlich hat der „im Rahmen einer Dienstleistung (§ 19) tätige Verarbeiter“ – also das Rechenzentrum – grundsätzlich vor der erstmaligen Übernahme von Verarbeitungen die Registrierung beim Datenverarbeitungsregister zu beantragen (§ 23 Abs. 3).

Der Transparenz der Datenverarbeitung dient auch das Datenverarbeitungsregister. Es wird beim Österreichischen Statistischen Zentralamt eingerichtet, das dieses nach den Anordnungen des Bundeskanzlers führt (§ 47 Abs. 1). Der Antrag auf Registrierung einer Datenverarbeitung hat außer Name und Anschrift des Auftraggebers die gesetzlichen Bestimmungen, behördlichen Bescheide oder sonstigen Vorschriften, aus denen sich der berechtigte Zweck des Rechtsträgers ergibt (§ 17), anzugeben, außerdem den Zweck der Verarbeitung, die Art der zu verarbeitenden Daten und den Kreis der Betroffenen und schließlich eine Aussage darüber, ob und welcher Art und an welchen Kreis von Empfängern Übermittlungen vorgesehen sind. Die Registrierung ist vom Datenverarbeitungsregister innerhalb von sechs Wochen vorzunehmen, es sei denn, daß es Bedenken gegen die Rechtmäßigkeit hat. In diesem Fall ist der Akt der Datenschutzkommission zu übermitteln, die entweder die Registrierung bescheidmäßig abzulehnen oder mitzuteilen hat, daß keine Bedenken gegen die Registrierung bestehen. Eine Ablehnung hat zu erfolgen, wenn „die beabsichtigte Verarbeitung einer behördlichen Bewilligung nach dem Vierten Abschnitt³⁷⁾ bedürfte und diese nicht erteilt ist, oder der Antrag unvollständig ist und dieser Mangel binnen angemessener Frist nicht behoben wird“ (§ 23 Abs. 5). Auch wenn eine Registrierung vorgenommen wurde, bleibt es den Gerichten in einem späteren Verfahren unbenommen, „die Rechtmäßigkeit der Datenverarbeitung im generellen oder im konkreten zu überprüfen“³⁸⁾. Beim Erlass der Verordnung über die Registerführung hat der Bundeskanzler u.a. „auf die Einfachheit der Einsichtnahme in das Register“ Bedacht zu nehmen (§ 47 Abs. 3).

³²⁾ Bericht des Verfassungsausschusses a.a.O., Ziff. 5.

³³⁾ Dem „Auftraggeber“ entspricht nach der Terminologie des HDSG (BDSG) die „speichernde Stelle“ (§ 2 Abs. 3 HDSG), d. h., die Behörde oder öffentliche Stelle, die Daten selbst verarbeitet oder verarbeiten läßt.

³⁴⁾ Dem „Verarbeiter“ entspricht nach unserer Terminologie der Anwender (Auftragnehmer, § 4 HDSG).

³⁵⁾ Bericht des Verfassungsausschusses a.a.O., Ziff. 6.

³⁶⁾ Bericht des Verfassungsausschusses a.a.O. zu § 10 Abs. 3.

³⁷⁾ „Internationaler Datenverkehr – Voraussetzungen für Überlassungen von Daten in das Ausland“.

³⁸⁾ Bericht des Verfassungsausschusses a.a.O. zu § 23.

Bei der Regelung der Zulässigkeit der Datenverarbeitung und der Übermittlung ist eine gewisse Ähnlichkeit mit der Regelung im HDSG (bzw. im BDSG) festzustellen: Im öffentlichen Bereich dürfen Daten nur aufgrund einer ausdrücklichen gesetzlichen Ermächtigung oder soweit dies zur Wahrnehmung der dem Auftraggeber gesetzlich übertragenen Aufgabe eine wesentliche Voraussetzung bildet, ermittelt und verarbeitet werden (§ 6). Für die Übermittlung ist darüber hinaus die ausdrückliche – widerrufbare – schriftliche Zustimmung des Betroffenen oder die Anonymisierung der zu übermittelnden Daten Zulässigkeitsvoraussetzung (§ 7). Im privaten Bereich ist die Ermittlung und Verarbeitung zulässig, „soweit sich dies in Art und Umfang auf den berechtigten Zweck des Rechtsträgers beschränkt und hierbei schutzwürdige Interessen des Betroffenen, insbesondere im Hinblick auf Achtung seines Privat- und Familienlebens, beachtet werden“ (§ 17). Die Übermittlung im privaten Bereich ist neben der ausdrücklichen schriftlichen Zustimmung dann zulässig, wenn die Übermittlung zum berechtigten Zweck des Rechtsträgers gehört oder zur Wahrung überwiegender berechtigter Interessen eines Dritten notwendig ist oder die Daten entsprechend anonymisiert worden sind (§ 18).

Als Rechte des Bürgers gegenüber der automatisierten Datenverarbeitung gewährt § 1 – außer dem in Abs. 1 bestimmten Grundrecht auf Datenschutz – jedermann, ähnlich wie das HDSG (BDSG), ein Recht auf Auskunft, ein Recht auf Richtigstellung unrichtiger und ein Recht auf Löschung unzulässigerweise ermittelter oder verarbeiteter Daten. Das Recht auf Auskunft umfaßt – weitergehend als das HDSG (BDSG) – nicht nur den Inhalt der gespeicherten Daten, sondern auch Angaben darüber, wer Daten über den Betroffenen ermittelt oder verarbeitet, woher die Daten stammen und wozu sie verwendet werden (§ 1 Abs. 3). Für den öffentlichen Bereich bestimmt § 11, daß dem Betroffenen „seine Daten in allgemein verständlicher Form sowie deren Herkunft und die Rechtsgrundlage für deren Ermittlung, Verarbeitung, Benutzung und Übermittlung binnen 4 Wochen schriftlich mitzuteilen“ sind. Ausgenommen davon sind solche Daten, „die aufgrund eines Gesetzes oder einer Verordnung bei überwiegendem öffentlichen Interesse auch im gegenüber geheimzuhaltenden sind“³⁹⁾. Ein pauschalier-

ter Kostenersatz kann für die Erteilung einer Auskunft vorgeschrieben werden (§ 11 Abs. 3).

Hinsichtlich des Berichtigungs- und des Löschungsrechts des Betroffenen im öffentlichen Bereich ist es interessant, daß der Beweis der Richtigkeit der Daten dem Auftraggeber obliegt (§ 12 Abs. 5). Auch muß der Auftraggeber die Empfänger solcher Daten benachrichtigen, die vor der Richtigstellung oder Löschung übermittelt worden sind (§ 12 Abs. 7). Die Richtigstellung oder Löschung ist nicht nur auf begründeten Antrag des Betroffenen durchzuführen, sondern ist in bestimmten Fällen auch von Amts wegen, aufgrund einer Entscheidung der sachlich zuständigen Behörde, aufgrund einer Entscheidung der Datenschutzkommission oder aufgrund einer Entscheidung des Verwaltungsgerichtshofes möglich (§ 12 Abs. 2).

Auch im privaten Bereich kann ein Betroffener „bei Nachweis seiner Identität beim Auftraggeber Auskunft über die zu seiner Person gespeicherten Daten und über deren Herkunft“ sowie bei Übermittlung auch über die Empfänger verlangen (§ 25 Abs. 1). Auch hier ist die Auskunft binnen 4 Wochen schriftlich in allgemein verständlicher Form zu erteilen, „sofern der Betroffene nicht mit einer mündlichen Auskunft einverstanden ist“. Ein über die notwendigen Kosten nicht hinausgehendes Entgelt darf für die Auskunft verlangt werden. Beim Berichtigungsrecht ist auf Verlangen des Betroffenen wegen von ihm bestrittener Daten, über deren Richtigkeit keine Einigung erzielt werden kann, „ein Vermerk über die Bestreitung beizufügen. Dieser Vermerk darf ohne Zustimmung des Betroffenen nur aufgrund eines rechtskräftigen Urteils gelöscht werden“ (§ 26 Abs. 2). Für die Löschung bestimmt § 27, daß Daten, die rechtswidrig erfaßt oder gespeichert oder für die Erfüllung der Zwecke der Verarbeitung nicht mehr erforderlich sind, gelöscht werden müssen, es sei denn, daß „überwiegende berechnete Interessen des Auftraggebers, eines Dritten oder gesetzliche Aufbewahrungspflichten entgegenstehen“.

Zur Geltendmachung seiner Rechte dient dem Bürger zunächst der Einblick in das Datenverarbeitungsregister (§ 47 Abs. 2), der jedermann zusteht; darüber hinaus kann er sich zur Verfolgung seiner ihm nach dem Datenschutzgesetz für den öffentlichen Bereich zustehenden Rechte an die Datenschutzkommission wenden (§ 14). „Soweit Rechtsträger in Formen des Privatrechts tätig sind, ist das Grundrecht auf Datenschutz im ordentlichen Rechtsweg geltend zu machen (§ 1 Abs. 6).“ Einen besonderen Unterlassungsanspruch gibt das Datenschutzgesetz dem Betroffenen in § 28, während das zivilgerichtliche Verfahren und die Möglichkeit einstweiliger Verfügungen

³⁹⁾ Diese Ausnahme gilt insbesondere: „1. für Zwecke des Schutzes der verfassungsmäßigen Einrichtungen der Republik Österreich und für Zwecke der Strafrechtspflege oder 2. für Zwecke der Sicherung der Einsatzbereitschaft des Bundesheeres oder 3. für Zwecke der umfassenden Landesverteidigung“ (§ 3).

in §§ 29 und 30 geregelt sind. Schadenersatzbestimmungen sind im österreichischen Datenschutzgesetz nicht enthalten. Wie eine Reihe anderer Datenschutzgesetze enthält auch das österreichische Datenschutzgesetz Strafbestimmungen (§§ 48 bis 50), die zwei besondere Straftatbestände, „Geheimnisbruch“ und „unbefugte Eingriffe in die Verarbeitungen“ enthalten, sowie eine Verwaltungsstrafbestimmung. Die Höchststrafen sind Freiheitsstrafe bis zu einem Jahr bzw. Geldstrafe bis zu 150 000 Schilling.

Der wachsenden Bedeutung des grenzüberschreitenden Datenverkehrs entsprechend enthält das Gesetz einen Abschnitt „internationaler Datenverkehr“. Nach den Bestimmungen der §§ 32 bis 34 ist grundsätzlich nur unter den für den öffentlichen bzw. privaten Bereich bestimmten Zulässigkeitsvoraussetzungen eine Überlassung von automationsunterstützt verarbeiteten Daten aus Österreich in das Ausland zulässig. Sie bedarf der Genehmigung der Datenschutzkommission (§ 32 Abs. 1). Die Genehmigung kann versagt werden, wenn öffentliche Interessen einschließlich völkerrechtlicher Verpflichtungen entgegenstehen oder wenn glaubhaft gemacht wird, daß durch die Überlassung in das Ausland schutzwürdige Interessen des Betroffenen beeinträchtigt werden (§ 32 Abs. 3). Die Verarbeitung von Daten in Österreich für ausländische Rechtsträger ist dem Datenverarbeitungsregister zu melden (§ 33).

Insgesamt erweist sich das österreichische Datenschutzgesetz als ein modernes, bürgerfreundliches Gesetz, dem zugute gekommen ist, daß seine „Väter“ die aus der internationalen Datenschutzdiskussion vorhandenen Erfahrungen genutzt und zu einer sorgfältig abgewogenen Regelung verwendet haben.

3.4 Schweden

Das Schwedische Datalag vom 11. Mai 1973 (SFS 1973: 289)⁴⁰⁾ war das erste Datenschutzgesetz auf nationaler Ebene. Da es – ähnlich wie das Hessische Datenschutzgesetz vom 7. Oktober 1970 für den Bereich eines Bundeslandes – als Vorstoß in gesetzgeberisches Neuland eine Pionierleistung war, wurde bereits bei seiner Vorlage im Reichstag die Feststellung getroffen, das Gesetz werde in naher Zukunft zu ergänzen und entsprechend der dann vorliegenden Erfahrung abzuändern sein. Aus diesem Grunde wurde im Mai 1976 ein Ausschuß für Datenschutzgesetzgebung (DALK) gebildet, der um die Jahreswende 1976/77 seine Arbeit aufnahm. Vor wenigen Wo-

chen hat DALK einen 20 Kapitel umfassenden Bericht in der Art eines Weißbuches vorgelegt, der gegenwärtig den zuständigen Ressorts zur Stellungnahme vorliegt. Er soll anschließend der Regierung übermittelt werden⁴¹⁾. Die genaue Aufgabenstellung von DALK ergibt sich aus dem ersten Kapitel des Berichts.

Die auch für die deutsche Datenschutzdiskussion interessanten Erkenntnisse des Berichts werden nachstehend kurz wiedergegeben, wobei aus Raumgründen nicht alle Kapitel behandelt werden können.

Kapitel 2 behandelt die bisherige Tätigkeit der Datenschutzbehörde (Datainspektionen), einer zentralen (nationalen) Verwaltungsbehörde mit der Aufgabe, Genehmigungen für „Personenregister“ zu erteilen und die Datenschutzkontrolle nach dem Datengesetz auszuüben⁴²⁾. In den ersten vier Jahren ihrer Tätigkeit hatte die Datainspektion rund 20 000 Fälle zu entscheiden, von denen 18 000 erledigt werden konnten; nur in 40 Fällen wurde gegen die Entscheidung der Datenschutzbehörde Berufung eingelegt⁴³⁾. Es hat sich erwiesen, daß etwa 65% der Genehmigungsanträge im sog. vereinfachten Verfahren („förenklade förfarandet“) entschieden werden. Das restliche Drittel von Genehmigungsanträgen, die im Detail geprüft werden mußten, hat einen relativ hohen Arbeits- und Zeitaufwand erfordert. Dies liegt vor allem daran, daß eine Beeinträchtigung („intrång“), der persönlichen Integrität registrierter Personen meist nur im Einzelfall unter Prüfung der Ausgestaltung des geplanten Registers festgestellt werden kann⁴⁴⁾. DALK ist der Auffassung, daß mit Hilfe der EDV geführte Personenregister auch weiterhin besonderen Bestimmungen unterworfen sein müssen; das Datengesetz sei mit einigen Ergänzungen und Abänderungen durchaus in der Lage, auch für die absehbare Zukunft diese Forderung zu erfüllen. Auf lange Sicht werde allerdings zu prüfen sein, ob eine allgemeinere Datenschutzgesetzgebung einschließlich bereichsspezifischer Regelungen für bestimmte Verfahren das Datengesetz ablösen solle. Entsprechende Überlegungen müßten auch das Arbeitsrecht, insbesondere das Gebiet der Mitbestimmung, und einige Fragen der Datensicherung einbeziehen⁴⁵⁾. DALK weist mit Blick auf mögliche Änderungen und Ergänzungen

⁴⁰⁾ Vgl. II, 2.3.5; III, 2.3.5.

⁴¹⁾ Eine Zusammenfassung des Berichts ist bereits zugänglich: „Sammanfattning“, SOU 1978: 54; eine englische Übersetzung ist ebenfalls erhältlich.

⁴²⁾ Vgl. III, 2.3.5; IV, 2.2.2; V, 3.2; VI, 3.2.4.

⁴³⁾ Vgl. § 25 des Datengesetzes.

⁴⁴⁾ Bericht a.a.O., Ziff. 22.3, S. 311.

⁴⁵⁾ Bericht a.a.O., Ziff. 22.2, S. 310.

des bestehenden Datengesetzes jedoch auch darauf hin, daß dies unter Umständen eine Neuprüfung der bisher bereits abgeschlossenen rund 20 000 Genehmigungsverfahren bedeuten könnte (Kap. 3).

Kapitel 4 behandelt Fragen der Datenschutzkontrolle über Behördenregister, was — angesichts der nicht vergleichbaren Behördenorganisation — nur wegen der Nachricht von Interesse ist, daß sich offenbar Datenschutzprobleme im Zusammenhang mit dem Prinzip der Aktenöffentlichkeit ergeben haben⁴⁶⁾. Gesetzesänderungen werden jedoch von DALK nicht für erforderlich gehalten.

Bei seiner Untersuchung über die das Genehmigungsverfahren beherrschenden Grundsätze hat DALK überprüft, ob zur Entscheidung über die Frage einer möglichen Gefährdung der persönlichen Integrität zusätzliche allgemeine und selbständige Kriterien aufgestellt werden können. Das Ergebnis ist bemerkenswert: DALK ist der Auffassung, daß Daten, die für einen bestimmten Zweck erhoben worden sind, grundsätzlich nicht für andere, sich später ergebende Zwecke, verwendet werden dürfen („inte få utnyttjas“).

Dieser Grundsatz soll auch gelten, wenn dadurch „die Vorteile der EDV nicht voll und ganz ausgenutzt“ werden können⁴⁷⁾. Die Härte dieser Aussage überrascht, zumal der Bericht an mehreren Stellen die Vorteile der EDV lobend hervorhebt. Der Grundsatz steht allerdings im Einklang mit einer Forderung, die mein Amtsvorgänger schon frühzeitig erhoben hatte: „Personenbezogene Informationen, die zweckgebunden gegeben worden sind, dürfen ohne Zustimmung des Betroffenen nicht für andere Zwecke verwendet oder weitergegeben werden“⁴⁸⁾. Das Hessische Datenschutzgesetz vom 30. Januar 1978 hat diesem Grundsatz wegen der Angleichung an die Formulierungen des BDSG nur unvollkommen Rechnung getragen: Zwar findet sich der Passus „... zur Erfüllung des gleichen Zweckes“ in den Bestimmungen über die Zulässigkeit der weiteren Übermittlung von Daten innerhalb des öffentlichen Bereichs (§ 12 Abs. 1 S. 2 HDStG), jedoch ist bei der ersten Übermittlung gespeicherter Daten — weder innerhalb noch außerhalb des öffentlichen Bereichs — der Grundsatz der Zweckbindung der Information berücksichtigt worden.

⁴⁶⁾ Dies ist ein bereits seit rund 200 Jahren in Schweden geltender Verfassungsgrundsatz, der es dem Bürger erlaubt, grundsätzlich alle bei Behörden geführten Akten einzusehen.

⁴⁷⁾ Bericht a.a.O., Ziff. 2.2.6 S. 313.

⁴⁸⁾ Vgl. „10 Gebote einer Datenverkehrsordnung“ — IV — Anlage I, Ziff. 7.

Dieser Grundsatz der Zweckbindung sollte nach Ansicht von DALK eines der Kriterien bilden, welche die Datainspektion bei der Entscheidung über Genehmigung zu berücksichtigen hat (Kap. 5). Dementsprechend hat der Ausschuß eine Ergänzung zu § 3 des Datalag vorgeschlagen: Es soll nach wie vor zulässig sein, ein Personenregister einzurichten, wenn unter Beachtung der zu erwartenden Auflagen die persönliche Integrität der Betroffenen nicht beeinträchtigt wird; dabei ist über den Tatbestand der Beeinträchtigung der persönlichen Integrität von Fall zu Fall zu entscheiden. Bei der Entscheidung über die Genehmigung ist zu beachten, ob der Zweck des Registers mit den Aufgaben der registerführenden Stelle vereinbar ist⁴⁹⁾.

Statt der im bisherigen Gesetz enthaltenen Bedürfnisprüfung für die Genehmigung eines Personenregisters schlägt DALK vor, das öffentliche Interesse an der Einrichtung des Registers zu prüfen (Kap. 6). Es begründet diese Ansicht damit, daß nur das öffentliche Interesse durch gesetzliche Bestimmungen genau abgrenzbar sei. Die bisherige Lösung habe zwar den Vorzug größerer Flexibilität, verleihe aber der Datainspektion Entscheidungsbefugnisse, die „eigentlich der Legislative vorbehalten sein sollten“⁵⁰⁾.

Besonders eingehend hat sich DALK mit der Datenübermittlung beschäftigt, insbesondere mit der durch eine Verbindung („samkörning“) von Personenregistern bewirkten Gefährdung der persönlichen Integrität (Kap. 7). Der Bericht verweist darauf, daß in diesem Zusammenhang Überlegungen angestellt worden seien, die Benutzung des — in Schweden bestehenden — Personenkennzeichens⁵¹⁾ für Personenregister einzuschränken oder ganz darauf zu verzichten⁵²⁾. DALK kommt jedoch zu dem Ergebnis, daß ein Verzicht auf das Personenkennzeichen in Personenregistern kein entscheidendes Hindernis für die Verbindung solcher Register sein würde. Nur vorübergehend würde dadurch eine Zusammenführung von Daten aus verschiedenen Registern technisch etwas erschwert. Aus diesem Grund wird eine Einschränkung oder ein Verzicht auf das Personenkennzeichen nicht empfohlen; nach Meinung des Ausschusses sollte allerdings der Frage der Datenübermittlung mehr Aufmerksamkeit zugewendet werden.

Besondere Beachtung hat DALK der Einrichtung von Einwohnerzentralregistern („befolkningsregi-

⁴⁹⁾ Bericht a.a.O., Ziff. 22.6, S. 314.

⁵⁰⁾ Bericht a.a.O., Ziff. 22.7, S. 315.

⁵¹⁾ Vgl. VI, 3.2.4.1.

⁵²⁾ Bericht a.a.O., Ziff. 22.8, S. 316.

ster“) zugewendet. Die Notwendigkeit, aus Datenschutzgründen die Anzahl flächendeckender (totaler) Personenregister⁵³⁾ zu begrenzen, hatte zu einer vorläufigen Ergänzung des Datengesetzes geführt. Das Gesetz enthält jetzt besondere Bestimmungen über Personenregister, die einen großen Teil der Bevölkerung des gesamten Landes oder einer Region umfassen. Der Bericht akzeptiert zwar die Begründung für die Gesetzesergänzung, vertritt jedoch die Ansicht, daß bei der bestehenden Behördenorganisation diese vorläufige Novellierung nicht zum gewünschten Erfolg führen werde⁵⁴⁾.

In der schwedischen Datenschutzdebatte war gefordert worden, für verschiedene besonders sensitive Daten (z. B. Rasse) strengere Bestimmungen zu erlassen. DALK weist zwar darauf hin, daß die „Sensitivität“ der Daten von dem Zusammenhang abhängt, in dem sie verwendet werden (sog. „Kontextbezogenheit“). Der Bericht schlägt jedoch vor, § 6 des Datengesetzes um einen dritten Absatz zu ergänzen, welcher es der Datenschutzbehörde ermöglicht, bei der Prüfung von Genehmigungsanträgen besonders darüber zu wachen, ob das beantragte Personenregister Daten enthält, die eine Wertung oder Einschätzung der betroffenen Personen darstellen.

Auch mit der Notwendigkeit, für Forschung und Statistik besondere Bestimmungen zu schaffen, hat sich DALK ausführlich (in Kap. 12) auseinandergesetzt. Zwar sei insbesondere von der empirischen Sozialforschung die Befürchtung erhoben worden, der Datenschutz gefährde die Freiheit und Unabhängigkeit der Wissenschaft; jedoch müsse der Ausgangspunkt für eine Regelung sein, daß die Forschung, wie jede andere Tätigkeit auch, „mit dem notwendigen Respekt vor der Privatsphäre des einzelnen betrieben wird“⁵⁵⁾. DALK ist der Auffassung, daß Personenregister, die für Forschung und Statistik angelegt werden, denselben Bestimmungen wie andere genehmigungsbedürftige Register unterworfen sein sollen. Die Genehmigung von Forschungsregistern im vereinfachten Verfahren könne nicht in Frage kommen, da diese häufig besonders sensitive Daten enthielten. Es bedürfe auch keiner zusätzlichen Bestimmung für die Genehmigung von Forschungsregistern. Allerdings regt DALK an zu prüfen, ob nicht die Datenschutzbehörde zusammen mit Vertretern der Forschung und der Statistik ein ständiges Organ schaffen sollte, das The-

men von gemeinsamen Interesse erörtert. Das Gremium müsse sich jedoch auf einen beratenden Status beschränken; die Entscheidung über Genehmigung für Forschungsregister müsse nach wie vor allein der Datainspektion zustehen⁵⁶⁾.

Die in § 10 des Datengesetzes enthaltene Verpflichtung für den Registerführer, den Personen, deren Daten gespeichert sind, auf Antrag einmal im Jahr Auskunft über diese Daten zu geben, hielt der Bericht für ausreichend; er bedürfe keiner Ausdehnung (Kap. 14).

Im letzten Kapitel seines Berichts (Kap. 20) vertritt DALK die Auffassung, daß die Zusammenhänge zwischen dem Prinzip der Aktenöffentlichkeit und den Forderungen des Datenschutzes untersucht werden sollten.

Insgesamt wird aus dem Bericht von DALK deutlich, daß das Datenschutzbewußtsein in der öffentlichen Diskussion Schwedens einen breiteren Raum einnimmt als in der Bundesrepublik Deutschland. Dieser Eindruck verstärkte sich auch in Gesprächen, die im Berichtszeitraum mit Vertretern der Datenschutzbehörde, des statistischen Zentralamtes und des Statskontor (Amt für Verwaltungsentwicklung) geführt wurden. Im Hinblick auf die relativ lange Datenschutzpraxis der schwedischen Stellen erweist sich dieser Erfahrungsaustausch als besonders wertvoll.

3.5 Europarat

Am 28. März 1977 besuchte eine Expertengruppe des Europarats unter Führung des Leiters der Abteilung Öffentliches Recht den Hessischen Datenschutzbeauftragten. Die Mitglieder der Gruppe, die aus Fachleuten des Einwohnermeldewesens von 17 europäischen Ländern bestand, wollte sich über die Datenschutzgesetzgebung in der Bundesrepublik informieren. Dabei interessierten sie sich insbesondere für die Praxis und Erfahrungen mit dem Hessischen Datenschutzgesetz und die Probleme der Datenübermittlung im Bereich des Meldewesens.

Da sich anlässlich dieses Besuches gezeigt hat, wie nützlich der gewonnene unmittelbare Eindruck und die dabei gegebenen Vergleichsmöglichkeiten für die Arbeit auf der europäischen Ebene sind, habe ich dem Europarat gegenüber meine Bereitschaft erklärt, von Zeit zu Zeit Fachleuten und Parlamentariern die Arbeit des Hessischen Datenschutzbeauftragten an Ort und Stelle zu erläutern. Von diesem Angebot machte eine Gruppe europäischer Parlamentarier am 30. November 1978 Gebrauch.

⁵³⁾ Bericht a.a.O., Ziff. 22.9, S. 319.

⁵⁴⁾ Bericht a.a.O., Ziff. 22.9, S. 318 bis 320.

⁵⁵⁾ Bericht a.a.O., Ziff. 22.13, S. 324.

⁵⁶⁾ Bericht a.a.O., Ziff. 22.13, S. 353.

4. EINWOHNERWESEN

4. Einwohnerwesen

4.1 Novellierung des Hessischen Meldegesetzes

Zusammen mit dem neuen Hessischen Datenschutzgesetz vom 31. Januar 1978 trat am 8. Februar 1978 der neu geschaffene § 16 a des Hessischen Meldegesetzes (HMG) in Kraft. Für die Übermittlung von Daten aus dem Einwohnermeldewesen ist er eine Spezialvorschrift, die den Vorschriften des Hessischen Datenschutzgesetzes (HDSG) über die Datenübermittlung gemäß § 35 HDSG vorgeht. § 16 a HMG beschränkte die Datenübermittlung aus dem Einwohnerwesen auf Name, akademischen Grad und Anschrift und verlangte für die Auskunft über eine Vielzahl von Personen ein öffentliches Interesse. Diese starre Regelung führte — wovon der Hessische Datenschutzbeauftragte während der Beratungen des Entwurfs für ein neues Hessisches Datenschutzgesetz gewarnt hatte — zu einer aus der Sicht der Verwaltung, der politischen Parteien und des Datenschutzes gleichermaßen unbefriedigenden Situation: Infolge der Beschränkung der zulässigen Datenübermittlung aus dem Einwohnermeldewesen auf Name, akademischen Grad und Adresse war es nicht mehr zulässig, auch das Alter oder Geburtsdatum eines Bürgers als Kriterium für die Übermittlung zu benutzen. Infolgedessen konnten z. B. Gemeinden keine sog. Jubiläumsdaten mehr veröffentlichen bzw. an die örtliche Presse oder an Abgeordnete übermitteln; die politischen Parteien konnten keine sog. Jung- oder Erstwählerdaten mehr bekommen, und karitative Organisationen durften keine Adressen von sog. Senioren mehr erhalten. Den Hessischen Datenschutzbeauftragten erreichten eine Vielzahl von Beschwerden von Gemeinden, Abgeordneten, politischen Parteien, karitativen Verbänden und nicht zuletzt von den betroffenen Bürgern selbst. Rasche Abhilfe erschien notwendig. Mit Schreiben vom 5. Juni 1978 legte ich daher dem Landtag einen Zwischenbericht⁵⁷⁾ vor, in dem auf die auch aus der Sicht des Datenschutzes negativen Auswirkungen der Neuregelung von § 16 a HMG hingewiesen und Vorschläge für die Regelung der Datenübermittlung aus dem Einwohnermeldewesen gemacht wurden.

Nach meinen wiederholt gemachten Vorschlägen⁵⁸⁾ sollte eine Neuregelung der Datenübermittlung

im Einwohnermeldewesen auf der Grundlage eines dem Bürger zustehenden Rechts auf Auskunftssperre vorgenommen werden. Eine dem Selbstbestimmungsrecht des Bürgers entsprechende Regelung der Datenübermittlung muß sich „aus einer zwischen den Interessen der Allgemeinheit und den Interessen des einzelnen abgewogenen, differenzierenden Regelung der Datenübermittlung ergeben“. Dabei sollte „das Selbstbestimmungsrecht des Bürgers über seine Daten grundsätzlich an erster Stelle stehen. Nur wenn er zum Ausdruck bringt, daß er im Einzelfall mit der Übermittlung seiner Daten an Stellen außerhalb des öffentlichen Bereichs einverstanden ist, sollte bei Nachweis des „öffentlichen Interesses“ bzw. des „berechtigten Interesses“ eine Datenübermittlung zulässig sein“⁵⁹⁾.

Die schnelle Reaktion aller Fraktionen des Hessischen Landtags ermöglichte es, bereits rund einen Monat später eine Neufassung des § 16 a HMG zu verabschieden. Dieses „Gesetz zur Änderung des Hessischen Meldegesetzes“ vom 12. Juli 1978⁶⁰⁾ räumt dem Bürger ein Recht auf Auskunftssperre ein, er kann ohne Angabe von Gründen vom Einwohnermeldeamt verlangen, daß über die Daten „Tag der Geburt“, „Familienstand“ und „Beruf“ keine Auskunft erteilt wird. Will er auch die sog. Grunddaten „Namen, akademische Grade und Anschrift“ sperren lassen, so muß er glaubhaft machen, „daß seine schutzwürdigen Belange durch die Auskunft beeinträchtigt werden“. Mit dieser abgestuften Regelung soll verhindert werden, daß z. B. unredliche Schuldner das Sperrecht zur Verschleierung ihres Aufenthalts mißbrauchen. Ist eine Auskunftssperre auf Antrag eines Bürgers vermerkt worden, so gilt sie auch für sog. „Massenauskünfte“, beispielsweise an Adreßbuchverlage⁶¹⁾. Diese Regelung trägt dem Datenschutz Rechnung, ermöglicht aber gleichzeitig — worauf der Hessische Minister des Innern in den Erlassen vom 21. Juli 1978⁶²⁾ und vom 2. Oktober 1978⁶³⁾ hingewiesen hat — auf Wunsch den Parteien Jungwählerdaten, der Presse und den karitativen Verbänden Jubiläums- und Seniorenad-

⁵⁹⁾ Vgl. Z. 2, 4.3.

⁶⁰⁾ GVBl. I, S. 464.

⁶¹⁾ § 16 a Abs. 4.

⁶²⁾ Az.: — III A 3 — 23 a 02.

⁶³⁾ Az.: — III A 3 — 23 a 02.

⁵⁷⁾ LT-Drucks. 8/6189.

⁵⁸⁾ Vgl. dazu VI, 4.3.

und den Adreßbuchverlagen Adreßdaten der Bürger zu übermitteln, die von ihrem Sperrecht nicht Gebrauch gemacht haben.

Die Daten der Bürger, die eine Auskunftssperre verlangt haben — gleichgültig, ob sich die Sperre auf die erweiterte Auskunft oder auch auf die Grundauskunft bezieht — müssen bei Massenauskünften von der Übermittlung ausgenommen werden. Die Auskunftssperre wirkt gegenüber allen Privatpersonen und nicht-öffentlichen Stellen; es ist nicht möglich, die Sperre nur gegenüber einem Adressenverlag oder einem Verband oder einer Partei einzurichten. Das Recht auf Auskunftssperre gemäß § 16 a HMG unterliegt keiner Frist, es besteht solange, bis der Bürger die Übermittlungssperre widerruft.

Die neue gesetzliche Regelung hat allerdings zur Voraussetzung, daß die Bürger in geeigneter Weise von der Möglichkeit, eine Auskunftssperre zu verlangen, informiert werden. Insbesondere sollte dies vor Erteilung von Massenauskünften geschehen; außerdem sollten Hinweise auf das Recht der Bürger, eine Auskunftssperre einzurichten zu lassen, in regelmäßigen Abständen wiederholt werden.

4.2 Auskunft aus dem Melderegister

Stellvertretend für eine Vielzahl von Anfragen über Zweifelsfälle der Datenübermittlung aus dem Melderegister und von Beanstandungen, die wegen unzulässiger Datenübermittlung erhoben wurden, seien nachstehende zwei Fälle berichtet:

Durch einen Hinweis des Hessischen Ministers des Innern wurde mir bekannt, daß die diplomatische Vertretung eines ausländischen Staates die Innenminister verschiedener Bundesländer um die Erlaubnis gebeten hatte, sich von den Meldebehörden die Namen und Adressen aller in dem jeweiligen Bundesland gemeldeten Angehörigen dieses Staates geben zu lassen. Die Adressenübermittlung sollte der Verteilung einer Zeitschrift an die in der Bundesrepublik lebenden Bürger dieses Staates dienen. Ich habe dem Hessischen Innenminister bestätigt, daß seine Absicht, den Antrag auf Genehmigung der Datenübermittlung abzulehnen, aus Gründen des Datenschutzes geboten sei. Es konnte jedoch eine Lösung gefunden werden, welche die Kontaktaufnahme des ausländischen Staates zu seinen Bürgern ermöglicht, ohne die Belange der betroffenen Ausländer zu beeinträchtigen: Auf Kosten der Botschaft teilen die zuständigen Ausländer-Meldebehörden den betroffenen ausländischen Staatsangehörigen mit, die Botschaft wünsche ihre Adresse zwecks Übersendung einer Ausländerzeitschrift; dabei wird erklärt, daß die Meldebehörden diesem Wunsch aus Datenschutzgründen nicht entsprechen kön-

nen. Die Betroffenen müßten entscheiden, ob sie selbst der Botschaft die Adresse mitteilen wollen oder nicht. Damit wurde es in die Entscheidung der betroffenen ausländischen Mitbürger gestellt, ob sie sich mit ihrer Botschaft in Verbindung setzen wollten.

In dem zweiten Fall hatte sich — nach dem vergeblichen Versuch, von der Grundschule einer südsetzes von 1970 bzw. der alten melderechtlichen Vorschriften fiel — müßte aufgrund § 16 a Abs. 2 HMG (neuer Fassung) außerdem die Einzelfallgenehmigung des Hessischen Ministers des Innern eingeholt werden, da bei der verlangten Auskunft außer den sog. Grunddaten auch das Datum „Staatsangehörigkeit“ ausgewertet würde.

In dem zweiten Fall hatte sich — nach dem vergeblichen Versuch, von der Grundschule einer süd-hessischen Stadt eine Liste der Schüleradressen zu erhalten — der Vertreter eines Lexikon-Verlages mit Erfolg an die zuständige Stadtverwaltung gewandt. Gegen Bezahlung erhielt er die gewünschten Schüleradressen und konnte Lexika im Werte von mehreren 100,— DM an der Haustür verkaufen. Meine aufgrund der Beschwerde eines betroffenen Bürgers erhobene Beanstandung beantwortete die Stadtverwaltung damit, es habe sich um ein Versehen gehandelt; die Unzulässigkeit der Datenübermittlung mangels öffentlichen Interesses sei von dem Einwohnermeldeamt nicht erkannt worden. Leider handelt es sich bei derartigen „Verschen“ nicht um Einzelfälle, wenn sie auch meist nur in kleineren Gemeinden vorkommen.

Im Hinblick auf die vielfältigen Mißbrauchsmöglichkeiten aufgrund unzulässiger Datenübermittlung aus dem Melderegister sollte die Kontrolle der Aufsichtsbehörden jedoch effektiver gehandhabt werden. Vor allem aber ist hier eine ausreichende Unterrichtung der Bediensteten über die Verwirklichung des Datenschutzes in der täglichen Verwaltungspraxis erforderlich.

4.3 Einsicht der Polizei in das Melderegister

Bis zur Verstaatlichung der Polizei wurden die Melderegister von den kommunalen Polizeidienststellen geführt, so daß sie der Polizei jederzeit zur Verfügung standen. Dies änderte sich infolge der Verstaatlichung der Polizei, weil das Melderegister weiterhin von den kommunalen Meldebehörden geführt wird. Weil aber zur Abwehr von Gefahren für die öffentliche Sicherheit und Ordnung der Zugang der Polizei zu den Melderegistern jederzeit notwendig ist, wurde dies in den Verwaltungsvorschriften zum Hessischen Meldegesetz vom 30. 11. 1971 sichergestellt. Seit Inkrafttreten des Änderungsgesetzes zum Hessischen Meldegesetz vom 12. 7. 1978 gilt nunmehr die Vorschrift

des § 16 a Abs. 6 HMG, wonach die Meldebehörden den Polizeidienststellen zur rechtmäßigen Erfüllung der in ihrer Zuständigkeit liegenden Aufgaben „jederzeit Einsicht in das Melderegister zu gewähren“ haben.

Die Praxis ist dabei unverändert geblieben. Während der Dienststunden der Einwohnermeldeämter hat die Polizei jederzeit Zugang zu dem Register. Sie muß aber auch nach Dienstschluß diese Möglichkeit besitzen, um eine Identitätsfeststellung unverzüglich vornehmen zu können. Deswegen überlassen die Meldebehörden im allgemeinen den Polizeidienststellen Schlüssel zu ihren Räumen.

Bei dieser Praxis kann die Polizei auch Kenntnis von Daten erhalten, die sie nicht „zur rechtmäßigen Erfüllung der in ihrer Zuständigkeit liegenden Aufgaben benötigt“ (§ 12 Abs. 1 Satz 1 HDSG; ebenso § 10 Abs. 1 Satz 1 BDSG), d.h., der Grundsatz der Erforderlichkeit tritt gegenüber der Spezialregelung des § 16 a HMG zurück. Aus der Begründung zu der im Entwurf der Landesregierung vorgesehenen Fassung zu § 16 a HMG⁶⁴⁾ ergibt sich, daß schon im Gesetzgebungsverfahren rechtliche Bedenken gegen diese Lösung aufgetreten waren. Es wurde auf die Problematik der Regelung verwiesen, die entsprechende Beschränkung aber als „in der Praxis – insbesondere außerhalb der Dienststunden der Meldebehörde – nicht möglich“ bezeichnet.

Mit dem Fortschreiten der Automatisierung rückt diese Beschränkung jetzt in den Bereich der Möglichkeit: Eine hessische Großstadt hatte ein Verfahren entwickelt, das dem Grundsatz der Erforderlichkeit nach § 12 HDSG Rechnung trägt. Die Stadt wollte bei der Überführung ihres Einwohnerwesens in ein automatisches Verfahren der Polizei eine Kurzinformation über jeden Einwohner zur Verfügung stellen, die nur Namen, Rufnamen, Straßenkennziffer, Hausnummer, Geburtstag und Geschlecht enthält (Indexfiche-Duplikate). Auf diese Weise könnte die Polizei auch außerhalb der Dienststunden der Meldebehörden ohne Verzug auf die für ihre Tätigkeit wichtigsten und im allgemeinen ausreichenden Daten des Melderegisters zugreifen.

Die Weiterverfolgung dieses Verfahrens wurde jedoch wegen angeblicher rechtlicher Bedenken zurückgestellt. Ich hätte gegen dieses Verfahren keine Bedenken: § 16 a HMG gestattet der Polizei, jederzeit Einsicht in die Melderegister zu nehmen. Das Gesetz regelt nicht das Verfahren für die Einsicht, es nimmt aber in Kauf, daß die Polizei auch Kenntnis von Daten erhalten könnte, die sie für ihre Tätigkeit nicht benötigt. Bei dem zurück-

gestellten Verfahren wird zwar ebenfalls die jederzeitige Einsicht sichergestellt; die Polizei erhält aber nur die für ihre Zwecke notwendige Kurzinformation. Der Schutz des einzelnen vor unbefugter Übermittlung seiner Daten ist besser als bisher gewahrt. Wenn die Polizei weitergehende Informationen benötigt, muß sie die Wünsche der zuständigen Meldebehörde vortragen und diese muß prüfen, ob sie das Anliegen für berechtigt hält.

Erhält die Polizei diese Indexfiche-Duplikate, so hat sie ihrerseits zu gewährleisten, daß die Daten nur für polizeiliche Zwecke verwendet und an keine nichtpolizeiliche Dienststelle übermittelt werden. Sie muß ferner die organisatorischen und technischen Sicherungsvorkehrungen treffen, die notwendig sind, um einen unbefugten Zugriff bzw. Zugang zu verhindern.

4.4 Überwachung des Datenschutzes im Meldewesen

Bereits im Sechsten Tätigkeitsbericht habe ich darauf hingewiesen⁶⁵⁾, daß Gemeinden in zahlreichen Fällen Adressenlisten (z. B. von Ausländern, Haushaltsvorständen, Kirchenmitgliedern, 18-Jährigen usw.) an Dritte weitergegeben haben, die sie zuvor vom Kommunalen Gebietsrechenzentrum (KGRZ) für angeblich eigene Zwecke hatten anfertigen lassen. Diese Praxis ist unzulässig. Sie verletzt den Datenschutz. Trotzdem ist aufgrund von Stichproben bzw. Bürgerbeschwerden aus dem Bereich aller fünf KGRZ festzustellen, daß sie weiterhin besteht. Charakteristisch dafür ist ein Fall, der sich erst jüngst im Zuständigkeitsbereich des KGRZ Gießen ereignete: Eine Stadt hatte von dem KGRZ eine Auswertung aus der Einwohnerdatei angefordert, die die Anschriften aller in der Stadt wohnenden Kinder der Geburtsjahrgänge 1962–1975 umfassen sollte. Die in dem Anforderungsformular enthaltene Frage „Ist die Arbeit für Dritte“ wurde ausdrücklich mit „nein“ beantwortet. Diese für „eigene Zwecke“ angeforderte Adressenliste hatte die Stadt, wie sich aufgrund meiner Ermittlungen herausstellte, an eine politische Partei weitergegeben, die mit Hilfe dieser Adressenliste im Rahmen des Landtagswahlkampfes die Eltern aller schulpflichtigen Kinder zu einer Veranstaltung einlud. Dem KGRZ und der politischen Partei kann kein Vorwurf gemacht werden. Das KGRZ war verpflichtet, die Anforderung seines Mitgliedes für Verwaltungszwecke zu erfüllen; die Partei konnte davon ausgehen, daß die um Adressen gebetene Stadtverwaltung sich bei der Datenübermittlung im Rahmen der gesetzlichen Bestimmungen halten würde. Die betroffene

⁶⁴⁾ LT-Drucks. 8/4745 S. 28.

⁶⁵⁾ VI, 4.3.

Stadtverwaltung jedoch hätte — im September 1978 — wissen müssen, daß aufgrund § 16 a Abs. 3 HMG (i.d.F. vom 12. Juli 1978) und des dazu ergangenen Erlasses des Hessischen Ministers des Innern vom 21. Juli 1978 die Datenübermittlung nicht zulässig war, da es an einem öffentlichen Interesse fehlte. Lediglich für die Übermittlung von Jung- bzw. Erstwählerlisten bestätigt der Erlaß unter bestimmten Voraussetzungen ein öffentliches Interesse, nicht jedoch für die Übermittlung der Adreßdaten aller schulpflichtigen Kinder. Hätte der Magistrat bei Anforderung der Auswertung die Frage, ob die Arbeit für Dritte sei, wahrheitsgemäß mit „ja“ beantwortet, so hätte ihn das KGRZ aufgrund einer dort bestehenden Übung auf die Unzulässigkeit der gewünschten Datenübermittlung für Dritte hingewiesen. Schließlich muß in diesem Zusammenhang festgehalten werden, daß die kritisierte Verfahrensweise dieser und anderer Gemeinden dazu geeignet ist, die Leistungsfähigkeit des hessischen Datenverarbeitungsverbundes zu beeinträchtigen:

Während Datenanforderungen für Mitgliedsgemeinden der KGRZ kostenlos sind, entsteht für Auswertungen, die für Dritte verlangt werden, eine Gebührenforderung des KGRZ. Deshalb entstehen durch diese Praxis — der angeblich für eigene Zwecke, in Wirklichkeit aber für Dritte verlangten Datenauswertungen — dem Land finanzielle Schäden⁶⁶⁾.

4.5 Übermittlung von Daten durch das Kraftfahrt-Bundesamt

Die Übermittlung von personenbezogenen Daten durch das Kraftfahrt-Bundesamt (KBA) in Flensburg an Dritte für Zwecke der Werbung und Meinungsforschung ist von mir in der Vergangenheit mehrfach beanstandet worden. Abgesehen von grundsätzlichen Bedenken habe ich insbesondere Kritik daran geübt, daß

- die Einwilligungserklärung vielfach von Bevollmächtigten ausgefüllt wurde und der Anmelder selbst nicht über die Weitergabe seiner Daten durch das KBA und die Möglichkeit, sie sperren zu lassen, informiert war;
- der Sperrvermerk durch die Zulassungsstelle oft nicht an das KBA weitergeleitet wurde und
- aus der Einwilligungserklärung nicht hervorging, welche Daten durch das KBA übermittelt werden dürfen.

Meine Beanstandungen habe ich auch dem Hessischen Minister für Wirtschaft und Technik, dem

Kraftfahrt-Bundesamt und dem Bundesminister für Verkehr mitgeteilt. Der Hessische Minister für Wirtschaft und Technik hat daraufhin in einem Erlaß noch einmal darauf hingewiesen, daß die Einwilligungserklärung vom Anmelder persönlich unterzeichnet sein und bei An- und Ummeldungen des Fahrzeugs durch einen Beauftragten eine besondere Vollmachtserklärung des Antragstellers vorliegen müsse. Fehle diese Erklärung, so sei der Antrag so zu behandeln, als ob die Frage nach der Zustimmung zur Weitergabe der Daten mit nein beantwortet worden ist⁶⁷⁾. Das Kraftfahrt-Bundesamt hatte mir bereits vorher mitgeteilt, daß es nach dieser Praxis verfare. Der Bundesminister für Verkehr hat meine Anregungen bei der Neugestaltung der An- und Ummeldeformulare berücksichtigt. Neben der Notwendigkeit der persönlichen Einwilligung des Antragstellers wird in der Erklärung jetzt auch aufgeführt, welche Daten vom Kraftfahrt-Bundesamt an Dritte übermittelt werden dürfen. Leider ist in der Veröffentlichung des Verkehrsblattes der Hinweis, daß alte Vordrucke nicht mehr verwendet werden dürfen, mißverständlich abgefaßt⁶⁸⁾.

4.6 Verkauf von Adrema-Platteien

Durch eine Beschwerde wurde ich darauf hingewiesen, daß eine Gemeinde nicht mehr gebrauchte Adrema-Anlagen an zwei private Unternehmen verkauft und dabei auch die Platteien weitergegeben habe. Eine Nachprüfung bestätigte diese Angaben. Die Platten enthielten empfindliche personenbezogene Daten, wie z. B. den Familienstand (verheiratet, ledig, geschieden), die Zahl der Familienmitglieder, die Lohnsteuerklasse, den Geburtsort, das Geburtsdatum und die Religionszugehörigkeit. Ich habe die Gemeinde darauf hingewiesen, daß die Veräußerung dieser Platten mit personenbezogenen Daten einen Verstoß gegen das Datenschutzrecht darstellt. Die Beschriftung auf den Platten mit den personenbezogenen Angaben müsse daher unter Kontrolle unkenntlich gemacht oder die Platten müßten vernichtet werden; der Vollzug sei in einem Protokoll festzuhalten. Die Gemeinde hat mir inzwischen mitgeteilt, daß in einem Fall die Platten eingeschmolzen worden seien, in dem zweiten Fall habe sie die Platten in „Verwahrung“ genommen.

Bei der Zusammenlegung von Gemeinden im Rahmen der Gebietsreform und aufgrund der inzwischen erfolgten Einbeziehung vieler Gemeinden in das Datenverarbeitungsprogramm

⁶⁶⁾ Vgl. Datenverarbeitungsgesetz vom 16. 12. 1969 § 8 Abs. 1.

⁶⁷⁾ Erlaß vom 14. 2. 1978, Az.: III b 2 — 66 106 a 33.

⁶⁸⁾ Veröffentlicht im Verkehrsblatt vom 31. Oktober 1978 S. 435.

„Grundstufe Einwohnerwesen“ sind zahlreiche Adrema-Anlagen überflüssig geworden. Ich habe den Hessischen Minister des Innern über den oben geschilderten Vorgang unterrichtet und empfohlen, in einem Erlaß die Gemeinden darauf hinzu-

weisen, daß bei dem Verkauf von solchen Anlagen die Platteien mit personenbezogenen Daten nicht mitverkauft werden dürfen, es sei denn, daß die Beschriftung vorher unleserlich gemacht worden ist.

5. DATENSCHUTZ IM SICHERHEITSBEREICH

5. Datenschutz im Sicherheitsbereich

5.1 Hepolis und Kriminalakten

Die datenschutzrechtlichen Probleme, die das Hessische Polizeiinformationssystem HEPOLIS aufwirft, sind schon im Zweiten Tätigkeitsbericht von 1973⁶⁹⁾ in ihren Grundzügen dargestellt und in den Tätigkeitsberichten von 1974–1976⁷⁰⁾ weiter behandelt worden. Es geht dabei um folgende Fragen:

- die Einbeziehung der Personen (Kriminal-) Akten in das automatisierte Informationssystem,
- die Sicherung gegen Zugriffe Unbefugter,
- die Kontrolle der Benutzung des Systems durch Protokollierung,
- die Löschung von Daten im polizeilichen Informationssystem unter besonderer Berücksichtigung der Regelung des Bundeszentralregisters,
- die Auskunft aus Kriminalakten.

5.1.1 Im Unterschied zum Datenschutzgesetz vom 7. Oktober 1970, das alle Unterlagen erfaßte, die für Zwecke der maschinellen Datenverarbeitung erstellt wurden, verwendet das Hessische Datenschutzgesetz vom 31. 1. 1978 den Begriff der Datei und klammert Akten und Aktensammlungen aus, sofern sie nicht durch automatisierte Verfahren umgeordnet und ausgewertet werden können. Für das kriminalpolizeiliche Informationssystem HEPOLIS ist jedoch der Datenschutz nicht verkürzt worden. Die Unterscheidung zwischen Akten (Aktensammlungen) und Dateien ist hier bedeutungslos; denn obwohl HEPOLIS auch Kurzhinweise auf Personen, Sachen und/oder Ereignisse enthält, bilden die kriminalpolizeilichen (Personen-) Akten mit HEPOLIS, insbesondere mit der Täter- und mit der Tat-Datei eine Einheit. In den Dateien wird auf die Personen-Akten, in denen die kriminalpolizeilichen Erkenntnisse gesammelt sind, verwiesen, indem einmal der Name, das andere mal die Straftat als Ordnungsbegriff verwendet wird. Ohne die Zugriffsmöglichkeit auf die Akten wäre das System wertlos und ohne die automatisierte Aufschließung des Aktenbestandes wäre die Aktensammlung nicht auswertbar.

⁶⁹⁾ II, 4.1.1.3 c.

⁷⁰⁾ III, 4.1.5.1; IV, 4.5; V, 4.7.

Außerdem könnten mit Hilfe computerunterstützter Ausdrücke aus dem System die in den Akten erfaßten Kenntnisse auch nach anderen Kriterien umgeordnet und ausgewertet werden. HEPOLIS und die entsprechenden Polizei-Informationssysteme der anderen Länder und des Bundeskriminalamtes sind daher im Sinne sowohl des Bundesdatenschutzgesetzes (§ 2 Abs. 3 Nr. 3) als auch des Hessischen Datenschutzgesetzes (§ 2 Abs. 3 Nr. 3) ein automatisiertes Verfahren, mittels dessen die zugrundeliegenden Personen-Akten der Kriminalpolizei umgeordnet und ausgewertet werden können⁷¹⁾.

5.1.2 In der Praxis sind jedoch die Datenschutzprobleme nicht befriedigend gelöst: Der Abruf polizeilicher Erkenntnisse über eine bestimmte Person aus dem Informationssystem über ein Terminal ist eine Datenübermittlung innerhalb des öffentlichen Bereichs im Sinne des § 12 HDSG. Die Übermittlung ist nur zulässig, wenn sie zur rechtmäßigen Erfüllung der in der Zuständigkeit des Empfängers liegenden Aufgabe erforderlich ist. Selbst der Nachweis, daß der Abrufende (der Empfänger) ein Beamter der Kriminalpolizei ist, schließt nicht aus, daß die Übermittlung nicht zur rechtmäßigen Erfüllung seiner beruflichen Aufgabe, sondern für private Zwecke genutzt wird. Die Protokollierung der Übermittlungen ist eine Möglichkeit, nachträglich zu kontrollieren, ob die Abrufe berechtigt waren. Sie verhindert jedoch nicht den Mißbrauch, sondern ermöglicht nur seine dienstrechtliche Verfolgung.

Der Zugriff auf das Informationssystem muß daher zusätzlich gesichert werden, in erster Linie durch eine Beschränkung des Zugriffsrechts auf bestimmte, einer besonderen Auswahl unterzogene Bedienstete. Neben einer strikten Zugangskontrolle ist eine wirksame Benutzerkontrolle im Sinne der Nrn. 1 und 4 der Anlage zu § 10 HDSG notwendig. Die oberste Landesbehörde sollte nach §§ 5, 6 HDSG die notwendigen Maßnahmen treffen und ihre Durchführung sicherstellen.

5.1.3 Vorfälle der letzten Zeit haben gezeigt, daß Informationssysteme auch dann unzureichend gesichert sind, wenn trotz konkreter Vorschriften

⁷¹⁾ Vgl. Auernhammer BDSG § 2 Rdnr. 28; Dammann in Simitis/Dammann/Mallmann/Reh BDSG § 2 Rdnr. 194 ff.

diese aus Nachlässigkeit nicht oder nicht ausreichend beachtet werden. So berichtete die Presse von einem Mechaniker, dem es mehrfach gelungen sein soll, aus dem polizeilichen Informationssystem Auskünfte zu seiner Person und über Dritte zu erhalten, weil die auskunftgebenden Bediensteten nicht — wie ausdrücklich vorgeschrieben — nach dem Codewort gefragt bzw. durch Rückruf festgestellt hatten, ob der Anfragende befugt war, diese Auskunft zu erhalten. Dies war Anlaß für das Hessische Landeskriminalamt, nochmals alle Bediensteten auf die strikte Beachtung der Vorschriften hinzuweisen. Weitere Sicherungen durch täglich wechselnde Codeworte sollen in Vorbereitung sein.

5.1.4 Künftig soll HEPOLIS eine Art Subsystem des Informationssystems des Bundeskriminalamtes INPOL werden. Alle Datenendgeräte dieses Systems in Bund und Ländern sollen durch ein integriertes digitales Sondernetz (DISPOL) von ihrer Bindung an Bundes- oder Landesrechner entkoppelt und über programmierbare DISPOL-Netzknoten direkt an INPOL angeschlossen werden. Die Programmierung für die Verwaltung und Speicherung der Datenbestände von INPOL erfolgt durch das Bundeskriminalamt. Auch die verbleibenden länderspezifischen Anwendungen sind dann über DISPOL erreichbar. Damit werden sich die Probleme noch weiter verschärfen. Denn je mehr Stellen Zugriff auf die zentralen oder auch dezentralisierten Datensammlungen bei den Landeskriminalämtern und dem Bundeskriminalamt haben und je mehr Terminals angeschlossen sind, umso größer sind die Mißbrauchsgefahren.

5.1.5 Eine weitere Rechtsunsicherheit, die wiederholt zu Beschwerden von Bürgern geführt hat, herrscht hinsichtlich der Praxis der Kriminalpolizeien, die strafgerichtlichen Verurteilungen der von ihnen erfaßten Personen ohne Beachtung der im Bundeszentralregister festgesetzten Tilgungsfristen aufzubewahren.

Hessische Polizeidienststellen berufen sich gegenüber Einwendungen gegen diese Praxis auf den Erlaß des Ministers des Innern betr. Auskunft aus den Kriminalakten an Behörden vom 10. 7. 1974. Die dort vertretene Auffassung, das Bundeszentralregister enthalte keine Vorschriften, die es verböten, in Kriminalakten strafgerichtliche Verurteilungen einzutragen, oder die es geböten, die Tilgungsvorschriften des BZRG auf solche Eintragungen in Kriminalakten anzuwenden, bedarf spätestens seit der Verkündung des Hessischen Datenschutzgesetzes vom 31. 1. 1978 der Überprüfung.

5.1.5a) Nach § 11 Abs. 1 HDSG ist das Speichern personenbezogener Daten — um die es sich bei strafge-

richtlichen Verurteilungen handelt — nur zulässig, wenn das Speichern zur rechtmäßigen Erfüllung der in der Zuständigkeit der Kriminalpolizei liegenden Aufgabe erforderlich ist. Strafgerichtliche Verurteilungen bestimmter Personen, die als Beschuldigte oder Verdächtige in Erscheinung getreten sind, werden in den Kriminalakten registriert, um der Polizei künftige Ermittlungen, insbesondere die Identifizierung tatverdächtiger Personen, zu erleichtern (Nr. 3 des vorgenannten Erlasses). Dieser Zweck kann die Registrierung von Verurteilungen nur solange rechtfertigen, als ihr keine rechtlichen Hindernisse entgegenstehen, mit anderen Worten, solange die Registrierung rechtmäßig ist.

Nun verbietet aber § 49 BZRG, dem Betroffenen im „Rechtsverkehr“ seine Tat und seine Verurteilung vorzuhalten oder zu seinem Nachteil zu verwenden, wenn die Eintragung der Verurteilung im Zentralregister getilgt worden oder wegen Ablaufs der Tilgungsfrist tilgungsreif ist. Der Begriff des „Rechtsverkehrs“ umfaßt alle Bereiche des Rechtslebens, auch die Beziehungen zwischen dem Bürger und den Verwaltungsbehörden. Eine Verwertung zum Nachteil des Betroffenen liegt stets vor, wenn aus der Tat oder der Verurteilung für ihn ungünstige Folgerungen gezogen werden. Mit anderen Worten: Tat und Verurteilung dürfen von der Verwaltung — vorbehaltlich der speziellen Ausnahmen in § 50 BZRG — nicht als Begründung dafür herangezogen werden, daß der Betroffene nicht unbescholten oder nicht zuverlässig sei, oder zur Begehung strafbarer Handlungen neige und dgl.⁷²⁾ Der Schutz der im Bundeszentralregister gespeicherten Daten vor Mißbrauch ist vom Gesetzgeber schon vom Beginn der Beratung des Gesetzes an sorgfältig beachtet worden. Alle Vorschriften, welche die Auskunft aus dem Register mit Rücksicht auf die Resozialisierung des Betroffenen beschränken, sind zugleich Maßnahmen des Datenschutzes⁷³⁾. Dies gilt im besonderen für die Tilgungsvorschriften und für das Verwertungsverbot nach § 49 BZRG. Die Vorschriften des BZRG haben nach § 45 Nr. 7 BDSG Vorrang vor den Vorschriften dieses Gesetzes. Gegenüber dem HDSG ergibt sich der Vorrang des BZRG aus Art. 31 GG, wonach Bundesrecht Landesrecht bricht.

Das Speichern strafgerichtlicher Verurteilungen in kriminalpolizeilichen Akten ist daher nach Eintritt der Tilgungsreife im Sinne des BZRG nicht mehr rechtmäßig.

⁷²⁾ Vgl. Götz, Das Bundeszentralregistergesetz § 49 Erl. 13 ff.

⁷³⁾ Vgl. Götz a.a.O. Einleitung Nr. 39.

5.1.5b) Darüber hinaus ist das Speichern strafgerichtlicher Verurteilungen nach Eintritt ihrer Rechtskraft, d.h. nach Eintragung im BZRG, auch nicht mehr erforderlich, damit die Kriminalpolizei ihre Aufgabe erfüllen kann. Erforderlich im Sinne des § 11 Abs. 1 des HDSG heißt, daß die Aufgabe ohne die Speicherung nicht erfüllbar ist⁷⁴⁾. Die Kriminalpolizei hat ein unbeschränktes Auskunftsrecht gegenüber dem Bundeszentralregister, kann also jederzeit feststellen, ob und welche Verurteilungen gegen den Betroffenen vorliegen. Gerichtliche Verurteilungen, die im Bundeszentralregister eingetragen sind, daneben in den kriminalpolizeilichen Akten festzuhalten, ist deswegen überflüssig, d.h. nicht erforderlich.

5.1.6 Daraus ergibt sich folgendes:

Nur solange die Verurteilung des Betroffenen nicht rechtskräftig ist, ist gegen das Festhalten dieser Verurteilung in den Kriminalakten nichts einzuwenden.

Mit dem Eintritt der Rechtskraft der Verurteilung, das bedeutet zugleich mit der Eintragung in das Bundeszentralregister, entfällt die Erforderlichkeit der weiteren Speicherung in den Kriminalakten. Damit entfällt eine der Voraussetzungen für die Zulässigkeit der Datenspeicherung nach § 11 HDSG.

Nach Wegfall der ursprünglich erfüllten Voraussetzungen für die Speicherung hat der Betroffene nach § 8 Nr. 3 HDSG das Recht, die Sperrung dieser Daten zu verlangen. Zugleich ist die Kriminalpolizei nach § 19 Abs. 2 Satz 2 HDSG verpflichtet, die Sperrung von Amts wegen vorzunehmen.

Außer der Sperrung kann der Betroffene nach § 8 Nr. 4 HDSG die Löschung der Eintragung in den Kriminalakten verlangen. Die Behörde hat diesem Antrage stattzugeben, wie sich aus § 19 Abs. 3 letzter Satz ergibt⁷⁵⁾.

Die gleiche Rechtslage besteht, wenn die Eintragung im Bundeszentralregister tilgungsreif und demgemäß die Verwertung von Tat und Verurteilung zum Nachteil des Betroffenen unzulässig geworden ist. Von diesem Zeitpunkt an ermangelt die Verwendung des Eintrags in den Kriminalakten, abgesehen von den Ausnahmen des § 50 BZRG, die sich mit dem Verwertungsverbot nach § 19 Abs. 2 Satz 3 HDSG weitgehend decken, der Rechtsmäßigkeit im Sinne des § 11 Abs. 1 HDSG.

⁷⁴⁾ Vgl. Auernhammer BDSG § 9 Rdnr. 4; Dammann a.a.O. Rdnr. 20 zu § 9.

⁷⁵⁾ Vgl. für die gleichlautenden Vorschriften im BDSG Reh in Simitis/Dammann/Mallmann/Reh BDSG § 4 Rdnr. 24.

5.1.7 Wie mir aus Anlaß der Beschwerde eines Beamten bekanntgeworden ist, werden auch Disziplinarmaßnahmen in die Kriminalakten aufgenommen und damit auch in HEPOLIS registriert, wenn gegen den Beamten gleichzeitig ein Disziplinar- und ein Strafverfahren anhängig ist. Der Eintrag der Disziplinarmaßnahmen in den Kriminalakten wird ebenso behandelt, wie die anderen kriminalpolizeilichen Erkenntnisse mit der Folge, daß sie erst nach Ablauf der in den „vorläufigen Richtlinien für die Führung von Kriminalakten vom 6. 10. 1975“ festgelegten Fristen getilgt werden, obwohl die Tilgungsfristen für die Disziplinarmaßnahmen nach § 110 der Hessischen Disziplinarordnung (HDO) in der Regel kürzer sind. Dieses Verfahren verstößt gegen § 110 HDO, der bestimmt: „Nach Ablauf der Tilgungsfrist gilt der Beamte als von Disziplinarmaßnahmen nicht betroffen.“ Diese gesetzliche – und nicht widerlegbare – Vermutung, ist stärker als das Verbot des § 49 BZRG, tilgungsreife Eintragungen im Bundeszentralregister im Rechtsverkehr zum Nachteil des Betroffenen zu verwerten. Abgesehen von der Frage, ob die Mitteilung von Disziplinarmaßnahmen an die Kriminalpolizei und die Eintragung in Kriminalakten über ein parallel laufendes Strafverfahren datenschutzrechtlich zulässig ist, ist jedenfalls die Nicht-Beachtung der Tilgungsfristen gesetzwidrig. Es genügt daher nicht, die Bediensteten des Hessischen Landeskriminalamtes und aller Polizeidienststellen gemäß dem Gemeinsamen Runderlaß der Hessischen Landesregierung vom 15. März 1978⁷⁶⁾ zu befehlen. Vielmehr muß sichergestellt werden, daß die Eintragung von Disziplinarmaßnahmen in den Kriminalakten spätestens im gleichen Zeitpunkt gelöscht wird, in welchem die über die Disziplinarmaßnahme entstandenen Vorgänge aus den Personalakten nach § 110 Abs. 2 Satz 2 entfernt und vernichtet werden.

5.1.8 Wie bereits im Fünften Tätigkeitsbericht berichtet⁷⁷⁾, ist aufgrund meiner Anregung der Datenschutz durch die „vorläufigen Richtlinien für Auskünfte aus Kriminalakten“ verbessert worden. Eine Besonderheit dieser innerdienstlichen Regelung für die Hessische Kriminalpolizei besteht darin, daß diese Richtlinien bei Auskünften nicht zwischen Kriminalakten und Datenträgern unterscheiden und daß die Zulässigkeit von Auskünften an die Tilgungsfristen der §§ 43 ff. BZRG gebunden ist, allerdings mit den Ausnahmen zugunsten der Kriminaldienststellen, wenn die Auskunft der Verhinderung und Verfolgung von Straftaten dient; gleiches gilt zugunsten anderer Behörden,

⁷⁶⁾ S. StAnz. S. 624.

⁷⁷⁾ V, 4.7.

wenn sie die Auskunft benötigen, um eine Störung der öffentlichen Sicherheit und Ordnung zu beseitigen oder eine unmittelbare bevorstehende Gefahr abzuwehren.

Das Bayerische Datenschutzgesetz vom 28. April 1978⁷⁸⁾ enthält eine für den Betroffenen günstigere Regelung in Art. 8 Nr. 3; danach entfällt der Auskunftsanspruch des Betroffenen gegenüber der Polizei nur, „soweit sie strafverfolgend oder zur Aufrechterhaltung der öffentlichen Sicherheit und Ordnung tätig wird.“

- 5.1.9 Es erscheint dringend geboten, daß die Landesregierung das Festhalten strafgerichtlicher Verurteilungen in Kriminalakten über die dem Datenschutz dienenden Bestimmungen des Bundeszentralregistergesetzes hinaus durch eine Rechtsverordnung gemäß § 19 Abs. 4 HDSG unterbindet und die Sperrung und Löschung solcher Eintragungen in Übereinstimmung mit den Fristen des BZRG regelt. Im Interesse der rechtseinheitlichen Anwendung der Datenschutzvorschriften sollte die Landesregierung eine entsprechende Regelung auch bei den anderen Ländern anregen.

5.2 Verfassungsschutz und Bibliotheksdaten

Seit 1975 wird in Massenmedien und Publikationen immer wieder berichtet, daß Verfassungsschutzbehörden in öffentlichen Bibliotheken die Ausleihlisten einsähen um festzustellen, wer Leser bestimmter politischer Literatur ist. Als 1978 dieser Vorwurf auch von Mitgliedern des „Vereins der Bibliothekare an öffentlichen Bibliotheken“ und des „Verbandes deutscher Bibliothekare“ erhoben wurde, hat dies in der Öffentlichkeit erhebliches Aufsehen erregt. Bibliotheksbenutzer und Bibliothekare äußerten in Anfragen und auf Fachtagungen ihre Besorgnis über eine Beeinträchtigung der grundsätzlich geschützten Informationsfreiheit durch eine staatliche Kontrolle des Leseverhaltens. Verstärkt wurden diese Bedenken als bekannt wurde, daß der Bundesgrenzschutz Lektüre-Kontrollen beim Grenzübertritt vorgenommen hatte, eine Praxis, die der Bundesminister sofort unterbunden hat.

Auch der Hessische Landtag befaßte sich mit der aufgeworfenen Problematik⁷⁹⁾.

Obwohl bereits frühere Nachforschungen keine Bestätigung der erhobenen Vorwürfe ergeben hat-

ten, bin ich den Meldungen erneut nachgegangen und habe an verschiedenen hessischen Bibliotheken recherchiert. Dabei konnte ich keine Verstöße gegen den Datenschutz feststellen. Auch das Landesamt für Verfassungsschutz hat mir versichert, daß es Überprüfungen der geschilderten Art weder durchgeführt hat noch beabsichtigt. Zu entsprechenden Ergebnissen sind für ihre Bereiche auch die angesprochenen Datenschutzbeauftragten des Bundes und der Länder gekommen.

Soweit bei den Vorwürfen konkrete Fälle festgestellt werden konnten, handelte es sich um polizeiliche Personenfahndungen oder um Maßnahmen der Gefahrenabwehr. Aus Anlaß der Ermordung des Vorstandsvorsitzenden einer Großbank wurde in Hamburger Bibliotheken aus den Entleihkarten bestimmter Tatverdächtiger festgestellt, über welche anderen Personen und deren Lebensgewohnheiten sie sich Informationen verschafft hatten. Die gefährdeten Personen konnten daraufhin gewarnt und unter besonderen Schutz gestellt werden.

In Hessen ist die Erstellung von „Leserprofilen“ oder die Erteilung unzulässiger Einzelauskünfte technisch wesentlich erschwert worden, nachdem 1974 bei der Entwicklung des automatisierten Ausleihverfahrens für die hessischen Bibliotheken (HEBIS-LEIH) auf Anregung des Datenschutzbeauftragten Speicherung, Zugriff und Weitergabe von Benutzerdaten besonders geregelt worden sind. Danach werden bei der Rückgabe des ausgeliehenen Buches die persönlichen Daten des Ausleihers in der Datei automatisch gelöscht. Festgehalten werden nur statistische Angaben (z. B. Altersgruppe, Geschlecht, Beruf), die eine Rückidentifizierung im allgemeinen verhindern. Es kann lediglich festgestellt werden, zu welcher Personengruppe die Ausleiher des Buches gehören. „Leserprofile“ für einzelne Ausleiher können jedoch nicht erstellt werden.

Somit hat die Automatisierung des Bibliothekswesens zu einer Verbesserung des Datenschutzes geführt. Schwachstellen liegen eher bei den manuellen Ausleihkarteien, wie sie in kleineren Bibliotheken, aber auch noch in manchen Großbibliotheken benutzt werden. Bisher sind zwar keine Mißbrauchsfälle bekannt; es ist jedoch erforderlich, auch manuelle Benutzer- und Ausleihkarteien vor jedem unbefugten Zugriff zu schützen. Vor allem aber sind die Bibliotheksbediensteten über die Bedeutung des Datenschutzes eingehend zu belehren.

⁷⁸⁾ BayGVBl. 9/1978, S. 165.

⁷⁹⁾ Vgl. LT-Drucks. 8/5831.

6. BILDUNGSWESEN

6. Bildungswesen

6.1 Datenschutz bei Schülerbefragungen

Wie bereits in früheren Tätigkeitsberichten⁸⁰⁾ dargestellt, ist die Befragung von Schülern nicht unproblematisch und nur unter bestimmten Voraussetzungen zulässig. Im Berichtszeitraum beschwerte sich bei mir der Elternbeirat einer hessischen Schule darüber, daß an der betreffenden Schule ohne Wissen der Eltern eine Fragebogen-Aktion bei den Schülern „zur Erfassung von Freizeitverhalten und Freizeitwünschen bei Jugendlichen“ durchgeführt worden war. Dabei sei der Datenschutz der Schüler und ihrer Eltern verletzt worden. So sei bei den insgesamt ca. 130 Fragen u. a. nach der Berufstätigkeit der Eltern, Art und Größe der Wohnung, Erziehungsmaßnahmen der Eltern, Streitigkeiten der Eltern untereinander oder mit Nachbarn, der Kinderfreundlichkeit der Erwachsenen, den Trinkgewohnheiten der Schüler, deren Ansichten über den Schulunterricht, über das „Klauen“, die Eß- und Fernseh-Gewohnheiten der Familie und „ob das Mädchen einen Freund bzw. der Junge eine Freundin“ habe, gefragt worden.

Ich habe die Richtigkeit dieser Angaben und darüber hinaus die Tatsache festgestellt, daß die mit Name und Anschrift der Schüler versehenen Fragebogen längere Zeit offen im Lehrerzimmer lagen und dort jedermann zugänglich waren, bevor sie an die für ihre Auswertung zuständige Projektgruppe des Hessischen Kultusministers übersandt wurden. Aufgrund meines Hinweises ermittelte der Kultusminister, daß die Befragung zwar im Rahmen eines von ihm veranlaßten Projekts durchgeführt worden war, die dafür geltenden gesetzlichen Bestimmungen und ein Erlaß des Kultusministers jedoch nicht berücksichtigt worden waren. Diese Mängel konnten nachträglich nicht mehr „geheilt“ werden. Auf Anordnung des Kultusministers wurden deshalb die Fragebogen unter Aufsicht eines Vertreters des Kultusministers und im Beisein von Vertretern des Elternbeirats und meines Amtes im Reißwolf vernichtet.

Bei dieser Fragebogen-Aktion wurden Bestimmungen des Datenschutzes sowie des Elternrechts verletzt:

- Für eine Befragung von Schülern über deren Freizeitverhalten fehlt die gesetzliche Grund-

lage. Deshalb hätte die Befragung nur auf freiwilliger Grundlage erfolgen dürfen.

- Im Hinblick auf die Sensitivität der erfragten Daten hätte die Befragung anonym stattfinden sollen. Dies war auf den Fragebogen auch angekündigt, dann aber — versehentlich — durch Aufkleber mit den Namen der Schüler nicht eingehalten worden.
- Die betroffenen Schüler (7. und 9. Schuljahr) waren minderjährig. Sie konnten sich von den möglichen Auswirkungen der Teilnahme an einer solchen Befragung keine Vorstellung machen. Deshalb hätten die Eltern als gesetzliche Vertreter vor der Befragung informiert und um Einwilligung gebeten werden müssen; dies umso mehr, als die Schüler auch nach Verhaltensweisen der Eltern gefragt wurden, was besonders problematisch ist.
- Schließlich war es unzulässig, die mit den Namen der Schüler versehenen Fragebogen offen im Lehrerzimmer herumliegen zu lassen, und so jedem, der Zutritt hatte, Informationen über die Schüler und deren Familien zu ermöglichen.

Die Tatsache, daß bei keinem der für die Durchführung der Aktion Verantwortlichen böse Absicht im Spiel war, sondern eher Übereifer und mangelnde Sorgfalt, erweist die Notwendigkeit, noch stärker als bisher alle mit Datenverarbeitung Beschäftigten auf mögliche Mißbrauchsgefahren und die Notwendigkeit des Datenschutzes hinzuweisen. Ebenso ist zu überlegen, wie mittels besserer Unterrichtung und einer verstärkten Kontrolle durch die zuständige Behörde die Einhaltung des Datenschutzes gesichert werden kann.

Der Fall ist gleichzeitig ein Beispiel für die gute Zusammenarbeit zwischen dem zuständige Ressort und mir. Durch schnelles Handeln konnten ernste Nachteile für die Betroffenen vermieden werden. Es wurde vereinbart, daß ich regelmäßig über die Planung ähnlicher Projekte unterrichtet werde, damit ich frühzeitig Anregungen zum Datenschutz geben kann. So soll verhindert werden, daß sich ein solcher Fall wiederholt. Inzwischen sind eine Reihe von Fragen in dem bisher verwendeten Fragebogen geändert oder gestrichen worden. Es soll besonders darauf geachtet werden, daß künftig vor Schülerbefragungen die Zustimmung der Eltern eingeholt wird. Soweit die Fragen Daten der Eltern selbst betreffen, sind auch deren

⁸⁰⁾ Vgl. IV, 1.6 und 4.7.5; VI, 4.2.1.

schutzwürdigen Belange zu beachten. In solchen Fällen müssen die Erziehungsberechtigten nicht nur für die Befragung ihrer Kinder, sondern auch für die sie selbst betreffenden Fragen um Einwilligung gebeten werden.

6.2 Wissenschaftliche Untersuchungen im Schulbereich

Unabhängig von der Regelung der Datenübermittlung für wissenschaftliche Zwecke in § 15 HDSG treten bei Befragungen in Schulen durch Universitäten, Fachhochschulen, wissenschaftliche Arbeitsgruppen, Doktoranden und Meinungsforschungsinstitute besondere Probleme auf. Im Hinblick auf die wachsende Zahl dieser Befragungen erwies sich der bisher geltende Erlaß des Kultusministers vom 20. März 1973 als nicht mehr ausreichend. Deshalb hat der Kultusminister aufgrund meiner Anregung die Zulassung wissenschaftlicher Untersuchungen im Schulbereich neu geregelt. In seinem Erlaß vom 4. Mai 1977⁸¹⁾ heißt es nunmehr:

„Anträge auf Durchführung wissenschaftlicher Untersuchungen im Schulbereich müssen über folgende Fakten Aufschluß geben:

- Präzise Beschreibung des Projekts.
- Name und Qualifikation des verantwortlichen Projektleiters.
- Anzahl und Qualifikation der beteiligten Mitarbeiter.
- Erhebungsunterlagen.
Aus ihnen muß deutlich der Zweck der Untersuchung, die durch den Antragsteller vorgesehene Behandlung der Erhebungspapiere und deren endgültiger Verbleib hervorgehen. Im Antrag sollen Hinweise über die voraussichtliche Dauer der Datenspeicherung und den Zeitpunkt der Löschung des Datenmaterials enthalten sein.
- Genaue Angaben über den zeitlichen Ablauf und zeitlichen Umfang des Projekts.
- Angaben zur örtlichen Abgrenzung des Vorhabens (Benennung der Schulen bzw. Schülergruppen).

Im Einvernehmen mit dem Hessischen Datenschutzbeauftragten werde ich meine Zustimmung zur Durchführung wissenschaftlicher Untersuchungen u. a. auch von der Erfüllung folgender Auflagen abhängig machen:

- Die Anonymität der zu Befragenden muß gewahrt sein.

- Eingriffe in die Intimsphäre des zu untersuchenden Personenkreises sind auszuschließen.
- Die Freiwilligkeit der Beteiligung muß garantiert sein.

Bei Befragungen Minderjähriger werde ich nur noch in Ausnahmefällen die Zustimmung von Klassen- oder Schulleiternbeiräten als ausreichend anerkennen. Im Regelfalle muß die Einwilligung der Erziehungsberechtigten vorliegen.“

Der neue Erlaß trägt den Datenschutzforderungen Rechnung, die ich wiederholt in meinen Tätigkeitsberichten erhoben hatte⁸²⁾.

Die nunmehr über einjährige praktische Erfahrung mit diesem Erlaß zeigt jedoch, daß wissenschaftliche Befragungen von Schulkindern im Rahmen des Unterrichtes nach wie vor zu Beschwerden Anlaß geben. Sie kommen von Elternbeiräten, einzelnen Eltern und Schülern und von Lehrern. Beispielhaft sind zwei Befragungen, die trotz Genehmigung des Projekts durch den Kultusminister und trotz Erteilung von Auflagen zu Beschwerden der Betroffenen wegen unzureichenden Datenschutzes geführt haben.

Für das Forschungsprojekt einer hessischen Universität „Fluktuation im Sportverein“ sollte das Verhältnis der Jugend zum Sportverein und insbesondere die Gründe für ihr Abwandern aus dem Sportverein mit zunehmendem Alter erforscht werden. Aufgrund des o. g. Erlasses genehmigte der Hessische Kultusminister die „schriftliche Befragung von ca. 3 600 jugendlichen Schülern zwischen 12 und 18 Jahren aller Schulformen aller Regionen in Hessen mit standardisiertem Fragebogen ... im Schulklassenverband (90 Min.)“, nachdem der Projektleiter sich bereit erklärt hatte, das Kapitel „Einstellung zur Gesellschaft“ aus dem Fragebogen herauszunehmen.

Trotz dieses Verzichts bleiben Zweifel offen: Zwar heißt es im Genehmigungsantrag „Die Anonymität der Einzelperson ist voll gewährt ... jedem Schüler ist die Teilnahme freigestellt“; in der Praxis sind beide Aussagen jedoch zweifelhaft:

Obwohl die Fragebogen nicht mit Name und Adresse der Schüler versehen sind, ist eine Reindividualisierung möglich: Die Befragung wurde klassenweise durchgeführt, so daß die Befragungsergebnisse einer kleinen Menge zuzuordnen sind. Aufgrund der gestellten Fragen nach Geburtsjahr, Geschlecht, Größe, Gewicht, Brillenträger oder nicht, körperbehindert oder nicht, evtl. Bildungsabschluß sowie die eigene Mitgliedschaft oder die der Eltern in Vereinen, Gewerk-

⁸¹⁾ Az.: IV C 2-990/24, veröffentlicht im Amtsblatt des Hessischen Kultusministers 1977 S. 256 f.

⁸²⁾ Vgl. IV, 1.6, 1.7, 4.7.5; VI, 4.2.

schaften oder politischen Organisationen ist daher die Zuordnung des ausgefüllten Fragebogens zu einer Person ohne weiteres möglich.

Auch das Merkmal der freiwilligen Teilnahme ist nur bedingt erfüllt: Wenn im Rahmen des Schulunterrichtes die ganze Klasse aufgefordert wird, an einer Befragung teilzunehmen, so entsteht für den einzelnen Schüler ein psychologischer Zwang mitzumachen, dem insbesondere die jüngeren Jahrgänge sich nur schwer entziehen werden. Eine wirklich freiwillige Teilnahme kann nur dann vorliegen — dies gilt für die Schüler wie auch die Erziehungsberechtigten —, wenn die Auswirkungen einer alternativen Entscheidung zu übersehen sind. Dies setzt in jedem Fall die Kenntnis des gesamten Fragebogens vor dem Entscheid über eine Teilnahme voraus. Diese Voraussetzung wird aber in den wenigsten Fällen erfüllt, weil die Befrager die vorherige Bekanntgabe der Fragebogen ablehnen mit der Begründung, damit werde die Spontanität der Antwort eingeschränkt und damit der wissenschaftliche Wert der Befragung verfälscht.

Bei Kenntnis der Praxis solcher Schülerbefragungen während des Unterrichts, mit denen manche Schulen in den letzten Jahren geradezu überflutet wurden, erheben sich Zweifel, ob der wissenschaftliche Aussagewert solcher Befragungen nicht an ganz anderer Stelle leidet: In verständlichem Überdruß gegen die häufigen Befragungen sind einige Schulklassen dazu übergegangen, die Fragen laut vorzulesen und per Akklamation zu beantworten. So wird aus der langweiligen Befragung ein reizvolles Mannschaftsspiel. Ist aber der wissenschaftliche Wert solcher Erhebungen fraglich, dann müssen Zweifel erlaubt sein, ob die damit notwendigerweise verbundene Gefährdung der schutzwürdigen Belange der Jugendlichen und ihrer Erziehungsberechtigten noch vertretbar ist.

Obwohl ich bereits in meinem Vierten Tätigkeitsbericht⁸³⁾ betont hatte: „Aus der Schulpflicht ergibt sich nicht die Pflicht zur Teilnahme an wissenschaftlichen Testuntersuchungen. Es ist auch nicht primäre Aufgabe der Schule, die Schüler für Forschungszwecke bereitzustellen“, ist die Zahl der Schülerbefragungen weiter angestiegen. Es sollte überlegt werden, ob dieses Übermaß an Befragungen der Schüler für wissenschaftliche Zwecke nicht herabgesetzt werden sollte und ob nicht bei allen Beteiligten, nämlich bei Schule und Elternhaus wie auch bei Forschern und bei der Schulverwaltung ein Prozeß des Umdenkens einsetzen sollte.

Es ist kennzeichnend für die Situation, daß im Zusammenhang mit dem Projekt „Fluktuation im

Sportverein“ ein Landtagsabgeordneter öffentlich von „rechtswidriger Gesinnungsschnüffelei“ gesprochen und seine Meinung zum Ausdruck gebracht hat, die Fragebögen seien „eindeutig auf eine unzulässige Ausforschung der Privatsphäre der Familie“ abgestellt.

6.3 **Angaben über Schüler gegenüber Außenstehenden**

Im Rahmen des gegenseitigen Informationsaustausches übermittelte mir der Kultusminister den Entwurf eines Erlasses über die Bekanntgabe der Personalien von Schülern, der den Schulen die Entscheidung darüber erleichtern soll, ob sie im Einzelfall die Daten eines Schülers weitergeben dürfen oder nicht. Solche Anforderungen von Daten erhalten die Schulen von Firmen (z. B. Versicherungen, Sparkassen), Vereinen, Kirchen, Verbänden. Aufgrund meiner Anregungen konnte der Text präzisiert werden. Es wurde festgelegt, daß Angaben über Schüler, wie Namen und Anschriften Außenstehenden, gegenüber grundsätzlich nicht gemacht werden dürfen. Die Ausnahmen von diesem Grundsatz (z. B. Amtshilfe, Weitergabe an Kirchen) wurden entsprechend den Erfordernissen des Datenschutzes genau abgegrenzt.

6.4 **Hochschulstatistik**

Ohne gesetzliche Grundlage darf die Verwaltung dem Bürger keine Auskünfte abverlangen. Die in den Datenschutzgesetzen enthaltene Verpflichtung, den Bürger bei einer Erhebung über die Rechtsgrundlage für seine Auskunftspflicht bzw. über die Freiwilligkeit seiner Angaben aufzuklären (§ 11 Abs. 2 HDSG, § 9 Abs. 2 BDSG) dient der praktischen Durchsetzung dieses Prinzips. Auch bei der Durchführung von Bundesstatistiken besteht eine entsprechende Belehrungspflicht (§ 7 Bundesstatistikgesetz). Im Berichtszeitraum wurden zwei Verstöße gegen diesen Grundsatz bekannt.

In dem einen Fall handelt es sich um eine Personalerhebung, die das Hessische Statistische Landesamt auf der Grundlage des Hochschulstatistikgesetzes eingeleitet hat. Der auskunftspflichtige Personenkreis ist im Gesetz genau bestimmt. Er umfaßt „wissenschaftliches und künstlerisches Personal, Lehrkräfte für besondere Aufgaben, Lehrbeauftragte, Tutoren und nichtstudentische wissenschaftliche Hilfskräfte“. In die Erhebung wurde jedoch auch „übriges Personal im höheren Dienst“ einbezogen. Auf meine Beanstandung hin hat der Hessische Ministerpräsident — Staatskanzlei — als Aufsichtsbehörde mitgeteilt, daß der betreffende Personenkreis nicht weiter befragt und bereits ausgefüllte Erhebungsbögen vernichtet

⁸³⁾ IV, 4.7.5.

werden. Das „übrige Personal im höheren Dienst“ sei entsprechend einer bundeseinheitlichen Absprache der statistischen Ämter einbezogen worden, wobei man davon ausgegangen sei, daß das Personal im höheren Dienst aufgrund seiner Ausbildung als wissenschaftliches Personal angesehen werden könne. Eine Trennung des sonstigen Personals vom wissenschaftlichen und künstlerischen nach anderen Kriterien sei praktisch nicht durchführbar erschienen.

Angesichts der Tatsache, daß das Hochschulstatistikgesetz „Wissenschaftliches und künstlerisches Personal“ (§ 7) und „Technisches, Verwaltungs- und sonstiges Personal“ (Überschrift § 8) ausdrücklich unterscheidet, vermag diese Erklärung schwerlich zu überzeugen. Es besteht eher der Eindruck, daß die Konferenz der statistischen Ämter sich allein von organisatorischen Erwägungen leiten und dabei den Anspruch der Betroffenen, nicht ohne gesetzliche Grundlage zu Auskünften herangezogen zu werden, unbeachtet ließ. Ich habe die Präsidenten der statistischen Ämter der anderen Länder und des Statistischen Bundesamtes von meinen rechtlichen Bedenken unterrichtet. Denn unabhängig von diesen Bedenken kann nur durch eine bundeseinheitliche Korrektur die Vergleichbarkeit der statistischen Ergebnisse gesichert werden.

Im zweiten Fall wurde ich davon unterrichtet, daß an den Hochschulen des Landes für die Erhebung von Daten der Studenten eine Stammkarte verwendet wird, in der eine Reihe von Auskünften abverlangt werden, für die es keine gesetzliche Grundlage gibt. Der Hinweis auf der Stammkarte über die Rechtsgrundlage vermittelt jedoch den Eindruck, für alle Fragen bestehe nach dem Hochschulstatistikgesetz oder nach den Allgemeinen Vorschriften für Studierende eine rechtliche Auskunftspflicht. Die Stammkarte enthält weiter eine drucktechnisch hervorgehobene Warnung „Achtung ... unvollständig ausgefüllte Anträge ... werden nicht bearbeitet“. Ohne gesetzliche Grundlage wird beispielsweise gefragt „Ehepartner (nur ausfüllen, wenn verheiratet) Student: ja/nein; berufstätig: ja/nein; Kinderzahl (wieviele, wieviele unter 6 Jahren); wie kommen sie vorwiegend zur Hochschule (Verkehrsmittel); wohnen sie bei Eltern, Verwandten, in Privatzimmer, in Wohnheim, in Wohngemeinschaft, in eigener Wohnung, sonstiges; Tätigkeiten vor Beginn des Studiums (Art und Dauer); Finanzierung des Studiums (Mittel der Eltern, des Ehegatten, Eigenerwerbstätigkeit, staatliche Förderung, sonstiges Mittel); Name, Anschrift und Telefon des Vaters, der Mutter oder des Ehegatten“. Der auf der Stammkarte weiter aufgedruckte Hinweis auf die statistische Geheimhaltung vermittelt den Ein-

druck, alle auf der Stammkarte enthaltenen Auskünfte unterlägen der statistischen Geheimhaltung. Dies trifft jedoch nur für einen Teil der Angaben zu. Ich habe den Kultusminister darauf aufmerksam gemacht. Sein Ministerium teilte mir mit, daß meine Anregung „aus terminlichen Gründen bei der Drucklegung für die Formblätter bis zum Sommersemester 1978 nicht mehr berücksichtigt werden“ könne. Ich habe in meiner Antwort betont, daß mich der in der Erklärung „zum Ausdruck kommende Mangel an Respekt vor der persönlichen Integrität der Betroffenen beunruhigt“ und angeregt,

- „die Erhebung umgehend den Anforderungen des Datenschutzes (vgl. § 9 BDSG, § 11 HDSG, § 19 Abs. 4 HStatG) anzupassen und
- die in der Vergangenheit unzulässig erhobenen Daten zu löschen bzw. anonymisieren.“

Dieser Anregung ist das Kultusministerium in einem Erlaß an die Präsidenten und Rektoren der hessischen Hochschulen nur teilweise gefolgt.

Parallel zu meinen Bemühungen um eine Verbesserung des Datenschutzes in der Hochschulstatistik hat auch der Bundesbeauftragte für den Datenschutz beim Bundesminister für Bildung und Wissenschaft Bedenken erhoben gegen die Erhebungsprogramme des Statistischen Bundesamtes

- für die Statistik der Prüfungskandidaten (§ 3 Nr. 10 HStatG), soweit darin Angaben über die Berechtigung zum Hochschulstudium erfragt werden und
- über wissenschaftliches und künstlerisches Personal (§ 3 Nr. 4 HStatG), soweit darin nach der Personalnummer der Hochschule und nach weiteren anzeigepflichtigen Beschäftigungen gefragt wird.

6.5 Datenschutz im Bereich der Volkshochschulen

Im Bereich des Volkshochschulwesens sind Datenschutzprobleme bei der Erhebung von Name und Anschrift von Kursteilnehmern sowie bei der Erhebung personenbezogener Daten für die Statistik bei der Anmeldung von Kursteilnehmern entstanden.

So hatte eine Kreisvolkshochschule, die Landeszuschüsse für die örtlichen Volkshochschulen beantragt und sie verteilt, im Gegensatz zu früheren Jahren Sammel-Daten über die durchgeführten Kurse als Verwendungsnachweis nicht akzeptiert, sondern unter Hinweis auf die Rechnungsprüfung durch das Land verlangt, daß für jede Veranstaltung eine Liste der Teilnehmer mit Namen, Vornamen, Anschrift, Telefon, Beruf, Altersgruppe,

Zahlung der Gebühr und Angaben zur Anwesenheit bei den einzelnen Kursstunden vorgelegt wird. Eine örtliche Volkshochschule hatte Bedenken, personenbezogene Daten ihrer Kursteilnehmer weiterzugeben. Ich habe dazu die Auffassung vertreten, daß die Teilnehmer der Veranstaltungen, die mit öffentlichen Mitteln gefördert werden, grundsätzlich hinnehmen müssen, daß Angaben zu ihrer Person außer dem Träger der Bildungseinrichtung auch den mit der Prüfung der ordnungsgemäßen Mittelverwendung befaßten öffentlichen Stellen zugänglich sind. Als Kompromiß hatte ich vorgeschlagen, der Kreisvolkshochschule anonymisierte Teilnehmerlisten zu übergeben, die Original-Listen jedoch bei der Volkshochschule aufzubewahren und sie, sollte ihre Kenntnis im Einzelfall für die Prüfung notwendig werden, den Rechnungsprüfern unmittelbar zugänglich zu machen.

Die Überprüfung des Falles durch den Hessischen Kultusminister und den Hessischen Rechnungshof hat ergeben, daß im Interesse einer effektiven Rechnungsprüfung und zur Erschwerung von Manipulationen mit fiktiven Teilnehmern — wie sie in der Vergangenheit mehrmals aufgetreten seien — auf die Übermittlung der Teilnehmerlisten für die einzelnen Kurse an das zuständige Rechnungsprüfungsamt nicht verzichtet werden könne. Außerdem sei eine Gefährdung schutzwürdiger Belange der Betroffenen durch die Übermittlung nicht gegeben, da die Daten nur zum Zwecke der Rechnungsprüfung verwendet und keinen dritten Personen zur Kenntnis gegeben würden. Schließlich sei auch aus formalen Gründen („keine Datei“) zweifelhaft, ob das Hessische Datenschutzgesetz auf diesen Fall anwendbar sei.

Datenschutzrechtlich kann gegen die von den

Landesbehörden vertretene Auffassung nichts eingewendet werden: Einerlei, ob die Volkshochschule — als privatrechtlich organisierter Verein — vertraglich verpflichtet ist, dem Volkshochschulträger (Stadt, Kreis) die Teilnehmerdaten zu übermitteln, oder ob die Volkshochschule als — öffentlich-rechtlich organisierte — Dienststelle des Magistrats verpflichtet ist, der Anforderung des Rechnungsprüfungsamtes Folge zu leisten: Die jeweiligen Voraussetzungen für die Datenübermittlung (§ 24 BDSG, § 12 HDSG) müssen als gegeben angesehen werden.

In einem anderen Falle ging es um die Beschwerde eines Bürgers wegen der von der Volkshochschule verwendeten Anmeldeformulare. Beispielsweise wurden von dem Hörer eines Kurses Angaben über Alter, Schulbildung und berufliche Stellung verlangt, die für die Aufgabe der Volkshochschule nicht erforderlich seien und für die es keine Rechtsgrundlage gebe. Wie ich feststellte, werden diese Daten zwar für statistische Zwecke verwendet, jedoch personenbezogen erhoben. Die Erhebung erfolgt aufgrund eines Erlasses des Kultusministers nach § 6 (1) der Richtlinien zum Volkshochschulgesetz. Eine gesetzliche Grundlage nach §§ 7 bzw. 11 Abs. 2 HDSG fehlt. Ohne Zweifel aber sind für den Nachweis über die geleistete Arbeit statistische Übersichten wünschenswert. Der Hessische Volkshochschulverband hat daher aufgrund meiner Beanstandung veranlaßt, daß auf allen Anmeldeformularen, die mit Angaben zur Person untrennbar verbunden sind, ab sofort der Hinweis erfolgt: „Freiwillige Angabe zu statistischen Zwecken — Weitergabe nur anonym.“ Nach einem Jahr sollen die Konsequenzen dieses Hinweises auf der Anmeldekarte für die Statistik überprüft werden.

7. PERSONALWESEN

7. Personalwesen

7.1 Unbefugte Übermittlung der Adressen von Lehramtskandidaten und Referendaren

Aufgrund von Pressemeldungen und Beschwerden einzelner Betroffener wurde mir bekannt, daß in einer offenbar nicht geringen Zahl von Fällen Adressen von Lehramtskandidaten, Studien- und Rechtsreferendaren unbefugt an Versicherungsunternehmen, Parteien oder andere private Stellen weitergeleitet worden sind. Trotz umfangreicher Ermittlungen, die aufgrund meiner Anregung vom Hessischen Kultusminister, vom Hessischen Minister der Justiz und den beiden Regierungspräsidenten angestellt wurden, konnte nicht geklärt werden, welche Personen oder Stellen entsprechende Informationen aus der Verwaltung weitergegeben haben. Aufgrund dieser Vorfälle haben der Kultusminister – und ähnlich der Minister der Justiz – durch Rundverfügung alle betroffenen Verwaltungsstellen nochmals darauf hingewiesen, „daß Adressenmaterial und andere Personaldaten der Referenten grundsätzlich nicht an Dritte zur Verwendung für privatwirtschaftliche Zwecke weitergegeben werden dürfen“. Darüber hinaus wurden die zuständigen Mitarbeiter auf die in Personalangelegenheiten bestehende Verschwiegenheitspflicht hingewiesen und disziplinarrechtliche Maßnahmen bei Nichtbeachtung dieser Verpflichtung angekündigt. Entsprechende Maßnahmen hinsichtlich der unbefugten Weitergabe der Adressen von Lehramtskandidaten wurden bereits zu einem früheren Zeitpunkt von den Regierungspräsidenten getroffen.

7.2 Datenschutz bei Eignungsprüfungen

Das Land Hessen und einige kommunale Gebietskörperschaften sind an einer als eingetragener Verein organisierten privaten Gesellschaft beteiligt, die in ihrem Auftrag Einstellungstests für Bewerber des mittleren und gehobenen Dienstes durchführt. Die Eignungsprüfungen erfolgen nach den „Richtlinien für die Durchführung von Eignungsprüfungen bei der Einstellung von Bewerbern in die staatlichen Verwaltungen“, die der Direktor des Landespersonalamtes Hessen am 20. Juli 1971 erlassen hat⁸⁴⁾. Die umfangreichen Tests werden von der Gesellschaft zu einem „psychologischen Untersuchungsbefund“ ausgewertet, aus

dem ein „Anforderungsprofil“ erstellt wird. Die Übermittlung der Untersuchungsbefunde an die auftraggebende Behörde hält sich im Rahmen des § 12 HDSG. Eine Gefährdung des Datenschutzes der betroffenen Bewerber könnte allerdings darin gesehen werden, daß die gesamten, für die Tests verwendeten Fragebögen sowie die durch Auswertung daraus gewonnenen Befundbögen bei der Gesellschaft bzw. deren Auftraggebern nicht nur auf unbestimmte Zeit aufbewahrt, sondern auch – ohne Wissen und Einwilligung des Betroffenen – für Forschungszwecke an andere Stellen weitergegeben werden. Ich halte dieses Verfahren für unzulässig: Die Vorschriften der §§ 7 und 11 HDSG lassen eine Speicherung der mit den Fragebögen erhobenen Angaben nur bis zur Zweckerreichung zu, d. h. bis zur Erstellung des Untersuchungsbefundes und einer Eignungsbewertung. Danach müssen die ursprünglichen Unterlagen vernichtet werden. Eine Weitergabe des Untersuchungsbefundes bzw. des Anforderungsprofils an andere Stellen ist grundsätzlich nur mit Einwilligung des Betroffenen zulässig.

7.3 Speicherung und Abrechnung von Telefongesprächen

In mehreren Eingaben und Beschwerden wurde ich darüber unterrichtet, daß zur Abrechnung und zur Kontrolle von Telefongesprächen, die über amtliche Apparate laufen, Listen geführt werden. Darin sollen über die einzelnen Gespräche Informationen enthalten sein, die für die Kontrolle nicht benötigt werden. Außerdem sollen diese Listen oft nur unzureichend vor dem Zugriff Unbefugter geschützt sein. Ich habe daraufhin die Praxis in einigen öffentlichen Dienststellen in Hessen überprüft. Dabei stellte ich fest, daß in manchen Fällen Daten erfaßt und gespeichert werden, die für die Abrechnung nicht erforderlich sind.

Inzwischen hat die Aktion eines Stadtschulamtes zur tabellarischen Erfassung aller von Schulen ausgeführten Telefongespräche zu einer parlamentarischen Anfrage geführt⁸⁵⁾. Der Hessische Kultusminister hat in seiner Stellungnahme das Verfahren im Interesse einer Kostensenkung für „sachgerecht und vertretbar“ befunden, nachdem aufgrund der Beschwerden der Umfang der erfaßten Daten wesentlich eingeschränkt worden war. Während ursprünglich von allen dienstlichen und

⁸⁴⁾ StAnz. S. 1290.

⁸⁵⁾ LT-Drucks. 8/4901.

privaten Orts- und Ferngesprächen das Gesprächsdatum, der Name des Anrufers, Vorwahl- und Anschlußnummer des Gesprächsteilnehmers und die Zahl der Gesprächseinheiten festgehalten werden sollten, werden jetzt nur noch dienstliche und private Ferngespräche erfaßt. Bei letzteren werden für die Abrechnung nur noch der Name des Anrufers, das Datum und die Zahl der Gesprächseinheiten für die Abrechnung weitergegeben.

Ein Urteil des Bremer Verwaltungsgerichts über die Speicherung und Abrechnung von Telefongesprächen, die über dienstliche Apparate gelaufen sind, hatte zuvor in der Presse Schlagzeilen gemacht. In dem noch nicht rechtskräftigen Urteil vom 15. Juni 1977 (I A 39/77) wird festgestellt, daß es mangels gesetzlicher Grundlage mit dem in Art. 10 GG garantierten Fernmeldegeheimnis unvereinbar ist, wenn eine Behörde die von ihren Fernsprechern ausgeführten Telefongespräche ohne Einwilligung des betroffenen Bediensteten nach der Telefonnummer des Angerufenen, dem Datum und der Uhrzeit des Gesprächs registriert. Auch das Bemühen um sparsamen Umgang mit öffentlichen Mitteln berechtige nicht zum Eingriff in das Fernmeldegeheimnis. Diese Frage könne nicht fernmelderechtlich, sondern nur dienstrechtlich gelöst werden.

Dagegen hat die Aufsichtsbehörde des Landes Baden-Württemberg in einer Veröffentlichung im Staatsanzeiger vom 1. 7. 1978 die Erfassung und Speicherung von Telefondaten in Wirtschaftsunternehmen für zulässig erklärt, wenn sie für die Kostenrechnung, die Abrechnung von Privatgesprächen und die Kontrolle erforderlich seien. Die Einführung und Anwendung der automatischen Telefonüberwachung unterliege allerdings gemäß § 87 Abs. 1 Nr. 6 des Betriebsverfassungsgesetzes der Mitbestimmung des Betriebsrats.

Aufgrund meiner Beobachtungen bei den von mir überprüften Behörden habe ich der Hessischen Landesregierung vorgeschlagen, sie möge alle Behörden sowie die nachgeordneten und die ihrer Aufsicht unterstehenden öffentlichen Stellen und juristischen Personen des öffentlichen Rechts und deren Vereinigungen darauf hinweisen, daß bei der Überprüfung und Abrechnung von Telefongesprächen, die über amtliche Telefonanschlüsse geführt werden, folgende Grundsätze beachtet werden sollten:

- Alle Bediensteten sind darüber zu unterrichten, daß die von ihnen geführten Gespräche registriert werden, und welche Stellen Unterlagen zur Kontrolle dienstlicher bzw. zur Abrechnung privater Ferngespräche erhalten.
- Die Unterlagen über die geführten Telefongespräche sind so aufzubewahren, daß kein Unbefugter sie einsehen, kopieren oder sich aneignen kann.
- Die zur Kontrolle dienstlicher Ferngespräche erforderlichen Angaben über den Zeitpunkt, die Vorwahl- und Anschlußnummer sowie die Zahl der Gesprächseinheiten sind in geschlossenen Umschlägen an die mit der Kontrolle beauftragte Stelle weiterzuleiten. Nach erfolgter Kontrolle sind die Unterlagen zu vernichten, sofern sie nicht später noch benötigt werden. In diesem Fall sind sie zu sperren.
- Die Unterlagen zur Abrechnung von privaten Telefongesprächen sind dem anmeldenden Nebenanschlußinhaber in einem geschlossenen Umschlag zuzuleiten.
- Der Stelle, bei der private Gespräche zu bezahlen sind, wird nur der Name des Nebenanschlußinhabers und die Zahl der Gesprächseinheiten bzw. die zu entrichtende Gesamtsumme mitgeteilt.

8. GESUNDHEITSWESEN

8. Gesundheitswesen

8.1 Schulsportärztlicher Untersuchungsbogen

Bei dem vorwiegend zur Förderung des Leistungssports verwendeten schulsportärztlichen Untersuchungsbogen⁸⁶⁾ zeigten wiederholte Beschwerden von Bürgern, daß die Praxis nicht immer den Datenschutz ausreichend berücksichtigte. Insbesondere ging es dabei um die Freiwilligkeit der Teilnahme der Schüler und um die Information und Einwilligung der gesetzlichen Vertreter. Kritisiert wurden ferner Fragen wie „Familienstand der Eltern?“, „Werden sie leicht wütend oder sind sie launisch?“ oder „quälen sie sich selbst oder sind sie rücksichtslos gegen andere?“.

Auf meine Anregung hat der Hessische Sozialminister veranlaßt, daß der für den schulsportärztlichen Untersuchungsbogen bisher verwendete Fragebogen überarbeitet wurde. Darüber hinaus wurde den schulsportärztlichen Untersuchungszentren aufgetragen sicherzustellen, daß nur Untersuchungsbögen zur Auswertung weitergeleitet werden, die eine Einwilligungserklärung der Erziehungsberechtigten enthalten. Um den Sportlern bzw. ihren Eltern die Entscheidung zu erleichtern, soll in einem besonderen Informationsschreiben dargestellt werden, „warum die sportärztliche Untersuchung einen notwendigen Bestandteil vom Leistungssport darstellt“, und daß die Zusammenführung der erhobenen Daten und Befunde mit Namen und Anschrift des betreffenden Sportlers allein der zuständigen sportärztlichen Untersuchungsstelle möglich ist.

Trotz dieser Maßnahmen hat die sportärztliche Untersuchungsstelle beim Gesundheitsamt einer hessischen Großstadt den beanstandeten alten Anamnesebogen noch rund ein Jahr weiterverwendet. Ich halte ein solches Verhalten für bedenklich. Werden Fragebogen aufgrund meiner oder anderer Beanstandungen in wichtigen Punkten geändert, so muß sichergestellt sein, daß die alten Formulare nicht weiter verwendet werden. Der Bürger hat Anspruch darauf, daß die Verwaltung erkannte Datenschutzmängel rasch und unbürokratisch beseitigt.

8.2 Vorsorgeuntersuchung bei der Einschulung

Zur Feststellung der Schulreife werden von den Gesundheitsämtern bei Kindern im Vorschulalter

Vorsorgeuntersuchungen durchgeführt. Zur Vorbereitung werden Fragebogen verwendet, die vom Kindergarten bzw. der zuständigen Grundschule ausgegeben und auch wieder zurückgefordert werden. Die Art und Weise der Befragung, deren Rechtsgrundlage zum Teil noch auf der Dienstordnung für Gesundheitsämter vom 30. März 1935 beruht, entspricht nicht den Grundsätzen des Datenschutzes. Bevor mir bekannt wurde, daß der Fragebogen bei allen Gesundheitsämtern verwendet wird, hatte ich aufgrund von Bürgerbeschwerden bereits in mehreren Einzelfällen das Verfahren beanstandet. So war bei der Datenerhebung für den Betroffenen nicht erkennbar, ob sie auf gesetzlicher Grundlage oder aufgrund freiwilliger Angaben erfolgte; auch ließ sich aus den Fragebögen meist nicht erkennen, für welchen Zweck die Daten erhoben wurden, welche Stellen Kenntnis davon erlangen bzw. an wen die Daten weitergegeben werden. Diese Angaben sind jedoch bei einer Datenerhebung auf freiwilliger Grundlage für die Entscheidung des Erziehungsberechtigten über die Teilnahme seines Kindes unbedingt notwendig. In dem Fragebogen werden sehr ins Detail gehende Angaben hinsichtlich der medizinischen und sozialen Anamnese nicht nur des Kindes, sondern auch der Familie — also dritter Personen — verlangt. So wurde unter anderem nach „Geistes- oder Gemütskrankheiten in der Familie“ gefragt, nach dem Familienstand und dem Beruf der Eltern, danach, ob das Kind ein eigenes Zimmer, ein eigenes Bett habe, ob es Bettnäse sei usw. Soweit diese Fragen nicht gemäß §§ 7 und 11 Abs. 1 HDSG aufgrund einer Rechtsvorschrift erhoben werden, sollte in jedem Einzelfall geprüft werden, ob die Frage zur Beurteilung der Schulfähigkeit des Kindes notwendig ist.

Schließlich hatte ich kritisiert, daß in einigen Fällen die Fragebögen von dem Verwaltungspersonal des Kindergartens bzw. der Schule ausgegeben und auch wieder eingesammelt wurden, obwohl die Kenntnis der erhobenen Daten nur für den Schularzt bestimmt ist.

Die mit dem Fragebogen erhobenen Daten sollten nach Abschluß der Schulreifeuntersuchung des Kindes gemäß § 19 Abs. 3 HDSG gelöscht werden. Erfahrungsgemäß bringt nämlich die Speicherung solcher Daten über längere Zeit ein erhöhtes Datenschutzrisiko mit sich.

Der Hessische Sozialminister hat mir aufgrund

⁸⁶⁾ Vgl. III, 4.1.1.3; IV, 4.7.1, 4.7.2.

meiner Anfrage mitgeteilt, daß die vom jugendärztlichen Dienst der Gesundheitsämter aufgrund früherer Erlasse verwendeten Fragebögen zur Zeit „unter Zuziehung namhafter Sachverständiger und Kinderärzte der jugendärztlichen Praxis“ überarbeitet werden. Dabei will man die Belange des Datenschutzes berücksichtigen. Ich habe die Anregung gegeben, in Hessen künftig keine alten Formulare mehr zu verwenden. Das Land Niedersachsen hat bei einem ähnlichen Fragebogen bereits dessen Verwendung bzw. Weitergabe an die Schulen untersagt, „da er in weiten Teilen als problematisch anzusehen ist und auch Fragen des Datenschutzes berührt werden“.

8.3 Auskunftsrecht des Patienten

Das im Zusammenhang mit Fragen des Datenschutzes unter Medizinern mit am meisten diskutierte Thema ist die Frage der praktischen Ausgestaltung des Auskunftsrechts des Bürgers über seine medizinischen Daten: Mit Inkrafttreten des neuen Hessischen Datenschutzgesetzes gilt allgemein — also auch für den medizinischen Bereich — das in § 18 HDSG geregelte Auskunftsrecht des Betroffenen. Das bedeutet, daß ohne eine einschränkende spezialgesetzliche Regelung jeder Bürger von allen Stellen, die seine medizinischen Daten speichern, unbeschränkt Auskunft darüber verlangen kann, welche medizinischen Daten über ihn gespeichert sind, beispielsweise auch von der Allgemeinen Ortskrankenkasse.

In diesem Zusammenhang ist darauf hinzuweisen, daß das Hessische Krankenhausgesetz vom 4. 4. 1973 (HKG)⁸⁷⁾ in § 14 Abs. 1 dem Patienten ein unbeschränktes Auskunftsrecht darüber einräumt, „welche medizinischen Daten über ihn gespeichert und an welche Stellen sie weitergeleitet werden“. Es regelt jedoch nicht die Art und Weise, wie dieses Recht verwirklicht wird; auch ist die Anwendbarkeit des HKG bisher zweifelhaft, da die dafür bestimmte Voraussetzung, nämlich ein Verbund mehrerer Krankenhäuser, noch nicht besteht. Eine spezialgesetzliche Regelung erscheint daher wünschenswert.

Die Praxis hat erwiesen, daß es in der großen Mehrzahl aller Fälle für den Patienten wichtig ist zu erfahren, welche ärztlichen Leistungen für ihn erbracht worden sind; Privatpatienten erfahren dies ohnehin durch die ihnen vom Arzt übermittelte Rechnung. Andererseits muß gesehen werden, daß bei lebensbedrohenden Krankheiten — wie z. B. Krebs — Zeit und Umfang der Mitteilung darüber an den Patienten nur von dem behandelnden Arzt richtig eingeschätzt werden kann. Eine

unvermittelte Auskunft dieser Art, beispielsweise durch eine Krankenhausverwaltung oder Krankenkasse, könnte manchen Patienten zu Kurzschlußhandlungen veranlassen. Diese Überlegung darf jedoch nicht zu der von einigen Ärztevertretern erhobenen Forderung führen, daß der Patient über die bei Krankenhäusern, Gesundheitsämtern, Sozialversicherungsträgern und anderen Stellen über ihn gespeicherten medizinischen Daten generell keine Auskunft erhalten soll. Auch die Rechtsprechung zum Arztrecht hat anerkannt, daß das Selbstbestimmungsrecht des Bürgers als Patient nicht allgemein von der Pflicht des Arztes, das Wohl des Kranken zu fördern, verdrängt wird, sondern vielmehr im Einzelfall der Abwägung bedarf. Es muß daher eine differenzierende Lösung gefunden werden, die von dem Grundsatz des Auskunftsrechts des Bürgers ausgehend für bestimmte Fälle Einschränkungen oestattet.

Der Gesetzgeber hat die Möglichkeit, für den Bereich des Gesundheitswesens besondere gesetzliche Bestimmungen zu erlassen, die die Ausgestaltung des Auskunftsrechts für diesen Bereich im einzelnen regeln. Diese Bestimmungen würden als „lex specialis“ denen des Hessischen Datenschutzgesetzes vorgehen. Sozialversicherungsträger, Ärztekammern und Ärzteverbände sowie Krankenhausverwaltungen und Gesundheitsämter sind dringend an einer baldigen Lösung dieser Frage interessiert. Es sollte deshalb unter Federführung des Hessischen Sozialministers evtl. im Wege einer Sachverständigenanhörung und unter Beteiligung der Verbraucherverbände ein praktischer Lösungsvorschlag gesucht werden.

8.4 Krebsregister

Im Zusammenhang mit Krebs-Vorsorgeuntersuchungen erhielt ich Anfragen aus der Bevölkerung, ob bei bestehenden Krebsregistern der Datenschutz gewährleistet sei. Der Hessische Sozialminister teilte mir auf meine Erkundigung mit, daß für das Land Hessen „kein sog. Krebsregister geführt wird und vorläufig auch kein solches geplant ist“. Allerdings ist nach Ansicht von Fachleuten der Aufbau von Krebsregistern dringend notwendig, da nur so aussagekräftige Daten über Krebserkrankungen zu ermitteln sind. Sollte in Zukunft für Hessen ein entsprechendes Projekt in Angriff genommen werden, so werde ich dabei bereits in der Entwicklungsphase die Forderungen des Datenschutzes zur Sprache bringen. Dies ist notwendig: Wie das im Saarland ergangene Verbot für das Krebsregister erweist, fehlt bisher eine gesetzliche Grundlage für eine solche Aufgabe, die einen starken Eingriff in das Persönlichkeitsrecht des Bürgers bewirkt.

⁸⁷⁾ GVBl. I S. 145.

9. SOZIALWESEN

9. Sozialwesen

9.1 Projekt einer „Heimkinderdatei“

Das Hessische Sozialministerium hat mich frühzeitig über die Datenschutzprobleme bei dem Projekt „Heimkinderdatei“ unterrichtet. In der Datei werden Individualdaten gespeichert; sie wird aber auch für Planungszwecke ausgewertet, für die nur aggregierte Daten erforderlich sind. In Zusammenarbeit mit den beteiligten Dienststellen – Sozialministerium, Innenministerium, Landesjugendamt, Landeswohlfahrtsverband, Hessische Zentrale für Datenverarbeitung und Hessischer Datenschutzbeauftragter – wird z. Z. nach einer den Datenschutz befriedigenden Lösung gesucht.

Die „Heimkinderdatei“ dient einmal der Adoptionsvermittlung. Nach § 12 des Adoptionsvermittlungsgesetzes (AdVermG) vom 2. 7. 1976⁸⁸⁾ hat die zentrale Adoptionsstelle des Landesjugendamtes zu prüfen, für welche Heimkinder die Annahme als Kind in Betracht kommt. Deshalb verpflichtet § 78 a des Jugendwohlfahrtsgesetzes (JWG) vom 25. 4. 1977⁸⁹⁾ die Heimträger, dem Landesjugendamt die in den Heimen untergebrachten Minderjährigen zu melden. Die Meldung enthält außer dem Namen noch eine Reihe von Individualdaten zur Person des Kindes und zu seiner Familie. Diese für die Adoption benötigten Daten sollen in der „Heimkinderdatei“ in individualisierter Form gespeichert werden. Die Datei soll aber auch für eine sachgerechte Heimplanung ausgewertet werden. Dafür ist jedoch nur die Kenntnis aggregierter Daten erforderlich. Notwendig ist daher eine genaue Zugriffsregelung für die einzelnen Daten der Datei und entsprechende Maßnahmen der Datensicherung. Die organisatorische und technische Lösung wird z. Z. gesucht. Dabei besteht zwischen den beteiligten Dienststellen Einigkeit darüber, daß auf die Individualdaten der Datei nur die Adoptionsvermittlungsstelle beim Landesjugendamt Zugriff haben darf.

Aufgrund der o. a. Gesetze wurde für die Adoptionsvermittlung ein Fragebogen entwickelt, der eine Anzahl meist sehr sensibler Daten enthält; einmal über die Jugendlichen selbst (körperliche, geistige oder seelische Behinderung, Schwierigkeiten im Schulbesuch oder der Berufsausbildung, Erziehungsschwierigkeiten) und zum anderen

über ihre Eltern (Gesundheitszustand, geistige Behinderung oder psychologische Erkrankung, Scheidung/Trennung, Erziehungsunfähigkeit, Vernachlässigung oder Mißhandlung des Kindes). Diese Daten werden z. Z. ohne Wissen und Zustimmung der Eltern erhoben. Der Datenschutzgrundsatz, daß die Datenverarbeitung nur zulässig ist aufgrund einer Rechtsvorschrift oder mit Einwilligung des Betroffenen (§ 7 HDStG), wird zwar bei der Datenerhebung für die Adoptionsvermittlung nach § 78 a JWG und § 12 AdVermG erfüllt. Trotzdem sollte – worauf der Landeswohlfahrtsverband hingewiesen hat – überlegt werden, ob der Betroffene nicht von der Speicherung, ähnlich wie in § 14 Hessisches Krankenhausgesetz, unterrichtet werden müßte: dies ist jedoch keine Entscheidung der Verwaltung; vielmehr müßte der Gesetzgeber die Bestimmungen entsprechend ergänzen. Da das JWG gegenwärtig novelliert wird, sollte die Landesregierung über den Bundesrat eine entsprechende Ergänzung des Gesetzes vorschlagen.

9.2 Zuschußgewährung an Behinderten-Clubs

Die Landesarbeitsgemeinschaft der Hessischen Clubs Behinderter und ihrer Freunde hatte sich mit der Beschwerde an mich gewandt, das Sozialamt einer hessischen Großstadt verlange als Voraussetzung für einen Zuschuß zur Behindertenarbeit der in der Landesarbeitsgemeinschaft zusammengeschlossenen Clubs eine Liste mit Namen und Adressen der diesen angehörenden Mitglieder. Diese Praxis verstoße gegen den Datenschutz, zumal es sich nicht um Beihilfen und Zuschüsse an Einzelpersonen, sondern jeweils an einen Verein handele.

Es liegt auf der Hand, daß die Anlage einer Datei mit Namen und Adressen der Mitglieder von Behinderten-Clubs für diese eine Beeinträchtigung ihrer schutzwürdigen Belange bedeuten kann, da es sich um besonders sensitive Daten handelt – insbesondere, wenn aus der Club-Bezeichnung die Art der Behinderung (z. B. Blinde) deutlich wird – und nicht erkennbar ist, an welche Stellen die geforderten Daten übermittelt werden sollen oder wer auf sie Zugriff haben kann. Die betreffende Stadt machte geltend, mit der Anforderung der Mitgliederlisten solle lediglich ausgeschlossen werden, daß infolge Doppelmitgliedschaften in mehreren Clubs die Bemessung des Zuschusses von falschen Berechnungen ausgehen würde. Al-

⁸⁸⁾ BGBl. I S. 1262.

⁸⁹⁾ BGBl. I S. 633.

lerdings sollte man einen aus der Sicht des Datenschutzes problematischen Bemessungsmodus nur dann anwenden, wenn es keine andere Möglichkeiten der gerechten Verteilung von Zuschüssen gibt. Nach dem in § 7 HDSG enthaltenen Grundsatz ist eine Registrierung von Behinderten nur

aufgrund einer Rechtsvorschrift oder mit Zustimmung der Betroffenen zulässig. Diese Voraussetzungen waren im geschilderten Fall nicht erfüllt. Auf meine Anregung hin wurde eine einvernehmliche Lösung zwischen Stadt und Arbeitsgemeinschaft der Behinderten-Clubs gefunden.

10. KOMMUNEN

10. Kommunen

10.1 Probleme bei der Anwendung des neuen HDSG

Obwohl ich einleitend darauf verwiesen habe, daß bei Bürger und Verwaltung das Datenschutzbewußtsein gewachsen ist, werden mir nach wie vor Verstöße gemeldet. In einem Fall hatte das Personalamt einer hessischen Großstadt eine Liste mit Namen sowie persönlichen und dienstlichen Daten aller städtischer Mitarbeiter dem Mitglied einer Stadtverordneten-Fraktion übergeben. Nach Bekanntwerden dieser Übermittlung hatten die beiden anderen Fraktionen die gleiche Liste mit Personendaten der ca. 6 000 städtischen Bediensteten angefordert und erhalten. Die infolge meines Auskunftersuchens an die Stadt veranlaßte Überprüfung durch das städtische Rechtsamt bestätigte, daß die Aushändigung des Stellenplans mit Stellenbesetzungsverzeichnis unzulässig war. Der zuständige Dezernent bedauerte die von ihm gebilligte Übermittlung und brachte zum Ausdruck, er sei sich der Unzulässigkeit der Weitergabe nicht bewußt gewesen. Die ausgehändigten Unterlagen seien von den Betroffenen inzwischen wieder zurückgegeben worden.

Abgesehen von der Möglichkeit der Städte und Gemeinden, sich in EDV-technischen Fragen vom Hessischen Datenverarbeitungsverbund (HZD und KGRZ) beraten zu lassen, zeigt die Erfahrung, daß es für die zahlreichen konkreten Fragen des Datenschutzes und der Datensicherung in der täglichen Verwaltungspraxis an ausreichender Beratung und Unterstützung durch die Kommunalaufsichtsbehörden fehlt. Trotz meines Hinweises auf diese Situation im letzten Tätigkeitsbericht⁹⁰⁾ hat sich diese Unsicherheit nach Verabschiedung des neuen HDSG eher noch verstärkt.

Ich habe die Datenschutzreferenten der hessischen Großstädte zu einem Erfahrungsaustausch eingeladen, bei dem die in der täglichen Praxis auftretenden Datenschutzprobleme zunächst einmal gesammelt, diskutiert und nach Möglichkeit einer einvernehmlichen Lösung zugeführt werden sollen. Diese Initiative ist bei den Großstädten auf so großes Interesse gestoßen, daß ich überlege, wie auch den kreisangehörigen Städten und Gemeinden eine Unterstützung bei Lösung ihrer Datenschutzprobleme vermittelt werden kann.

⁹⁰⁾ Vgl. VI, 4.3 letzter Abs.

10.2 Öffentlich-rechtliche Wettbewerbsunternehmen

Für öffentlich-rechtliche Unternehmen, die am Wettbewerb teilnehmen, gelten nach § 3 Abs. 2 HDSG die Datenschutzvorschriften des BDSG für private Unternehmen. Das HDSG folgt damit den Regelungen des § 7 Abs. 1, § 22 Abs. 1 und § 31 BDSG. Hiermit soll vermieden werden, daß die Datenschutzvorschriften zu Wettbewerbsverzerrungen führen; Unternehmen, die miteinander konkurrieren, sollen von Rechts wegen gleich behandelt werden. Für die Frage, ob eine Teilnahme am Wettbewerb stattfindet, kommt es maßgeblich auf die Art der Leistung an, die das Unternehmen auf dem Markt anbietet; ob mit der Beteiligung am Wettbewerb Gewinn erzielt werden soll, ist dagegen unerheblich⁹¹⁾.

Nun gibt es öffentlich-rechtliche Unternehmen, vornehmlich der Gemeinden oder Gemeindeverbände, die sowohl Leistungen im Wettbewerb, für welche Verbrauchskosten, als auch öffentliche Versorgungsleistungen, für welche Gebühren gezahlt werden, erbringen. Ein solches, als Eigenbetrieb geführtes Unternehmen einer hessischen Gemeinde, das die Einwohner mit Gas und mit Wasser versorgt und die Verbrauchskosten bzw. die Gebühren über eine einheitliche Datei im „Querverbund“ abrechnet, hat mir die Frage gestellt, welche Datenschutzvorschriften des Bundes und des Landes bei dieser Art der Geschäftsführung zu beachten sind und ob ein betrieblicher Datenschutzbeauftragter bestellt werden muß.

Die auf öffentlich-rechtliche Wettbewerbsunternehmen anzuwendenden Vorschriften des Bundesrechts (§ 22 Abs. 2 und 3, §§ 23 bis 27 BDSG) unterscheiden sich nicht unwesentlich von den Vorschriften, die für die öffentliche Verwaltung des Landes einschließlich der nicht am Wettbewerb teilnehmenden öffentlich-rechtlichen Unternehmen gelten.

Für Wettbewerbsunternehmen ergeben sich folgende Abweichungen vom Hessischen Datenschutzgesetz:

- Die Zulässigkeit der Datenverarbeitung, die Pflichten zur Veröffentlichung über die gespeicherten Daten, zur Auskunft an den Be-

⁹¹⁾ Vgl. Auernhammer, BDSG § 7 Rdnr. 11; Orde-mann/Schomerus, BDSG § 7 Erl. 4; Simitis, BDSG § 22 Rdnr. 77.

troffenen, zur Berichtigung, Sperrung und Löschung von Daten richten sich nach Bundesrecht, und zwar nach den für die Datenverarbeitung nichtöffentlicher Stellen für eigene Zwecke geltenden §§ 23 bis 27 BDSG. Dahinter verbirgt sich folgender grundsätzlicher Unterschied:

Im Bereich der öffentlichen Verwaltung kommt es darauf an, ob die Datenverarbeitung zur rechtmäßigen Erfüllung der in der Zuständigkeit der speichernden Stelle liegenden Aufgabe erforderlich ist. Liegen diese Voraussetzungen vor, überlagern sie die individuellen Interessen des einzelnen, d. h., Belange des Betroffenen sind nicht als schutzwürdig zu berücksichtigen. Dagegen ist nach dem für öffentlich-rechtliche Wettbewerbsunternehmen geltenden Bundesrecht die Datenverarbeitung zulässig, wenn sie im Rahmen der Zweckbestimmung des Vertragsverhältnisses oder des vertragsähnlichen Vertrauensverhältnisses mit den Betroffenen erfolgt oder wenn sie den berechtigten Interessen der speichernden Stelle entspricht und keine schutzwürdigen Belange des Betroffenen entgegenstehen. Diese Regelung berücksichtigt in beiden Fällen der Alternative die schutzwürdigen Belange des Betroffenen; denn sie sind zugleich ein Element des vertrags- oder des vertragsähnlichen Vertrauensverhältnisses.

- Im Falle der Vergabe der Verarbeitung an ein privates Unternehmen entfällt die sonst nach § 4 Abs. 1 Satz 2 HDSG bestehende Verpflichtung, vertraglich sicherzustellen, daß der Auftragnehmer die Bestimmungen des Datenschutzgesetzes beachtet und sich der Kontrolle des Hessischen Datenschutzbeauftragten unterwirft. Für den privatrechtlich organisierten Auftragnehmer gelten nur die Vorschriften der §§ 38 bis 40 über die Bestellung eines betrieblichen Datenschutzbeauftragten und über die Kontrolle durch die nach Landesrecht zuständige Aufsichtsbehörde.

Die Kontrolle des Hessischen Datenschutzbeauftragten entfällt auch in den Fällen, bei

denen dem Land oder einer der Aufsicht des Landes unterstehenden Körperschaft, Anstalt oder Stiftung des öffentlichen Rechts die Mehrheit der Anteile des beauftragten Privatunternehmens oder die Mehrheit der Stimmen in dessen Organen zusteht (§ 4 Abs. 3 HDSG).

- Schließlich entfällt der Schadensersatzanspruch des Betroffenen (§ 8 Abs. 2 HDSG).

Diesen grundsätzlichen Unterschieden muß die Organisation der Datenverarbeitung Rechnung tragen, wenn ein öffentlich-rechtliches Unternehmen mit einem Teil der Leistungen am Wettbewerb teilnimmt und mit einem anderen Teil seiner Leistungen eine öffentliche Aufgabe in einer Monopolstellung erfüllt.

Die Konsequenzen aus dieser Rechtslage sind unbefriedigend. Das übliche Verfahren, die Gebühren und die Verbrauchskosten für die verschiedenen Leistungen des Versorgungsbetriebes in einer Abrechnung zusammenzufassen, ist für die Verwaltung rationeller und für den zahlungspflichtigen Betroffenen einfacher. Die rechtspolitischen Gründe, denen zufolge für die verschiedenen Versorgungsleistungen ein und desselben öffentlich-rechtlichen Unternehmens verschiedenes Recht — teils Bundesrecht, teils Landesrecht — gilt, werden weder bei der Verwaltung noch beim Betroffenen auf Verständnis oder auf Anerkennung stoßen.

Eine Auslegung des § 3 Abs. 2 HDSG in dem Sinne, daß der Eigenbetrieb mit seinen verschiedenartigen Leistungen im Ganzen als Wettbewerbsunternehmen zu behandeln ist, sofern nur eine seiner Leistungen eine Wettbewerbsleistung ist, halte ich für unzulässig, weil dadurch die Rechtstellung des Betroffenen verschlechtert werden würde.

Ich halte es daher für notwendig, die Gemeinden auf die dargestellte Rechtslage hinzuweisen und darauf hinzuwirken, daß durch technische Maßnahmen sichergestellt wird, daß der sog. Querverbund, soweit dies im Interesse des Bürgers erforderlich erscheint, auch auflösbar ist.

11. DATENÜBERMITTLUNG AN ÖFFENTLICH-RECHTLICHE RELIGIONSGESELLSCHAFTEN

11. Datenübermittlung an Öffentlich-Rechtliche Religionsgesellschaften

- a) Die Übermittlung personenbezogener Daten aus dem öffentlichen Bereich an die Kirchen ist als Datenschutzproblem schon in den vorangegangenen Tätigkeitsberichten (TB) — mit Ausnahme des sechsten — behandelt worden:
- TB vom 29. März 1972 — 4.1.2, 4.1.1.3
— LT-Drucks. 7/1495;
 - TB vom 29. März 1973 — 2.2.1, 4.1.1.3
— LT-Drucks. 7/3137;
 - TB vom 1. April 1974 — 4.1.6
— LT-Drucks. 7/5146;
 - TB vom 26. März 1975 — 4.4
— LT-Drucks. 8/438;
 - TB vom 30. März 1976 — 3.1
— LT-Drucks. 8/2475.

Dort geht es vor allem um die Frage, ob die Übermittlung von Daten solcher Personen, die nicht Mitglieder der empfangenden Kirche sind, ohne deren Einwilligung zulässig ist.

Nach den gleichlautenden Vorschriften in § 10 Abs. 2 BDSG und in § 12 Abs. 2 HDSG sind bei der Datenübermittlung aus dem Bereich der öffentlichen Verwaltung in den Bereich der öffentlich-rechtlichen Religionsgesellschaften die Zulässigkeitsvoraussetzungen für die Datenübermittlung innerhalb des öffentlichen Bereichs entsprechend zu beachten. Diese Regelung gibt keine Antwort auf die Frage: In welcher Modifizierung ist sie auf das Verhältnis zwischen Staat und Kirche übertragbar und in welcher Weise ist die Voraussetzung zu verwirklichen und zu kontrollieren, daß ausreichende Datenschutzmaßnahmen im kirchlichen Bereich getroffen sind?

- b) Die Bedeutung des § 10 Abs. 2 BDSG und des § 12 Abs. 2 HDSG kann nur auf dem Hintergrund des verfassungsrechtlichen Verhältnisses zwischen dem Staat und den öffentlich-rechtlichen Religionsgesellschaften erschlossen werden.

Nach Art. 140 GG i.V.m. Art. 137 Abs. 3 WV ordnet und verwaltet jede Religionsgesellschaft ihre Angelegenheiten selbständig innerhalb der Schranken des für alle geltenden

Gesetzes. „Die Kirchen sind ungeachtet ihrer Anerkennung als Körperschaften des öffentlichen Rechts dem Staat in keiner Weise inkorporiert, also auch nicht im weitesten Sinn „staatsmittelbare“ Organisationen oder Verwaltungseinrichtungen. Ihre wesentlichen Aufgaben, Befugnisse, Zuständigkeiten sind originäre und nicht vom Staat abgeleitete (BVerfGE 18, 385 (386); 19, 129 (133 f.))“⁹²⁾.

Die Aufgaben der Behörden und öffentlichen Stellen im staatlichen Bereich unterliegen der rechtsstaatlichen Bindung an Gesetz und Recht (Prinzip der Gesetzmäßigkeit der Verwaltung), ihre Zuständigkeiten sind in Rechtsvorschriften festgelegt. Die zugewiesenen Aufgaben werden nach Rechtsregeln ausgeführt, die eine gemeinsame Rechtsgrundlage für die übermittelnde und für die empfangende Behörde oder öffentliche Stelle bilden. Der Regelung des § 12 Abs. 1 HDSG — wie des § 10 Abs. 1 BDSG — liegt die gesetzgeberische Abwägung einer möglichen Beeinträchtigung schutzwürdiger Belange der Betroffenen gegenüber dem Gemeinwohl-Interesse an der Erfüllung der öffentlichen Aufgabe zugrunde, und zwar zugunsten der letzteren. An dieser gemeinsamen rechtlichen Handlungsgrundlage innerhalb des öffentlichen Bereichs fehlt es, wenn personenbezogene Daten aus dem öffentlichen Bereich heraus an eine öffentlich-rechtliche Religionsgesellschaft übermittelt werden. Gerade hinsichtlich der Aufgabenstellung und der Rechtfertigung ihrer Ausführung unterscheiden sich staatliches und kirchliches Recht.

Ob eine öffentlich-rechtliche Religionsgesellschaft Daten speichert und weiter verarbeitet und für welche ihrer — selbst bestimmten — Aufgaben sie sie verwendet, ist eine innerkirchliche Angelegenheit, die sie autonom, in Unabhängigkeit vom Staat, ordnet und verwaltet. Staatliche Datenschutzgesetze können, soweit sie Datenschutz durch eine Regelung der Datenverarbeitung — deren Zulässigkeit in den einzelnen Verarbeitungsphasen — gewährleisten, für den innerkirchlichen Bereich keine Geltung beanspruchen. Anders als bei der Presse war daher eine Klarstellung

⁹²⁾ Vgl. BVerfGE 42, 312.

des Geltungsbereichs des Datenschutzgesetzes durch eine ausdrückliche Ausklammerung der Religionsgesellschaften unnötig.

- c) Die Bedeutung des § 10 Abs. 2 HDSG — bzw. des § 12 Abs. 2 BDSG — liegt vielmehr darin, daß die öffentlich-rechtlichen Religionsgesellschaften in die Regelung der Datenübermittlung innerhalb des öffentlichen Bereichs einbezogen werden, und zwar mit dem verfassungsmäßigen Zweck, den Informationsfluß aufrecht zu erhalten, auf den die Religionsgesellschaften nach Art. 140 GG i.V.m. Art. 136 ff. WV Anspruch erheben können. Darin liegt zugleich aber eine Beschränkung. Die Religionsgesellschaften können von den Behörden und öffentlichen Stellen der Landesverwaltung keine „Amtshilfe“ verlangen, mit deren Gewährung diese gegen die staatliche Rechtsordnung verstießen. Die Autonomie der Religionsgesellschaften besteht nur innerhalb der Schranken des für alle geltenden Gesetzes (Art. 137 Abs. 3 WV). Diese Schrankenformel ist „heute die Basis für eine Konkordanz zwischen staatlicher und kirchlicher Ordnung . . . , die es gestattet, auf beiden Seiten davon auszugehen, daß staatliche Gesetze nicht die den Kirchen wesentlichen eigenen Ordnungen beeinträchtigen und daß kirchliche Gesetze nicht die für den Staat unabdingbare Ordnung kränken werden“⁹³⁾. Zum richtigen Verständnis einer partnerschaftlichen Kooperation auf dieser Grundlage gehört die Bereitschaft der Religionsgesellschaft, die Pflicht der vollziehenden Gewalt zu respektieren, die Grundrechte zu achten. Im Zusammenhang mit der eingangs gestellten Frage ist hier auf Art. 4 Abs. 1 GG i.V.m. Art. 137 Abs. 3 WV zu verweisen.

Zu dem von staatlicher Einflußnahme freien Rechtsraum nach Art. 4 Abs. 1 GG gehört auch die sog. negative Bekenntnisfreiheit, d. h. das Recht zu verschweigen, ob man einer Religionsgesellschaft oder welcher man angehört. „Den in Abs. 1 und 2 des Art. 4 GG gewährleisteten Freiheiten können nach dem Grundsatz der Einheit der Verfassung allein durch andere Bestimmungen des Grundgesetzes Grenzen gezogen werden. Gesetzliche Bestimmungen, die die in Art. 4 Abs. 1 gewährleistete Freiheit einschränken, können vor dem Grundgesetz nur dann Bestand haben, wenn sie sich als Ausgestaltung einer Begrenzung durch die Verfassung selbst erweisen“⁹⁴⁾. Eine Einschränkung des Grund-

rechts enthält Art. 136 Abs. 3 WV. Danach haben die Behörden das Recht, nach der Zugehörigkeit zu einer Religionsgesellschaft zu fragen, insoweit, als davon Rechte und Pflichten abhängen oder eine gesetzlich angeordnete statistische Erhebung dies erfordert. Aus dieser Beschränkung und Bindung des Auskunftrechts an konkrete staatliche Zwecke, für deren Erfüllung die Kenntnis der Zugehörigkeit zu einer Religionsgesellschaft unabweisbar ist, folgt andererseits das Verbot, die zulässig erlangte Kenntnis für andere Zwecke zu verwerten oder sie weiterzugeben.

Schon daraus folgt, daß es der öffentlichen Verwaltung verwehrt ist, einer öffentlich-rechtlichen Religionsgesellschaft Daten zu übermitteln, aus denen sich ergibt, daß der Betroffene keiner öffentlich-rechtlichen Religionsgesellschaft angehört oder daß er Mitglied einer anderen Religionsgesellschaft ist. Die Übermittlung ist nur zulässig, wenn der Betroffene der empfangenden Kirche gegenüber kirchensteuerpflichtig ist⁹⁵⁾.

Aus dieser Sicht — mit der sich aus Art. 137 Abs. 6 ergebenden Einschränkung — ist die Regelung in § 16 a Abs. 5 des Hessischen Meldegesetzes (HMG) i. d. F. vom 12. Juli 1978 verfassungsrechtlich insofern zu beanstanden, als nach dem Wortlaut der Vorschrift auch die Angaben des Meldepflichtigen zu der Frage der Zugehörigkeit zu einer öffentlich-rechtlichen Religionsgesellschaft durch Weitergabe der Meldescheine bis zum 1. 1. 1982 zulässig ist.

Gesetzliche Vorschriften sind, soweit sie auslegungsfähig sind, in einem Sinne anzuwenden, der mit der Verfassung im Einklang steht. § 16 a Abs. 5 bezweckt nicht, etwas zu gestatten, was in anderen, spezielleren Rechtsvorschriften verboten ist. Die Vorschrift enthält vielmehr die unbeschriebene Schranke der Rechtmäßigkeit der Weitergabe. Eine verfassungskonforme Auslegung ergibt daher, daß die Weitergabe der Meldescheine an die öffentlich-rechtlichen Religionsgesellschaften nur unter Beachtung des Art. 4 GG statthaft ist, d. h., daß die Weitergabe nur zulässig ist, wenn die Angaben über die Zugehörigkeit oder Nicht-Zugehörigkeit zu einer Religionsgesellschaft vorher eliminiert worden sind.

- d) Dadurch, daß § 10 Abs. 2 HDSG — § 12 Abs. 2 BDSG — die entsprechende Anwendung der Übermittlungsregelung an die Voraussetzung knüpft, daß die Religionsgesellschaft ausrei-

⁹³⁾ Vgl. BVerfGE 42, 312 (340).

⁹⁴⁾ Vgl. BVerfGE 44, 59 (67).

⁹⁵⁾ Vgl. Art. 137 Abs. 6 WV.

- chende Datenschutzmaßnahmen getroffen hat, werden auch die Grundsätze des für den öffentlichen Bereich normierten Datenschutzes für die Religionsgesellschaften verbindlich, und zwar in dem Sinne, daß sie die Übermittlung personenbezogener Daten — auch solcher, auf die sie nach geltendem Recht einen Anspruch haben — nur fordern können, wenn sie dem Betroffenen Datenschutz im gleichen Umfange wie die Behörden und öffentlichen Stellen der öffentlichen Verwaltung gewähren. Dies bedeutet im Konkreten, daß die Grundnormen des Datenschutzes, die in den allgemeinen Vorschriften im ersten Teil des HDSG — bzw. im ersten Abschnitt des BDSG — zusammengefaßt sind, in die Schrankenformel des Art. 137 Abs. 3 WV einbezogen werden. Mit anderen Worten: Die Zweckbestimmung des Datenschutzes (§ 1 Abs. 1 Nr. 1 HDSG), die Verantwortlichkeit der speichernden Stelle bei Auftragsverarbeitung (§ 4 HDSG), das Datenverarbeitungs-Verbot mit dem Erlaubnisvorbehalt der gesetzlichen Zulassung oder der Einwilligung des Betroffenen (§ 7 HDSG), die Rechte des Betroffenen (§ 8 HDSG), das Datengeheimnis (§ 9 HDSG) und die Datensicherung (§ 10 HDSG) sind Normen des für alle geltenden Gesetzes und damit auch für die Religionsgesellschaften verbindlich.
- e) Der Rahmen, innerhalb dessen die übermittelnde Behörde diese Voraussetzungen prüfen kann, ist sehr eng. Aus der entsprechenden Anwendung der Grundregel des § 7 HDSG (§ 3 BDSG) folgt nur, — von der Einwilligung des Betroffenen abgesehen — daß die Religionsgesellschaft die Datenverarbeitung für ihren Bereich in der ihr angemessenen Form rechtl. erlaubt haben muß. Im übrigen aber kann die übermittelnde Behörde oder öffentliche Stelle nur prüfen, ob die Regelungen der Religionsgesellschaften dem Betroffenen eine Rechtsstellung einräumen, die dem Datenschutz, welchen das staatliche Gesetz gewährt, gleichwertig ist. Dagegen kann die Ausführung der Rechtsnormen der öffentlich-rechtlichen Religionsgesellschaft von Staats wegen nicht überprüft werden. Dem steht die grundsätzliche Trennung des kirchlichen von dem weltlichen Herrschaftsbereich entgegen; sie schließt eine staatliche Kontrolle im innerkirchlichen Bereich aus.
- Nach § 25 Abs. 2 Bayerisches Datenschutzgesetz vom 2. 5. 1978 sind die Vorschriften über die „Überwachung des Datenschutzes bei öffentlichen Stellen“ entsprechend anzuwenden, soweit personenbezogene Daten an Stellen der öffentlich-rechtlichen Religionsgesellschaften übermittelt werden. Diese im HDSG nicht enthaltene Regelung wirft wieder die Frage auf, welche Grenzen das Grundgesetz einer Überwachung der Religionsgesellschaften durch die für den staatlichen Bereich eingesetzte Kontrollinstitution zieht.
- f) Ob die bisher vorliegenden Kirchengesetze über den Datenschutz und ihre Durchführungsverordnungen ausreichende Datenschutzmaßnahmen im vorstehend erörterten Sinne enthalten, bedarf noch einer weiteren Prüfung.
- g) Nach einer Entscheidung des Bundesverfassungsgerichts vom 11. Oktober 1977 — Band 46, 73 — sind nicht nur die organisierte Kirche und die rechtlich selbständigen Teile dieser Organisation, sondern alle der Kirche in bestimmter Weise zugeordneten Einrichtungen ohne Rücksicht auf ihre Rechtsform Objekte, bei deren Ordnung und Verwaltung die Kirche grundsätzlich frei ist, wenn sie nach kirchlichem Selbstverständnis ihrem Zweck oder ihrer Aufgabe entsprechend berufen sind, ein Stück Auftrag der Kirche in dieser Welt wahrzunehmen und zu erfüllen. Dieser Leitsatz ist aus Anlaß der Prüfung aufgestellt worden, ob das Betriebsverfassungsgesetz auf ein gemeinnütziges katholisches Krankenhaus anzuwenden ist, das in der Form einer rechtsfähigen Stiftung des privaten Rechts geführt wird. Es bedarf daher der weiteren Prüfung, ob auch § 12 Abs. 2 HDSG (bzw. § 10 Abs. 2 BDSG) nicht allein für die verfaßte Kirche oder Religionsgesellschaft gilt (vgl. Simitis, BDSG § 22 Rdnr. 65). Hier ist eine sachgerechte Lösung besonders im Hinblick auf die Sachverhalte notwendig, in denen es sich um die Zusammenarbeit zwischen staatlichen oder privaten Einrichtungen mit kirchlichen Einrichtungen handelt. Ein Beispiel hierfür bildet der in § 13 f des Hessischen Krankenhausgesetzes vorgesehene Datenverbund.

12. DATENSICHERUNG

12. Datensicherung

Das Bundesdatenschutzgesetz (BDSG) vom 27. 1. 1978 hat erstmals einen Anforderungskatalog für die zur Ausführung des Gesetzes erforderlichen technischen und organisatorischen Maßnahmen bei der automatischen Verarbeitung geschützter personenbezogener Daten in der Anlage zu § 6 aufgestellt. Die in 10 Punkten zusammengefaßten Zielvorgaben bauen unter anderem auf den Erfahrungen auf, wie sie auch im hessischen DV-Verband gemacht wurden. Sie stellen im wesentlichen die als technisch realisierbar erkannten Ziele der Datensicherung dar. Das Hessische Datenschutzgesetz (HDSG) vom 31. 1. 1978 hat diesen Maßnahmenkatalog als Anlage zu § 10 im Wortlaut übernommen.

12.1 Realisierungsmöglichkeiten

Die notwendigen Maßnahmen können nach Art, Umfang und Ausgestaltung für jeden Einzelfall sehr unterschiedlich sein. Eine detaillierte technische Regelung aller denkbaren Möglichkeiten im Gesetz liefe Gefahr, nicht vollständig zu sein und vom technischen Fortschritt überholt zu werden. Der Gesetzgeber hat deshalb lediglich einen Rahmen von Anforderungen an diese Maßnahmen geschaffen, die den Bereich der Datensicherung im wesentlichen abdecken. Die hier aufgeführten Beispiele können deshalb nur erläuternden Charakter haben und erheben keinen Anspruch auf Vollständigkeit:

Zugangskontrolle

Closed-shop-Betrieb, Abgrenzung von Sicherheitszonen, Ausweisleser an den Eingängen der Rechenzentren und den Zugängen zum closed-shop, persönliche Kontrolle durch Pförtner, Einbruchssicherungen, FS-Monitore, Zeiterfassung aller Personen im Rechenzentrum, Besucherkontrolle, Vier-Augen-Prinzip, Arbeiten außerhalb der Dienstzeit nur mit besonderer Genehmigung.

Abgangskontrolle

Geschütztes Datenträgerarchiv mit separater Zugangskontrolle, Datenträgerbestandsführung mit schriftlicher Aufzeichnung bei Entnahme, Begleitscheine, genau bezeichnete Datenträger (entfällt bei systemgesteuerten sog. „anonymen“ Archiven), Schränke mit Sicherheitsschlössern für be-

sonders sensitive Datenträger, gesonderte Datenträgerschleuße zur Abgangskontrolle evtl. unter Verwendung von Detektoren, Verhinderung des unbefugten Kopierens von Datenträgern, nicht transportable Datenträger (Festplatten, Massenspeicher).

Speicherkontrolle

Identifikation und Autorisation der Berechtigten festlegen, z. B. durch Richtlinien für Dateneingabe, Datenveränderung und Datenlöschung (Benutzerprofile); Speicherschutzschlüssel bei Multiprocessing; Passwortschutz auf Datei und Memberebene; Einsatz von Datenbanksystemen; umfassende Protokollierung und Auswertung aller Systemaktivitäten; Kontrolle der Benutzung von Dienstprogrammen (sog. Utilities) z. B. durch Einstellung in eine gesonderte „Bibliothek“ mit eingeschränktem Benutzerkreis und Passwortschutz auf Memberebene.

Benutzerkontrolle

Benutzeridentifikation bei Datenfernverarbeitung z. B. durch Vergabe einer Benutzerkennung (User-id); automatische Identifizierung der Datenstation mit festgelegter Autorisation (Umfang und Zeitraum des Zugriffs); dezentrale Passwortvergabe; Sicherung der Datenstationen (Terminals) durch Schlüssel oder Ausweiskontrolle.

Zugriffskontrolle

Definition, wer auf welche Daten zugreifen darf, z. B. in Datenbanksystemen durch Differenzierung der Zugriffsrechte bis auf Feldebene bei gleichzeitiger Festlegung der Operation (read/write/delete); bei kleinen Systemen hierarchische Zuordnung von Dateiklassen zu Benutzerklassen, Einsatz von DS-Lizenzprogrammen (z. B. RACF, SECURE, APOS und andere).

Übermittlungskontrolle

Die Maßnahmen sind bereits bei der Benutzer-, Speicher- und Zugriffskontrolle erläutert. Automatische Protokollierung ist zu empfehlen.

Eingabekontrolle

Automatische Systemaufzeichnung; Auswertung der Systemprotokolle (z. B. der Änderungsprotokolle durch die Fachabteilungen oder programmtechnische Auswertungen); Festlegung von Aufbewahrungsfristen für Protokolle.

Auftragskontrolle

Eindeutige Vertragsgestaltung mit dem Auftraggeber (Abgrenzung der Kompetenzen und der Verantwortung); klare Organisation des Arbeitsablaufs unter Verwendung standardisierter Auftragsformulare; Prüfung der Identität des Auftraggebers; Vollständigkeitsprüfung der Unterlagen; detaillierte Ablaufplanung und Beschreibung für Arbeitsvorbereitung, Operating und Arbeitsnachbereitung; Führung eines manuellen Operatorlogbuchs; Sonderauswertungen nur mit schriftlichem Auftrag.

Transportkontrolle

Bei Datenfernübertragung: Sorgfältige Wahl des Übertragungsweges (Datex-Netz, Telex-Netz, öffentliches Fernsprechnetz, Standleitung); Datenstationen müssen vom DV-System identifiziert werden können (Hardwareadresse); Leitungsweg einschließlich der Schaltungspunkte stichprobenartig überprüfen; Einsatz von Chiffrier-Hard- oder Software.

Bei Transport von Datenträgern: Transportwege genau festlegen; Empfänger muß genau bekannt sein; Versand in festen verschließbaren Behältern; Transportbegleitpapiere; Datenträgeraustausch stets mit den gleichen Magnetbändern (beim Lesen von „Restdaten“ gewinnt der Empfänger keine neuen Erkenntnisse), Verwendung von offline-Löschgeräten mit Kennsatzschutz vor einer Neubeschriftung der Bänder oder online per Programm.

Organisationskontrolle

Organisatorische Sicherungsmaßnahmen berühren Rechenzentrumsbetrieb und Fachabteilung gleichermaßen. Bei dem Umfang der Möglichkeiten können die Beispiele nur hinweisenden Charakter haben: Strikte Funktionstrennung innerhalb der ADV-Abteilung (Anwendungsprogrammierung/Systemprogrammierung /Operating/Arbeitsvor- und Arbeitsnachbereitung/Programm- und Datenarchiv; genaue Festlegung des Systemstehungsganges (Projektplan); getrennte Bibliotheken für Quellen- und Lademodule der Produktions- und Testdateien; Schutz der Bibliotheken durch Benutzerautorisation (Passwort, Einsatz eines DS-Lizenzprogramms); Katastrophenplan; Revision; Bestellung eines Datenschutzauftrags.

12.2 Auswirkungen des HDSG auf den DV-Verbund

Der Hessische DV-Verbund verarbeitet — mit Ausnahme der Personaldaten seiner Mitarbeiter — Daten nur im Auftrag der Verwaltung oder Drit-

ter. Er hat sicherzustellen, daß die nach § 10 HDSG erforderlichen Maßnahmen technischer und organisatorischer Art getroffen werden. Sofern der DV-Verbund DV-Arbeiten an andere Stellen vergibt, hat er § 4 HDSG zu beachten.

Richtlinien

In den vergangenen Jahren sind eine Vielzahl von Datensicherungsmaßnahmen in verbundeinheitlichen Richtlinien festgehalten worden:

BAL Richtlinien zum Betriebsablauf im DV-Verbund

DASCH Richtlinien zur Gewährleistung des Datenschutzes und der Datensicherheit im DV-Verbund

DVL Arbeitsrichtlinien für die Automatisierung von Aufgaben der Landesverwaltung und der Kommunalverwaltung

PR Programmierrichtlinien

RAU Richtlinien über den Inhalt und die Gestaltung von Arbeitsunterlagen für DV-Verfahren

Diese Richtlinien müssen jetzt den Erfordernissen des Hessischen Datenschutzgesetzes vom 31. Januar 1978 angepaßt werden. Der Koordinierungsausschuß der HZD hat zu diesem Zweck eine Arbeitsgruppe „Datenschutz“ gebildet, die sich unter meiner Mitwirkung dieser Aufgabe widmet.

12.3 Datensicherungsmaßnahme im DV-Verbund

Um den Anforderungen (12.1) zu genügen, sind verschiedene Maßnahmen im Bereich der Hardware, Software und Orgware zu ergreifen:

Hardware-Sicherung

Hierunter fallen beispielsweise in DV-Anlagen und Geräten der Peripherie fest eingebaute Sicherungen wie Schösser, Mehrfachauslegung von Bauelementen, Sicherungen zum Erkennen und Bereinigen von Maschinenfehlern.

Software-Sicherung

Dies sind programmtechnische Sicherungsmaßnahmen. Sie sind teilweise in dem System-Steuerprogramm der Hersteller (Betriebssystem), teilweise in den Anwendungsprogrammen eingebaut, so z. B. in den Betriebssystemen: Routinen zur Benutzeridentifikation, Identifikation der Ressourcen, Festlegung von Benutzerprofilen, Abschottung der Adreßräume bei Multiprogramming, automatische Umkonfiguration bei Ausfall von Peripherieeinheiten, Checkpointrestart, Testhilfen, automatisches accounting usw.; in Anwen-

derprogrammen: Plausibilitätsläufe, Abstimmungenbildung, Prüfpunkte usw.⁹⁶⁾.

Orgware-Sicherung

Hierunter fällt das ganze Spektrum der Maßnahmen, insbesondere baulicher und personeller Art, die die Hard- und Software-Sicherungen ergänzen, um eine umfassende Datensicherung zu gewährleisten.

Einsatz von DS-Software

Die im Hessischen DV-Verbund eingesetzten Betriebssysteme MVS, VS1 und SVS bieten in Verbindung mit besonderen Komponenten wie z. B. dem Einsatz von PCF für das Timesharingssystem TSO oder Datenbanksystemen wie IMS oder ADABAS unterschiedlich komfortable Möglichkeiten der Zugriffskontrolle auf Dateiebene. Eine umfassende Lösung auftretender Datenschutzprobleme ist durch den Einsatz von spezifischen Datensicherungsprogrammen möglich, wie sie seit einiger Zeit auf dem Software-Markt angeboten werden. Beispiele dafür sind die Lizenzprogramme RACF, SECUR und APOS. Der Koordinierungsausschuß der HZD hat nach einer umfangreichen vergleichenden Untersuchung des Leistungsverhältnisses dieser Programme beschlossen, von Oktober 1978 an, das Software-Produkt SECUR einzusetzen.

Realisierung

Inzwischen wurden technische und organisatorische Maßnahmen ergriffen bzw. eingeleitet, um in den Rechenzentren des DV-Verbundes die Datensicherung und den Datenschutz zu gewährleisten. Es handelt sich dabei um

Closed-Shop-Betrieb, Besucherkontrolle, separate Datenträgerarchive, Verwendung von Festplattenspeichern, Identifikation und Autorisation von Benutzern, Passwortschutz von Dateien, Protokollierung und Auswertung der Systemaktivität

ten, klare Organisation der Arbeitsabläufe, Transportsicherungen, Funktionstrennung, einheitlicher Projektablauf, bauliche Sicherungsmaßnahmen, Ernennung eines Datenschutzbeauftragten.

Forderungen an die künftige Entwicklung

Nach dem heutigen Stand der Technik sind zur Weiterentwicklung der Datensicherungs- und Datenschutzmaßnahmen im Sinne der Anlage zu § 10 HDSG vom Hessischen DV-Verbund künftig folgende Maßnahmen zu ergreifen:

Die von bisher vorhandener Software angebotenen Möglichkeiten zur Datensicherung sind voll auszuschöpfen; Protokollierung und Auswertung aller Änderungen an Programmen des Betriebssystems oder dieses unterstützender Software (TECAM, INTERCOMM, ADABAS usw.), Trennung von Produktions- und Testbibliotheken, Verwaltung und Kontrolle der Quellen- und Ladeprogramme durch Einsatz von DS-Software; bei Datenfernverarbeitung ist eine Terminalidentifikation durchzuführen, besonders sensitive Daten sind verschlüsselt zu übermitteln (Hard- oder Software-Verschlüsselung), Einsatz eines automatischen Bandverwaltungssystems; im Datenträgeraustausch versandte Bänder sind vor Verwendung physisch zu löschen, um ein Lesen evtl. „Restdaten“ zu verhindern.

Durch den Einsatz des COM-Verfahrens (Computer Output Microfilm) entsteht ein erhöhtes Sicherheits- und Datenschutzrisiko, wenn, wie im hessischen DV-Verbund z. Z. üblich, die COM-Verfilmung durch private Service-Firmen erfolgt. Eine lückenlose Kontrolle des Auftraggebers, die eine unbefugte Verwendung der zu verfilmenden Daten bzw. die unbefugte Anfertigung von Duplikaten der Mikrofilme verhindern soll, ist sehr schwierig, wenn nicht gar unmöglich.

Die Anschaffung eines verbundeigenen COM-Recorders ist deshalb zu fordern.

⁹⁶⁾ Vgl. Datensicherheitsfunktion im IBM-Systemsteuerprogramm, IBM 1977.

Anlage zu Abschnitt 1

STELLUNGNAHME ZUM ENTWURF EINES BUNDESMELDEGESETZES IM RAHMEN DER ANHÖRUNG AM 20./21. NOVEMBER 1978

Zu 1: (Aufgabenstellung des Meldewesens)

Mit dem Bundesdatenschutzgesetz vom 27. 1. 1977 hat der Gesetzgeber allgemeine Grundsätze des Datenschutzes formuliert. Seither steht fest: Wer personenbezogene Daten verarbeiten will, darf es nur tun, wenn er sich auf eine Rechtsnorm oder auf das Einverständnis des Betroffenen berufen kann. Eine vom Datenschutz freigestellte Verarbeitung gibt es mit anderen Worten grundsätzlich ebensowenig wie das Gesetz datenschutzfreie Bereiche kennt. Nur wer sich an diese vom Gesetzgeber ausdrücklich festgehaltene Bedingung (§ 3 Bundesdatenschutzgesetz — BDSG) hält, handelt rechtmäßig.

So klar die Intention des BDSG aber auch ist, so wenig läßt sich darüber streiten, daß sich der Gesetzgeber nahezu durchweg mit allgemeinen Formulierungen begnügt hat. Sie sind verständlich, solange man den weiten Anwendungsbereich des BDSG bedenkt. Sie verpflichten aber zugleich dazu, auf das BDSG bereichsspezifische Regelungen folgen zu lassen, denen die Aufgabe zufallen muß, Voraussetzungen und Grenzen der Datenverarbeitung konkret für einzelne Problembereiche zu regeln. Nur wenn sich der Gesetzgeber einzelner Konfliktfelder annimmt, also auf allgemeine und allumfassende Aussagen verzichtet, kann es gelingen, jenes Maß an Präzision zurückzugewinnen, das allein die Verständlichkeit und Plausibilität der gesetzgeberischen Entscheidung zu garantieren vermag, zugleich aber auch den Betroffenen Gewißheit über ihren Handlungsspielraum verschafft.

Konkret und auf das Melderecht bezogen folgt daraus: Der Gesetzgeber kann und darf sich nicht damit begnügen, das BDSG unter einem anderen Etikett zu wiederholen. Die Meldegesetzgebung ist kein paraphrasiertes BDSG, sondern Musterfall einer bereichsspezifischen Regelung.

Dieser Anforderung wird der Gesetzgeber nur dann genügen, wenn er sich vor allem anderen dazu entschließt, die Aufgabe der beabsichtigten gesetzlichen Regelung zu formulieren und im Rahmen dieser Regelung festzuschreiben. Eine konsistente und überzeugende bereichsspezifische Regelung ist erst möglich, wenn ihre Ziele eindeutig feststehen, jede ihrer Vorschriften also an diesen Zielen gemessen und von ihnen her überprüft werden kann.

Dieser Erwartung genügt der vorgelegte Entwurf nicht. Daran ändern auch die Paragraphen-Überschriften nichts. Wer nicht mehr sagt, als daß es darum gehen soll, nur „zum Zwecke rechtmäßiger Erfüllung öffentlicher Aufgaben nach Maßgabe dieses Gesetzes und der dazu erlassenen Durchführungsvorschriften zu speichern, zu verwalten und anderen Meldebehörden zu übermitteln“ (§

1), vermeidet genau genommen jede verbindliche Aussage. Mit dem abstrakten Hinweis auf die „rechtmäßige Erfüllung öffentlicher Aufgaben“ läßt sich ebensowenig etwas anfangen wie mit der Bemerkung, die Verarbeitung sei an die im Gesetz formulierten Voraussetzungen gebunden. Die gesetzliche Regelung wird aus der Perspektive des Betroffenen erst verständlich, wenn die „öffentlichen Aufgaben“ offengelegt und im Gesetz präzise festgehalten werden. Nur unter diesen Umständen ist es möglich, den konkreten Verarbeitungszweck und damit auch die Tragweite der Datenverarbeitung zu erkennen.

Auch das Argument, das Gesetz habe es ohnehin nur mit den „Meldebehörden“ zu tun, damit würde aber zugleich der Aufgabenbereich deutlich genug umschrieben, hilft nicht weiter. Die ganze Diskussion über die Reform des Melderechts wird nur verständlich, wenn man den Funktionswandel der Meldebehörden bedenkt. Längst kann von, wie auch immer näher präzisieren, polizeilichen Aufgaben nicht mehr die Rede sein. Der veränderte Sprachgebrauch ist bezeichnend genug: Statt vom „Melde-“ wird fast nur noch vom „Einwohnerwesen“ gesprochen. In eben dieser Umschreibung dokumentiert sich ein qualitativer Wandel. Die Meldebehörden sind, um die Formulierung der Begründung zum Entwurf aufzugreifen, mehr und mehr zur „Informationsquelle für die Erledigung kommunaler und staatlicher Aufgaben“ geworden. Nicht von ungefähr sieht deshalb § 13 Abs. 1 eine Ermächtigung der Bundesregierung vor, regelmäßige Übermittlungen an andere Behörden mit Hilfe einer Rechtsverordnung vorzusehen. Die Meldebehörden verwandeln sich damit genau genommen mehr und mehr in zentrale Speicherstellen der von der öffentlichen Verwaltung für eine Vielzahl von Aufgaben benötigten Informationen.

Sicher fällt es nicht schwer, diesen Funktionswandel zu begründen. Die veränderten staatlichen Aufgaben wirken sich zwangsläufig auf die Informationsmenge aus. Insofern ist es letztlich nur konsequent, wenn sich die öffentliche Verwaltung mit der Rationalisierung des Informationsprozesses beschäftigt und Organisationsformen anstrebt, die eine bessere Steuerung dieses Prozesses sicherstellen sollen.

Darum geht es allerdings nicht. Spätestens seit dem BDSG steht fest: Die Rechtmäßigkeit der Verarbeitung mißt sich an der Bedeutung, die den jeweils in Betracht kommenden Daten für die konkrete staatliche Aufgabe zukommt. Der einzelne ist kein beliebig verwendbares Informationsobjekt. Information darf vielmehr von ihm erst verlangt werden, wenn der Informationszweck bereits definiert und auch Sorge dafür getragen ist, daß die Infor-

mation nur im Zusammenhang mit diesem Zweck verwendet werden wird. Die Sicherheit des Bürgers liegt in erster Linie in der erkennbaren und jederzeit nachvollziehbaren Zweckbindung der Information. Eine Regelung, wie sie insbesondere durch die §§ 1 und 13 des Entwurfs vorgesehen ist, steht insofern nicht nur in Widerspruch zu der im Grundgesetz garantierten persönlichen Integrität des einzelnen, sondern auch zu den sowohl vom Bundesgesetzgeber als auch von den Landesgesetzgebern anerkannten Prämissen aller Anstrengungen für einen wirksameren Datenschutz. Anders ausgedrückt: Solange die geplante Reform des Melderechts nicht mit einer klaren Aufgabendefinition beginnt, verstößt sie gegen den in der Datenschutzgesetzgebung festgelegten Rahmen staatlicher Informationsverarbeitung.

Die Verpflichtung, die Informationsziele offenzulegen, präjudiziert in keiner Weise die Entscheidung über die Ziele selbst. Diese können insofern durchaus unterschiedlich sein, nur gilt es, Gewißheit über sie zu gewinnen. Sie dürfen nicht am Gesetz vorbei formuliert oder variabel gehalten werden.

Zu den möglichen Zielen soviel: Sicher spricht zunächst sehr viel dafür, den Aufgabenbereich der Meldebehörden möglichst eng zu definieren. Die Konsequenz ist dann eine von vornherein äußerst begrenzte Verarbeitung personenbezogener Daten. Denkbare Gefahren für den einzelnen reduzieren sich, die Kontrolle wird leichter. Umgekehrt darf aber auch nicht übersehen werden, daß sich eine solche Einschränkung kaum mit den veränderten Funktionen der öffentlichen Verwaltung verträgt. Der zunehmende Bedarf an Daten ist eben weder zufällig noch willkürlich, sondern hängt unmittelbar mit den gewandelten staatlichen Aufgaben zusammen. Deshalb gilt es vor allem anderen zu fragen, ob eine Rückkehr zu einer mehr oder weniger rein sicherungsrechtlichen Funktion sich nicht nachteilig auf die auch aus der Perspektive des Bürgers veränderten Funktion der öffentlichen Verwaltung auswirken würde.

Ziel einer datenschutzkonformen Meldegesetzgebung muß es sein, Transparenz und Kontrolle der Datenverarbeitung zu garantieren. Beides läßt sich dann durchführen, wenn der Gesetzgeber in voller Kenntnis der veränderten Verwaltungsfunktion die gesetzliche Regelung zum Anlaß nimmt, um eben diese gewandelte Aufgabenstellung offenzulegen und gesetzlich festzuschreiben. Für den Bürger wäre damit das unverzichtbare Mindestmaß an Sicherheit erreicht, für die Verwaltung aber eine Revision der Aufgaben der Meldebehörden vermieden, die wahrscheinlich nur schwer in Einklang mit den Zielen einer leistenden Verwaltung zu bringen ist.

Zu 2.1: (Meldegeheimnis)

Zu den zusätzlichen Sicherungen, die das BDSG im Interesse des Betroffenen eingeführt hat, gehört die besonders in § 5 vorgesehene Verpflichtung auf das Datengeheimnis. Sie soll die Aufmerksamkeit all derjenigen, die mit der Verarbeitung personenbezogener Daten beschäftigt sind,

auf die Bedeutung dieser Verarbeitung und damit zugleich auch auf die damit für den Betroffenen verbundenen Gefahren lenken. Man könnte nun durchaus der Meinung sein, der Gesetzgeber habe damit hinreichend vorgesorgt, einer eigenen bereichsspezifischen Verpflichtung bedürfe es daneben nicht. Jede solche Argumentation läßt freilich außer acht, daß die Verpflichtung ihr Ziel erst in dem Augenblick erreicht, in dem es dem Verpflichteten klar wird, welche Tragweite seiner konkreten Beschäftigung zukommt. Eine abstrakte Verpflichtung auf das Datengeheimnis reicht dafür nicht aus. Wiederum kommt es in ganz besonderem Maße darauf an, vom konkreten Sachverhalt her zu formulieren und eben diesen Sachverhalt in den Mittelpunkt zu stellen. Insofern ist die Einführung eines Meldegeheimnisses ebensowenig überflüssig, wie Aussagen über besondere Berufsgeheimnisse.

Das Meldegeheimnis hat ferner eine nicht zu unterschätzende psychologische Wirkung. Es ist der gleichsam handfeste Beweis für die Bedeutung, die der Gesetzgeber den Interessen der Betroffenen beimißt und damit zugleich eine klare Aussage über die Bereitschaft des Gesetzgebers, eine Verarbeitung grundsätzlich nur solange zu dulden, wie sie auf die schutzwürdigen Belange der Betroffenen Rücksicht nimmt. Wiederum kommt es aber darauf an, eine Formulierung zu finden, die auf die spezifischen Aufgaben der Meldebehörden ebenso eingeht, wie auf die von ihnen vorzunehmende Verarbeitung personenbezogener Daten.

Zu 2.2: (Datenübermittlung an andere Behörden)

Für die Übermittlung an andere Behörden und öffentliche Stellen läge es zunächst nahe, die Grundsätze des BDSG zu übernehmen (§ 10). Nur: Spätestens am Melderecht erweist sich, wie problematisch die vom Gesetzgeber im Rahmen des BDSG verwendeten Formeln sind, wie wenig sie also weiterhelfen, sobald man mit ihrer Hilfe die für einen bestimmten Verwaltungsbereich typischen Übermittlungsschwierigkeiten zu lösen sucht. Je mehr man beispielsweise das Aufgabengebiet der Meldebehörden ausweitet, je nachhaltiger sie zum staatlichen „Datendepot“ werden, desto bedeutungsloser sind Vorschriften wie § 10 BDSG. Wo die Meldebehörden zum institutionalisierenden Informationslieferanten einer als Informationseinheit begriffenen öffentlichen Verwaltung werden, gibt es praktisch keine Übermittlungsschranken mehr. Umgekehrt führt auch eine konsequent kasuistische Regelung nicht weiter. Sie bringt Kommunikationsschwierigkeiten mit sich, die den von den Verwaltungsleistungen abhängigen Bürgern letztlich nur schaden. So sinnvoll eine strikte Abschottung in bestimmten Einzelsituationen (z. B. Gesundheitsdaten) sein mag, so wenig läßt sie sich in einen allgemeinen Grundsatz verwandeln.

Den Ausschlag gibt unter diesen Umständen einmal mehr die Aufgabendefinition der Meldebehörden. Sie ist das primäre Steuerungsmittel des Übermittlungsprozesses. Eine konkrete, gesetzlich verankerte Funktionsbeschreibung grenzt den Übermittlungsrahmen von vornherein

ein. Dennoch gilt es dabei nicht stehenzubleiben, schon mit Rücksicht auf die Informationsanforderungen anderer Behörden. Gerade im Interesse eines besseren Datenschutzes kommt es darauf an, sich nicht mit den Generalklauseln des § 10 BDSG abzufinden, sondern mehr Präzision anzustreben, und zwar in Kenntnis der spezifischen Situation der Meldebehörden.

So gesehen, gehört zum notwendigen Inhalt eines Meldegesetzes eine exakte und abschließende Aufzählung der regelmäßigen Informationsempfänger. Sie schränkt nicht nur das Ausmaß der Übermittlungen ein, sondern vermittelt zugleich dem Betroffenen einen genauen Überblick der möglichen Empfänger seiner Daten. Nur wenn die Informationsverarbeitung so transparent gehalten wird, lassen sich auch die Anforderungen an eine Benachrichtigung des Betroffenen reduzieren. Ein mit dem Meldevorgang verbundener Hinweis auf die regelmäßigen Empfänger dürfte unter diesen Umständen ausreichen.

Viel schwerer fällt es, Regeln für die gelegentlichen Übermittlungen zu formulieren. Der mögliche Ausgangspunkt ist in § 10 BDSG angedeutet: So wenig sich eine Übermittlung vermeiden läßt, so sehr muß der Gesetzgeber darauf bedacht sein, eine restriktive Übermittlungspraxis sicherzustellen. Diesem Ziel entspricht es, eine Übermittlung zunächst einmal immer dann zu untersagen, wenn der Empfänger seine Aufgaben auch ohne die verlangten Daten erfüllen kann. Der Datenschutz zwingt dazu, die Verwaltungsaufgaben mit einem Mindestmaß an personenbezogenen Daten durchzuführen. Jede Behörde hat sich daher vor allem anderen zu fragen, ob sie sich nicht in der Lage sieht, auf die Daten zu verzichten. Erst wenn die Kenntnis der Angaben zur *conditio sine qua non* für die Aufgabenerfüllung wird, erscheint es gerechtfertigt, eine Übermittlung zuzulassen.

Ferner: Gerade weil die Übermittlung immer nur mit Rücksicht auf eine bestimmte Aufgabe hingenommen werden darf, ist es auch konsequent vom Empfänger zu fordern, die Daten ausschließlich für die Zwecke zu nutzen, für die ihm die Angaben überlassen worden sind. Wenn schon eine Abschottung der Meldebehörden nicht akzeptiert werden kann, so muß zumindest für eine strikte zweckgebundene Verwendung gesorgt werden. Die Verbreitungsgrenze mag mithin zunehmen, die Verarbeitung bleibt dennoch übersichtlich und kontrollierbar.

Zu 2.3: (Auskunft an Dritte)

Wer auf staatliches Geheiß Informationen zur Verfügung stellt, ist keineswegs ohne weiteres bereit, diese seine Angaben Privaten zu überlassen. Die Übermittlung wird auch nicht deshalb akzeptabel, weil „nur“ der Name oder „nur“ die Adresse weitergegeben wird. Maßgeblich ist vielmehr die durch die Übermittlung bewirkte Richtungsänderung: Informationsadressat ist nicht mehr allein die öffentliche Verwaltung, die personenbezogenen Daten gelangen zugleich in den Verfügungsbereich privater Unternehmen.

Das BDSG (§ 11) bietet keinen Ausweg. Seine Formulierungen sind viel zu allgemein gehalten. Zudem vermeidet es das Gesetz, den zunächst einzig akzeptablen Anknüpfungspunkt in den Vordergrund zu stellen: die Entscheidung des Betroffenen selbst. Er gibt seine Daten an die öffentliche Verwaltung. Er muß deshalb zumindest ein Mitspracherecht immer dann haben, wenn die Angaben von nicht-staatlichen Stellen verwendet werden sollen. Ganz in diesem Sinn haben sich einzelne Länder bemüht, das BDSG für ihren Bereich zu korrigieren, sich also nicht mit einer schlichten Wiedergabe des § 11 in der Landesdatenschutzgesetzgebung begnügt. Im Unterschied zum Bundesgesetzgeber räumen sie dem Betroffenen ein Recht auf Auskunftssperre ein. Während das Berliner Datenschutzgesetz jedoch eine grundsätzlich generelle Auskunftssperre kennt, spricht sich Hessen nur im Meldebereich dafür aus (§ 16 a Hessisches Meldegesetz – HMG). Ähnliche Überlegungen sprechen übrigens dafür, dem Betroffenen das Recht auf eine Auskunftssperre dann einzuräumen, wenn es um die Übermittlung seiner Daten an eine öffentlich-rechtliche Religionsgesellschaft geht.

Genaugenommen geht es dabei um eine Entwicklung, die in der Diskussion über die Reform des Melderechts begonnen hat. Hier war zum ersten Mal die Notwendigkeit einer Auskunftssperre erkannt worden und hier hatte man sich konsequenterweise auch zuallererst bereit gefunden, eine in diese Richtung zielende gesetzliche Regelung zu erörtern. § 15 Abs. 5 des Entwurfs ist der Beweis dafür. Soviel gilt es jedoch nicht zu übersehen: Das Melderecht ist nicht mehr als ein Modellfall für die Auskunftssperre. Sie mag gerade im Zusammenhang mit der Übermittlung personenbezogener Daten durch die Meldebehörden besonders erforderlich sein, sie ist aber genauso in allen weiteren Fällen angebracht, in denen die öffentliche Verwaltung zum Informationslieferanten nicht-staatlicher Stellen wird. § 16 a HMG verdeutlicht zugleich die möglichen Kompromißgrenzen. Der Gesetzgeber kann nicht einerseits die Auskunftssperre anerkennen und sie andererseits von vornherein auf bestimmte Übermittlungen beschränken. Dem Interesse des Betroffenen ist nur Genüge getan, wenn er sich grundsätzlich gegen jede Informationsweitergabe aussprechen kann. Diskutabel ist unter diesen Umständen nur eine Einschränkung: erhöhte Anforderungen an die Geltendmachung der Auskunftssperre, und auch dies nur, soweit es um Namen, akad. Grade und Anschriften geht. So fordert § 16 a Abs. 4 HMG bei einer Auskunftssperre, die sich auf die Melderegisterauskunft bezieht, vom Betroffenen „glaubhaft zu machen“, daß seine schutzwürdigen Belange beeinträchtigt werden. In allen anderen Fällen bleibt es dabei: Mehr als die Mitteilung, die eigenen Daten sperren zu wollen, kann und darf nicht verlangt werden.

Allzu leicht neigt man allerdings dazu, die Tragweite einer solchen Regelung zu überschätzen. Die gesetzliche Anerkennung der Auskunftssperre genügt für sich genommen nicht. Sie hat nur solange einen Sinn, wie von ihr auch Gebrauch gemacht wird. Die Anerkennung der Aus-

kunftssperre muß daher mit einer Informationspolitik der öffentlichen Verwaltung verknüpft werden, die von vornherein an der Aufgabe auszurichten ist, nicht nur den Verarbeitungsprozeß zu verdeutlichen, sondern den Betroffenen zugleich mit seinem Recht zu konfrontieren, steuernd in diesen Prozeß einzugreifen. Eine Auskunftssperre, die nicht mit einem ausdrücklichen Hinweis des Betroffenen auf seine Rechte verknüpft wird, und zwar sowohl im Zusammenhang mit dem Meldevorgang als auch zu einem regelmäßig wiederkehrenden Zeitpunkt, ist nutzlos.

Im übrigen sollte sich der Gesetzgeber bei der Formulierung der Übermittlung an nicht-staatliche Stellen an der Vorschrift des § 16 a HMG orientieren. Diese Bestimmung ist nicht nur sehr viel übersichtlicher gefaßt, sondern enthält auch sehr viel präzisere im Interesse des Betroffenen festgelegte Einschränkungen.

Soweit es schließlich um die Unterrichtung des Betroffenen bei einer „erweiterten Melderegisterauskunft“ geht, wäre erneut daran zu denken, zwischen regelmäßigen Empfängern und gelegentlich erteilten Informationen zu unterscheiden. Bei regelmäßigen Empfängern halte ich eine solche Unterrichtung für angebracht.

Zu 2.4: (Sperrung und Löschung)

Auch im Rahmen des Bundesmeldegesetzes kann davon nicht abgesehen werden, Daten zu sperren und zu löschen. Die Meldebehörden bekommen die von ihnen gespeicherten personenbezogenen Daten keineswegs nur vom Betroffenen. Gerade im Rahmen der Übermittlung von Behörde zu Behörde können sich aber Fehler einschleichen. Kontroversen über die Daten mit dem Betroffenen lassen sich deshalb nicht ausschließen. Im Hinblick darauf muß der Gesetzgeber die Behörden verpflichten, die Daten zumindest immer so lange zu sperren, wie sie nicht den Nachweis der Richtigkeit erbringen können. Es ist Aufgabe der Behörden, sich um eine Aufklärung des Sachverhalts zu kümmern. Gelingt ihnen dies nicht, so müssen die Daten gelöscht werden.

Ob darüber hinaus eine Löschung vorgesehen werden muß, sobald die Daten nicht mehr zur Erfüllung der den Meldebehörden obliegenden Aufgaben benötigt werden, läßt sich abstrakt nicht beantworten. Entscheidend ist vielmehr einmal mehr die vom Gesetzgeber den Meldebehörden zugewiesene Funktion. Sollte ihre Aufgabe unter anderem darin bestehen, Daten, die der öffentlichen Verwaltung zur Verfügung gestellt werden, zu archivieren, dann wäre eine Löschung fehl am Platz. Der gegenwärtigen Praxis lassen sich manche Anhaltspunkte entnehmen, die in diese Richtung weisen. Oft genug sind es die Meldebehörden, die auch nach mehreren Jahrzehnten den Betroffenen Daten zur Verfügung stellen, die er etwa für bestimmte Anträge braucht.

Mit der unter bestimmten Voraussetzungen erforderlichen Speicherung und Löschung von Daten hängt auch die Notwendigkeit zusammen, dem Betroffenen entspre-

chende Rechte einzuräumen. Man kann sich nicht mit dem Hinweis begnügen, die Meldebehörden würden ohnehin von sich aus ihren gesetzlichen Pflichten nachkommen und beispielsweise gespeicherte falsche Daten löschen.

Der Betroffene muß auch die Möglichkeit haben, von sich aus darauf zu dringen, auf eigene Initiative also, die Verwirklichung der gesetzlichen Vorschriften zu verlangen und durchzusetzen.

Zu 3: (Weitere Regelungen)

Die gesetzliche Regelung sollte sich nicht damit begnügen, ein Auskunftsrecht des Betroffenen vorzusehen. Sie muß darüber hinaus die Gebührenfreiheit bei der Auskunftserteilung ausdrücklich garantieren. Die Erfahrung lehrt, daß Gebühren auch und gerade bei der Auskunftserteilung eine prohibitive Wirkung haben. Man kann nicht einerseits vom Betroffenen erwarten, von sich aus alles zu unternehmen, um die Korrektheit seiner Daten zu gewährleisten, ihn aber andererseits von der notwendigen Kontrolle durch die Gebühren abzuhalten. Auch die Überlegung, nur mit Hilfe der Gebühren ließen sich unberechtigte Fragen abwehren, hilft nicht weiter. Will man dagegen vorgehen, so gilt es, gezielte Vorkehrungen zu treffen und nicht eine allgemeine Gebührenpflicht einzuführen, die letztlich auch diejenigen abschreckt, die sich keineswegs nur mutwillig nach ihren Daten erkunden.

Zu 4 und 5: (Datenkatalog — Landesadreibregister)

Den Anforderungen des Datenschutzes entspricht es, die von den Meldebehörden zu speichernden Daten gesetzlich festzulegen. Abstrakte Datenkataloge, wie sie sich etwa im Anhang zum Entwurf finden, entsprechen allerdings diesen Anforderungen nicht. Niemand bestreitet, daß die Erhebung der dort genannten Angaben durch gesetzliche Vorschriften abgedeckt ist. Der Streit geht nicht um die Legalität der Verarbeitung im Sinne einer gesetzlichen Ermächtigung. Er entzündet sich vielmehr an jenem im BDSG und in den Landesdatenschutzgesetzen formulierten fundamentalen Prinzip einer rechtlich zulässigen Verarbeitung personenbezogener Daten: der Erforderlichkeit. Der Gesetzgeber hat sich damit selbst Zurückhaltung verordnet. Verarbeitungsfähig ist immer nur eine begrenzte Zahl von Angaben.

Die bloße Existenz einer gesetzlichen Grundlage reicht jedoch nicht aus, um die „Erforderlichkeit“ zu bejahen. Die öffentliche Verwaltung ist vielmehr auch dann, wenn sie auf eine gesetzliche Vorschrift verweisen kann, verpflichtet, sich zu fragen, inwieweit die Daten wirklich benötigt, ob und in welchem Umfang also nicht auf manche von ihnen verzichtet werden kann. Der Datenschutz verpflichtet zur permanenten Inventarisierung der staatlichen Datenbestände, um eine Verarbeitung überflüssiger Angaben rechtzeitig zu verhindern. Keineswegs geht es infolgedessen nur darum, jedem Versuch, Daten auf Vorrat zu verarbeiten, einen Riegel vorzuschieben. Auch dort, wo vordergründig kein Anlaß besteht, an der Verarbei-

tungsfähigkeit zu zweifeln, kommt es genauso darauf an, den Verwendungszweck konsequent als Überprüfungsmaßstab zu nutzen. Dies umso mehr als viele der gesetzlichen Regelungen, die zur Verarbeitung ermächtigen, aus einer Zeit stammen, zu der die Verpflichtung zur Zurückhaltung und die strenge Bindung an den Verwendungszweck keineswegs gesetzlich sanktioniert waren. Betrachtet man unter diesem Aspekt den Datenkatalog, so wird das Datenschutzdefizit sofort sichtbar. Vier Beispiele mögen dies verdeutlichen: Zu dem mehr oder weniger selbstverständlichen Grundbestand an Daten, die von den Betroffenen den Meldebehörden zur Verfügung gestellt werden, zählen auch Angaben zum Beruf. Trotzdem fällt es schwer einzusehen, welchen Sinn diese Angaben haben. Der Verwendungszweck bleibt offen. Soweit die Kenntnis des Berufs für statistische Zwecke notwendig sein sollte, würde es vollauf genügen, eine Regelung in den entsprechenden Gesetzen zu treffen. Unabhängig davon zählen gerade die Angaben zum Beruf zu den unzuverlässigsten. Sie werden kaum berichtet und dennoch übermittelt. Es kann aber nicht Aufgabe der gesetzlichen Regelung sein, eine offenkundige Quelle von Fehlinformationen zu institutionalisieren.

Nach den Vorstellungen des Entwurfs obliegt es den Meldebehörden, auch die Gründe zu speichern, aus denen ein Paß versagt wird. Nur: Auch nach der Reform des Melderechts bleibt es bei der Existenz besonderer Paßbehörden. Nach wie vor wird es also so sein, daß niemand anderes als diese Behörden sich damit auseinanderzusetzen haben, ob im konkreten Fall der Paß verweigert werden darf. Infolgedessen ist auch die Frage, ob und in welchem Umfang es überhaupt erforderlich sein kann, solche Gründe zu verarbeiten, erst im Zusammenhang mit ihrer Tätigkeit zu entscheiden und ihnen müßte konsequenterweise die Speicheraufgabe zufallen.

Man meine nicht, derlei Überlegungen zeugten von einem überspitzten Kompetenzdenken und ließen jegliche der Verwaltungsrealität entgegenkommende Flexibilität vermissen. Es geht ausschließlich darum Regelungen zu treffen, die im Interesse des Betroffenen die Datenzirkulation gezielt unterbrechen. Der Gesetzgeber muß gerade dort, wo der Sensibilitätsgrad der Daten zunimmt, den Datentransfer von vornherein einschränken. Die sorgfältige Abschottung der Datenbestände gehört zu den elementaren Voraussetzungen wirksamen Datenschutzes.

Welche Bedeutung dieser Forderung zukommt, läßt sich wahrscheinlich am ehesten bei der Verarbeitung der Wahlausschlußgründe ermesen. Unstreitig zählt die Führung der Wählerverzeichnisse zu den allgemein akzeptier-

ten Aufgaben der Meldebehörden. Ebenso wenig bedarf es deshalb der Diskussion, daß sie ihrer Verpflichtung nur solange genügen können, wie sie zuverlässig über die Wahlberechtigung informiert sind. Nur folgt daraus noch keineswegs die Notwendigkeit, die Wahlausschlußgründe zu kennen. Für die Meldebehörde kann und darf es keine Rolle spielen, was dem Wahlrecht entgegensteht. Sie hat nicht mehr zu tun, als die gesetzlich verordnete Sperre zu registrieren. Mehr als die Kenntnis, daß ein Wahlausschlußgrund vorliegt, ist dafür nicht erforderlich.

Man unterschätze die Tragweite dieser Aussage nicht. Für den Betroffenen steht viel auf dem Spiel. Wahlausschlußgründe sind extrem sensitive Daten. Entmündigung und Geisteskrankheit sind Beispiele, die wohl keiner Kommentierung bedürfen. Jede Übermittlung dieser Daten ist für den Betroffenen mit dem Risiko einer Stigmatisierung behaftet. Der Gesetzgeber hat deshalb keine Wahl: er muß die Verarbeitung von Informationen von vornherein unterbinden.

Noch eine Bemerkung zu den Lohnsteuerdaten. Wiederum steht die Aufgabe der Meldebehörden außer Zweifel. Sie stellen jene Daten zur Verfügung, die von den Gemeinden im Zusammenhang mit den Lohnsteuerkarten benötigt werden. Der Datenkatalog des Entwurfs hält sich insofern zunächst durchaus im Rahmen verständlicher akzeptierter Verarbeitungsziele. Bedenklich stimmt freilich die Ausführlichkeit. So bleibt etwa unklar, warum Adoptiv- von Stief- und leiblichen Kindern unterschieden werden müssen. Die einschlägige gesetzliche Vorschrift (§ 32 Abs. 4 EStG) hilft jedenfalls nicht weiter. Im Gegenteil, sie lehnt solche anderswo durchaus sinnvolle Unterscheidungen ab. Für die Meldebehörden kann und darf es aber nicht darauf ankommen, welche Kriterien beispielsweise das Familienrecht seinen Regeln zugrundelegt. Solange steuerrechtliche Aufgaben im Vordergrund stehen, müssen sich die Meldebehörden auch nach den für das Steuerrecht geltenden Maßstäben richten. Im Interesse eines wirksamen Datenschutzes ist davon abzusehen, den Katalog der zu speichernden Daten landesrechtlich zu erweitern. Der Bundesgesetzgeber hat sich bei der Formulierung des Meldegesetzes ohnehin eingehend mit den Erwartungen der Länder auseinanderzusetzen. Insofern erscheint es durchaus möglich und gerechtfertigt, den Datenkatalog abschließend zu formulieren. Auch wenn daher die Notwendigkeit von Landesadreßregistern bejaht werden sollte, muß sich bereits aus dem Bundesmeldegesetz eindeutig ergeben, welche Daten dort aufgenommen werden dürfen. Ebenso muß von vornherein feststehen, daß die Verarbeitungsvoraussetzungen, vor allem die Übermittlungsbedingungen, nicht variieren dürfen.

SACHWÖRTERVERZEICHNIS FÜR DEN SIEBENTEN TÄTIGKEITSBERICHT

- Abgangskontrolle 12.1
 Adoptionsvermittlung 9.1
 Adressenhandel 4.1, 2, 4; 7.1; 2.Z 1.3
 Amtshilfe 6.3
 Anonymisierung 6.1, 2, 5; 9.1
 APOS 12.3
 Auftragskontrolle 12.1
 Auftragsverarbeitung 3.3
 Auskunft
 — aus Kriminalakten 5.1.8
 Auskunftspflicht 10.1
 Auskunftsrecht
 — des Betroffenen 1.1 b; 2; 3.1 — 4; 8.3
 — des Parlaments 2; 2.Z 1 — 1.2
 Auskunftssperre 1.1 a; 4.1; 2.Z 2.2
 Automation
 — automatisiertes Verfahren 5.1.1

 BAL 12.2
 Bayerisches Datenschutzgesetz 1.1 b; 2; 5.1.8; 11 c
 Befragungen 6.1 — 2; 8.1
 Bekenntnisfreiheit 11 c
 Benutzerkontrolle 12.1
 Berichtigungsanspruch 3.1, 3
 Berliner Datenschutzgesetz 2
 Bibliotheksdaten
 — Weitergabe an Verfassungsschutz 5.2
 Bremisches Datenschutzgesetz 2
 Bundesmeldegesetz
 — Entwürfe zu einem 1.1 a
 Bundeszentralregister 5.1.5; 5.1.5 a; 5.1.9

 COM-Verfahren 12.3

 DASCH 12.2
 Datenbanken
 — im Einwohnerwesen 3.4
 — medizinische 8.4
 Datenbankregister (Dateienregister) 3.3 — 4
 Datenfernübertragung 12.1
 Datensicherung 3.4; 10.1; 12
 Datenschutz
 — im Sicherheitsbereich 5
 Datenschutzbeauftragte
 — Zusammenarbeit der 1.2
 Datenschutzbeauftragter
 — betrieblicher 10.2
 Datenschutzbewußtsein der Bürger 1.3; 3.4
 Datenschutzgesetzgebung in den Ländern
 (mit tabellarischer Übersicht) 2
 Datenschutzkommission 3.1 — 4
 DISPOL 5.1.4

 Disziplinarmaßnahmen
 — in Kriminalakten 5.1.7
 Disziplinarordnung 5.1.7
 — Hessische (HDO), § 110
 DS-Software 12.3
 DVL 12.2

 Eigenbetrieb 10.2
 Eingabekontrolle 12.1
 Einverständnis des Betroffenen 1.1; 7.2; 8.1 — 2
 Einwilligungserklärung 2; 7.2
 Einwohnerwesen 3.4 — 5; 4.1 — 6; 2.Z 1 — 2.2
 Elternrecht 3.3; 4.4; 6.1 — 2; 8.2

 Gesundheitswesen 3.2; 8.1 — 4

 Hardware-Sicherung 12.3
 Heimkinderdatei 9.1
 HEPOLIS 5.1 ff.
 HZD 9.1

 Informationsgleichgewicht 2
 INPOL 5.1.4

 Jubiläumsdaten 4.1
 Jungwählerdaten 4.1; 4.4; 2.Z 1.1 — 1.1.3

 Kindergarten 8.2
 Kirche
 — verfaßte 6.3; 11 g
 Kirchliche Einrichtungen 11 g
 Kommunen 10.1; 10.2
 Konferenz, Ständige;
 der Datenschutzbeauftragten der
 Länder und des Bundes 1.2
 Kraftfahrt-Bundesamt
 — Übermittlung für Forschung und Werbung 4.5
 Krankenhausgesetz
 — Hessisches 8.3; 11 g
 Krebsregister 8.4
 Kriminalakten
 — Auskünfte aus 1.1 b

 Länderdatenschutzgesetze
 (mit tabellarischer Übersicht) 2
 Landesjugendamt 9.1
 Landespersonalrat 1.1 b
 Landeswahlordnung 2.Z 1.1.3
 Leserprofile 5.2
 Leseverhalten
 — von Bibliotheksbenutzern 5.2
 Löschung 1.1 b; 3.1, 3; 5.1.6; 7.2; 8.2

- Medizinische Daten 3.2; 8.1 – 4
 Meldegesetz (HMG)
 – Hessisches 11 e
 – Hessisches § 16 a 1.1 a; 4.1 – 2
 Melderegister
 – Übermittlung aus dem 1.1 a; 4.3

 Niedersächsisches Datenschutzgesetz 2
 Nordrhein-Westfalen 3.3

 Organisationskontrolle 12.1
 Orgware-Sicherung 12.3

 Parteien 2.Z 1; 1.1.1
 Personalwesen 6.3; 7.1 – 2; 10.1
 Polizei
 – Auskunft aus Melderegister 4.3
 Polizeigesetz
 – Entwurf für ein einheitliches – des Bundes und der
 Länder 1.1 b
 Polizeiliche Informationssysteme
 (s. auch HEPOLIS – INPOL) 4.3; 5.1 ff.

 RACF 12.3
 RAU 12.2
 Rechtmäßigkeit 5.1.6
 Rechtsverkehr 5.1.5 a
 Religionsgesellschaften
 – Autonomie der 11 b, c
 – Datenübermittlung an öffentlich-rechtliche 11 a
 Richtlinien
 – vorläufige – für die Führung von Kriminalakten
 5.1.7
 – vorläufige – für die Auskunft aus Kriminalakten
 5.1.8

 Saarländisches Datenschutzgesetz 2
 Schadenersatz
 – Haftung, verschuldensunabhängige 2
 Schweden 3.3 – 4
 Schleswig-Holsteinisches Datenschutzgesetz 2
 Schulsportärztlicher Untersuchungsbogen 8.1
 SECURE 12.3
 Software-Sicherung 12.3
 Sozialwesen 8.3; 9
 Speicherkontrolle 12.1
 Speicherungsverbot 9.1 – 2
 Sperrecht des Bürgers 2; 4.1

 Sperren 4.1
 Sperrung 5.1.6
 Statistik 3.3 – 4; 6.5
 StPO, Neufassung des § 81 1.1 b
 Strafverfolgung 1.1 b

 Telefon-Abrechnung
 – Datenschutz und Kontrolle bei 7.3
 Tilgungsfrist 5.1.5 a; 5.1.7
 Tilgungsreife 5.1.5 a
 – tilgungsreif 5.1.6
 Transparenz 1.3; 3.3
 Transportkontrolle 12.1
 Transport von Datenträgern 12.1

 Übermittlungskontrolle 12.1
 Übermittlungssperre 1.1 a

 Verfassungsschutz und Bibliotheksdaten 5.2
 Vernichtung von Unterlagen 1.1 b
 Versicherungen 7.1
 Verurteilungen
 – strafgerichtliche 5.1.5; 5.1.5 a; 5.1.5 b; 5.1.6;
 5.1.9
 Verwertungsverbot 5.1.5 a
 Volkshochschulen 6.5

 Wettbewerbsunternehmen
 – öffentlich-rechtliche 10.2
 Wissenschaft, Forschung 1.1 c

 Zugangskontrolle 12.1
 Zugriff
 – allg. 9.1
 – auf Daten aus HEPOLIS 5.1.2 – 3
 – skontrolle 12.1
 Zulässigkeit der DV 1.1 a; 1.1 b; 2; 9.2
 Zweckbindung der DV 1.1 c

 Der Siebente Tätigkeitsbericht ist – nach dem 2. Zwischenbericht (2.Z) – der erste Jahresbericht, der nach dem neuen Hessischen Datenschutzgesetz vom 31. Januar 1978 vorgelegt worden ist. Es wurde deshalb davon Abstand genommen, das Sachwortregister der Berichte I bis VI und des 1. Zwischenberichts fortzuführen. Rückgriffe sind über das Sachwortregister im Sechsten Tätigkeitsbericht (Drucks. 8/3962) oder im Sammelband möglich.