HESSISCHER LANDTAG

8. Wahlperiode

Drucksache **8/2475**

30. 03. 76

Fünfter Tätigkeitsbericht des Hessischen Datenschutzbeauftragten

Mit Schreiben vom 29. März 1976 legt der Datenschutzbeauftragte gemäß § 14 Abs. 1 des Hessischen Datenschutzgesetzes vom 7. Oktober 1970 dem Landtag den folgenden Tätigkeitsbericht vor:

Eingegangen am 30. März 1976 · Ausgegeben am 2. Juni 1976

Druck: Carl Ritter & Co., Wiesbaden · Vertrieb: Verlag Dr. H. Heger, Goethestr. 56, 53 BN-Bad Godesberg, Tel. (02221)/363551

INHALTSVERZEICHNIS

Bei den Hinweisen (Fußnoten) bezeichnen I, II, III und IV den Ersten, Zweiten, Dritten bzw. Vierten Tätigkeitsbericht, die arabischen Ziffern die angesprochenen Abschnitte in dem Bericht. Z 1 verweist auf den Zwischenbericht vom 9. 2. 76 (LT-Drucks. 8/2239)

1. EINLEITUNG

1. Einleitung

1.1 Zum fünften Mal seit 1972 legt der Hessische Datenschutzbeauftragte einen Tätigkeitsbericht vor. In zweifacher Hinsicht ist der diesjährige Bericht allerdings mehr als nur die Fortführung einer schon eingespielten Übung:

Am 18. 6. 1975 legte Staatssekretär a. D. Birkelbach sein Amt als Datenschutzbeauftragter nieder. Er war es, der durch seine Initiative und sein Engagement die ersten vier Jahre in der Geschichte des Hessischen Datenschutzgesetzes geprägt hat. Und er war es auch, der diesem Bericht seine seither allgemein akzeptierte Form gegeben hat. Wer die früheren Berichte kennt, wird unschwer feststellen, daß sich an dieser Form nichts geändert hat. Dokumentiert ist damit freilich weitaus mehr als nur eine rein äußerliche Übereinstimmung. Vielmehr soll dadurch deutlich zum Ausdruck gebracht werden, daß der personelle Wechsel nicht auch einen Interpretationswandel der für die Anwendung des Datenschutzgesetzes maßgebenden Prinzipien bedeutet. Die in den vergangenen fünf Jahren formulierten Grundsätze bestimmen auch weiterhin die Tätigkeit des Datenschutzbeauftragten.

Unabhängig aber von aller personellen Veränderung signalisiert dieser fünfte Tätigkeitsbericht den Abschluß einer ersten, gleichsam einführenden Etappe in der Entwicklung des Datenschutzes. Als das Gesetz entstand, war es national wie international eine Pionierleistung. Zwar war auch anderswo die Forderung nach Datenschutz nachdrücklich vorgebracht worden, doch nirgends hatte sich bis dahin der Gesetzgeber mit solcher Konsequenz bereitgefunden, die Voraussetzungen für einen wirksamen Schutz des einzelnen zu schaffen. Nur, so wichtig, ja unerläßlich dieser Schritt auch war, so sehr hing nunmehr alles davon ab, ob es gelingen würde, Datenschutz aus einem vom Gesetzgeber anerkannten Grundsatz in ein von der Verwaltung respektiertes und praktiziertes Prinzip zu verwandeln.

Aufgabe der vergangenen fünf Jahre war es deshalb, „Datenschutzbewußtsein" zu wecken, verständlich zu machen, daß der Datenschutz für die administrative Tätigkeit eine nicht minder verbindliche Richtlinie darstellt als die bis dahin maßgeblichen Regeln. Alle Bemühungen, dieser Aufgabe gerecht zu werden, haben sich von einer Überlegung leiten lassen: Datenschutz ist Bürgerrecht. Die Sorge des Gesetzgebers gilt dem einzelnen Bürger und den sich für seine Position ergebenden Konsequenzen aus der Inanspruchnahme der Vorteile des technologischen Fortschritts durch eine auf Rationalisierung und Effizienz bedachte öffentliche Verwaltung. Der Konflikt zwischen dem Recht des Bürgers auf seine persönliche Integrität und dem wachsenden Informationsbedarf der Administration verpflichtet den Gesetzgeber, Regeln zu entwickeln, die den an den Bürger gestellten Informationserwartungen der Verwaltung Grenzen setzen, um die Interessen des Bürgers zu schützen.

Datenschutz ist deshalb keineswegs, wie mancher immer noch zu meinen scheint, Fahndung nach „Mißbrauchsfällen". Er rechtfertigt die Notwendigkeit seiner Existenz nicht durch eine möglichst lange Liste von Verstößen. Vielmehr kommt es vor allem anderen darauf an, in ständiger Zusammenarbeit mit der Administration präventiv Vorkehrungen zu entwickeln, die „Mißbräuche" gar nicht erst entstehen lassen. Die vergangenen fünf Jahre haben gezeigt, in welch hohem Maße die Verwaltung Verständnis dafür aufbringt und auch zur Kooperation bereit ist. Auch an den im diesjährigen Tätigkeitsbericht enthaltenen Beispielen läßt sich ablesen, wie sehr der Datenschutz auf eine solche Zusammenarbeit angewiesen ist. Hervorzuheben wären etwa die Bemerkungen zu den im Bereich der Polizei ausgearbeiteten Richtlinien oder die Anregungen für eine rechtzeitige Auseinandersetzung mit den sich aus Personaldatenbanken für die Bediensteten des Landes Hessen ergebenden Konsequenzen.

Datenschutz heißt insofern in erster Linie Bereitschaft zum Umdenken sowie zur kritischen Überprüfung traditioneller Institute und Regulative administrativer Tätigkeit. Deshalb hat der Datenschutzbeauftragte eine Datenverkehrs-Ordnung vorgelegt[1]). Und aus genau demselben Grund wird auch in Zukunft der Weitergabe von Informationen im Bereich der öffentlichen Verwaltung ganz besondere Aufmerksamkeit zu widmen sein, ebenso wie dem Ziel, dem Bürger durch ein ihm garantiertes Auskunftsrecht den Zugang zu den ihn betreffenden Informationen sicherzustellen.

Die Tätigkeit des Datenschutzbeauftragten in den vergangenen fünf Jahren mußte sich darauf

[1]) Siehe IV, Anl. I

konzentrieren, die Voraussetzungen für einen wirksamen Datenschutz zu schaffen, Schwerpunkte zu setzen, Konfliktherde auszumachen und erste Ansätze für die Lösung solcher Konflikte zu formulieren. Von nun an gilt es, sich auf dem Hintergrund der geleisteten Arbeit dieser Schwerpunkte anzunehmen und für die Verwirklichung genauso präziser wie detaillierter, den Schutz des Bürgers garantierender Regelungen zu sorgen.

1.2 Mehr denn je erweist sich allerdings, daß Datenschutz weit davon entfernt ist, eine Routineaufgabe zu sein. Die Zunahme der gesetzlichen Regelungen außerhalb Hessens, insbesondere die Bemühungen um ein Bundesdatenschutzgesetz zwingen dazu, sich intensiv mit der Frage auseinanderzusetzen, wie das Hessische Datenschutzgesetz verbessert werden kann. Deshalb beschäftigt sich ein großer Teil dieses Berichts mit der geplanten Bundesregelung und enthält zugleich präzise Vorschläge für eine Ergänzung des Hessischen Datenschutzgesetzes. In diesen Vorschlägen konkretisiert sich die Überzeugung, daß eine Datenschutzregelung ihre Aufgabe nur durch ein Höchstmaß an Lernfähigkeit und Flexibilität erfüllen kann.

Die Verabschiedung des Hessischen Datenschutzgesetzes war, so gesehen, auch aus der Perspektive des Gesetzgebers kein Schlußpunkt, sondern ein Anfang. Die Erfahrungen der letzten fünf Jahre unterstreichen, daß an manchen Punkten eine Reform überfällig ist. Das gilt in ganz besonderem Maß für den Anwendungsbereich des Gesetzes und das Auskunftsrecht des Bürgers. Was getan werden muß, steht bereits fest. Mit seinen Vorschlägen will der Bericht der Intention des Gesetzgebers Rechnung tragen, einen wirksamen Datenschutz zu ermöglichen, zugleich aber der parlamentarischen Diskussion eine Reihe von Anregungen geben. Eine Gesetzesreform würde auch zeigen, daß der hessische Gesetzgeber nicht gewillt ist, auf seine Pionierfunktion zu verzichten, weil sich der Bund ebenfalls anschickt, den Datenschutz sicherzustellen. Erst recht kommt es in einem solchen Augenblick darauf an, die notwendigen Korrekturen vorzunehmen, um zu demonstrieren, in welche Richtung sich der Datenschutz weiterentwickeln muß.

1.3 Das Verständnis des Datenschutzes als einer sich ständig neu stellenden Aufgabe hat in der Vergangenheit dazu geführt, im Tätigkeitsbericht einen Überblick über die Datenschutzgesetzgebung im Ausland zu geben. Der diesjährige Tätigkeitsbericht greift diese Übung bewußt auf. Wahrscheinlich nichts dokumentiert die Tatsache besser, daß es sich beim Datenschutz um fundamentale Fragen der Existenz des Bürgers in einer demokratischen Gesellschaft handelt, als die Vielzahl der Versuche, für eine wirksame gesetzliche Regelung zu sorgen. Wer den Bericht liest, wird leicht erkennen, welchen Einfluß das hessische Gesetz dabei ausgeübt hat. So hat sich beispielsweise die zuerst vom hessischen Gesetzgeber konsequent verwirklichte Forderung nach einer externen Kontrolle gegen anfängliche Zweifel und Widerstände nahezu überall durchgesetzt. Ebensosehr fällt aber auf, daß manche der in Hessen noch nicht verwirklichten Anregungen des Datenschutzbeauftragten zu den universell anerkannten Postulaten eines wirksamen Datenschutzes zählen. Wohl das wichtigste Beispiel dafür dürfte das Auskunftsrecht des Bürgers sein.

1.4 Dem Versuch, das Gesetz so flexibel wie nur möglich zu gestalten, dienen auch die in diesen Bericht erstmals aufgenommenen und insbesondere an die Adresse der Wissenschaft gerichteten Anregungen für eine ebenso intensive wie gezielte Forschung auf dem Gebiet des Datenschutzes. Auf die Notwendigkeit, die Forschung zu fördern, war bereits in der Vergangenheit hingewiesen worden. Der Bericht unternimmt es nun, die Erkenntnisse der letzten fünf Jahre zu nutzen, um über allgemeine Anregungen hinaus konkret anzugeben, wo sich Problembereiche abzeichnen, die vordringlich einer wissenschaftlichen Untersuchung bedürfen. Die Reaktionsfähigkeit der gesetzlichen Regelung auf technologische Innovationen hängt nicht zuletzt von einer erfolgreichen Zusammenarbeit mit der Wissenschaft ab.

1.5 Der Bericht vermittelt – wie auch in der Vergangenheit – einen Überblick über die Erfahrungen des letzten Jahres. Sicherlich, spektakuläre Fälle gibt es kaum. Doch wäre es falsch, die Tragweite der gebrachten Beispiele zu unterschätzen. Jedes von ihnen zeigt, wie sehr der Datenschutz alle Bereiche der öffentlichen Verwaltung berührt. Seine Notwendigkeit erweist sich an prinzipiellen Fragen wie der Auskunftspflicht ebenso wie an Alltagsproblemen der Administration, wie etwa der Weitergabe und publizistischen Verwertung bestimmter keineswegs außergewöhnlicher Angaben über die Bürger.

Ich habe bewußt darauf verzichtet, einige, in den vergangenen Tätigkeitsberichten bereits erwähnte, noch in der Entwicklung befindliche Vorgänge wieder aufzugreifen. Dazu gehört insbesondere das Demonstrationsprojekt DOMINIG II

über den Einsatz der automatischen Datenverarbeitung zur Lösung überbetrieblicher Organisationsaufgaben im Informationsverbund mehrerer Krankenhäuser. Diese Vorgänge werden jedoch weiterhin sorgfältig verfolgt, um zu den möglichen Auswirkungen für den Datenschutz rechtzeitig Stellung nehmen zu können.

1.6 Ein Fragenkomplex hat im Berichtszeitraum besondere Bedeutung erlangt: die mit der Interpretation des § 6 DSG zusammenhängenden Probleme. Verständlicherweise hat bislang die gleichsam klassische Aufgabe des Datenschutzes, Vorkehrungen über die Verwendung von Angaben zur Person des einzelnen zu treffen, im Vordergrund gestanden. Der hessische Gesetzgeber hat aber mit seiner Regelung mehr gewollt. Seine Aufmerksamkeit galt von Anfang an den Konsequenzen des technologischen Fortschritts für die Struktur und die Entwicklung einer demokratischen Gesellschaft. Zu diesen Folgen gehört sicherlich in erster Linie die Notwendigkeit, den Bürger vor einer Gefährdung seiner persönlichen Integrität zu schützen. Zu ihnen rechnet aber auch die Sicherung des Gleichgewichts zwischen den für eine demokratische Gesellschaft konstitutiven Institutionen. Datenschutz ist insofern Bürgerschutz auch in einem anderen, wenn man so will, mittelbaren Sinn. Im Interesse des Bürgers werden die Funktionsvoraussetzungen einer parlamentarischen Demokratie garantiert.

Konkrete Fragen zu diesem Problemkomplex haben sich zum ersten Mal während des Berichtszeitraums gestellt. Mit Rücksicht auf die weitreichende Bedeutung dieser Fragen habe ich dazu in einem Zwischenbericht Stellung genommen und beschränke mich hier, darauf zu verweisen[2]). Ich möchte allerdings noch einmal unterstreichen, daß das Hessische Datenschutzgesetz seiner beispielgebenden Funktion letztlich nur dann genügen wird, wenn es gelingen sollte, den Respekt vor dem Parlament und die Notwendigkeit seiner Information genauso ernst zu nehmen wie den Schutz des einzelnen Bürgers. Der hessische Gesetzgeber hat seine Intention, das Informationsgleichgewicht zwischen Regierung und Parlament zu wahren, unmißverständlich in § 6 DSG dokumentiert. Von der weiteren Handhabung dieser Bestimmung wird es abhängen, ob Intention und Realität auseinanderfallen oder sich decken.

[2]) LT-Drucks. 8/2239 vom 9. 2. 1976

2. KONSEQUENZEN DES GEPLANTEN BUNDESDATENSCHUTZGESETZES FÜR DAS HESSISCHE RECHT

2. **Konsequenzen des geplanten Bundesdatenschutzgesetzes für das hessische Recht**

Der Regierungsentwurf eines Bundesdatenschutzgesetzes (EBDSG)[1]), der z. Z. in den Ausschüssen des Deutschen Bundestages beraten wird, regelt die Verarbeitung personenbezogener Daten im Bereich der öffentlichen Verwaltung nicht nur des Bundes, sondern auch der Länder. Die Einbeziehung der Länder nötigt dazu, die Einwirkungen des künftigen Bundesdatenschutzrechtes auf das Hessische Datenschutzgesetz (DSG) zu untersuchen. Denn „Bundesrecht bricht Landesrecht" (Art. 31 GG), d. h. das Landesrecht wird vom Bundesrecht verdrängt oder außer Kraft gesetzt, soweit ein Bundesgesetz dasselbe Sachgebiet regelt.

Damit die Kontinuität des Datenschutzes im Interesse sowohl der Bürger als auch der Verwaltung gesichert bleibt, ist es geboten, die verfassungsrechtlichen Folgen der Bundesgesetzgebung für die Fortgeltung des Hessischen Datenschutzrechtes möglichst frühzeitig zu untersuchen. Als Grundlage der hier folgenden Analyse dient die Fassung des EBDSG, die der federführende Innenausschuß des Deutschen Bundestages erarbeitet hat[2]).

2.1 Da das Hessische Datenschutzgesetz den Datenschutz nur im Bereich der öffentlichen Verwaltung regelt, stehen unter dem Blickpunkt der Gesetzeskonkurrenz die Vorschriften des EBDSG, die sich auf den öffentlichen Bereich erstrecken, im Vordergrund des Interesses.

2.2 Unterschiede zwischen dem EBDSG und dem DSG bestehen zunächst hinsichtlich des Geltungsbereichs. Das Hessische Datenschutzgesetz erfaßt alle für Zwecke der maschinellen Datenverarbeitung erstellten Unterlagen sowie alle gespeicherten Daten und die Ergebnisse ihrer Verarbeitung im Bereich der gesamten Verwaltung des Landes einschließlich der Kommunalverwaltung ohne zu unterscheiden, ob die Datenverarbeitung der Ausführung von Bundes- oder Landesrecht oder ob sie anderen Aufgaben dient. Dagegen soll das Bundesgesetz für die Länder nur insoweit gelten, als sie Bundesrecht ausführen (§ 5 Abs. 2 Nr. 1 EBDSG). Diese Beschränkung ergibt sich aus § 1 Abs. 2 in Verbindung mit den Eingangsbestimmungen des zweiten, des dritten und des vierten Abschnitts (§§ 5, 16, 23). Jede dieser Vorschriften bestimmt den „Anwendungsbereich" des Gesetzes. Die „allgemeinen Vorschriften" des ersten Abschnitts (§§ 1—4) sind nicht allgemein gültige Rechtsnormen, sondern nur vor die Klammer gezogene, für alle drei Anwendungsbereiche geltende Grundsätze.

Ausgangspunkt für die hier angestellte Untersuchung ist daher § 5 Abs. 2 EBDSG. Danach gelten die Vorschriften des ersten und zweiten Abschnitts des Bundesgesetzes für

„1. Behörden und sonstige öffentliche Stellen der Länder, der Gemeinden und Gemeindeverbände und der sonstigen der Aufsicht des Landes unterstehenden juristischen Personen des öffentlichen Rechts und für deren Vereinigungen, soweit sie Bundesrecht ausführen

2. Behörden und sonstige öffentliche Stellen der Länder, soweit sie als Organe der Rechtspflege tätig werden, ausgenommen in Verwaltungsangelegenheiten."

Diesen Anwendungsbereich erfaßt auch das Hessische Datenschutzgesetz, mit Ausnahme der Rechtsprechungsorgane. Eine Kollision von Bundesrecht mit Landesrecht mit der Wirkung des Art. 31 GG läge nur vor, soweit die übereinstimmend angesprochenen Adressaten Bundesrecht ausführen. Beim Einsatz der maschinellen Datenverarbeitung für andere Aufgaben der Landesverwaltung gilt das Hessische Datenschutzgesetz uneingeschränkt weiter.

2.2.1 Auch innerhalb dieses auf die Tätigkeit der Verwaltung abgestellten Anwendungsbereichs ergeben sich Unterschiede in dem Umfang der gesetzlichen Regelungen. Der sachliche Geltungsbereich des Bundesgesetzes soll teils enger, teils weiter als der des Hessischen Datenschutzgesetzes sein.

2.2.1.1 Er ist enger, weil nach § 1 Abs. 2 EBDSG Gegenstand des Datenschutzes nur personenbezogene Daten sind, die von Behörden oder sonstigen öffentlichen Stellen verarbeitet werden.

---

[1]) BT-Drucks. 7/1027 s. auch I, 2.2; III, 2.2; IV, 2.1

[2]) Ausschußdrucks. 7/237

Personenbezogene Daten werden in § 2 EBDSG als Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener) definiert.

Der Datenschutz nach dem DSG geht weiter. Er erstreckt sich auf alle Arten von Daten, nicht nur auf personenbezogene im Sinne der Definition in § 2 Abs. 1 EBDSG, sondern auch auf unpersönliche oder sachbezogene Daten.

2.2.1.2 Nach dem EBDSG setzt der Datenschutz in einem früheren Zeitpunkt der Informationsverarbeitung ein als nach dem DSG. Als Datenverarbeitung wird nach § 2 Abs. 2 EBDSG das Speichern einschließlich des Erfassens und Aufnehmens, das Verändern, das Übermitteln und das Löschen gespeicherter Daten verstanden, und zwar ungeachtet der dabei angewendeten Verfahren. Es werden auch Daten in manuell geführten Dateien erfaßt (§ 1 Abs. 2, § 2 Abs. 3 Nr. 3 EBDSG).

Der Datenschutz nach DSG ist enger: Er erstreckt sich nur auf die maschinelle Datenverarbeitung und die für ihre Zwecke erstellten Unterlagen.

2.2.1.3 Daraus ergibt sich für die künftige Rechtslage in Hessen folgendes:

Nach den Regeln des Bundesgesetzes ist Datenschutz zu gewährleisten,

soweit die in § 1 DSG genannten Behörden und Stellen der öffentlichen Verwaltung des Landes Bundesrecht ausführen und

dabei personenbezogene Daten verarbeiten — beginnend mit dem Erfassen und Aufnehmen —, und zwar ungeachtet der dabei angewandten Verfahren.

Nach dem DSG ist Datenschutz zu gewährleisten,

soweit im Bereich des § 1 DSG Landesrecht ausgeführt oder eine andere Aufgabe aus dem Landesbereich wahrgenommen wird und

dabei personenbezogene und/oder sachbezogene Daten maschinell verarbeitet oder hierfür in Unterlagen erfaßt werden.

2.3 Im Anwendungsbereich des Bundesgesetzes wird ferner folgende Ausweitung des Datenschutzes beachtet werden müssen:

Im Sinne des Bundesgesetzes ist es Aufgabe des Datenschutzes, die Datenverarbeitung nur unter gesetzlich normierten Voraussetzungen zuzulassen.

Dies ist für den Bundesgesetzgeber auch aus einem weiteren Grund wichtig: Die Regeln über die Zulässigkeit der Datenverarbeitung im öffentlichen Bereich bei der Ausführung von Gesetzen sind Regeln für das Verwaltungsverfahren, die der Bund mit Zustimmung des Bundesrats den Ländern für die Ausführung von Bundesgesetzen vorschreiben kann (Art. 84 Abs. 1, Art. 85 Abs. 2 GG). Hierauf gründet der Bund seine Gesetzgebungskompetenz. Ob die Befugnis, das Verwaltungsverfahren zu regeln, auch das Datenschutzrecht des Bürgers auf Auskunft, Berichtigung, Löschung oder Sperrung umgreift, soll hier dahingestellt bleiben.

Demgegenüber ist es nach dem DSG Aufgabe des Datenschutzes, die Vertraulichkeit der Angaben des Bürgers im Rahmen der Gesetze zu wahren (§ 2, § 10 Abs. 1 DSG).

Die formal sehr weitgehende Beschränkung des Einsatzes der Datenverarbeitung im EBDSG erweist sich jedoch praktisch als eine Leerformel:

§§ 6, 7, 8 EBDSG lassen die Datenverarbeitung zu, wenn das Speichern, das Verändern oder das Übermitteln von Daten zur rechtmäßigen Erfüllung der in der Zuständigkeit der speichernden, übermittelnden bzw. empfangenden Stelle liegenden Aufgabe erforderlich ist. Aufgrund dieser allgemeinen Ermächtigung dürfte in der Praxis das Verwaltungsverfahren, vor allem bei der Automation des Verwaltungsvollzuges, unverändert bleiben. Schon seither mußten bei allen Automationsverfahren die in den §§ 6 ff EBDSG normierten Voraussetzungen stets erfüllt sein, um rechtsstaatlichen Anforderungen zu genügen.

Daß die Erfüllung der Aufgabe rechtmäßig sein muß, ist eine überflüssige Floskel, weil eine unrechtmäßige Erfüllung von Verwaltungsaufgaben, ob mit oder ohne Datenverarbeitung, ohnehin unzulässig ist. Im übrigen wird eine Verwaltungsaufgabe nur dann rechtmäßig erfüllt, wenn auch die Datenschutzvorschriften berücksichtigt werden.

Zweifel könnten allenfalls über den Inhalt des im Entwurf gebrauchten Begriffs der Erforderlichkeit bestehen. Die Auslegung wird sich an dem Ziel zu orientieren haben, eine nicht von der jeweiligen Verwaltungsaufgabe her gerechtfertigte Datenverarbeitung zu unterbinden.

2.4 Aus dem Blickfeld des Bürgers betrachtet liegen die wesentlichsten Unterschiede zwischen dem Entwurf des Bundesgesetzes und dem Hessischen Datenschutzgesetz in den Regeln des materiellen Datenschutzrechtes, d. h. in den Rechten des Bürgers gegenüber der Verwaltung, deren Grundlage das grundrechtlich geschützte Persönlichkeitsrecht des Bürgers und nicht das Verfahrensrecht der Verwaltung ist.

Das Hessische Datenschutzgesetz gewährt in § 4 nur einen Berichtigungsanspruch, dessen Durchsetzung mangels eines Auskunftsrechts zweifelhaft ist. Der Wiedergutmachungsanspruch ist mehr von theoretischer als von praktischer Bedeutung; er könnte auch auf andere Vorschriften der Rechtsordnung gestützt werden.

Demgegenüber soll der Bürger nach § 3 b der allgemeinen Vorschriften des EBDSG folgende Datenschutzrechte erhalten, die in den einzelnen Anwendungsbereichen des Gesetzes noch spezifiziert werden:

Ein Recht auf Auskunft über die zu seiner Person gespeicherten Daten,

ein Recht auf Berichtigung dieser Daten, wenn sie unrichtig sind,

ein Recht auf Sperrung der zu seiner Person gespeicherten Daten, wenn sich weder deren Richtigkeit noch Unrichtigkeit feststellen läßt oder wenn die Voraussetzungen für die Speicherung nachträglich weggefallen sind,

ein Recht auf Löschung der zu seiner Person gespeicherten Daten, wenn ihre Speicherung unzulässig war oder – wahlweise neben dem Recht auf Sperrung – wenn die Voraussetzungen für die Speicherung nachträglich weggefallen sind.

2.5 Für die öffentliche Verwaltung des Landes ergibt sich daraus der Zwang, vom Inkrafttreten des Bundesgesetzes an zweierlei Datenschutzrecht anzuwenden:

Für die Ausführung von Bundesgesetzen das Bundesrecht, für die Ausführung von Landesrecht und von anderen Verwaltungsaufgaben des Landes das Hessische Datenschutzrecht.

Dabei wird in der Verwaltungspraxis deutlich werden, daß das Bundesrecht – trotz mancherlei Mängel, die dem EBDSG anhaften, – die Entwicklung, welche das Datenschutzrecht seit dem Inkrafttreten des DSG durch die Wissenschaft und die Praxis erfahren hat, weitgehend einfängt. Daran gemessen ist das DSG inzwischen veraltet.

Auf diesen Rückstand, in den das DSG allein durch den Zeitablauf geraten ist, ist in den früheren Tätigkeitsberichten des Datenschutzbeauftragten wiederholt hingewiesen worden. Anregungen meines Vorgängers, das Gesetz den praktischen Erfahrungen anzupassen[3]), sind von der Landesregierung bisher mit der Begründung abgelehnt worden, daß es zweckmäßig sei, erst den Erlaß des Bundesdatenschutzgesetzes abzuwarten.

Diese Auffassung kann ich wegen ihrer Konsequenzen für den Bürger nicht teilen:

Werden personenbezogene Daten zur Ausführung von Landesrecht oder zur Erfüllung von Aufgaben der Landesverwaltung verarbeitet, hat der Bürger geringere Datenschutzrechte als wenn dieselben Daten von derselben oder einer anderen Verwaltung zur Ausführung von Bundesrecht verarbeitet werden. Es wird dem Bürger schwerlich verständlich gemacht werden können, aus welchen Gründen er eine solche Schlechterstellung hinnehmen muß.

Aber auch den Behörden und Stellen des Landes kann kaum zugemutet werden, den Datenschutz des Bürgers nach zwei verschiedenen Rechtsquellen unterschiedlich zu berücksichtigen. Vielmehr ist zu erwarten, daß sich in der Praxis eine Angleichung an die Vorschriften des Bundesgesetzes vollziehen wird, auch in den Bereichen, in denen es im Lande nicht gilt. Dies könnte für den Bürger hilfreich sein, es räumte aber nicht die Verunsicherung über die wahre Rechtslage aus. Diese Situation könnte vermieden werden, wenn man schon jetzt das DSG novelliert und dem Entwurf des Bundesdatenschutzgesetzes anpaßt. Dabei könnte in Kauf genommen werden, daß Ungleichheiten bestehen bleiben, weil die endgültige Fassung des Gesetzes unbekannt ist. Wesentliche Änderungen sind für den öffentlichen Bereich nicht zu erwarten. Dafür erhält aber der Bürger schon mit der Novellierung des Datenschutzgesetzes einen besseren Rechtsschutz.

2.6 Die Landesregierung hat es bisher abgelehnt, dem Bürger ein Auskunftsrecht einzuräumen, sei es, weil sie den Erlaß des Bundesdatenschutzgesetzes abwarten wollte, sei es, weil sie die Normierung eines Auskunftsrechts für unnötig hält. In der „Synopse der Auffassungen zur Datenverkehrs-Ordnung“ die auf Veranlassung des EDV-Ausschusses des Landtages erstellt worden ist, sind die gegensätzlichen Auffassungen dargestellt worden.

Das Auskunftsrecht ist Bestandteil aller Datenschutzgesetze und -gesetzentwürfe. Auch in der Diskussion des EBDSG ist niemals in Frage gestellt worden, daß das Auskunftsrecht ein notwendiges Instrument des Bürgers ist, damit er sein Persönlichkeitsrecht wahren kann.

In Rheinland-Pfalz ist das in den früheren Tätigkeitsberichten des Hessischen Datenschutzbeauftragten geforderte Auskunftsrecht bereits verwirklicht worden. In § 4 des Landesdatenschutzgesetzes von Rheinland-Pfalz i. d. F. vom 24. 2. 1975[4]) hat jedermann ein Recht auf Auskunft

[3]) Vgl. IV, 1.5

[4]) GVBl. S. 84

über die zu seiner Person gespeicherten Daten mit den im wesentlichen unbestrittenen Einschränkungen. Die Auffassung, daß die Länder insoweit keine Gesetzgebungskompetenz besäßen, hat demnach auch das Land Rheinland-Pfalz nicht geteilt.

Im Entwurf des Bundesgesetzes ist das Auskunftsrecht für den öffentlichen Bereich in § 11 in der Weise geregelt, daß „in dem Antrag ... die Art der personenbezogenen Daten, über die Auskunft erteilt werden soll, näher bezeichnet werden. Die speichernde Stelle bestimmt das Verfahren, insbesondere die Form der Auskunftserteilung nach pflichtgemäßem Ermessen".

Der Wortlaut ist mißverständlich. Der Bürger, der wissen möchte, ob und welche Daten über ihn gespeichert sind, könnte in Schwierigkeiten kommen, wenn er die Art der Daten nicht bezeichnen kann. Das Bestreben der Verwaltung, die Auskünfte nach Anzahl und nach Inhalt in möglichst engen Grenzen zu halten – das unterstellt werden kann –, wird noch dadurch gestärkt, daß die speichernde Stelle, also die Auskunftsstelle, selbst die Form der Auskunft nach pflichtgemäßem Ermessen bestimmen kann. Jedoch wäre das auch im EBDSG vorgesehene Datenbankregister, das nach § 15 c a. a. O. der Bundesbeauftragte für den Datenschutz führen soll, geeignet, dem Bürger die notwendige Hilfe zu leisten.

Um es zu erleichtern, diese wiederholt geäußerte Forderung des Hessischen Datenschutzbeauftragten zu verwirklichen, habe ich meine Vorstellungen über den Inhalt einer in das DSG einzufügenden Vorschrift in einem Vorschlag für eine gesetzliche Regelung konkretisiert[5]).

Die von der Verwaltung wiederholt geäußerte Befürchtung, diese Auskunftsregelung könne zu einer übermäßigen Belastung der Verwaltung führen, teile ich nicht. Die Belastung der Verwaltung könnte jedoch erheblich verringert werden, wenn der Auskunft heischende Bürger zunächst aus dem Datenbankregister des Datenschutzbeauftragten feststellen lassen könnte, welche Datenarten, von welcher Behörde und für welchen Verwaltungszweck überhaupt gespeichert werden und an welche Behörde er sich wegen des Inhalts der über ihn gespeicherten Daten wenden müßte. Deswegen halte ich eine gesetzliche Regelung über das vom Datenschutzbeauftragten zu führende Register im Zusammenhang mit der Regelung des Auskunftsrechts für empfehlenswert. Dieser Vorstellung entspricht § 4 b der oben genannten Anlage.

[5]) S. Anlage I

2.7 Die Kompetenz des Datenschutzbeauftragten nach dem Wortlaut des Gesetzes ist, die in den früheren Tätigkeitsberichten[6]) dargelegt, unzulänglich, wenn eine in § 1 DSG genannte Behörde oder Stelle für die Erfüllung ihrer Aufgaben andere Personen oder Stellen mit der maschinellen Datenverarbeitung beauftragt.

Im EBDSG ist dieser Sacherhalt in einer besonderen Vorschrift (§ 5 a) geregelt. Dort wird klargestellt, daß die Verantwortung für den Datenschutz bei dem Auftraggeber verbleibt[7]), daß der Auftragnehmer sorgfältig auszuwählen ist und daß dieser, sei er eine Behörde oder Stelle der öffentlichen Verwaltung, sei er eine juristische Person, Gesellschaft oder andere Personenvereinigung des privaten Rechts, personenbezogene Daten nur im Rahmen der Weisungen des Auftraggebers verarbeiten darf[8]). Mit anderen Worten: Die Vorschriften über Datenspeicherung, -verarbeitung, -übermittlung sowie über die Rechte auf Auskunft, Berichtigung, Sperrung oder Löschung im öffentlichen Bereich gelten für die Auftragnehmer nicht; an deren Stelle treten die Weisungen des Auftraggebers. Die beauftragten Behörden oder Stellen haben keinerlei Verfügungsbefugnis über die Daten; sie werden den natürlichen oder juristischen Personen des privaten Rechts, welche Datenverarbeitung geschäftsmäßig im Auftrag für Dritte betreiben, gleichgestellt.

Die gleiche Weisungsgebundenheit soll auch für solche juristischen Personen, Gesellschaften oder Personenvereinigungen des privaten Rechts gelten, bei denen der öffentlichen Hand die Mehrheit der Anteile gehört oder die Mehrheit der Stimmen zusteht.

Hier interessiert die Tatsache, daß der Bundesgesetzgeber es für notwendig hält, die Fälle ausdrücklich zu regeln, in denen die öffentliche Verwaltung mit der Verarbeitung ihrer Daten andere Stellen oder Personen oder Gesellschaften beauftragt. Daher wiederhole ich die Anregung meines Vorgängers, in das Hessische Datenschutzgesetz eine entsprechende Regelung aufzunehmen. Sie würde es dem Datenschutzbeauftragten nicht nur ermöglichen, seine Aufgaben nach § 10 DSG umfassend zu erfüllen, sondern auch klarstellen, gegenüber welcher Stelle der Bürger seine Datenschutzrechte geltend machen kann.

[6]) II, 4.1.3; III, 1.5.1; IV, 4.3

[7]) § 5 a Abs. 1; § 23 Abs. 2 EBDSG

[8]) § 5 a Abs. 2, Satz 2; § 5 a Abs. 3 letzter Satz; § 23 Abs. 1 Nr. 3 i. V. m. § 29 EBDSG

Bereits im Jahr 1974 ist in den Beratungen der EDV-Arbeitsgruppe des Hauptausschusses des Hessischen Landtags eine entsprechende Ergänzung des Gesetzes behandelt worden. Die Landesregierung hatte auch die Anregung zunächst aufgegriffen, sie aber nicht weiter verfolgt. Um auch hier die weitere Diskussion zu erleichtern, füge ich einen Formulierungsvorschlag bei[9]).

Dieser Vorschlag geht davon aus, daß die Befugnis des Landes zur Gesetzgebung durch die Inanspruchnahme konkurrierender Gesetzgebungsrechte des Bundes (Art. 72, 74 GG) nicht untergegangen ist.

§ 1 DSG in der von mir vorgeschlagenen Fassung geht allerdings über die von mir bereits dargestellten Absichten des Bundesgesetzgebers hinaus:

Der Anwendungsbereich des Gesetzes soll auch auf privatrechtlich organisierte Unternehmen erstreckt werden, wenn sie von der öffentlichen Hand beherrscht werden oder/und wenn sie im Auftrage der öffentlichen Verwaltung als Dienstleistungsbetrieb Daten verarbeiten. Solange und soweit der Bundesgesetzgeber keine Regelung dieser Fallgruppen getroffen hat — und bisher ist dies nicht geschehen — ist das Land im Rahmen des DSG zur Regelung befugt.

Nun sieht der EBDSG eine allgemeine Regelung der Datenverarbeitung durch privatrechtliche Unternehmen in seinem dritten und vierten Abschnitt und eine spezielle Regelung für die Fälle vor, in denen von der öffentlichen Hand beherrschte privatrechtliche Unternehmen Daten im Auftrage der öffentlichen Verwaltung verarbeiten (§ 5a EBDSG). Mit dem Inkrafttreten dieser bundesgesetzlichen Regelung würde in der Tat mein Vorschlag zu § 1 Abs. 1 Nr. 3 „gebrochen" werden (Art. 31 GG), jedoch nur im Rahmen des Anwendungsbereiches des künftigen Bundesgesetzes, d. h. soweit die Datenverarbeitung der Ausführung von Bundesrecht dient.

Für den unter § 1 Abs. 1 Nr. 2 vorgeschlagenen Sachverhalt gibt es keine spezielle Regelung im EBDSG; dort fielen vielmehr diese Fälle unter den Anwendungsbereich des dritten und vierten Abschnittes, d. h. unter die Regelung der Datenverarbeitung im nicht-öffentlichen Bereich. Für die Frage, welche Konsequenzen sich hieraus auf die Zulässigkeit oder das Fortbestehen einer solchen landesrechtlichen Regelung ergeben, gewinnt der unter 2.3 erörterte Umstand noch einmal Bedeutung: Das Hessische Datenschutzgesetz beschränkt sich darauf, Abwehrrechte gegen Eingriffe in grundrechtlich geschützte Rechtspositionen des Bürgers zu statuieren, und stellt nicht — wie es der EBDSG beabsichtigt — Zulässigkeitsvoraussetzungen für die Datenverarbeitung als Regeln für das Verwaltungsverfahren der Behörden oder — quasi — Berufsausübungsregeln für den nicht-öffentlichen Bereich auf.

Die größtmögliche Realisierung der Grundrechte ist eine Aufgabe, die dem Gesetzgeber sowohl im Bunde wie in den Ländern obliegt. Sollte der Entwurf nicht mehr verabschiedet werden, dann bestehen keine Bedenken, § 1 Abs. 1 Nr. 2 ebenfalls in die Neufassung des § 1 DSG aufzunehmen. Kommt es dagegen zu einer bundesgesetzlichen Regelung, dann hängt es vom Inhalt dieser Regelung ab, in welchem Umfang eine Novellierung des § 1 im Sinne dieses Vorschlages erforderlich ist.

2.8 § 4 Abs. 1 DSG gewährt dem Bürger einen Berichtigungsanspruch. Das Gesetz — und auch der Änderungsvorschlag nach der Anlage 1 — regelt jedoch nicht den Fall, daß sich die datenverarbeitende Stelle und der Betroffene über Richtigkeit oder Unrichtigkeit gespeicherter Daten nicht einig sind. In § 12 EBDSG ist für diesen Sachverhalt vorgesehen, daß Verarbeitung und Weitergabe der Daten, deren Richtigkeit von Betroffenen bestritten wird, zu unterbleiben hat, — daß die Daten zu sperren sind —, wenn sich weder die Richtigkeit noch die Unrichtigkeit feststellen läßt.

Auch in dieser Hinsicht ist eine Ergänzung des Datenschutzgesetzes nötig. Da das Gesetz insoweit lückenhaft ist, könnte es auch nicht der Rechtsprechung überlassen bleiben, die Frage zu klären.

2.9 Schließlich wird auch die Frage, ob und unter welchen Voraussetzungen gespeicherte Daten zu löschen oder zu sperren sind im Datenschutzgesetz nicht behandelt, obwohl das Recht des Bürgers, die Löschung oder das Sperren von Daten unter bestimmten Voraussetzungen zu verlangen, ein wesentliches Element des Datenschutzes ist.

§ 12 EBDSG regelt auch diesen Sachverhalt.

In den Arbeitsausschüssen für die Automation von Verwaltungsaufgaben und im Zusammenhang mit einer Reihe von Datensammlungen für Verwaltungszwecke oder für wissenschaftliche Untersuchungen, die mit Hilfe der Verwaltung durchgeführt worden sind, haben mein Vorgänger und ich darauf hingewirkt, die Löschung gespeicherter Daten vorzuschreiben, wenn ihre Unrichtigkeit feststeht, wenn der Zweck der Spei-

[9]) S. Anlage II

cherung erreicht oder weggefallen oder wenn eine bestimmte Zeitspanne abgelaufen ist.
Nach den Erfahrungen aus der Praxis halte ich es für geboten, gesetzlich festzulegen, unter welchen allgemeinen Voraussetzungen Daten zu löschen oder zu sperren sind.

3. TENDENZEN IM DATENSCHUTZRECHT

3. Tendenzen im Datenschutzrecht

3.1 In der Bundesrepublik

Die neuere Gesetzgebung des Bundes bringt in einigen Gebieten für den Datenschutz wichtige Einzelbestimmungen.

Mit den §§ 30, 31 der neuen Abgabeordnung wird das Steuergeheimnis neu geregelt. Verglichen mit dem bisherigen § 22 AO hat die Regelung den Vorzug größerer Präzision und Detailliertheit. Das Gesetz bestimmt im einzelnen, unter welchen Voraussetzungen geschützte Kenntnisse ausnahmsweise von den Steuerbehörden offenbart werden dürfen. Die dabei vorgenommene begrenzte Lockerung des Steuergeheimnisses entspricht der Absicht des Gesetzgebers, die Bekämpfung der Wirtschaftskriminalität zu erleichtern. Bedenken aus der Sicht des Datenschutzes bestehen dagegen nicht.

Das kurz vor der Verabschiedung stehende Verwaltungsverfahrensgesetz[1]) unternimmt in den §§ 4 bis 8 erstmals eine allgemeine gesetzliche Regelung der Amtshilfe. Den in der Regierungsvorlage[2]) enthaltenen Grundsatz, daß eine Amtshilfe unzulässig ist, wenn „die ersuchte Behörde aus rechtlichen Gründen (zur Hilfeleistung) nicht in der Lage ist", hat der Innenausschuß des Bundestages dahin konkretisiert, daß insbesondere „zur Vorlage von Urkunden oder Akten sowie zur Erteilung von Auskünften (keine Befugnis besteht), wenn die Vorgänge nach einem Gesetz oder ihrem Wesen nach geheim gehalten werden müssen" (§ 5 Abs. 2 Satz 2).

Der Allgemeine Teil des neuen Sozialgesetzbuches (SGB)[3]) enthält ein umfassendes Auskunftsrecht des Bürgers, das „sich auf alle Sach- und Rechtsfragen, die für den Auskunftsuchenden von Bedeutung sein können" (§ 15), also auch auf gespeicherte Daten, erstreckt. § 35 Abs. 1 SGB gibt dem Bürger einen „Anspruch darauf, daß seine Geheimnisse, insbesondere die zum persönlichen Lebensbereich gehörenden Geheimnisse ... von den Leistungsträgern, ihren Verbänden, ... Vereinigungen und den Aufsichtsbehörden nicht unbefugt offenbart werden. Eine Offenbarung ist dann nicht unbefugt, wenn der Betroffene zustimmt oder eine gesetzliche Mitteilungspflicht besteht". Abs. 2 bestimmt, daß die für die Aufgabenerfüllung notwendige Amtshilfe unter den Leistungsträgern durch Abs. 1 nicht beschränkt wird.

Diese Entwicklung ist positiv zu beurteilen, denn sie zeigt erste Schritte zu der notwendigen bereichsspezifischen Ausgestaltung des Datenschutzes. Durch die genannten Beispiele sehe ich meine Auffassung zum Verhältnis von Datenschutz und Amtshilfe bestätigt. Wie ich an anderer Stelle dargelegt habe[4]), darf die Amtshilfe nicht länger als Ausdruck eines prinzipiell umfassenden, nur punktuell eingeschränkten staatlichen Informationsverbundes verstanden werden. Der Informationsaustausch findet vielmehr in den Grundrechten der Bürger seine Grenzen. Diese Grenzen für die Verwaltungspraxis zu verdeutlichen, ist eine der Aufgaben konkretisierender gesetzlicher Regelungen in den einzelnen Verwaltungsbereichen.

Der Entwurf des Bundesmeldegesetzes (EBMG) in der vom Innenausschuß beschlossenen Fassung stellt bei der Regelung der Datenweitergabe im Rahmen der Amtshilfe (§ 1) die „Stellen der öffentlich-rechtlichen Religionsgemeinschaften" den staatlichen Behörden und Gerichten gleich. Sie können demgemäß personenbezogene Daten aus dem Einwohnerwesen erhalten, „soweit dies zur rechtmäßigen Erfüllung der in der Zuständigkeit des Empfängers liegenden öffentlichen Aufgabe erforderlich ist" und soweit „sichergestellt ist, daß bei dem Empfänger ausreichende Datenschutzmaßnahmen getroffen werden" (§ 17 EMBG). Entsprechend sieht der Entwurf des Bundesdatenschutzgesetzes (EBDSG) für die sonstige Verwaltung vor, daß die Weitergabe von Daten an Behörden wie an Religionsgemeinschaften zulässig ist, wenn die Kenntnis der Daten zur „rechtmäßigen Erfüllung der in der Zuständigkeit des Empfängers liegenden Aufgaben" erforderlich ist (§ 7 Abs. 1).

Zu den Aufgaben der Kirchen zählen auch die Seelsorge, die pastorale Arbeit, die soziale Betreuung und die Mission — also das Einwirken auf Personen, die keiner oder einer anderen Religionsgemeinschaft angehören. Die Kirchen

[1]) BT-Drucks. 7/4494

[2]) BT-Drucks. 7/910

[3]) BGBl. I 1975, S. 3015

[4]) Synopse zur Datenverkehrs-Ordnung vom September 1975, Bemerkung zu Gebot 7, IV, 1.5.2

haben daher in Verhandlungen mit der Innenministerkonferenz den Wunsch erklärt, daß die Meldebehörden den Kirchen auch Daten von Nichtmitgliedern übermitteln, z. B. von Familienangehörigen und von noch nicht getauften Kindern. Sie haben dabei geltend gemacht, daß die seelsorgerische und soziale Betreuung ihrer Mitglieder zu den „öffentlichen Aufgaben" im Sinne des § 17 EBMG gehörten. Die Kirchenmitgliedschaft strahle auch auf Familienangehörige aus; der ganzheitliche Anspruch der Kirchen gegenüber dem Mitglied betreffe auch dessen Stellung innerhalb der Familie, jedenfalls soweit es um die seelsorgerische und soziale Betreuung ginge.

In den Verhandlungen über eine für alle Länder gleiche Regelung in den Ausführungsverordnungen zu den Landesmeldegesetzen hat der Unterausschuß EDV im Einwohnerwesen des Arbeitskreises II der Innenministerkonferenz zwar einen Beschluß über eine ländereinheitliche Regelung zunächst bis zur Verabschiedung des Bundesmeldegesetzes zurückgestellt. Grundsätzlich war aber der Unterausschuß zu einem „Kompromiß" bereit. Die Kirchen sollen danach das Recht auf bestimmte Auskünfte über den gesamten „Familienverband" erhalten, soweit ein Ehepartner Kirchenmitglied ist: Von neugeborenen noch nicht getauften Kindern und von Familienangehörigen, die nicht derselben Religionsgemeinschaft angehören, sollen den Kirchen von den Meldebehörden das Personenkennzeichen, der Familienname und der Vorname mitgeteilt werden. Der Unterausschuß ging dabei davon aus, „daß die Seelsorge gegenüber den eigenen Mitgliedern erfordere, den Kirchen den Familienverband in Umrissen erkennbar zu machen".
Es kann nicht Aufgabe dieses Tätigkeitsberichts sein, einen Beitrag zur Definition der öffentlichen Aufgabe der Kirchen zu leisten. Unter dem Blickpunkt des Datenschutzes muß jedoch die Frage aufgeworfen werden, ob der öffentlichen Verwaltung gestattet sein kann, von ihr erhobene personenbezogene Daten ohne Wissen und Willen des Betroffenen einer Kirche, der er nicht angehört, zu übermitteln.

Diese Frage ist, da es sich um den Schutz einer grundrechtlich geschützten Rechtsposition des Bürgers handelt, aus dem Zusammenhang der Verfassung zu beantworten. Danach haben die Kirchen einen verfassungsrechtlichen Anspruch auf Auskünfte aus den „bürgerlichen Steuerlisten" nach Maßgabe landesrechtlicher Bestimmungen (Art. 140 GG i. V. m. Art. 137 WV). Nach § 8 des Hessischen Kirchensteuergesetzes vom 27. 4. 1950 sind die Unterlagen, „deren die Kirchen (Kirchengemeinden) für die Besteuerung bedürfen, . . . ihnen auf Anforderung von den zuständigen Staats- und Gemeindebehörden mitzuteilen. Diese Regelung ist zugleich eine Begrenzung des quasi-amtshilfemäßigen Zusammenwirkens von Staat und Kirche. Eine restriktive Auslegung gebieten auch die Vorschriften der Hessischen Verfassung in Art. 48 ff., die ebenso wie das Grundgesetz von der grundsätzlichen Trennung von Staat und Kirche und der daraus und aus der Verpflichtung zum Schutze der Grundrechte folgenden Neutralitätspflicht des Staates ausgehen.

Die schon in den früheren Tätigkeitsberichten geäußerten Bedenken gegen die Einbeziehung der Kirchen in die allgemeine Amtshilfpflicht der staatlichen Behörden müssen auch den in der Bundesgesetzgebung erkennbaren gegenläufigen Tendenzen entgegengehalten werden[5]).

3.2 Im Ausland

Die Entwicklung des Datenschutzes im Ausland läßt sich durch drei Momente kennzeichnen:

a) Fast alle wesentlichen Industriestaaten haben den Datenschutz als wichtige Aufgabe im Überschneidungsbereich von Gesellschafts- und Technologiepolitik erkannt. Die Mehrzahl bemüht sich, Anschluß an die „Datenschutzpioniere" zu finden. Verschiedene internationale und supranationale Organisationen — wie etwa der Europarat und die Europäische Gemeinschaft — leisten dazu Hilfe.

In Großbritannien hat die Regierung ihre Absicht erklärt, den Datenschutz im privaten und im öffentlichen Bereich gesetzlich zu regeln. Ein „Data Protection Committee" soll die notwendigen Vorarbeiten leisten und die Zeit bis zur Schaffung eines Kontrollorgans auf gesetzlicher Grundlage überbrücken[6]).

In der Schweiz hat die Expertenkommission für die Überprüfung des zivilrechtlichen Schutzes der Persönlichkeit Änderungen des Zivilgesetzbuches und des Obligationsrechts vorgeschlagen[7]). Sie stellen klar, daß gegenüber „jede(r) Sammlung oder Verwendung von Angaben über persönliche Verhältnisse . . . mit dem Beseitigungsanspruch . . . verlangt werden kann, daß

[5]) Siehe II, 4.1.1.3 f

[6]) Computers and Privacy, White Paper, Presented to Parliament by the Secretary of State for the Home Department by Command of Her Majesty December 1975, Her Majesty's Stationary Office, Cmnd. 6353, 6354.

[7]) Schlußbericht vom Dezember 1974

eine unerlaubte Speicherung aufgehoben und eine unrichtige Angabe berichtigt wird". Werden Angaben „in Karteien, Datenbanken oder auf ähnliche Weise . . . (gesammelt und) Dritten zur Verfügung" gehalten, so besteht außerdem ein Auskunftsrecht (Abs. 2); die Unternehmung haftet in diesem Fall auf „Schadenersatz und Genugtuung auch dann, wenn kein Verschulden vorliegt".

Die Kommission sieht hierin nicht mehr als „gewisse minimale Schutzvorschriften". Das Problem habe aber „eine so große Bedeutung erlangt, daß eine möglichst rasche Regelung als vordringlich (erscheine), auch wenn die Mittel des Privatrechts . . . nur von beschränkter Wirkung sein (könnten)"[8]).

In Österreich wurde der in der letzten Legislaturperiode nicht mehr verabschiedete Regierungsentwurf eines Datenschutzgesetzes in unwesentlich modifizierter Fassung erneut dem Nationalrat vorgelegt[9]). Durch eine Verpflichtung der Regierung, für jede Datenbank eine „Datenbank-Verordnung" zu erlassen, wird eine differenzierte Realisierung der Datenschutzvorkehrungen ermöglicht. Einen eigenen Weg beschreitet der Entwurf auch in der Frage der Überwachung. Eine fünfzehnköpfige, mehrheitlich mit Richtern zu besetzende Bundes-Datenschutzkommission sowie Landes-Datenschutzkommissionen sollen in einem gerichtsähnlichen Verfahren über Datenschutz-Beschwerden der Betroffenen „in erster Instanz" entscheiden. Präventive Aufgaben haben diese Kommissionen nicht.

In Japan, einem in der EDV-Technologie führenden Land, ist der Datenschutz erst mit einer gewissen Verzögerung zur öffentlichen Diskussion gelangt. Unter Mitwirkung mehrerer großer Gewerkschaften, unter ihnen die All Japan Telecommunication Workers Union, wurde eine Organisation gegründet, die sich den Kampf für den Datenschutz gegen die Einführung einer Bürgernummer zum Ziel gesetzt hat (Central Congress für Privacy Protection and against Personal Identification Numbering Plan). Nachdem die Sozialistische und die Liberale Partei Datenschutzgesetzentwürfe vorgelegt haben, hat auch die Regierung ihre Absicht bekundet, gesetzgeberisch aktiv zu werden. Die beiden Gesetzentwürfe der Sozialistischen Partei Japans, die mir auszugsweise in englischer Übersetzung vorliegen, enthalten Grundsätze zum Schutz der personenbezogenen Information im Rahmen der EDV und Ausführungsbestimmungen. Zur Verwirklichung dieser Grundsätze soll auf nationaler Ebene unter der Aufsicht des Premierministers eine „zentrale Überwachungskommission für die Verarbeitung personenbezogener Daten" geschaffen werden, deren fünf Mitglieder mit Zustimmung des Parlaments vom Premierminister ernannt werden, und der es obliegen soll, allgemeine Grundsätze für die Datenverarbeitung festzulegen und Genehmigungen zu erteilen. Dieser Zentralkommission untersteht ein aus zwanzig Mitgliedern bestehender Rat, der die Aufgabe hat, wichtige Probleme der Anwendung der Datenschutzgesetze zu untersuchen und der Kommission Vorschläge zu unterbreiten. Auf regionaler Ebene soll bei den fünfzig Präfekturen und bei verschiedenen mit Sonderstatus versehenen Großstädten je eine „lokale Überwachungskommission für die Verarbeitung personenbezogener Daten" gebildet werden. Die Ausführungsvorschriften bestimmen, daß jede Institution, gleichviel, ob es sich um ein privates Unternehmen oder um eine Behörde handelt, vor Beginn der automatischen Verarbeitung personenbezogener Daten einer Genehmigung durch die zentrale Kommission bedarf. Die in Japan angestellten Überlegungen sind von den schwedischen und hessischen Erfahrungen stark beeinfluß worden.

b) In den Staaten, die bereits Datenschutzgesetze in Kraft gesetzt haben, wie Schweden (Datalagen 1973) und die Vereinigten Staaten (Privacy Act 1974), steht die Frage nach der Bewährung der neugeschaffenen Kontrollinstrumente im Vordergrund.

Die schwedische Data Inspektionen hat bis Ende 1975 über 7500 Anträge auf Genehmigung von Datensammlungen bearbeitet. In einem an Regierung und Parlament adressierten Bericht werden die Erfahrungen mit dem Gesetz positiv beurteilt. Einige Entscheidungen der Data Inspektionen haben — auch international — Aufsehen erregt. Dem Statistischen Zentralamt wurde z. B. der Betrieb eines zentralen Verweisregisters untersagt, welches für jeden Bürger angibt, in welchen einzelnen Registern (Dateien) des Amtes Daten zu seiner Person enthalten sind. Zur Begründung wurde angeführt, das Verweisregister erhöhe die Mißbrauchsgefahr und könne, soweit keine gesetzliche Geheimhaltungspflicht bestehe und daher das Prinzip der Aktenöffentlichkeit eingreife, schutzbedürftige Daten allgemein zugänglich machen.

Zum US Privacy Act of 1974 wurden inzwischen umfangreiche Durchführungsvorschriften

[8]) a. a. O. S. 30

[9]) Nr. 72 der Beilagen zu dem stenograf. Protokoll des Nationalrates XIV. GP vom 17. Dez. 1975

und Richtlinien erlassen[10]). Mit der amerikanischen Privacy Study Commission, die ihre Arbeit im Herbst 1975 aufgenommen hat, wurde ein Erfahrungsaustausch aufgenommen.

Die Stadt Berkeley/Kalifornien hat einen sehr interessanten Versuch gemacht, den Datenschutz einem öffentlichen Entscheidungsprozeß zu unterwerfen. Das Stadtparlament hat eine Regelung in Kraft gesetzt[11]), nach der vor einer Entscheidung über die Einführung oder eine wichtige Änderung eines Automationsverfahrens für personenbezogene Daten ein „social impact statement" erstellt werden muß. Darin sind die Folgen, insbesondere die möglichen Beeinträchtigungen der Rechte der Bürger, darzustellen und Alternativen anzugeben. Dieses Gutachten ist in der Lokalpresse zu veröffentlichen. Jedermann kann schriftlich Einwendungen erheben oder im Rahmen einer öffentlichen Anhörung Stellung nehmen.

c) Die dritte Entwicklungslinie besteht in der Hinwendung zu den besonders empfindlichen Bereichen und dem Versuch, für diese schärfer greifende Lösungen zu finden. Ausgangspunkt dafür ist die Erkenntnis, daß die Generalklauseln, auf welche allgemeine Datenschutznormen notgedrungen zurückgreifen müssen[12]), dem Norm-Anwender zuviel Spielraum überlassen und deshalb Gefahr laufen, den erwünschten Schutzeffekt zu verfehlen.

Gesetzliche Datenschutzregelungen für den Bereich der Kreditinformation, wie sie in den USA, in amerikanischen Einzelstaaten und in kanadischen Provinzen schon seit einigen Jahren existieren, wurden in Schweden verabschiedet[13]); in Dänemark (Entwurf der Trolle-Kommission) und Norwegen[14]) werden Entwürfe beraten.

Ein weiterer Schwerpunkt der bereichsbezogenen Datenschutzgesetzgebung bildet die Polizei- und Kriminalinformation. Die Vereinigten Staaten sind hier am weitesten fortgeschritten. Die Bundesregierung hat ausführliche Datenschutzregelungen für alle durch das National Crime Information Center erfaßten Daten erlassen[15]). Über die Hälfte der Einzelstaaten haben den Datenschutz in ihren Kriminalinformationssystemen gesetzlich geregelt[16]). Das im Dritten Tätigkeitsbericht[17]) näher beschriebene Gesetz des Staates Massachussetts ist in seinen materiellen und insbesondere in den institutionellen Vorkehrungen (Privacy and Security Council) nach wie vor beispielhaft. Die fachliche Spezialisierung auf Kriminaldaten ermöglicht ebenso detaillierte wie sachgemäße Regelungen, und zwar nicht nur für die gängigen Datenschutzinstrumente wie Auskunft, Berichtigung und Weitergabe, sondern z. B. auch für die Datenermittlung für personelle und technische Sicherheitsmaßnahmen und Einzelheiten der Protokollierung.

---

[10]) Office of Management and Budget: Privacy Act Implementation, Guidelines and Responsibilities; Federal Register, Vol. 40, No. 132, Part III, July 9, 1975. Office of the Federal Register: Publication Guidelines for the Privacy Act of 1974; Federal Register, Vol. 40, No. 119, Part V, June 19, 1975.

[11]) Ordinance No. 4732 — N. S. vom 26. Sept. 1974

[12]) „Beeinträchtigung schutzwürdiger Belange" (EBDSG), „otillbörligt intrång i personliga integritet" (datalagen), „such accuracy, relevance, timeliness, and completeness as is reasonably necessary to assure fairness to the individual in the determination" (US-Privacy Act).

[13]) SFS 1973: 1173, vgl. III, 2.3.5

[14]) NOU 1974: 22

[15]) Department of Justice, Criminal Justice Information Systems, Federal Register, Vol. 40 No. 98 Part IV

[16]) Vgl.: Compendium of State Laws Governing the Privacy and Security of Criminal Justice Information, U.S. Department of Justice, Law Enforcement Assistance Administration, Office of General Counsel, Washington 1975

[17]) 2.3.1.1

4. ERFAHRUNGEN IM BERICHTSZEITRAUM

4. Erfahrungen im Berichtszeitraum

4.1 Datenbankregister

Das Datenbankregister[1]) ist auch im abgelaufenen Jahr manuell fortgeführt worden. Es muß ständig auf dem laufenden gehalten werden, wenn es einen Überblick über alle Behörden und Stellen nach § 1 DSG geben soll, die Aufgaben durch die EDV erledigen.

Bei der Überarbeitung des bisher erstellten Inhalts des Registers bestätigte es sich, daß die Angaben der Stellen, die Aufgaben außerhalb des Hessischen DV-Verbundes erledigen lassen, noch lückenhaft sind. Deshalb sind Erhebungsbogen an die Ressorts versandt und diese gebeten worden, die notwendigen ergänzenden Angaben aus ihrem Geschäftsbereich zu machen. Der zügige Fortgang des Ausbaus des Datenbankregisters hat sich anfänglich dadurch verzögert, daß es Schwierigkeiten machte, die Bereitschaft der Ressorts zu gewinnen, die notwendige Unterstützung bei der Fortführung des Registers zu leisten. Dies war wohl eine Auswirkung der zurückhaltenden und in der Interpretation der Funktionen des Registers nicht ganz zutreffenden Stellungnahme der Landesregierung zum Vierten Tätigkeitsbericht[2]).

Diese Schwierigkeiten scheinen durch die wiederholten aufklärenden Darlegungen im Arbeitsausschuß für die Automation von Landesaufgaben überwunden worden zu sein.

Die vielseitigen Verwendungsmöglichkeiten des Registers und ihr Nutzen nicht nur für den Bürger, sondern auch für die Verwaltung werden offenbar nicht mehr geleugnet; im Gegenteil: die Hessische Zentrale für Datenverarbeitung stellt für ihren Eigengebrauch ein ähnliches Register (Data Dictionary) auf; die gegenseitige Unterstützung bei dieser Aufgabe ist vereinbart worden.

Die Absicht, das Register automatisch zu erstellen und fortzuführen, besteht nach wie vor. Das vorgenannte Projekt der Hessischen Zentrale für Datenverarbeitung bietet bei dessen Einführung hierzu eine Möglichkeit.

Notwendigkeit und Wert eines Datenbankregisters ist auch in den Beratungen des Innenausschusses des Bundestages über den EBDSG erkannt worden: Nach § 15 c Abs. 4 soll der dort vorgesehene Bundesbeauftragte für den Datenschutz ein Datenbankregister führen, das dem für das Land Hessen entwickelten in etwa entspricht.

4.2 Datenfernverarbeitung

Die Datenfernverarbeitung spielt gegenwärtig im DV-Verbund noch eine untergeordnete Rolle. Bei einer Gemeinde wird ein Auskunftssystem für das Einwohnerwesen im Großversuch getestet. Im medizinischen Sektor nutzen elf Krankenhäuser die Möglichkeit, die Daten für die Leistungsabrechnung im stationären Bereich über Fernleitungen an die HZD bzw. die KGRZ zu überspielen. Im Finanzwesen soll die Datenfernübertragung in Kürze eingesetzt werden. Schließlich gibt es für die Landtags-Dokumentation und einige andere Anwendungen einen Testbetrieb mit Dialogverarbeitung.

Die weitere Entwicklung hängt in erster Linie davon ab, ob für verschiedene große Anwendungen, wie Einwohnerwesen, Online-Besteuerungsverfahren und Grundstücksdatenbank, eine Grundsatz-Entscheidung zugunsten eines flächendeckenden Einsatzes der Fernverarbeitung fällt und damit der Aufbau eine Grundnetzes erforderlich wird.

Diese Entscheidungen sind, insbesondere wegen ihrer sehr erheblichen finanziellen Auswirkungen, heute noch offen.

Die Datenfernverarbeitung verändert die Strukturen des Informationsflusses grundlegend. Sie erlaubt es, die Leistungen des Computers dem einzelnen Mitarbeiter direkt an seinem Arbeitsplatz zur Verfügung zu stellen. Das Leitungsnetz garantiert einen ungehinderten Datenaustausch zwischen allen angeschlossenen Stellen.

Daraus ergeben sich für den Datenschutz neue Aufgaben. Es muß sichergestellt werden, daß jeder Teilnehmer von den technischen Möglichkeiten nur im Rahmen seiner Befugnisse Gebrauch macht. Dazu müssen diese genau definiert und entsprechende technische Zugriffsregeln programmiert werden.

Im Hinblick auf die erhöhten und ganz anders gearteten Mißbrauchsgefahren muß darüber hinaus das gesamte Datensicherheitskonzept grundsätzlich überprüft und ausgebaut werden.

---

[1]) Vgl. IV, 3.

[2]) LT-Drucks. 8/973 Abschn. V

Dies bestätigte sich bei der Überprüfung eines nicht dem DV-Verbund angehörenden Rechenzentrums. Dort arbeiteten bis zu acht Benutzer aus verschiedenen Verwaltungen gleichzeitig im Online-Betrieb auf einer DV-Anlage, ohne daß irgendwelche Zugriffsregeln und Sperren vorhanden waren. Damit war es jedem Teilnehmer möglich, unerkannt Daten der anderen Benutzer abzurufen und zu verändern.

Die Datenschutzrichtlinien des DV-Verbundes (DASCH) enthalten noch keine speziellen Vorschriften für die Fernverarbeitung. Diese Lücke sollte geschlossen werden, damit der Datenschutz der Bürger auch in der Aufbauphase der Datenfernverarbeitung nicht gefährdet wird.

4.3 DV-Leitsätze und Datenschutz

Der Arbeitsausschuß für die Automation von Verwaltungsaufgaben in der Landesverwaltung hat Datenverarbeitungs-Leitsätze mit Arbeitsrichtlinien für die Entwicklung von Automationsverfahren für die Landes- und die Kommunalverwaltung vorgelegt. Sie sollen die bisher getrennten Richtlinien vereinheitlichen.

In den neuen Leitsätzen fanden die praktischen Erfahrungen mit den bisherigen Leitsätzen und Richtlinien – an deren Stelle sie treten sollen – ihren Niederschlag. Die von mir angeregten Vorschriften für den Datenschutz[3]) wurden bei der Neuformulierung der Leitsätze weitgehend berücksichtigt. So wird darin vorgeschrieben, daß in der Hauptuntersuchung, welche die Grundlage für die Programmierung ist, die Aufbewahrungsfristen für die zu verarbeitenden Daten, die Programme, die Programmdokumentation und die Verarbeitungsergebnisse anzugeben sind. Sofern Datenträger konventionell geführte Bücher, Belege und Daten nicht ersetzen, sondern nur der Maschinensteuerung dienen, sind sie nach Ablauf der Aufbewahrungsfristen zu vernichten oder zu löschen. Falls sie noch benötigt werden, muß ein neuer Überprüfungstermin festgelegt werden. Diese Bestimmungen tragen den Forderungen des Datenschutzes Rechnung.

Eine andere Lösung ist für Datenträger vorgesehen, die an die Stelle der bisher konventionell geführten Bücher, Belege oder Akten treten. Hier wird nur auf die geltenden allgemeinen gesetzlichen Regelungen und Verwaltungsvorschriften verwiesen, insbesondere auf den Runderlaß des Ministers des Innern vom 24. Dezember 1971[4]). In diesem Erlaß werden jedoch nur Mindestaufbewahrungsfristen vorgeschrieben. Eine Tilgung nach Fristablauf, wie sie der Datenschutz verlangt, wird nicht gefordert. Diese Lücke sollte geschlossen werden.

Einer anderen Anregung folgend hat die Landesregierung den Entwurf einer Verpflichtungserklärung vorgelegt, die bei der Vergabe von Arbeiten im Rahmen der EDV an private DV-Unternehmen von dem Auftragnehmer abzugeben ist. Dem Vorschlag, dem Verpflichteten neben dem Verweis auf die gesetzlichen Bestimmungen durch Aushändigung der Gesetzestexte besonders auf die Rechtslage hinzuweisen wurde jedoch nicht gefolgt, weil er „unüblich" sei.

Diese Ablehnungsbegründung geht anscheinend davon aus, daß bei innerdienstlichem Schriftverkehr zwischen Behörden Gesetzesverweise genügen, da die einschlägigen Gesetze als bekannt vorausgesetzt werden können. Anders ist die Lage jedoch zu beurteilen, wenn private Unternehmen zur Geheimhaltung verpflichtet werden, um für die öffentliche Verwaltung Dienstleistungen übernehmen zu können, die unter das Amtsgeheimnis fallen. Deshalb schreibt z. B. auch der Minister des Innern in der Durchführungsverordnung zum Verpflichtungsgesetz vor, daß der Verpflichtete über Inhalt und Bedeutung der Strafvorschriften nicht nur mündlich unterrichtet wird, sondern daß ihm außerdem eine auszugsweise Abschrift der Strafvorschriften auszuhändigen ist[5]). Es gibt keinen vernünftigen Grund, bei der Verpflichtung von privaten Service-Unternehmen, die für die öffentliche Verwaltung Aufgaben der Datenerfassung, Datenverarbeitung, Programmierung und ähnliches durchführen, weniger zu verlangen.

4.4 Personal-Informationssysteme

Zur Zeit wird in Hessen für die öffentliche Verwaltung des Landes eine „Personal-Strukturdatei" vorbereitet. Sie soll hauptsächlich dazu dienen, die Personalplanung zu verbessern. Außerdem besteht für den Bereich der Schulverwaltung das Projekt einer Lehrer-Individualdatei. Die damit angestrebten Personal-Informationssysteme werfen unabhängig vom gegenwärtigen Stadium ihres Ausbaues eine Reihe grundsätzlicher Fragen auf.

Zu erinnern ist zunächst an § 107 des Hessischen Beamtengesetzes (HBG). Danach steht jedem Beamten ein Recht auf Einsicht in seine vollständigen Personalakten zu. Wie sich eine solche Bestimmung konkret auf automatisch gespeicherte Personaldateien auswirkt, ist noch

[3]) Siehe IV, 4.3

[4]) StAnz. 1972, S. 42

[5]) StAnz. 1975, S. 298 Abschn. 3 Abs. 5 Satz 2 und S. 299

nicht abzusehen. Dennoch steht fest, daß die Intention des Gesetzes nur verwirklicht werden kann, wenn das dem Beamten zugestandene Einsichtsrecht nicht dadurch gefährdet oder gar gegenstandslos wird, daß sich der Arbeitgeber für neue Methoden der Sammlung und Aufbewahrung persönlicher Angaben entscheidet.

Zu erinnern ist ferner an Bestimmungen wie die §§ 110 des Hessischen Beamtengesetzes sowie 66 und 57 a des Hessischen Personalvertretungsgesetzes. Allen diesen Vorschriften ist eines gemeinsam: Sie sehen ein Mitwirkungsrecht der Arbeitnehmervertretung in bestimmten Fällen vor, die Probleme der Personalstruktur betreffen. Für die Personal-Informationssysteme kann dies nur zur Folge haben: Die Vertretungen der Arbeitnehmer müssen auch bei den Bestrebungen, Personaldatenbanken zu errichten, mitwirken. Das Gesetz begnügt sich nicht damit, wie im Falle des bereits erwähnten § 107 HBG dem einzelnen ein Kontrollrecht zuzugestehen. Es schaltet gleichzeitig auch die Vertretung der Arbeitnehmer ein, wenngleich auf einer anderen Ebene. Aufgabe dieser Vertretung ist es, für die notwendigen institutionellen Vorkehrungen zu sorgen, die einerseits generell den Datenschutz sicherstellen und es andererseits speziell dem einzelnen ermöglichen, das ihm garantierte Einsichtsrecht auch tatsächlich ausüben zu können.

Insofern erscheint es unerläßlich, daß sich sowohl die im öffentlichen Dienst Tätigen als auch die Personalvertretungen und die Gewerkschaften weit mehr als bisher mit Fragen des Datenschutzes beschäftigen. Ein erster Schritt in diese Richtung ist bereits getan. Das Kultusministerium arbeitet im Falle der Lehrer-Individualdatei mit der Personalvertretung zusammen. Ähnliches sollte überall praktiziert werden. Nur unter dieser Voraussetzung wird es möglich sein sicherzustellen, daß über die fraglos notwendigen Rationalisierungsvorteile der Persönlichkeitsschutz des Arbeitnehmers nicht vernachlässigt oder vergessen wird.

4.5 Datenübermittlung an Dritte

Die Weitergabe von Daten aus dem öffentlichen Bereich an Dritte wirft am häufigsten Datenschutz-Fragen auf.

Gibt die Stelle, die Daten zuerst erfaßt und gespeichert hat, diese an Dritte weiter, so darf man bei der rechtlichen Beurteilung nicht außer Acht lassen, daß Informationen nur zu bestimmten Zwecken erteilt werden. Außerdem erschweren Übermittlungen von personenbezogenen Daten den Einblick des Bürgers in die Verwendung der zu seiner Person gesammelten Information. Darunter leidet die Transparenz des Verwaltungshandelns. Auf diese Fälle beziehen sich die Gebote Nr. 4 und Nr. 7 der Datenverkehrs-Ordnung[6]). Die Notwendigkeit, die Verfügung über Daten zu begrenzen, findet auch in § 5 Abs. 1 des Hessischen Datenverarbeitungsgesetzes vom 16. Dezember 1969[7]) Ausdruck.

Die Problematik, die mit der Übermittlung von Daten an andere als den Erstempfänger verbunden ist, stand daher auch bei der Beratung des EBDSG und bei den Anhörungen im Gesetzgebungsverfahren stets im Vordergrund.

Dabei machen sich zwei allerdings gegenläufige Tendenzen bemerkbar: einerseits die von der Technik ermöglichte Einmalerfassung für vielseitige Verwendungszwecke, die es dem Bürger erspart, immer wieder dieselbe Auskunft über sich geben zu müssen, und andererseits der Schutz des Persönlichkeitsrechts des Bürgers vor einer von ihm nicht kontrollierbaren Verwendung seiner Auskünfte. Beispiele für diese Interessenkollissionen sind auch im Berichtszeitraum bekannt geworden.

4.5.1 Der Bundesverband der Ortskrankenkassen hat die Zentralstelle für die Vergabe von Studienplätzen in Dortmund (ZVS) aufgefordert, seinen Mitgliedern Datenmaterial über Studenten zu Zwecken der Direktwerbung zur Verfügung zu stellen. Die ZVS, zu deren Trägern auch das Land Hessen gehört, hat dieses Ansinnen aus Datenschutzgründen abgelehnt. Nachdem mir bekannt wurde, daß der Bundesverband empfohlen haben soll, die Daten direkt von den Universitäten zu beziehen, habe ich die von den Hochschulen in Hessen geübte Praxis überprüft. Dabei ergab sich, daß eine ganze Anzahl von Versicherungsunternehmen wegen Datenmaterial an hessische Hochschulen herangetreten sind; in allen Fällen aber ohne Erfolg.

4.5.2 In den Tätigkeitsberichten ist wiederholt kritisiert worden, daß die Behörden personenbezogene Daten an private Firmen und an die Presse weitergeben[8]). Denn „die Weitergabe der . . . Informationen an Personen und Stellen außerhalb der öffentlichen Verwaltung stellt . . . einen Eingriff in das Recht des Bürgers dar, über die Verwendung von Informationen über seine Person selbst zu bestimmen . . .“[9]).

---

[6]) Vgl. IV Anlage I

[7]) GVBl. I S. 304

[8]) II, 1.3.2; III, 1.5.6; IV, 1.6, 4.7.8 und 5.1.6;

[9]) III, 1.5.6

4.5.2.1 Besonders beanstandet wurde dabei die Praxis der Standesämter, Anschriften von Neuvermählten oder von Eltern neugeborener Kinder an interessierte Firmen weiterzugeben[10]).

Die Landesregierung hat sich aufgrund dieser Vorkommnisse für eine Änderung der bundesrechtlich geregelten Dienstanweisung für Standesbeamte (DA) eingesetzt. Auch die von der Bundesregierung beschlossene Neufassung des § 104 sah vor, daß „der Standesbeamte Angaben über die von ihm beurkundeten Personenstandsfälle weder veröffentlichen noch Interessenten zur Verfügung stellen (darf)". Diese Neufassung ist jedoch im Bundesrat als zu weitgehend – insbesondere im Hinblick auf die Interessen der Presse – abgelehnt worden.

Es kann in der Tat zweifelhaft sein, ob ein Verbot der Datenweitergabe notwendig ist. Der Bürger muß jedoch in der Lage sein, mögliche Unannehmlichkeiten oder Gefährdungen, die durch die Weitergabe seiner Daten entstehen können, selbst zu erkennen und sich dann für oder gegen die Weitergabe zu entscheiden.

Bei einer Neufassung von § 104 DA müßte daher vorgeschrieben werden, daß vor jeder standesamtlichen Beurkundung der Standesbeamte die Betroffenen über die mögliche Veröffentlichung ihrer Personenstandsdaten bzw. deren Übermittlung an Privatfirmen informiert. Eine Weitergabe der Daten durch den Standesbeamten sollte dabei nur auf Antrag der Betroffenen erfolgen. Auch dem Interesse der Presse wäre durch eine solche Regelung ausreichend Rechnung getragen. Ein „unangemessener Verwaltungsaufwand" entstünde dabei nicht.

4.5.2.2 Die Forderung der Lokalpresse an die Gemeindeverwaltungen, sie rechtzeitig über Jubiläumsdaten der Einwohner zu inforieren, wirft ähnliche Probleme auf wie im Standesamtswesen. Aufgrund von § 3 des Hessischen Pressegesetzes vom 23. Juni 1949[11]) kann eine Behörde die Auskunft an die Presse nur verweigern, „soweit Auskünfte über persönliche Angelegenheiten einzelner verlangt werden, an deren öffentlicher Bekanntgabe kein berechtigtes Interesse besteht". Inwieweit für die öffentliche Bekanntgabe von Jubiläumsdaten – die zweifellos Angaben über persönliche Angelegenheiten einzelner sind – ein berechtigtes Interesse besteht, dürfte in Großstädten und ländlichen Gemeinden unterschiedlich beurteilt werden. In jedem Falle verlangt es das Persönlichkeitsrecht, daß Daten, die der Bürger dem Einwohnermeldeamt aufgrund der melderechtlichen Vorschriften gegeben hat, nicht ohne gesetzliche Anordnung oder ohne seine Zustimmung an Dritte herausgegeben werden. Eine entsprechende Praxis der Standesämter, der Postreklame und des Kraftfahrtbundesamtes wurde bereits wiederholt kritisiert[12]).

Eine praktikable Regelung erscheint in der Weise möglich, daß die Gemeindeverwaltungen bei den Bürgern, die keine Bekanntgabe ihrer „Jubiläumsdaten" an die Presse wünschen, von einer Mitteilung absehen. Dort, wo die Bürger selbst an einer Veröffentlichung interessiert sind, wird die Presse die einschlägigen Daten nach wie vor erhalten.

4.5.3 Der Kreisausschuß eines Landkreises hat den Gemeinden des Kreisgebietes erklärt, es sei zur Erledigung seiner Aufgaben notwendig, daß die Gemeinden ihm Angaben bzw. Unterlagen vorlegen, so z. B. auch Daten von Einwohnern. In einer vorbereiteten Erklärung sollten die Gemeinden den Kreisausschuß ermächtigen, „zur Erledigung von Arbeiten, bei denen Einwohnerdaten benötigt werden, . . . diese Daten jeweils beim KGRZ . . . direkt anzufordern".

In dieser pauschalen Form trägt die Ermächtigungserklärung den Erfordernissen des Datenschutzes nicht Rechnung. Zwar verlangen es die Grundsätze der Amtshilfe, daß die Gemeinde dem Kreis die für die Erfüllung seiner Aufgaben erforderlichen Informationen zur Verfügung stellt. Die Gemeinde hat dabei aber sorgfältig zu prüfen, inwieweit eine Datenweitergabe unter Datenschutzgesichtspunkten zulässig ist. So könnten etwa Bedenken gegen die offene Weitergabe von Einzelangaben für Planungszwecke bestehen. Besonders sensible Daten, z. B. über Wahlrechtsbeschränkungen und Fahndungsvermerke, können weiteren Beschränkungen unterliegen. Gegenüber der Stadt, die mir den Sachverhalt unterbreitet hat, habe ich deshalb angeregt, nur auf der Grundlage einer nach Inhalt und Zweck spezifizierten Datenanforderung des Kreises zu entscheiden, und dabei den Datenschutz der Bürger besonders zu beachten.

Es bedarf näherer Prüfung, ob sich eine Musterregelung durch die Kommunalen Spitzenverbände empfiehlt.

4.5.4 Zur Auszahlung der Bezüge an ihre Bediensteten benutzen Landesbehörden Überweisungsträger, auf die neben den zur Vornahme der Gutschrift notwendigen Daten zusätzliche Angaben über

[10]) IV, 4.7.8

[11]) i. d. F. vom 20. Nov. 1958, GVBl. S. 183

[12]) Vgl. IV, 4.7.8 sowie V, 4.5.5

persönliche Verhältnisse des Empfängers wie, z. B. Grundbezüge, Zulagen, Lohn- und Kirchensteuer und weitere Abzüge ausgedruckt werden. Es gibt keine Rechtsvorschrift, die es erlaubt, diese Angaben den Bankinstituten zugänglich zu machen.

Die Überweisungsmitteilungen sollten daher so gefaßt werden, daß die Geldinstitute nur Kenntnis von den Endbeträgen, nicht aber von einzelnen Rechnungsposten erhalten. Die vom Finanzministerium gegen eine Umstellung angeführten Argumente überzeugen nicht. Ob die Festsetzung und Auszahlung der Dienstbezüge dem Steuergeheimnis unterliegt, ist ohne Bedeutung, da jedenfalls das Datengeheimnis des § 3 DSG und das Amtsgeheimnis eingreifen. Die mit der Bekanntgabe der Bankverbindung zwecks Überweisung der Bezüge erklärte Einwilligung des Betroffenen deckt nicht die Weiterleitung der erwähnten zusätzlichen Angaben. Der Hinweis auf die Kosten einer Verfahrensumstellung verkennt den gesetzlich verbürgten Datenschutz der Bürger, überzeugt aber auch deshalb nicht, weil die kommunalen Gebietskörperschaften seit Jahren ein ebenfalls automatisiertes Überweisungsverfahren betreiben, das dem Datenschutz voll entspricht.

4.5.5 In früheren Tätigkeitsberichten ist kritisiert worden, daß Behörden personenbezogene Daten für gewerbliche Zwecke an Dritte weitergeben[13]). So teilt z. B. das Kraftfahrtbundesamt „die Zulassung oder Umschreibung von Kraftfahrzeugen Dritten für Zwecke von Werbung und Meinungsforschung" mit, wenn der An- oder Ummelder sich damit einverstanden erklärt hat. In diesem Zusammenhang hat der Hessische Minister für Wirtschaft und Technik mit Erlaß vom 6. Juli 1974 die Oberbürgermeister und Landräte darauf hingewiesen, daß diese Zustimmung auch in der Vollmacht enthalten sein muß, die der Erwerber des Fahrzeugs dem Verkäufer oder einem sonstigen Beauftragten erteilt, wenn dieser für ihn das Fahrzeug anmeldet.

Aus dem Wortlaut der Zustimmung ist zu entnehmen, daß neben Namen und Adresse auch alle sonstigen in dem Zulassungs-/Umschreibungsantrag enthaltenen Angaben weitergegeben werden können, darunter Geburtsort und -datum, Bankverbindung und -konto, Zahlungsweise der Kfz.-Steuer, Fahrgestell- und Motornummer und vieles andere mehr. Das Kraftfahrtbundesamt hat sich zwar verpflichtet, im Höchstfall nur 16 bestimmte Datenarten weiterzugeben. Um welche Daten es sich dabei handelt, ist der Öffentlichkeit aber nicht bekannt und wird auch dem An- oder Ummelder nicht mitgeteilt.

Diese Kenntnis braucht aber der Bürger, um sein Zustimmungsrecht ausüben zu können. Unabhängig davon bleiben die grundsätzlichen Bedenken gegen die Weitergabe von Daten durch das Kfz.-Bundesamt für Werbezwecke bestehen.

[13]) Siehe III, 1.5.6, 4.1; IV, 3.1 und 4.7.8

4.6 Datenschutz bei Prüfungsstatistiken

Bei der Erhebung und Speicherung von Angaben der Studierenden für hochschulinterne Zwecke wird der Datenschutz nicht immer beachtet. Angehörige einer hessischen Universität haben sich darüber beschwert, daß von Studenten, die sich zu einer Prüfung anmelden wollen, die Beantwortung eines „Fragebogens für Prüfungskandidaten" gefordert wird.

Meine Nachforschungen haben ergeben, daß es sich um eine Befragung handelt, die seit mehreren Jahren zu statistischen Zwecken von der „Stelle für Hochschulstatistik" der Universität durchgeführt wird. Diese Stelle tritt gegenüber den Befragten aber nicht in Erscheinung. Die Fragebögen weisen die Universität (ohne weiteren Zusatz) als Träger der Befragung aus. Die Erhebung erfolgt durch die Prüfungsämter, die die Fragebögen zusammen mit den für die Meldung erforderlichen Formularen ausgeben.

Die Fragebögen enthalten mehr als 30 Fragen. Nur bei drei Fragen wird die Beantwortung freigestellt. Keine Freiwilligkeit besteht zum Beispiel bei folgenden Fragen: „Haben Sie sich nach Erwerb der Hochschulreife zum unmittelbar folgenden Semester an einer Hochschule einschreiben lassen?" „Wenn nein, was haben Sie in der Zwischenzeit gemacht? . . . Reisen? Sonstiges?" „Welches war der Hauptgrund für die Unterbrechung(en) (Ihres Studiums)? . . . Finanzielle Gründe? . . . Krankheit? Zeitweise keine Lust? Sonstiges?"

Die Prüfungskandidaten müssen die Fragebogen mit Namen, Vornamen und Fakultät bzw. Abteilung kennzeichnen und beim zuständigen Prüfungsamt abgeben. Dieses ergänzt den Fragebogen nach Abschluß des Prüfungsverfahrens um Angaben über das Prüfungsergebnis und ggf. um die Gründe für einen Rücktritt von der Prüfung. Die Fragebögen werden dann der Stelle für Hochschulstatistik der Universität zugeleitet und von dieser statistisch ausgewertet.

Diese Praxis der Universität verstößt in mehrfacher Hinsicht gegen Grundsätze des Datenschutzes:

a) Mit der Forderung von Auskünften wird in unzulässiger Weise in das Persönlichkeitsrecht der Prüfungskandidaten eingegriffen.

Für die Befragung gibt es keine gesetzliche Grundlage. Deshalb besteht in Wahrheit auch keine Auskunftspflicht. Angesichts des eindeutig entgegengesetzten Inhalts des Fragebogens, der engen Verbindung der Erhebung mit dem Prüfungsverfahren und des Fehlens einer Zusicherung, daß die Angaben ausschließlich statistischen Zwecken dienen, ist diese Rechtslage für die Befragten freilich kaum erkennbar. Sie können deshalb auch nicht ausschließen, daß eine Auskunftsverweigerung persönliche Nachteile zur Folge haben könnte.

Die Auffassung der Universität, daß „gegen die ... Fragen an sich keine Bedenken" bestünden, geht an der daraus für die Prüfungskandidaten resultierenden Zwangslage vollständig vorbei.

b) Die Art und Weise, wie die Befragung durchgeführt wird, entspricht nicht dem Gebot des § 2 DSG, vom Datenschutz erfaßte Unterlagen so aufzubewahren und weiterzuleiten, daß sie nicht durch Unbefugte eingesehen werden können.

Da die Erhebung nur statistischen Zwecken dient, dürften die ausgefüllten Fragebögen den Prüfungsämtern nicht zugänglich gemacht werden. Ihre Aufbewahrung bei den Prüfungsämtern für die gesamte Dauer des Prüfungsverfahrens begründet die Gefahr, daß durch Versehen oder unkorrektes Verhalten der Bediensteten auch Prüfer Kenntnis von den persönlichen Angaben erhalten.

c) Die von der Stelle für Hochschulstatistik in Form eines Berichts herausgegebenen Auswertungen verstoßen gegen den Grundsatz, daß statistische Veröffentlichungen keine Einzelangaben erkennen lassen dürfen.

Bei der tabellarischen Darstellung wurden offensichtlich alle anfallenden Werte unverändert und vollständig eingesetzt. Durch die Aufnahme auch sehr kleiner Tabellenwerte bis hinab zur Zahl 1 ist es auch dem Laien leicht möglich, die Angaben zu einzelnen Personen zu isolieren. Dieses Vorgehen ist um so weniger verständlich, als der Bericht selbst auf die mangelnde statistische Aussagekraft kleiner Zahlen hinweist.

Um nur ein Beispiel für mögliche Rückschlüsse zu nennen: Im ausgewerteten Studienjahr hat in einem bestimmten, aus Gründen des Datenschutzes hier nicht näher bezeichneten Fach nur ein Kandidat eine Prüfung abgelegt. Zu dieser Person läßt sich aus dem Bericht in wenigen Minuten folgendes Dossier aufbauen:

- 24 Jahre
- weiblich
- verheiratet
- keine Kinder
- Vater ist Beamter
- Vater hat Hochschulabschluß
- Person stammt aus Hessen
- hat neusprachliches Gymnasium besucht
- hat nach Abitur ohne Unterbrechung Studium aufgenommen
- Erstimmatrikulation an einer deutschen Hochschule, jedoch nicht in Frankfurt, Gießen, Marburg
- nach drei oder vier Semestern Wechsel an die jetzige Hochschule
- kein weiterer Hochschulwechsel
- kein Fachwechsel
- keine Unterbrechung des Studiums
- Studiendauer elf Semester
- Note der Abschlußprüfung: eins

d) Zu meinem Bedauern konnte ich den Beschwerdeführern und den übrigen Betroffenen nicht so wirkungsvoll helfen, wie es dem Zweck des Datenschutzgesetzes entspricht, weil ich die von der Universität verlangten Auskünfte erst nach fünfzehn Monaten erhalten habe.

e) Die nunmehr vorliegende Erklärung der Leitung der Universität läßt leider nicht erkennen, ob inzwischen die gebotenen Maßnahmen zum Schutz gegen unbefugten Zugriff getroffen wurden und ob die sofortige Vernichtung ausgewerteter Fragebögen gewährleistet ist. Es scheint auch keine Bereitschaft zu bestehen, die Erhebung insgesamt den Anforderungen des Datenschutzes anzupassen.

Ich habe den Kultusminister auf meine Bedenken hingewiesen und um Auskunft gebeten, ob andere Hochschulen und Prüfungsämter ähnliche statistische Erhebungen durchführen.

4.7 Datenschutz und Polizeiinformationssysteme

Die fortschreitende Automatisierung der polizeilichen Informationssysteme und die sich daraus ergebenden Konsequenzen für die Informationsverwertung machen es erforderlich, dafür verbindliche Regeln festzulegen. Es gibt keine bundeseinheitlichen Bestimmungen über die Aufbewahrung und Auswertung der erkennungsdienstlichen Unterlagen, die von der Kriminalpolizei aufgrund eigener Maßnahmen gewonnen oder von ihr aus dem Strafverfahren übernommen worden sind. Auf diese unbefriedigende Rechts-

lage ist in den früheren Tätigkeitsberichten hingewiesen worden[14]).

Das Hessische Landeskriminalamt (HLKA) hat die in diesen Berichten enthaltenen Anregungen aufgegriffen. Die bisher für das Land geltenden Richtlinien sind überarbeitet worden. Am 25. Juli 1975 hat das HLKA neue „vorläufige Richtlinien für Auskünfte aus Kriminalakten" in Kraft gesetzt, die Bestandteil der im Entwurf vorliegenden Neufassung der „Richtlinien für die Führung von Kriminalakten" sein werden. Die Richtlinien sehen vor, daß Filme oder Datenträger den Kriminalakten gleichgesetzt werden. Ferner werden darin die auskunftsberechtigten Dienststellen abschließend benannt, und es wird festgelegt, daß die Tilgungsfristen des § 43ff BZRG zu beachten sind. Unbeschränkte Auskünfte erhalten nur die „Kriminaldienst verrichtenden Dienststellen der Polizei für Zwecke der Verhütung und Verfolgung von Straftaten" bzw. andere Behörden, „wenn ausschließlich durch sie eine Störung der öffentlichen Sicherheit und Ordnung beseitigt oder von der Allgemeinheit oder dem einzelnen eine unmittelbar bevorstehende Gefahr abgewehrt werden kann".

Die neuen Richtlinien enthalten erstmals Bestimmungen über Auskunftsersuchen von Betroffenen. Über diese Ersuchen entscheiden die Behörden- oder Dienststellenleiter nach „pflichtgemäßem Ermessen". Dabei sind „das Interesse des Betroffenen und ein etwa entgegenstehendes öffentliches Interesse gegeneinander abzuwägen". In einem besonderen Abschnitt werden die „Aussonderung und Auflösung" von Kriminalakten geregelt. Kriminalakten können danach auf Antrag des Betroffenen aufgelöst werden. Dabei sind seine schutzwürdigen Belange und das öffentliche Interesse gegeneinander abzuwägen. Sie müssen allerdings aufgelöst werden, wenn der Betroffene 10 Jahre — bisher 25 Jahre — nicht mehr polizeilich in Erscheinung getreten ist oder wenn er das 75. — bisher das 90. — Lebensjahr vollendet hat. Von diesen Fristen kann abgewichen werden, wenn es zur Erfüllung der polizeilichen Aufgabe notwendig ist.

[14]) II, 4.1.1.3 c; III, 4.1.5.1; IV, 4.5

Aufgelöste Kriminalakten sind zu vernichten. Werden sie als „historisch wertvoll oder für Lehr- und Forschungszwecke geeignet" befunden und deshalb weiter aufbewahrt, so ist zu prüfen, ob die Personalien unkenntlich zu machen sind.

Zusammenfassend ist festzustellen: Die Richtlinien von 1975 erweitern im Vergleich zu den alten Richtlinien von 1965 die Möglichkeit, Auskunft aus Kriminalakten zu erteilen. Die Akten sind nicht mehr „ausschließlich" für den innerdienstlichen Gebrauch bestimmt. Für die Verwertung für Zwecke außerhalb des kriminalpolizeilichen Innendienstes wird jedoch festgelegt, an welche Stellen (oder Personen) unter welchen Voraussetzungen und in welchem Umfang Auskünfte zu erteilen sind. Neu sind die Gleichsetzung der im Hessischen Polizeiinformationssystem (HEPOLIS) gespeicherten Daten mit Kriminalakten, das Auskunftsrecht des Betroffenen, die Bestimmungen über den Datenschutz und die Veränderung der Fristen für die Aussonderung und Auflösung von Kriminalakten.

Die Regelungen in den Richtlinien kommen den Überlegungen entgegen, die der Datenschutzbeauftragte in seinen bisherigen Tätigkeitsberichten formuliert hat. Sie stellen aber noch nicht voll zufrieden. Richtlinien und Verwaltungsanweisungen legen den Beamten und Angestellten zwar dienstrechtliche Pflichten auf; daraus erwachsen jedoch für den einzelnen Bürger keine eigenständigen Rechte, wie dies bei Gesetzen oder Rechtsverordnungen der Fall ist; sie entsprechen daher nicht der Forderung nach einer Verrechtlichung des Datenschutzes.

Die Anregung, die Datenschutzregelungen im Bereich der Polizei zu verrechtlichen, besteht daher fort. Rechtsvorschriften sind auch erforderlich, um sicherzustellen, daß Daten aus dem polizeilichen Informationssystem, die Personen oder Stellen außerhalb der Kriminalpolizei zur Verfügung gestellt worden sind, von diesen nicht zweckentfremdet werden. Dies gilt selbstverständlich in Übereinstimmung mit den früheren Tätigkeitsberichten auch für den Bereich des Verfassungsschutzes.

5. WISSENSCHAFTLICHE FORSCHUNG AUF DEM GEBIET DES DATENSCHUTZES

5. Wissenschaftliche Forschung auf dem Gebiet des Datenschutzes

Als der Hessische Landtag vor fünf Jahren das erste Datenschutzgesetz der Welt verabschiedete, war das ein Vorstoß in ein bis dahin auch Fachleuten in Wissenschaft und Praxis weitgehend unbekanntes Gebiet. Seither hat sich die Situation freilich gründlich geändert. Die automatisierte Datenverarbeitung ist in fast alle Bereiche staatlicher und privater Administration vorgedrungen und vielerorts als Instrument für die Verarbeitung und Bereitstellung von Informationen unentbehrlich geworden.

Im Verlaufe dieser Entwicklung mußten sich die EDV-Anwender auch mit Fragen des Datenschutzes auseinandersetzen, sei es, weil die für den Umgang mit personenbezogenen Daten bereits vorhandenen Regeln den neuen technisch-organisatorischen Gegebenheiten und dem steigenden Schutzbedürfnis nicht mehr genügten, sei es, weil eine sich verändernde Informationsstruktur die bestehende Verteilung von Macht und Einfluß in Frage stellte. Vor allem die Diskussion über das geplante Bundesdatenschutzgesetz hat staatliche wie private EDV-Anwender veranlaßt, zur Wahrung ihrer Interessen eindeutig Position zu beziehen. Auch die Wissenschaft hat sich inzwischen Datenschutzproblemen stärker zugewandt, was eine kaum noch überblickbare und weiter ansteigende Flut von Fachliteratur dokumentiert.

Dennoch fehlt es nach wie vor an einer breiten Grundlage gesicherter wissenschaftlicher Erkenntnisse. Wer den Stand der Forschung aufmerksam verfolgt, stellt alsbald starke Ungleichgewichte fest. Einzelnen relativ gut bearbeiteten Teilbereichen, wie etwa der Methodik der Benutzeridentifikation und der Berechtigungsprüfung, stehen andere gegenüber, die kaum noch Gegenstand einer eingehenden Untersuchung gewesen sind, wie beispielsweise die Kosten-Nutzen-Analyse der einzelnen Datenschutzinstrumente aber auch der gesamte Komplex des verfassungspolitischen Datenschutzes (Gewaltenteilung, Informationsgleichgewicht). Die Ursachen für diese Disparität liegen teils bei der Wissenschaft selbst – es genügt, an die Schwierigkeiten der hier unentbehrlichen interdisziplinären Arbeit zu erinnern –, teils in der Praxis, die oft dazu tendiert, die Probleme zu verharmlosen oder durch improvisierte Maßnahmen zu überbrücken, statt sich nicht zuletzt mit Hilfe von gezielten Forschungsaufträgen mit ihnen eingehend auseinanderzusetzen.

Die unzureichende wissenschaftliche Erforschung des Datenschutzes interessiert hier allerdings nicht als Problem der Wissenschaft, sondern als Faktor, der sich auf die praktische Verwirklichung des Datenschutzes in Staat und Gesellschaft überaus nachteilig auswirken kann. Weder die rechtlich vorgegebenen Grundsätze noch die konkreten politischen Zielsetzungen können auf die Entwicklung und Anwendung der Computertechnologie Einfluß nehmen, wenn nicht der Trend der technologischen Entwicklung sowie die gesellschaftlichen und politischen Implikationen dieser Technologie laufend analysiert und von den politischen Entscheidungsträgern bei ihrer Meinungsbildung berücksichtigt werden. Datenschutzforschung ist ein untrennbarer Bestandteil der Datenschutzpolitik.

Zu den unmittelbaren praktischen Konsequenzen dieser Einsicht gehört die Aufgabe der für den Datenschutz verantwortlichen Instanzen, nach den für ihre Tätigkeit relevanten Problemstellungen zu fragen und sie zugleich als Forschungsgegenstände anzubieten. Anders formuliert: Wirksamer und überzeugender Datenschutz setzt auch voraus, daß die dafür Verantwortlichen die ständige Verbesserung als Problem der wissenschaftlichen Forschung verstehen und es deshalb zu ihren Zielen rechnen, Anregungen dafür zu vermitteln.

Zugleich gilt es jedoch, die finanziellen Voraussetzungen für ein solches Forschungsprogramm zu schaffen. Besondere Bedeutung kommt in diesem Zusammenhang dem in Kürze anlaufenden Dritten DV-Förderungsprogramm des Bundes zu. Aber auch alle anderen Förderungseinrichtungen, wie insbesondere die Deutsche Forschungsgemeinschaft und die Volkswagenstiftung, sind angesprochen. Es genügt allerdings nicht, sich für die Möglichkeit einzusetzen, im Rahmen anwendungsbezogener Entwicklungsprojekte neben vielem anderen auch Fragen des Datenschutzes zu behandeln. Vielmehr müßte bei allen Projekten, die sich mit der Verarbeitung peronenbezogener Daten beschäftigen oder die Implikationen der Datenverarbeitung für die politische Willensbildung und Machtbalance berüh-

ren, die Förderung an die Auflage gebunden werden, daß die Erforschung der dabei auftretenden Datenschutzprobleme sichergestellt wird. Darüber hinaus ist der Datenschutz auch als selbständiger Schwerpunkt in das Forschungsprogramm aufzunehmen.

Freilich kann es nicht darum gehen, nach dem Gießkannenprinzip unterschiedslos jedes mit dem Etikett „Datenschutz" versehene Vorhaben zu unterstützen. Vielmehr läßt sich das Ziel, bessere Grundlagen für die Gesetzgebung und für Durchführungsmaßnahmen auf dem Gebiet des Datenschutzes zu schaffen, nur dadurch rationell erreichen, daß bereits in den Förderungsprogrammen Schwerpunkte und Prioritäten angedeutet werden. Hierzu werden im folgenden einige Anregungen gegeben, die sich zugleich als Hinweise für Forschung und Wissenschaft selbst verstehen:

1. Informationsgleichgewicht

In dem Themenbereich, den man mit Stichworten wie parlamentarisches Informationsrecht oder Informationsgleichgewicht zu umschreiben pflegt, ist der Stand der wissenschaftlichen Forschung noch rudimentär. Dabei läßt sich gegenwärtig schon feststellen, daß mit diesem Problemkomplex Fragen angesprochen werden, die für die Entwicklung des parlamentarischen Regierungssystems und für den Fortbestand einer eigenständigen Selbstverwaltung von zentraler Bedeutung sind.

An konkreten Aufgaben aus diesem Bereich wären zu nennen:

- Internationale Bestandsaufnahme des Entwicklungsstandes und der Planungen für parlamentarische Informationssysteme aber auch der Verwendung von Informationssystemen der Regierung und der Verwaltung durch die Parlamente,
- Analyse des Informationsbedarfs und der Informationsdefizite des Parlaments,
- Analyse der verfassungsrechtlichen, verfassungspolitischen, organisatorischen und technischen Anforderungen an parlamentarische Informationssysteme und an die parlamentarische Nutzung von Informationssystemen der Regierung und Verwaltung.

2. Transparenz der Verwaltung

Die automatische Datenverarbeitung verstärkt den Informationsvorsprung des Staates gegenüber dem Bürger. Die Frage nach den Möglichkeiten, der zunehmend einseitigen Informationsverteilung entgegenzuwirken, gewinnt damit an Bedeutung und Aktualität. So wäre beispielsweise zu prüfen, ob nicht alle Akten der Verwaltung öffentlich zugänglich sein sollten, soweit nicht der Schutz der Person des einzelnen oder besondere, gesetzlich im einzelnen festgelegte, vorrangige öffentliche Interessen die Geheimhaltung von Informationen gebieten. In Schweden ist eine in diesem Sinne verstandene Aktenöffentlichkeit ein schon lange bestehendes Verfassungsprinzip, das aber gerade im Zeichen der zunehmenden Verwendung der automatischen Datenverarbeitung eine ganz neue Bedeutung bekommen hat. In den Vereinigten Staaten hat man mit dem vor einigen Jahren verabschiedeten „Freedom of Information Act" einen ähnlichen Weg beschritten. Nicht zuletzt die Erfahrungen dieser Länder wären auszuwerten.

3. Datenschutz für juristische Personen

Die bisherig Datenschutzdiskussion hat sich verständlicherweise nahezu ausschließlich am Schutzbedürfnis des einzelnen Bürgers orientiert. Offen ist nach wie vor die Frage, ob es ähnlicher Vorkehrungen nicht auch für juristische Personen und Personengruppen bedarf. Und zwar schon deshalb, weil Art. 19 Abs. 3 GG sich ausdrücklich für die Anwendung der Grundrechte auch bei juristischen Personen ausspricht. Ganz abgesehen davon zeigt die bisherige Erfahrung, daß ein wirklich effizienter Schutz des Bürgers oft nur zu erzielen ist, wenn die Grundsätze des Datenschutzes auch beim Umgang mit Personengruppen, denen der einzelne angehört, beachtet werden.

Bei der Vorbereitung des geplanten Bundesdatenschutzgesetzes sind diese Fragen ausgeklammert worden. Eine Entscheidung des Gesetzgebers setzt eine genaue Kenntnis der verschiedenen Fallkonstellationen voraus, aber auch der Auswirkungen von Datenschutzregeln auf den Handlungsspielraum und die Kontrollierbarkeit der betroffenen Gruppen und juristischen Personen.

4. Zweckbindung der Information

Je mehr sich die Bestrebungen, eine integrierte Datenverarbeitung zu realisieren, konkretisieren, desto deutlicher wird die Notwendigkeit, die rechtlichen Grenzen des Informationsaustausches zu bestimmen. Dabei geht es in erster Linie darum, die juristischen und informationswissenschaftlichen Grundlagen des Prinzips der Zweckbindung von Informationen zu erarbeiten und die sich daraus für die Integration ergebenden Konsequenzen zu analysieren. Überdies gilt es, die möglichen Auswirkungen der integrierten Datenverarbeitung für den einzelnen zu klären und empirisch zu überprüfen. Von den Ergebnissen einer solchen Untersuchung hängt es entscheidend ab, ob es gelingen kann, im Rahmen

von Kosten-Nutzen-Analysen für die einzelnen Integrationsbereiche die Interessen des Bürgers richtig zu bewerten.

5. Freiheit der Forschung und Datenschutz

Die automatische Datenverarbeitung eröffnet der wissenschaftlichen Forschung, vor allem im Bereich der Sozialwissenschaften, ganz neue Möglichkeiten der Datenspeicherung und -auswertung. Die Konsequenz ist freilich ein sich ständig verschärfender Gegensatz zwischen den von der Forschung postulierten Informationsbedürfnissen und dem Datenschutzinteresse des einzelnen. Ob sich dieser Konflikt lösen läßt, wird erst beantwortet werden können, wenn Untersuchungen zu den sich dafür anbietenden rechtlichen, organisatorischen und technischen Möglichkeiten vorliegen. Nicht zuletzt alle von dieser Entwicklung betroffenen Disziplinen haben ein eminentes Interesse, eine in diese Richtung zielende Forschung vorrangig zu unterstützen. Die Schwierigkeiten, die ein solcher Konflikt für die wissenschaftliche Arbeit mit sich bringt, machen sich gegenwärtig schon bemerkbar, wie sich etwa im Rahmen der Diskussion über das geplante Bundesdatenschutzgesetz gezeigt hat. Solange es aber an den notwendigen Untersuchungen fehlt, wird es für die verschiedenen Disziplinen kaum möglich sein, sich die von der Datenverarbeitung gebotenen Vorteile in dem erhofften Maß zunutze zu machen.

6. Bereichsspezifische Regelungen

Ein Bundesdatenschutzgesetz kann nur einen generellen Mindestschutz sicherstellen. Für einen wirksamen Datenschutz ist es erforderlich, spezialgesetzliche Regelungen so schnell wie möglich zu treffen. Zu den vordringlichen Aufgaben der Forschung gehört es deshalb, nicht nur besonders sensible Bereiche auszumachen, sondern auch Lösungsmodelle vorzulegen, die den jeweiligen bereichsspezifischen Bedingungen Rechnung tragen. Zu diesen kritischen Bereichen gehören das Kriminal- und Sicherheitswesen, das Gesundheitswesen, die Pressedatenbanken, die Personalinformationssysteme und die politische Planung. An dieser höchst unvollständigen Liste läßt sich bereits erkennen, wie wichtig die verschiedenen Bereiche aus der Perspektive des einzelnen sind. Der Datenschutz muß letztlich scheitern, wenn nicht in absehbarer Zeit über die allgemeinen Regeln hinaus gezielte Vorkehrungen für jedes dieser Gebiete getroffen werden.

7. Abgrenzung der Amtshilfe

Bereits die früheren Tätigkeitsberichte haben nachdrücklich gefordert, das Persönlichkeitsrecht der Bürger gegen einen ungehemmten Austausch von Informationen im Bereich der öffentlichen Verwaltung zu schützen. Im Hinblick darauf gilt es, Regelungen der Informationsweitergabe für die verschiedenen Verwaltungsbereiche auszuarbeiten, und zwar mit dem ausdrücklichen Ziel, die Amtshilfe zu kanalisieren, sie aber damit zugleich auch zu begrenzen.

Diese Forderung läßt sich allerdings nur erfüllen, wenn der Informationsfluß innerhalb der Administration offengelegt wird. Zugleich kommt es darauf an, die Interessen der jeweils Beteiligten genau zu ermitteln. Die angestrebten Regelungskriterien werden nur überzeugen können, wenn sie erkennen lassen, wie sich Datenschutz und öffentliche Aufgaben zueinander verhalten. Besondere Aufmerksamkeit ist deshalb der Frage nach dem optimalen Grad der Detailliertheit zu widmen.

8. Anonymisierung bei Datenbanken für statistische und planerische Zwecke

Vor allem bei Informationssystemen aus dem Bereich der Statistik und der Planung kommt es zu einem Zielkonflikt zwischen dem Persönlichkeitsrecht des Bürgers und dem Informationsinteresse der Öffentlichkeit. Einerseits muß die den Auskunftspersonen zugesagte Vertraulichkeit gewährleistet werden, andererseits sollen die gespeicherten Informationen allen Interessierten zur Verfügung stehen. Zu den sich aus dem Datenschutz ergebenden elementaren Anforderungen an Datenbanken für statistische und planerische Zwecke zählt eine Methode der Anonymisierung, die es den Benutzern ermöglicht, den Informationswert in Anspruch zu nehmen, zugleich aber Rückschlüsse auf Einzelpersonen ausschließt. Die Verwirklichung dieser Forderung setzt die Entwicklung geeigneter in Computer-Programme umzusetzender Verfahren voraus.

Wiesbaden, den 29. März 1976

Prof. Dr. S. Simitis

Anlage I

VORSCHLAG FÜR DIE NOVELLIERUNG DES DATENSCHUTZGESETZES

Auskunftsrecht und Wiedergutmachungsansprüche, Auskunfts- und Berichtigungsverpflichtete, Datenbankregister

1. § 4 des Datenschutzgesetzes vom 7. 10. 1970 – GVBl. I S. 625 – erhält folgende Fassung:

§ 4
Auskunftsrecht und Wiedergutmachungsansprüche

(1) Jedermann hat ein Recht auf Auskunft darüber, welche Einzelangaben über seine persönlichen oder sachlichen Verhältnisse (personenbezogene Daten) bei einer der in § 1 genannten Behörden oder Stellen in Unterlagen im Sinne des § 1 erfaßt sind oder maschinell verarbeitet werden und wohin sie übermittelt worden sind.

(2) Sind die personenbezogenen Daten in den Unterlagen, in den Datenspeichern oder in den Verarbeitungsergebnissen unrichtig, kann der Betroffene Berichtigung verlangen.

2. Abs. 2 und Abs. 3 des § 4 werden Abs. 3 und Abs. 4.

3. Nach § 4 werden folgende §§ 4 a und 4 b eingefügt:

§ 4 a
Auskunfts- und Berichtigungsverpflichtete

(1) Zur Auskunft und zur Berichtigung sind die in § 1 bezeichneten Behörden und Stellen verpflichtet, welche die Unterlagen erstellt haben, die Daten verarbeiten oder an welche personenbezogene Daten übermittelt worden sind. Dies gilt nicht für Behörden oder Stellen, welche die Erstellung der Unterlagen, die Verarbeitung oder die Übermittlung der Daten, auf die sich das Auskunfts- oder das Berichtigungsersuchen bezieht, lediglich als Dienstleistung im Auftrage anderer Behörden oder Stellen ausgeführt haben oder ausführen.

(2) Das Landesamt für Verfassungsschutz, das Landeskriminalamt und die Behörden der Kriminalpolizei des Landes können die Auskunft verweigern, sofern die Erfüllung ihrer Aufgaben durch die Erteilung der Auskunft gefährdet würde.

(3) Die Auskunft und die Berichtigung sind gebührenfrei. Eine kostendeckende Gebühr kann erhoben werden, wenn die personenbezogenen Daten, auf die sich das Auskunftsersuchen bezieht, vom Betroffenen unmittelbar erfragt worden waren oder wenn der Betroffene ihrer Erfassung oder maschinellen Verarbeitung ausdrücklich zugestimmt hatte.

(4) Vorhaltlich einer gesetzlichen Regelung bestimmt die Landesregierung die Voraussetzungen für die Verweigerung des Auskunftsrechts nach Abs. 2, für das Auskunftsverfahren, insbesondere die Form der Auskunft und für die Höhe der Gebühren durch Rechtsverordnung.

§ 4 b
Datenbankregister

(1) Alle in § 1 genannten Behörden oder Stellen, die personenbezogene Daten in Unterlagen im Sinne des § 1 erfaßt haben, speichern oder verarbeiten, und alle Behörden oder Stellen, an welche die Unterlagen, die Daten oder die Verarbeitungsergebnisse übermittelt werden, sowie die Arten der personenbezogenen Daten werden in ein Register aufgenommen.

(2) Das Register wird beim Datenschutzbeauftragten geführt. Es steht jedermann zur Einsicht offen. Eine Gebühr für die Einsicht wird nicht erhoben.

(3) Jede der in § 1 bezeichneten Behörden und Stellen hat für ihren Geschäftsbereich dem Datenschutzbeauftragten die für die Erstellung und für die Fortschreibung des Registers notwendigen Angaben zu machen.

(4) Der Datenschutzbeauftragte gibt aus dem Register auf Antrag schriftlich Auskunft, welche Arten personenbezogener Daten und bei welcher Behörde oder Stelle sie erfaßt sind, maschinell verarbeitet werden oder wohin sie übermittelt werden. Für die Auskunft kann eine gebührendeckende Gebühr erhoben werden.

(5) Die Landesregierung gibt die Eröffnung des Registers bekannt und regelt die Höhe der Gebühr durch Rechtsverordnung.

Anlage II

VORSCHLAG FÜR DIE NOVELLIERUNG DES DATENSCHUTZGESETZES

Bereich des Datenschutzes

1. § 1 des Datenschutzgesetzes vom 7. 10. 1970 – GVBl. I S. 625 – erhält folgende Fassung:

§ 1
Bereich des Datenschutzes

Der Datenschutz erfaßt alle für Zwecke der maschinellen Datenverarbeitung erstellten Unterlagen sowie alle gespeicherten Daten und die Ergebnisse ihrer Verarbeitung

1. im Bereich der Behörden des Landes und der der Aufsicht des Landes unterstehenden Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts,

2. im Bereich der juristischen Personen, Gesellschaften und anderen Personenvereinigungen des privaten Rechts, bei denen die unter Nummer 1 genannten Stellen einzeln oder gemeinsam die Mehrheit der Anteile innehaben oder die Mehrheit der Stimmen auf sich vereinigen,

3. im Bereich natürlicher Personen, juristischer Personen, Gesellschaften oder anderen Personenvereinigungen des privaten Rechts, wenn und soweit sie im Auftrag der unter Nummer 1 und 2 genannten öffentlichen Stellen, juristischen Personen, Gesellschaften oder anderen Personenvereinigungen des privaten Rechts Daten ermitteln, erfassen oder sonst verarbeiten

2. In § 5 Abs. 1, § 6 Abs. 2 Satz 1 und § 10 Abs. 2 Satz 1 wird hinter den Worten „in § 1" eingefügt „Nummer 1".

3. § 10 Abs. 1 wird wie folgt geändert:

Die Worte „durch die in § 1 genannten Stellen" werden ersetzt durch ein Komma und die Worte „in den Bereichen, auf die sich der Datenschutz nach § 1 erstreckt".

4. In § 11 werden die Worte „der in § 1 genannten Stellen" ersetzt durch die Worte „in den in § 1 genannten Bereichen".

5. § 13 wird wie folgt geändert:

Die Worte „alle in § 1 genannten Stellen haben" werden durch die Worte ersetzt „Jede öffentliche Stelle sowie jede juristische Person, Gesellschaft oder andere Personenvereinigung des privaten Rechts, hat in den Bereichen, auf die sich der Datenschutz nach § 1 erstreckt, . . ."

SACHWÖRTERVERZEICHNIS

(I, II, III, IV und V bezeichnen den Ersten, Zweiten, Dritten, Vierten bzw. Fünften Tätigkeitsbericht, die arabischen Ziffern die Abschnitte der Berichte; 1. Z bezeichnet den Zwischenbericht vom 6. 2.1976; s. bedeutet: siehe; s. a. bedeutet: siehe auch)