HESSISCHER LANDTAG

7. Wahlperiode . Drucksache 7/5146
01. 04. 74

Vorlage des Datenschutzbeauftragten
betreffend den Dritten Tätigkeitsbericht

Mit Schreiben vom 29. März 1974 legt der Datenschutzbeauftragte gemäß § 14 Abs. 1 des Datenschutzgesetzes vom 7. Oktober 1970 (GVBl. I S. 625) dem Landtag den folgenden Dritten Tätigkeitsbericht vor:

Eingegangen am 1. April 1974 . Ausgegeben am 12. Juni 1974

Druck: Carl Ritter & Co. Wiesbaden . Vertrieb: Verlag Dr. H. Heger 53 BN-Bad Godesberg Goethestr. 56 Tel. (0 22 21)/36 5 3 51

Dritter Tätigkeitsbericht

des

Hessischen Datenschutzbeauftragten

vorgelegt zum 31. März 1974

gemäß § 14 des Hessischen Datenschutzgesetzes vom 7. Oktober 1970

INHALTSVERZEICHNIS

		Seite
1.	**Allgemeine Erfahrungen aus dreijähriger Datenschutzpraxis**	7
1.1	Vorbemerkungen	7
1.2	EDV und Datenschutzverständnis in Bund und Ländern	7
1.2.1	Erfahrungen außerhalb der EDV	7
1.2.2	Umgang mit unbestätigten Informationen	8
1.3	Beobachtungen und Erkenntnisse	8
1.4	Neuregelungen in vorliegenden Gesetzentwürfen	9
1.5	Anpassung des Hessischen Datenschutzgesetzes	9
1.5.1	Geltungsbereich	10
1.5.2	Datenbankregister	11
1.5.3	Bereichsspezifische Regelungen	12
1.5.4	Verrechtlichung	12
1.5.5	Amtshilfe	12
1.5.6	Weitergabe außerhalb der Verwaltung	12
1.5.7	Zusammenarbeit zwischen Wissenschaft und Praxis	14
1.5.8	Ständiger Vorschlagswettbewerb: Datenschutz	15
2.	**Rechtliche Regelungen des Datenschutzes außerhalb Hessens**	17
2.1	Andere Länder – Überblick –	17
2.1.1	Schleswig-Holstein – Keine neuen Entwicklungen	17
2.1.2	Bayern – Keine neuen Entwicklungen	17
2.1.3	Rheinland-Pfalz	17
2.1.4	Niedersachsen	17
2.1.5	Baden-Württemberg – Keine neuen Entwicklungen	17
2.1.6	Nordrhein-Westfalen	17
2.1.7	Hamburg – Keine neuen Entwicklungen	18
2.1.8	Berlin	18
2.2	Gesetzgebungsstand im Bund	18
2.2.1 2.2.2	Bundesdatenschutzgesetz und Bundesmeldegesetz	18
2.2.3	Einführungsgesetz zum Strafgesetzbuch mit Verpflichtungsgesetz	19
2.3	Ausland	20
2.3.1	USA	20
2.3.1.1	Massachusetts	20
2.3.1.2	Georgia	20
2.3.2	Kanada	21
2.3.3	Großbritannien – Keine neuen Entwicklungen	21
2.3.4	Frankreich – Keine neuen Entwicklungen	21
2.3.5	Schweden	21
2.3.6	Dänemark	21
2.3.7	Österreich	21
2.3.8	Schweiz	21
2.3.9	Neuseeland	21
2.4	Tendenzen der Datenschutzgesetzgebung	22
2.5	Datenfernverarbeitung und Datenkommunikation	22

		Seite
3.	**Bestandsaufnahme**	23
4.	**Aufgaben und Tätigkeiten des Datenschutzbeauftragten**	25
4.1	Der Schutz des Persönlichkeitsrechts	25
4.1.1	Schutz medizinischer Daten	25
4.1.1.1	Krankenhauswesen	25
4.1.1.2	Krankentransport	26
4.1.1.3	Medizinische Datenbanken	26
4.1.2	Personaldatenbanken	27
4.1.3	Einwohnerwesen	27
4.1.4	Statistisches Landesamt und HZD	28
4.1.5	Besondere Informations-Systeme	29
4.1.5.1	Umgang mit Daten im Polizei-Informationssystem (HEPOLIS, INPOL)	29
4.1.5.2	Weitergabe von Informationen des Verfassungsschutzes	30
4.1.6	Datenschutz im Verhältnis zwischen Staat und Kirche	30
4.1.7	Richtlinien für Verfahrensentwicklung	30
4.2	Erhaltung der Gewaltenteilung	30
4.2.1	Parlamentarische Informationsrechte	30
4.2.2	Probleme der Verwirklichung	31
4.2.3	Statistische Veröffentlichungen und Parlament	32
4.3	Datensicherung	32
4.3.1	HZD und KGRZ	32
4.3.2	Außerhalb des Datenverarbeitungs-Verbundes	32
4.3.3	Weiterentwicklung von Kontrollverfahren	33
5.	**Anregungen**	33
5.1	Geltungsbereich des DSG und Service-Unternehmen	33
5.2	Weitergabeverbot	33
5.3	Konkretisierung des Amtshilfegebots	33
5.4	Verrechtlichung von Verwaltungsanordnungen	33
5.5	Umgang mit medizinischen Daten	34
5.6	Datenbankregister	34
5.7	Vorschlagswettbewerb Datenschutz	34
5.8	Zugriffsregelung für das Parlament	34
5.9	Vergabe von Forschungsaufträgen	34
6.	**Schlußbemerkungen**	35
	Sachwörterverzeichnis	37

Die beiden vorangegangenen Tätigkeitsberichte werden bei Hinweisen mit I und II benannt. Die nachfolgenden arabischen Ziffern bezeichnen den Abschnitt in dem entsprechenden Tätigkeitsbericht

1. ALLGEMEINE ERFAHRUNGEN AUS DREIJÄHRIGER DATENSCHUTZPRAXIS

1. Allgemeine Erfahrungen aus dreijähriger Datenschutzpraxis

1.1 Vorbemerkungen

Mehr als 3 Jahre sind seit dem Inkrafttreten des hessischen Datenschutzgesetzes und annähernd 3 Jahre seit der Aufnahme der Tätigkeit des Datenschutzbeauftragten vergangen. Dies gibt dem vorliegenden dritten Tätigkeitsbericht ein besonderes Gewicht. Er ist zwar erneut eine Fortschreibung der beiden bisher vorgelegten Berichte. Der Schwerpunkt hat sich jedoch verlagert. Im ersten Bericht wurde zunächst aufgezeigt, wie weit die elektronische Datenverarbeitung in der öffentlichen Verwaltung vorgedrungen ist, zu welchen Veränderungen des Verwaltungsablaufs sie geführt hat und welche Probleme für den Schutz des Persönlichkeitsrechts und die Wahrung des Informationsgleichgewichts sich daraus ergeben. Der zweite Tätigkeitsbericht konzentrierte sich auf die Erfahrungen, die der Datenschutzbeauftragte bei seiner Arbeit machen konnte. Zwar beschreibt auch der jetzt vorgelegte Bericht das weitere Vordringen der Datenverarbeitung in der öffentlichen Verwaltung und die gemachten Erfahrungen. Sein Schwergewicht ist aber stärker zukunftsorientiert. Deshalb faßt der Bericht in einer kritischen Betrachtung die Erkenntnisse und Erfahrungen – auch die in anderen Ländern – zusammen, die für den Aufbau und die Weiterentwicklung des Datenschutzes von wesentlicher Bedeutung sind, und prüft dann, welche Konsequenzen sich daraus für den Datenschutz in Hessen ergeben.

1.2 EDV und Datenschutzverständnis in Bund und Ländern

Der Aufbau von Datenbanken und Informationssystemen innerhalb der öffentlichen Verwaltung schreitet in Bund und Ländern fort, ohne daß die Öffentlichkeit davon viel Kenntnis nimmt. Der Bundesminister für Forschung und Technologie fördert verschiedene Forschungsvorhaben, die sich mit dem Einsatz und den Möglichkeiten der Datenverarbeitung befassen. Dazu gehört auch ein Projekt zur Erforschung der Probleme des Datenschutzes. Es handelt sich dabei um das Vorhaben DAMM („**Da**tenschutz-**M**ethoden und -**M**aßnahmen"), an dem auch das Land Hessen mitarbeitet.

Im allgemeinen aber muß man feststellen, daß Gesetzgebung und Verwaltung in Bund und Ländern den Problemen des Datenschutzes meist noch zu wenig Gewicht beimessen. Rationalisierung und Effektivität der Verwaltung haben Vorrang. Datenschutzfragen werden im allgemeinen nur als lästige Nebenverpflichtungen behandelt (vgl. II, 4.1.1.2). Auch bei den – z. Z. unterbrochenen – Vorarbeiten des Kooperationsausschusses ADV Bund/Länder/Gemeinden für ein Verwaltungsabkommen über Fragen der Datenverarbeitung war der Datenschutz nicht als ein der Datenverarbeitung inhärentes Problem behandelt, sondern nur an einer nachgeordneten Stelle der Entwurfsbegründung erwähnt worden.

In den Berichtszeitraum fiel die erste Lesung des Entwurfs eines Bundesdatenschutzgesetzes im Deutschen Bundestag. Darin werden die Probleme des Datenschutzes in der öffentlichen Verwaltung der Länder wegen der Kompetenzverteilung nur mit einigen Generalklauseln angesprochen. Die Rechtsverordnungs-Ermächtigung in § 4 Abs. 2 d. E. (deren Zulässigkeit allerdings verfassungsrechtlich umstritten ist) soll die Vereinheitlichung der Datenschutzmaßnahmen im Gebiet der Bundesrepublik Deutschland sicherstellen. Bei der konkreten Ausgestaltung dieser Maßnahmen könnten die Verwaltungserfahrungen in Bund und Ländern wertvolles Material darstellen. Denn die Erfahrungen der Praxis und das in den Verwaltungen anfallende Material sind eine wertvolle und unverzichtbare Erkenntnisquelle für Schwachstellen und Lücken in der jeweiligen Datenverarbeitungsorganisation und zeigen auf, wo und mit welchen Mitteln der Datenschutz ansetzen muß.

1.2.1 Erfahrungen außerhalb der EDV

Es liegt nahe, sich bei der Bekämpfung des Mißbrauchs personenbezogener Daten in der EDV auch an den Erfahrungen zu orientieren, die beim Umgang mit gewöhnlichen Karteien, Dateien, Personalakten usw. in der Vergangenheit gemacht wurden und auch jetzt noch gemacht werden. Als Illustration seien hier zwei Fälle wiedergegeben, die in der Berichtszeit öffentlich bekannt wurden.

a) Vor einem Frankfurter Arbeitsgericht wurde der Fall einer Sozialarbeiterin verhandelt, die nachträglich davon Kenntnis bekam, daß ihre bisherige Dienststelle ihrer Personalakte einen verschlossenen Umschlag mit der Aufschrift „Darf nur von einem Arzt geöffnet werden" beigefügt hatte. Dieser Umschlag enthielt die Diagnose einer Medizinalbeamtin, sie sei „nervlich labil". Da der Umschlag mit der Personalakte auch einem anderen Dienstherrn zugeleitet wurde, bei dem sich die Sozialarbeiterin beworben hatte, unterblieb zunächst die beabsichtigte Einstellung.

b) In dem anderen Fall handelt es sich um die Mitarbeiterin einer öffentlichen Klinik, die regelmäßig die Adressen von frisch eingelieferten Unfallpatienten ohne deren Wissen an einen Versicherungsvertreter gegen Entgelt weitergab.

Beide Vorfälle zeigen, daß schon manuell geführte Karteien Mißbrauchsmöglichkeiten eröffnen, wenn nicht ausreichende Sicherungs-

maßnahmen vorgesehen sind. Diese Gefahren gelten besonders für empfindliche Angaben (Krankheiten, Verdacht von Straftaten usw.), und sie werden vervielfacht, wenn die maschinelle Datenverarbeitung die Zusammenführung verschiedener Daten ermöglicht.

1.2.2 Umgang mit unbestätigten Informationen

Besonders Polizei und Verfassungsschutz sind bei ihrer Arbeit gezwungen, auch Informationen zu prüfen und zu verwerten, deren Richtigkeit nicht bestätigt ist. Deshalb muß auf jeden Fall sichergestellt sein, daß diese unbestätigten Informationen nicht in die Hände Unbefugter gelangen und so evtl. der Ruf unschuldiger Menschen geschädigt wird. In diesem Zusammenhang ist ein Urteil des Bundesverfassungsgerichts von Interesse, das dem Zweiten Deutschen Fernsehen untersagte, ein Dokumentarspiel über den Soldatenmord in Lebach auszustrahlen. In diesem Urteil*) ist nämlich ein Monitum enthalten, das sich auf den Umgang mit Polizei-Informationen bezieht. Es lautet: „Noch vor dem rechtskräftigen Abschluß des Strafverfahrens erschien ein vom Leiter der Hauptabteilung Dokumentarspiel des ZDF... und dem leitenden Kriminaldirektor beim Bundeskriminalamt ... unter Mitwirkung von... verfaßtes Buch über den Fall." Unter dem Gesichtspunkt des Schutzes des Persönlichkeitsrechts kann eine derartige Informationsverwendung nicht geduldet werden, weil dabei auch ungeprüfte, z. T. nur vermutete oder sogar falsche Informationen an die Öffentlichkeit gelangen können.

Was das für jeden einzelnen Bürger bedeutet, zeigt auch der bereits früher erschienene „Baader-Meinhof-Report". Dort werden mit dem Untertitel: „Auszug aus Akten des Bundeskriminalamtes, der Sonderkommission Bonn und des Bundesamtes für Verfassungsschutz" Informationen wiedergegeben, in denen namentlich genannte Personen nachgewiesenermaßen zu Unrecht in einen Zusammenhang mit Straftaten gebracht werden.

Ohne Zweifel liegt es auch und gerade im Interesse der mit der Verbrechensbekämpfung und Strafverfolgung befaßten Behörden, daß mit ihren Informationen kein Mißbrauch getrieben werden kann. Üblicherweise werden auch alle erforderlichen Vorkehrungen dazu getroffen. Es muß aber beunruhigen, daß anscheinend dann, wenn ein überragendes kommerzielles – oder auch ein entsprechendes politisch motiviertes – Interesse gegeben ist, diese Vorkehrungen durchbrochen werden können. Die Gefahr potenziert sich, wenn neben den Fahndungsdaten auch andere Polizei-Informationen in die automatische Datenverarbeitung übernommen werden und nicht gleichzeitig durch Rechtsnormen verbindlich geregelt wird, von wem, für wen und für welchen Zweck Informationen der Kriminalpolizei verwertet und verwendet werden. Die daraus folgenden organisatorischen und technischen Vorkehrungen einschließlich der fortlaufenden Protokollierung etc. müssen getroffen und ihre Einhaltung laufend überwacht werden (vgl. 4.1.6.1).

*) BVerfGE 35.202

1.3 **Beobachtungen und Erkenntnisse**

Ebenso wie im Bund und in den anderen Bundesländern nimmt auch in Hessen in der öffentlichen Verwaltung der Umfang der Datenverarbeitung rasch zu. Dabei wächst nicht so sehr die Zahl der Computer als vielmehr ihre Kapazität und die Zahl der ihnen zugeführten Aufgaben. Der Ausbau und die Integration von Spezialsystemen schreiten rasch fort. Auch die Vorbereitung eines integrierten Datenverarbeitungssystems der allgemeinen öffentlichen Verwaltung wird in der Planung vorangetrieben.

Einige Verwaltungen in Hessen scheinen das Gewicht der Datenschutzprobleme noch zu unterschätzen. So hatte eine Kreisverwaltung die vom Datenschutzbeauftragten nach § 10 DSG geforderte Auskunft im Zusammenhang mit der von ihr veranlaßten Befragungsaktion eines wissenschaftlichen Instituts trotz mehrfachen Mahnens nach über dreimonatiger Frist noch nicht beantwortet. Bei den unmittelbar für den Umgang mit personenbezogenen Daten Verantwortlichen und ihren Mitarbeitern ist aber erfreulicherweise wachsendes Verständnis für die Bedeutung des Datenschutzes festzustellen. Das gilt besonders für den Bereich der Universitäten (vgl. 4.3.2). Aber auch die anderen datenverarbeitenden Stellen sind um Datenschutz bemüht und suchten vermehrt den Gedankenaustausch mit dem Datenschutzbeauftragten.

Bei den Massenmedien, beim Fernsehen und beim Rundfunk, bei den Fachzeitschriften und bei den Tageszeitungen wächst ebenfalls das Interesse für den Datenschutz. Er war Thema einer großen Zahl von Berichten und kritischen Untersuchungen. Immer wieder wurde auch der Datenschutzbeauftragte von Verbänden, Institutionen und Zeitungen aufgefordert, über seine Tätigkeit und Erfahrungen in Vorträgen, Interviews oder Artikeln zu berichten.

Nicht uninteressant ist ferner, daß die Evangelische Kirche von Hessen und Nassau im Juli 1973 eine Datenschutzverordnung beschlossen hat, in der sie verschiedene Bestimmungen aus dem Entwurf des Bundesdatenschutzgesetzes und aus dem hessischen Datenschutzgesetz übernommen hat.

Verstärktes Interesse für Fragen des Datenschutzes zeigen seit einiger Zeit auch die Hersteller der Hard- und Software. Sie erwarten offensichtlich, daß eine Reihe von technischen und organisatorischen Regelungen für den Umgang mit personenbezogenen Daten in dem Entwurf des Bundesdatenschutzgesetzes in der weiteren parlamentarischen Behandlung keine größeren Abänderungen mehr erfährt und stellen sich darauf ein. Mit den ersten Vorarbeiten, der Untersuchung der Auswirkungen des erwarteten Gesetzes auf die Datenverarbeitung und mit den Überlegungen über die technischen und organisatorischen Konsequenzen, ist bereits begonnen worden. Die Hersteller wollen einmal ihren Kunden die von diesen geforderte Sicherheit bieten. Zum anderen haben sie erkannt, daß sich ihnen hier ein neuer Markt öffnet. Sie entwickeln bereits – analog der Umweltschutz-Technologie – eine spezielle Datenschutz-Technologie, die für die Datensicherung, aber auch für die Arbeit des Datenschutzbeauftragten bedeutsam ist und über deren Fortschreiten er sich laufend informiert.

Das zunehmende Interesse an Datenschutzfragen konzentriert sich zwar vorwiegend auf den Schutz des Persönlichkeitsrechts, der Privatsphäre, es beschränkt sich aber nicht darauf. Die Gefahr der Machtkonzentration, die Gefährdung des Informationsgleichgewichts und ihre Auswirkungen auf die freiheitlich-demokratische Ordnung finden neuerdings ebenfalls größere Beachtung. Die Informationsrechte des Parlaments wurden in dem im Berichtszeitraum verabschiedeten Landesdatenschutzgesetz für Rheinland-Pfalz und in dem ADV-Organisationsgesetz des Landes Nordrhein-Westfalen geregelt (vgl. 2.1.3 und 2.1.6). Auch der Berliner Entwurf eines Datenschutzgesetzes behandelt die Frage des Informationsgleichgewichts (vgl. 2.1.8). Eine vergleichbare Regelung sieht ebenfalls die Datenschutz-Gesetzesvorlage eines Schweizer Kantons vor (vgl. 2.3.8).

Im Berichtszeitraum wurde der Datenschutzbeauftragte mehr als in den früheren Jahren von Personen angerufen, die sich durch die Datenverarbeitung in ihren Rechten verletzt fühlten (§ 11 DSG). Die Zahl der Zuschriften ist aber noch immer nicht groß. In einigen Fällen glaubten die Verfasser, der Datenschutzbeauftragte verfüge selbst über Datenbanken mit personenbezogenen Daten. Das Mißverständnis wurde geklärt. Bei anderen Eingaben wurde die Überprüfung durch die betroffenen Verwaltungsstellen veranlaßt. Mehrfach mußte sich der Datenschutzbeauftragte für nicht zuständig erklären, weil es sich um die Datenverarbeitung von Stellen handelte, die nicht vom Datenschutzgesetz erfaßt werden. Viele der geschilderten Vorgänge unterstreichen aber, daß immer mehr Bürger sich durch häufige Auskunftsersuchen für statistische, planerische oder auch gewerbliche Zwecke belästigt fühlen (vgl. 2.1.5.1). Verschiedentlich wird dabei die Frage aufgeworfen, ob wirklich sichergestellt sei, daß diese Informationen nicht auch für andere als die angegebenen Zwecke Verwendung finden. Mehrfach zeigte sich, daß Adressenkarteien nach Gesichtspunkten ausgewertet werden, die den Betroffenen Anlaß zu Beanstandungen gaben.

In einem Fall berichtete ein Rechenzentrum dem Datenschutzbeauftragten, daß eine Privatperson versucht habe, durch Bestechung personenbezogene Daten aus einer Datei der öffentlichen Verwaltung zu erhalten (vgl. 4.3.1).

Die Aufgabe des Datenschutzbeauftragten beschränkt sich nicht darauf, eventuellen Verstößen nachzugehen. Er muß seine Aufmerksamkeit vor allem darauf richten, erkennbaren oder vermuteten Gefahren entgegenzuwirken. Diese Arbeit würde wesentlich erleichtert, wenn über eingetretene Gefährdungen oder Mißbräuche durch die öffentlichen und privaten Stellen besser als bisher berichtet würde. Es ist bekannt, daß im Bereich der privaten Wirtschaft die Dunkelziffer über Computermißbrauch verhältnismäßig hoch ist. Viele der betroffenen Unternehmen verschweigen derartige Vorfälle, weil sie befürchten, man könne sie nicht mehr für sicher und zuverlässig halten.

Aber auch aus der öffentlichen Verwaltung außerhalb Hessens sind zwei Fälle von „Computer-Kriminalität" bekanntgeworden. In einer bayerischen Verwaltungsdienststelle ließen sich zwei Bedienstete mit Hilfe gefälschter Lochkarten „Kindergeld"-Beträge in Höhe von 250 000,- D-Mark auszahlen. Das bayerische Justizministerium berichtete über diesen Fall bei der Beantwortung einer schriftlichen Anfrage vom 10. Dez. 1973 (Drucks. 7/5577) dem Landtag: „In dem Strafverfahren, das ein Vergehen im Bereich der Verwaltung zum Gegenstand hatte, wurde der Haupttäter zu einer Freiheitsstrafe von 3 Jahren ... verurteilt." In Hamburg hatte ein Operator im Zusammenhang mit Spielschulden versucht, die Daten über die Straftaten verschiedener Personen zu löschen („Hamburger Morgenpost" vom 19. 2. 1974). Der Täter wurde fristlos entlassen.

Der Datenschutzbeauftragte erfuhr von beiden Fällen aufgrund gezielter Nachfragen. Um wirksam überwachen zu können, ob die getroffenen Datenschutzmaßnahmen ausreichen und ob sie präventiv wirken, sollten alle derartigen Verstöße sorgfältig überprüft und für den Datenschutz ausgewertet werden. Der Datenschutzbeauftragte wird von den hessischen Behörden und Stellen informiert, wenn dort derartige Vorfälle festgestellt werden. Es wäre aber wünschenswert, wenn Bund und Länder einen Erfahrungsaustausch auf diesem Gebiet eröffneten, damit die in den Ländern gemachten Erfahrungen und Erkenntnisse von allen genutzt werden könnten.

1.4 Neuregelungen in vorliegenden Gesetzentwürfen

Das hessische Datenschutzgesetz, das als erstes verkündet worden ist, stellte für fast alle nachfolgenden Gesetze oder Gesetzentwürfe in den anderen Ländern ein Modell dar. Dies gilt – abgesehen von teilweise wörtlich übernommenen Formulierungen – vor allem für das Prinzip der Fremdkontrolle durch eine unabhängige Institution und für die Methode, den Datenschutz als ein System vornehmlich rechtlich verordneter Schutzmaßnahmen organisatorischer, personeller und technischer Art zu begreifen, die sich der jeweiligen Phase der Datenverarbeitung und ihrer Entwicklung anpassen können. Im Gegensatz hierzu steht allerdings der Regierungsentwurf eines Bundesdatenschutzgesetzes (vgl. 2.2.1). Er versteht unter Datenschutz nicht nur besondere, die Datenverarbeitung flankierende Maßnahmen, sondern knüpft auch die Sammlung und Verarbeitung von Informationen in Form von Daten an bestimmte Zulässigkeitsvoraussetzungen. Damit werden die Möglichkeiten der Datenverarbeitung rechtlich begrenzt. In dieser Weise geht auch ein niedersächsischer Referentenentwurf vor, der das Bundesdatenschutzgesetz als Ganzes in Landesrecht transformieren will (vgl. 2.1.4).

1.5 Anpassung des hessischen Datenschutzgesetzes

Der Bund und die anderen Länder, soweit sie bereits Datenschutzgesetze erlassen haben oder vorbereiten, haben sich jedoch die zahlreichen, inzwischen publizierten Erkenntnisse der Rechtsinformatik, der Rechtswissenschaft, der Soziologie und der Technologie zu eigen gemacht und die übernommenen Grundgedanken des hessischen Datenschutzgesetzes mit einem Instrumentarium einzelner, dem Datenschutz dienender Einrichtungen angereichert.

Während in den anderen Ländern zunächst der Gesetzgeber bemüht wird, diese Datenschutzmaßnahmen festzuschreiben, wird in Hessen der Datenschutz von den Verwaltungen im Benehmen mit dem Datenschutzbeauftragten praktiziert. Unter Zugrundelegung des Datenschutzgesetzes werden diejenigen organisatorischen, technischen und personellen Vorkehrungen (§ 2 DSG) getroffen oder in neuen Automationsvorhaben vorgesehen, die bei der Verwaltungsautomation zum Schutze des Persönlichkeitsrechts des Bürgers geboten sind. Dabei ist man bestrebt, auch die praktischen Erfahrungen und die wissenschaftlichen Erkenntnisse zu verwerten, die seit dem Erlaß des Gesetzes am 7. 10. 1970 hinzugekommen sind. Dieser Entwicklung sollte das Gesetz jetzt angepaßt werden, damit die Rechtsstellung des Bürgers abgesichert ist. Hierzu gehören vor allem die gesetzliche Normierung eines Auskunftsrechts, des Anspruchs auf Löschung – nicht nur auf Berichtigung – unrichtiger oder unzulässig gespeicherter Daten, die Benachrichtigungspflicht der speichernden Behörde über die erstmalige, ohne Kenntnis des Betroffenen vorgenommene Erfassung personenbezogener Daten, und die Verpflichtung der datenverarbeitenden Behörde, die Datenverarbeitungsvorgänge zu protokollieren, damit die Verwendung der Daten kontrollierbar ist. Solche Rechte und Pflichten sind im Entwurf des Bundesdatenschutzgesetzes und in einigen Landesgesetzen und Gesetzentwürfen geregelt.

1.5.1 Geltungsbereich

Nach den Erfahrungen im Berichtszeitraum verschärft sich auch das Problem, das im zweiten Tätigkeitsbericht unter 4.1.3 erörtert ist. Der Wirkungsbereich des Datenschutzbeauftragten nach § 10 Abs. 1 ist durch die Verweisung auf § 1 DSG in einer Weise begrenzt, die mit den Praktiken der öffentlichen Verwaltung nicht übereinstimmt. In zunehmendem Maße überträgt die öffentliche Verwaltung die Durchführung ihrer Aufgaben auf Organisationen des Privatrechts, die entweder schon vorhanden sind oder für diese Zwecke errichtet werden.

a) Zu den im zweiten Tätigkeitsbericht genannten privatrechtlichen Gesellschaften ist das „Rechenzentrum der hessischen Sparkassenorganisation" hinzugetreten, das als Gesellschaft mit beschränkter Haftung von der Hessischen Landesbank und dem Sparkassen- und Giroverband gegründet worden ist. Dieses Rechenzentrum ist wegen seiner privatrechtlichen Organisationsform der Überwachung durch den Hessischen Datenschutzbeauftragten entzogen.

b) In einem anderen Fall – auf den der Datenschutzbeauftragte durch einen Bürger hingewiesen wurde – handelt es sich um den privatrechtlich organisierten Verkehrsverbund im Rhein-Main-Gebiet. Dieser Verbund fordert jeden, der bei ihm eine „Kundenkarte" (Zeitkarte) beantragt, auf, einen Fragebogen mit 98 Fragen auszufüllen. Gefragt wird dabei u. a. nach dem Familienstand (verh., ledig, geschieden), dem Schulabschluß, dem Beruf, Namen und Art des Arbeitsbetriebs, Anzahl der Haushaltsmitglieder usw. Diese Informationen, die zur Privatsphäre gehören, werden namentlich erfaßt. Die vertrauliche Behandlung der Angaben wird zwar zugesagt. Es fehlt aber dafür die rechtliche Grundlage und damit die Verbindlichkeit. Der Antragsteller wird aufgefordert, den Bogen „vollständig" auszufüllen. Auf die Freiwilligkeit der Beantwortung wird er nicht hingewiesen, obwohl sie vorausgesetzt werden muß. Der Bürger ist sich dessen aber im allgemeinen nicht bewußt. Der Verbund kann sich deshalb nicht auf diese Freiwilligkeit berufen, weil viele Bürger glauben, sie müßten alle Fragen beantworten, wenn sie eine Kundenkarte erhalten wollen. Und selbst wenn der Bürger erkennt, daß er dazu nicht gezwungen werden kann, so wird er doch meist einem eventuellen Streit aus dem Wege gehen wollen, weil er befürchtet, daß er sonst Nachteile in Kauf nehmen müsse. Bei einer großen Zahl der 98 Fragen ist Zweifel angebracht, ob sie als Angaben für die Verkehrsplanung erforderlich sind, z. B. die Frage, ob der Verkehrsteilnehmer geschieden ist, welchen Schulabschluß er hat, wie groß sein Haushalt ist. Aber auch bei Fragen, die für die Verkehrsplanung wünschenswert oder notwendig sind, die aber gleichzeitig die Privatsphäre berühren, sollten die Antworten nicht personenbezogen, sondern anonym – auf getrennten Formblättern – erfaßt werden. Denn für die Verkehrsplanung werden Sammeldaten und nicht personenbezogene Daten benötigt.

c) Ferner ist dem Datenschutzbeauftragten bekanntgeworden, daß eine hessische Stadt einer Gesellschaft des bürgerlichen Rechts den Auftrag gegeben hat, die Möglichkeit einer späteren Sanierung eines Ortsteiles durch Befragung der von dem städtebaulichen Entwicklungsplan betroffenen Bürger und durch Auswertung ihrer Antworten zu untersuchen. Der hierfür vorliegende Fragebogen, den die privatrechtliche Gesellschaft entworfen hat, enthält eine Fülle von weit in den Privatbereich eindringenden Fragen, wie z. B. Schulabschluß, ungefähre *Höhe des* monatlichen Einkommens des Haushaltsvorstandes und des gesamten Haushaltes, Anschriften der Freunde und Bekannten, Mitgliedschaft in Vereinen. In einem Vorwort zum Fragebogen wird der Bürger über den Zweck der Befragung unterrichtet; er wird darüber aufgeklärt, daß seine Antworten „streng vertraulich" behandelt werden, „ausschließlich planerischen Zwecken" dienen, dem Datenschutz unterliegen und – etwas verklausuliert – daß seine Angaben freiwillig sind. Schließlich wird versichert, daß weder andere Ämter (z. B. das Finanzamt) noch Privatpersonen von den Antworten Kenntnis erhalten und daß alle an der Untersuchung Beteiligten zu strenger Verschwiegenheit verpflichtet sind.

Diese ausführliche Unterrichtung des betroffenen Bürgers ist ein gutes Vorbild für vergleichbare Befragungen, die von der öffentlichen Verwaltung unmittelbar veranstaltet werden. Unsicher ist aber auch hier die rechtliche Grundlage der darin enthaltenen Versprechungen.

Die Frage lautet, ob Unterlagen, Daten und Datenverarbeitungsergebnisse vom Datenschutz

nach § 1 DSG auch dann erfaßt werden, wenn die Ermittlung und die Verarbeitung der Informationen nicht von der öffentlichen Verwaltung, sondern in ihrem Auftrage von privatrechtlichen Unternehmen durchgeführt werden. Diese Frage sollte bejaht werden, weil es der Zweck des Gesetzes ist, den Datenschutz schlechthin auf die Datenverarbeitung im Bereich der öffentlichen Verwaltung zu erstrecken, auch wenn sich die zuständige Behörde dabei eines privatrechtlich organisierten Erfüllungsgehilfen bedient.

In diesem Sinne ist das Problem in § 5 Abs. 3 Satz 1 d.E. eines Bundesdatenschutzgesetzes geregelt. Eine solche – hier für erforderlich gehaltene – Klarstellung im hessischen Datenschutzgesetz müßte gleichzeitig die Überwachungsbefugnisse des Datenschutzbeauftragten nach § 10 Abs. 1 Satz 1 DSG erweitern.

1.5.2 Datenbankregister

Die steigende Zahl von Befragungsaktionen amtlicher, halbamtlicher und privater Stellen für die unterschiedlichsten Zwecke läßt in der Bevölkerung die Furcht vor einer totalen Kontrolle wachsen. Nicht zu Unrecht fragt man sich, wofür die einzelnen Angaben benötigt und ob sie nicht auch für andere als die genannten Zwecke verwendet und dabei mit den Informationen anderer Stellen zusammengeführt werden. Es fehlt dem Bürger der Überblick, welche Stellen für welche Zwecke Daten speichern. Dies führt zu einem allgemeinen Unbehagen gegen alle mit der Erfassung personenbezogener Daten zusammenhängenden Maßnahmen. Dieses Unbehagen wird von interessierter Seite offensichtlich bewußt geschürt, um die staatliche Verwaltung in ihrer Arbeit zu behindern.

So wurde von der angeblichen „Bundesanstalt für datenmäßige Personenerfassung in Bonn, NATO-Weg 15/08“ ein Fragebogen verschickt, der mit seinen aggressiven, z. T. weit in die Intimsphäre reichenden, z. T. auch unsinnigen Fragen offenbar in der Bevölkerung ein Unbehagen gegen das Personenkennzeichen hervorrufen und den Eindruck erwecken will, daß mit der Vergabe des Personenkennzeichens politische Zwecke verfolgt werden.

Für die Gesetzgebung und die Verwaltung ergibt sich daraus die Notwendigkeit, bei der Ermittlung personenbezogener Daten zu statistischen Zwecken oder für andere Aufgaben, in allgemeinverständlicher Weise zu begründen, welchem Zweck die Datenermittlung dienen soll und weshalb sie erforderlich ist. Ein Register sollte dem Bürger die Möglichkeit geben, aus der verwirrenden Vielzahl von Behörden und Stellen der öffentlichen Verwaltung diejenige herauszufinden, von der er die gewünschte Auskunft über die Speicherung und Weitergabe seiner Individualdaten erhalten kann.

Der Datenschutzbeauftragte hat mit den Vorarbeiten für das im zweiten Tätigkeitsbericht (II, 2.4.5) beschriebene Datenbankregister begonnen, das der Realisierung eines dem Bürger zu gewährenden Auskunftsrechts dienen soll. Die ihm vorgelegten Erfassungsbögen sollen für ein Register ausgewertet werden, über das der Bürger auf Verlangen Auskunft darüber erhält, welche Datenarten oder Datengruppen von welchen Behörden oder Stellen erfaßt werden. Dieses Register würde auch erkennbar machen, welche Behörden oder Stellen dieselben Daten erfassen, wo also eine Mehrfachbefragung des Bürgers stattfindet. Das nachfolgende Schaubild (s. nächste Seite) zeigt 55 der über 300 bekannten Datenarten und 14 Gruppen von Informationsempfängern, die insgesamt viele hundert Behörden oder Stellen im Sinne des § 1 DSG repräsentieren.

Damit das Register auf dem laufenden gehalten werden kann, müssen alle Behörden und Stellen, die Daten verarbeiten, angewiesen werden, den Datenschutzbeauftragten ständig über die Errichtung neuer Datenbanken und die Speicherung neuer Datenarten zu unterrichten. Der Datenschutzbeauftragte hat daher in den Ausschüssen der Verwaltung angeregt, schon bei der Entwicklung der Automationsverfahren die Informationsbedürfnisse des Datenschutzbeauftragen zu berücksichtigen (vgl. 4.1.7).

Einwohnerwesen

Vergabe und Verwaltung des Peronenkennzeichens,
Aufbau und Verwaltung der Einwohnerdatenbank,
Melderegister,
Erstellung der Lohnsteuerkarten,
Wehrerfassung,
Wählerverzeichnis,
Impflisten,
Schulanfängerlisten,
Einwohnerstatistik.

Finanzwesen

Feststellen von Übersichten bei der Aufstellung des Haushaltsplans,
Kontrolle des Planablaufes,
Abschlüsse der Finanzkassen,
Rechnungslegung,
Einkommensteuer,
Lohnsteuerjahresausgleich,
Gewerbesteurmeßbetragsfestsetzung,
Umsatzsteuer,
Vermögensteuer,
Einheitsbewertung,
Kommunaler Finanzausgleich.

Personalwesen

Beamtenbesoldung und -versorgung,
Angestelltenvergütung,
Arbeiterlöhne.

Gesundheitswesen

Leistungserfassung und Abrechnung für stationäre Patienten im Krankenhaus,
Krankentransport,
Statistik über Krebserkrankungen.

Sozialwesen

Berechnung und Zahlbarmachung von Renten nach dem BEG,
Kriegsschadenrente,
Statistik des Lastenausgleichs,
Rentenauskunftsverfahren.

Bildungswesen

Bewilligung, Berechnung und Zahlbarmachung der Leistungen nach dem Ausbildungsförderungsgesetz,
Lehrerdatei,
Schülerdatei.

Öffentliche Sicherheit und Ordnung

Verkehrsordnungswidrigkeiten.

Rechtswesen

Grundbuchwesen.

Wirtschaftliche Unternehmen, Landwirtschaft und Forsten

Festsetzung und Zahlbarmachung der Verbilligung nach dem Gasölverwendungsgesetz,
Flächenstandsfortschreibung der Revierförstereien,
Holzwerbungskosten und Stücklohnberechnung,
Forstschutzstatistik.

Technik

(Hier von 38 Teilaufgaben nur ein kleiner Ausschnitt, da die technischen Aufgaben wenig personenbezogen sind, z. B.):

Berechnungen im Rahmen von verkehrswirtschaftlichen Untersuchungen,
Vermessungen bei der Einrichtung des Liegenschaftskatasters und der Flurbereinigung,
Aufstellung des Katasterbuchwerkes,
Statische Berechnungen,
Zeichnen von Katasterkarten,
usw.

Über alle Arbeiten, die sich auf die Automation der vorgenannten Aufgaben beziehen, hat sich der Datenschutzbeauftragte informiert. Er nahm an zahlreichen Besprechungen und Ausschußsitzungen teil, in denen die vorgesehenen Schutzmaßnahmen behandelt wurden, und stellte dort seine Anregungen zur Diskussion.

Durch die laufende Unterrichtung wird sichergestellt, daß der Datenschutzbeauftragte in jedem Stadium der Entwicklung auf die unmittelbare Anpassung der Schutzmaßnahmen an die technische Entwicklung (Integration und Datenfernverarbeitung) einwirken kann.

(Siehe Tabelle auf Seite 13)

1.5.3 Bereichsspezifische Regelungen

Die verschiedenen, teilweise auch kontroversen Stellungnahmen zum Entwurf eines Bundesdatenschutzgesetzes stimmen weitgehend darin überein, daß für die verschiedenen Lebensbereiche spezielle Datenschutzvorschriften getroffen werden müssen, weil eine alle Bereiche umfassende Generalklausel keinen hinreichenden und befriedigenden Schutz gewährt. Inzwischen hat Hessen mit den Vorschriften der §§ 13, 14 des Krankenhausgesetzes einen ersten Schritt auf diesem Weg getan. Über die Realisierung der dort normierten Grundsätze und ihre Auswirkungen auf benachbarte Bereiche der Verwaltung wird unter 4.1.1.1 berichtet.

1.5.4 Verrechtlichung

Die Anregung im zweiten Tätigkeitsbericht (II, 5.3), die Befugnis zur Weitergabe und zur Verwendung „empfindlicher" personenbezogener Daten im Bereiche des Landeskriminalamtes und des Verfassungsschutzamtes zu verrechtlichen, d. h. durch Rechtsvorschriften einzugrenzen, muß wiederholt werden (vgl. unten 4.1.6.1 und 2.).

1.5.5 Amtshilfe

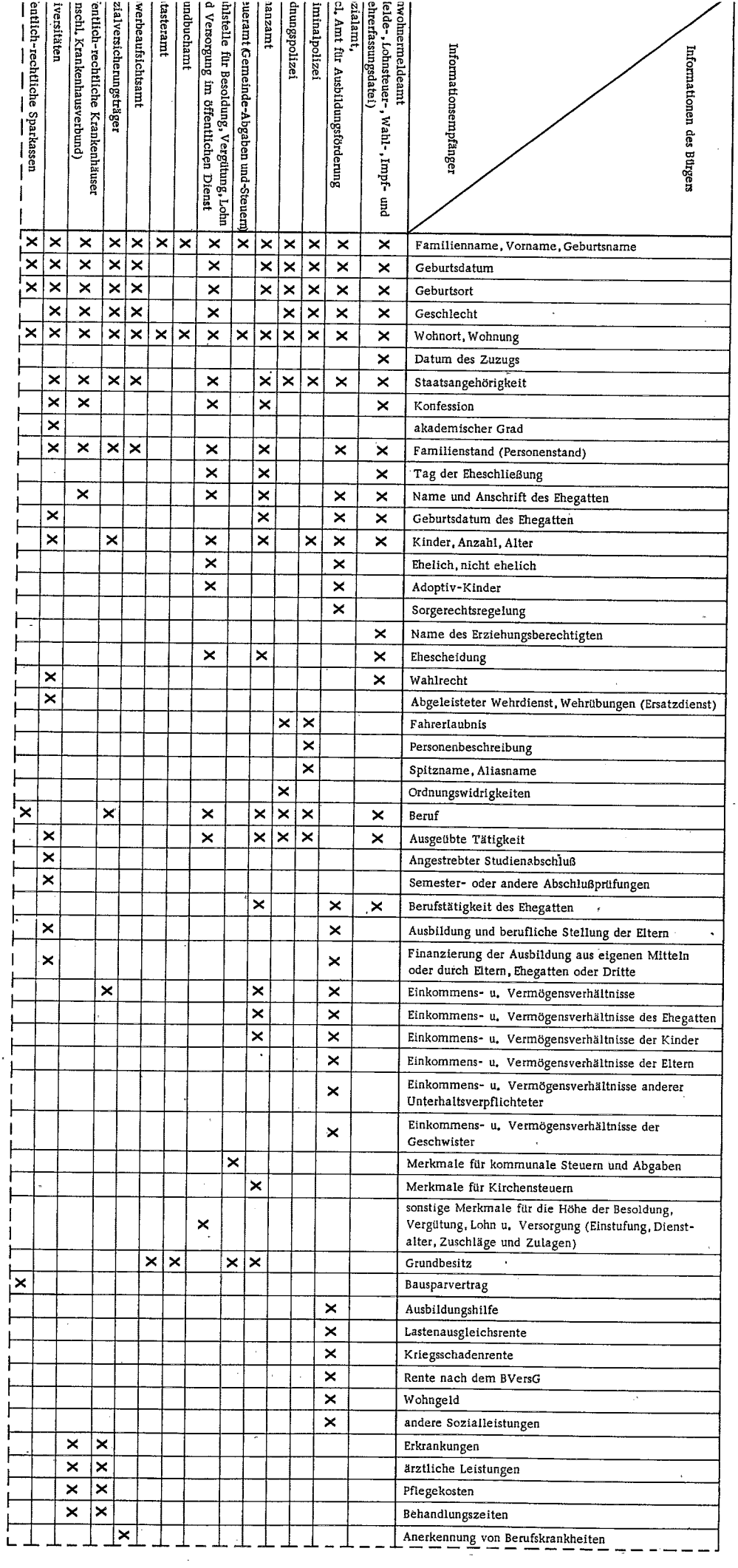
Im Zusammenhang hiermit stehen die Probleme, die sich aus der bislang undifferenzierten und nur teilweise und unzulänglich geregelten Amtshilfeverpflichtung im Bereich der öffentlichen Verwaltung ergeben (vgl. II, 4.1.1.1 b).

In der bisherigen Verwaltungspraxis spielen die schutzwürdigen Belange des Bürgers nur eine nachrangige Rolle. Das wird auch durch den Entwurf des Bundesdatenschutzgesetzes (s. § 8 Abs. 1) nicht geändert. Die Zulässigkeit, innerhalb des öffentlichen Bereiches personenbezogene Daten zu speichern und weiterzugeben, hängt allein davon ab, ob dies zur Erfüllung der Verwaltungsaufgabe erforderlich ist. Weder die Gesetzgeber noch die Verwaltungen haben die notwendigen Folgerungen aus der hierfür grundlegenden Entscheidung des Bundesverfassungsgerichts gezogen, die anläßlich der Überlassung gerichtlicher Ehescheidungsakten an eine Disziplinarbehörde zum Schutze des Persönlichkeitsrechts aufgestellt worden sind (vgl. II, 4.1.1 b). Zwar ist der strafrechtliche Schutz „des persönlichen Lebens- und Geheimbereichs" in der Neufassung des Strafgesetzbuches verbessert und durch das „Verpflichtungsgesetz" der Kreis der Personen erweitert worden, die – ohne Beamte zu sein – zur Geheimhaltung mit der Maßgabe verpflichtet werden können, daß die unbefugte Offenbarung von im Dienst erworbenen Kenntnissen bestraft wird. Für diesen Personenkreis, für die Amtsträger und für weitere Personengruppen gilt die Strafandrohung des neugefaßten § 203 StGB auch dann, wenn sie kein fremdes materielles Geheimnis, sondern schlechthin solche Einzelangaben über persönliche oder sachliche Verhältnisse eines anderen offenbaren, die für Aufgaben der öffentlichen Verwaltung erfaßt worden sind. Die Amtshilfe, d. h. die Weitergabe solcher Einzelangaben an andere Behörden oder Stellen für Aufgaben der öffentlichen Verwaltung, hat der Gesetzgeber jedoch von diesem Straftatbestand ausgenommen.

Auf hessischen Antrag hat der Bundesrat bei der Verabschiedung des das Strafgesetzbuch novellierenden Gesetzes die Bundesregierung ersucht, zu prüfen, ob die hier zitierte Regelung „nicht auf einigen Gebieten, z. B. auf dem Gebiet der Statistik, zu einem unerwünschten Abbau des strafrechtlichen Schutzes der Geheimsphäre führt" (vgl. auch 2.2.3).

1.5.6 Weitergabe außerhalb der Verwaltung

Die Verpflichtung der öffentlichen Verwaltung, den Datenschutz im Sinne des § 2 DSG sicherzustellen, gewinnt in zunehmendem Maße auch außerhalb der Amtshilfe im Bereich der öffentlichen Verwaltung an Bedeutung. Im Berichts-


Informationsempfänger
Informationen des Bürgers
nwohnermeldeamt
elde-, Lohnsteuer-, Wahl-, Impf- und
ehrerfassungsdatei)
ziamt,
el, Amt für Ausbildungsförderung
iminalpolizei
dnungspolizei
anzamt
ueramt (Gemeinde-Abgaben und -Steuern)
hlstelle für Besoldung, Vergütung, Lohn
d Versorgung im öffentlichen Dienst
undbuchamt
tasteramt
werbeaufsichtsamt
ziale Versicherungsträger
entlich-rechtliche Krankenhäuser
nschl. Krankenhausverbund)
iversitäten
entlich-rechtliche Sparkassen
Familienname, Vorname, Geburtsname
Geburtsdatum
Geburtsort
Geschlecht
Wohnort, Wohnung
Datum des Zuzugs
Staatsangehörigkeit
Konfession
akademischer Grad
Familienstand (Personenstand)
Tag der Eheschließung
Name und Anschrift des Ehegatten
Geburtsdatum des Ehegatten
Kinder, Anzahl, Alter
Ehelich, nicht ehelich
Adoptiv-Kinder
Sorgerechtsregelung
Name des Erziehungsberechtigten
Ehescheidung
Wahlrecht
Abgeleisteter Wehrdienst, Wehrübungen (Ersatzdienst)
Fahrerlaubnis
Personenbeschreibung
Spitzname, Aliasname
Ordnungswidrigkeiten
Beruf
Ausgeübte Tätigkeit
Angestrebter Studienabschluß
Semester- oder andere Abschlußprüfungen
Berufstätigkeit des Ehegatten
Ausbildung und berufliche Stellung der Eltern
Finanzierung der Ausbildung aus eigenen Mitteln oder durch Eltern, Ehegatten oder Dritte
Einkommens- u. Vermögensverhältnisse
Einkommens- u. Vermögensverhältnisse des Ehegatten
Einkommens- u. Vermögensverhältnisse der Kinder
Einkommens- u. Vermögensverhältnisse der Eltern
Einkommens- u. Vermögensverhältnisse anderer Unterhaltsverpflichteter
Einkommens- u. Vermögensverhältnisse der Geschwister
Merkmale für kommunale Steuern und Abgaben
Merkmale für Kirchensteuern
sonstige Merkmale für die Höhe der Besoldung, Vergütung, Lohn u. Versorgung (Einstufung, Dienstalter, Zuschläge und Zulagen)
Grundbesitz
Bausparvertrag
Ausbildungshilfe
Lastenausgleichsrente
Kriegsschadenrente
Rente nach dem BVersG
Wohngeld
andere Sozialleistungen
Erkrankungen
ärztliche Leistungen
Pflegekosten
Behandlungszeiten
Anerkennung von Berufskrankheiten

jahr sind verschiedene Fälle bekanntgeworden, in denen Behörden – vornehmlich der Kommunalverwaltung – Sammelauskünfte aus den gespeicherten Daten an Dritte, d. h. an Personen oder Stellen außerhalb der öffentlichen Verwaltung auf deren Verlangen und für deren Interessen, weitergegeben haben.

Die Bereitschaft, ohne größere Bedenken diese Wünsche zu erfüllen, läßt vermuten, daß nur ein Bruchteil aller Fälle bekanntgeworden ist und daß es hier eine hohe Dunkelziffer gibt.

Gegen diese Praxis bestehen ernsthafte Bedenken. Der Bürger gibt der öffentlichen Verwaltung Auskünfte über seine Person und seine persönlichen Verhältnisse, damit sie befähigt wird, bestimmte, ihr obliegende öffentliche Aufgaben zu erfüllen. Die Weitergabe der in dieser Weise erlangten Informationen an Personen und Stellen außerhalb der öffentlichen Verwaltung stellt in weit höherem Maße als die Weitergabe im Rahmen der Amtshilfe einen Eingriff in das Recht des Bürgers dar, über die Verwendung von Informationen über seine Person selbst zu bestimmen, sofern keine gesetzliche Regelung vorliegt. Dabei ist unerheblich, welche Bedeutung die Verwaltung der Information beilegt und wie sie die Notwendigkeit ihrer vertraulichen Behandlung bewertet. Für die Empfindlichkeit personenbezogener Daten gibt es keine objektiven Maßstäbe, an denen die öffentliche Verwaltung ihr Ermessen ausrichten könnte. Es muß daher der Grundsatz gelten, daß sie Daten und Datenbestände, die Einzelangaben über natürliche oder juristische Personen enthalten oder Rückschlüsse auf solche Einzelangaben zulassen, nur dann an Personen oder Stellen außerhalb der öffentlichen Verwaltung weitergeben darf, wenn dies gesetzlich zugelassen ist oder wenn ausnahmsweise ein wichtiges öffentliches Interesse die Weitergabe gebietet. Dieser Grundsatz ergibt sich aus dem Rückschluß aus § 5 Abs. 3 DSG. Gegenüber diesem Grundsatz des Datenschutzes schlägt die Berufung auf § 5 Abs. 1 des Datenverarbeitungsgesetzes, der mitunter zur Rechtfertigung herangezogen wird, nicht durch. Das dort geregelte Zugriffsrecht bezieht sich auf Mitgliedschaftsrechte innerhalb des Datenverbundes. Das Persönlichkeitsrecht des Bürgers kommt hierbei nicht zum Zuge.

Die bekanntgewordenen Fälle stellen jeder für sich betrachtet einen Eingriff in das Persönlichkeitsrecht des Bürgers dar:

> Eine Gemeinde hat dem KGRZ den Auftrag erteilt, aus ihrem Einwohnerverzeichnis eine Liste der Bürger bestimmter Jahrgangsgruppen unter Angabe von Vornamen, Zunamen, Jahrgang und Wohnung auszudrucken und an ein Versicherungsunternehmen zu schicken.
>
> Eine andere Gemeinde hat einem Adreßbuchverlag, mit dem sie zusammenarbeitet, die Bekanntgabe der gemeindeangehörigen Hauseigentümer vertraglich zugesichert.
>
> Eine dritte Gemeinde hat dem KGRZ den Auftrag gegeben, einer politischen Partei die Namen und Anschriften der gemeindeangehörigen Haushaltungsvorstände aufgrund der gespeicherten Einwohnerliste mitzuteilen.

Es handelt sich hier um eine grundsätzliche Frage des Datenschutzes bei der Weitergabe personenbezogener Daten aus dem öffentlichen Bereich heraus. Der Blick dafür darf nicht durch die scheinbare Harmlosigkeit der genannten Fälle versperrt werden; entscheidend ist, daß hier personenbezogene Daten bestimmter Personengruppen, welche die Gemeinde aufgrund gesetzlicher Vorschriften und Auskunftspflichten des Bürgers erhoben und gespeichert hat, ohne Wissen des Bürgers für Zwecke verwendet werden, die außerhalb der Aufgaben der Gemeinde liegen. Für die bevorstehende Entwicklung integrierter Datenbanken müssen schon jetzt gesicherte Grundsätze erarbeitet und von der Verwaltung praktiziert werden. Die Entstehung einer Verwaltungspraxis, auf die man sich in prekären Fällen und in anderen politischen Situationen berufen könnte, muß von vornherein verhindert werden, wenn man es mit dem Schutz des Persönlichkeitsrechts ernst nimmt.

Der hier entwickelte Grundsatz kommt auch in dem Entwurf der Bundesregierung für ein Bundesdatenschutzgesetz zum Ausdruck. Die Datenweitergabe an Dritte ist den Behörden und sonstigen Stellen nur unter engen Voraussetzungen gestattet (§ 8 d. E.). Diese Regelung entspricht nicht voll der hier vertretenen Auffassung, weil sie die „schutzwürdigen Belange" des Betroffenen nur nachrangig behandelt.

Die Weitergabe der sogenannten freien Daten, die sich aus Namen, Titel, akademischen Graden, Geburtsdatum, Beruf, Branchen- oder Geschäftsbezeichnung, Anschrift und – merkwürdigerweise – der Rufnummer zusammensetzen, soll unbeschränkt zulässig sein (§ 8 Abs. 2 d. E.).

Demgegenüber ist in § 19 d. E. eines Bundesmeldegesetzes das Auskunftsrecht über Personengruppen enger begrenzt: Auskünfte über Personengruppen dürfen nur den Namen, Vornamen, Anschrift und das Datum des Beziehens und des Auszugs aus der Wohnung beinhalten; die Auswahl einer Personengruppe nach anderen Kriterien als den genannten Daten soll nur zulässig sein, wenn das Landesrecht dies im öffentlichen Interesse zuläßt. Diese Regelung entspricht dem hier vertretenen Grundsatz, daß Auskünfte aus Dateien oder Auswertungen von Dateien der öffentlichen Verwaltung nur dann an Stellen oder Personen außerhalb der öffentlichen Verwaltung gegeben werden dürfen, wenn dies gesetzlich zugelassen ist.

1.5.7 Zusammenarbeit zwischen Wissenschaft und Praxis

Erkenntnisse der Wissenschaft, insbesondere der Informatik, auf der einen Seite und solche der Datenschutz-Praxis auf der anderen stehen noch relativ getrennt nebeneinander. Auch ist es beiden noch nicht gelungen, dem Bürger aufzuzeigen, wie wichtig ihre Erkenntnisse für seinen Freiheitsspielraum sind.

Deshalb ist es notwendig, daß die – bereits eingetretenen oder voraussehbaren – *Auswirkungen* des Computereinsatzes in der öffentlichen Verwaltung auf die Freiheitsrechte als Material in die öffentliche Diskussion eingeführt werden. Wissenschaftler (Rechtsinformatiker, Sozialwissenschaftler und Computerspezialisten) sollten die speziellen Fragestellungen untersuchen. Zu diesen Problemkreisen gehört z. B. die Tatsache,

daß der Computer grundsätzlich dahin tendiert, die Position etablierter Machtgruppierungen in Staat und Gesellschaft zu festigen und ihre Überlegenheit sowie ihren Vorsprung auszuweiten.

Eine besonders enge Zusammenarbeit der Datenschutzpraxis mit der freien Wissenschaft muß sichergestellt werden. Offensichtlich fehlt der Wissenschaft die Nähe der Praxis und damit die rechtzeitige kritische Betrachtung bereits übernommener Regelungen. Es muß deshalb eine ähnlich starke gegenseitige Durchdringung von Wissenschaft und Praxis erreicht werden, wie dies z. B. auf dem Gebiet der Medizin durch die Verbindung des Lehrstuhls mit der Universitätsklinik möglich ist.

1.5.8 Ständiger Vorschlagswettbewerb: Datenschutz

Um in der Bevölkerung und bei den Verwaltungsbediensteten das Interesse für Datenschutzfragen zu verstärken und gleichzeitig einen Beitrag zur Verbesserung der Vorkehrungen gegen Datenmißbrauch zu leisten, könnte die Landesregierung Geldprämien für Vorschläge zur Verbesserung der technischen und organisatorischen Sicherungen bei der EDV aussetzen. An dieser Ausschreibung sollten nicht nur die Bediensteten der öffentlichen Verwaltung teilnehmen können, sondern alle interessierten Bürger.

Für die Bediensteten der hessischen Landesverwaltung besteht bereits die Einrichtung eines ständigen Vorschlagwettbewerbs für die Vereinfachung, Verbesserung oder wirtschaftlichere Gestaltung der Verwaltung. Während es für die Bediensteten ausreichen würde, die schon bestehenden Richtlinien des allgemeinen Vorschlagwettbewerbs durch die Aufnahme von Maßnahmen zur Verbesserung des Datenschutzes und der Datensicherung zu erweitern, sollte für die Vorschläge der übrigen Bürger eine besondere Regelung geschaffen werden.

Mit der Einrichtung eines solchen Wettbewerbs würde gleichzeitig erreicht, daß alle mit der neuen Technologie in Berührung kommenden Mitbürger in regelmäßigen Abständen öffentlich mit dem Problem Datenschutz konfrontiert würden. Gleichzeitig würde damit an ihre Verantwortung für die Sicherung der Grundlagen des Rechtsstaates appelliert.

2. RECHTLICHE REGELUNGEN DES DATENSCHUTZES AUSSERHALB HESSENS

2. Rechtliche Regelungen des Datenschutzes außerhalb Hessens

2.1 Andere Länder – Überblick –

Der Gesetzgebungsstand in den Ländern hat sich nicht entscheidend verändert. Nach wie vor kennzeichnet eine abwartende Haltung mit Blick auf die Gesetzgebung des Bundes das Feld. Nur Rheinland-Pfalz hat ein Landesdatenschutzgesetz verabschiedet. Zu neuen Gesetzgebungsinitiativen ist es in Berlin, Niedersachsen und Nordrhein-Westfalen gekommen.

2.1.1 Schleswig-Holstein

keine neuen Entwicklungen

2.1.2 Bayern

keine neuen Entwicklungen

2.1.3 Rheinland-Pfalz

Das Landesdatenschutzgesetz wurde Anfang des Jahres vom Landtag beschlossen (Gesetz gegen mißbräuchliche Datennutzung vom 24. Jan. 1974, GVBl. Rheinland-Pfalz 1974, 31 ff.). Die bedeutendste Änderung gegenüber dem Urantrag der CDU-Fraktion (vgl. dazu II, 2.1.3, I, 2.1.3) besteht in der Einführung einer Gefährdungshaftung für den Fall einer widerrechtlichen Datenverarbeitung (Speicherung, Änderung, Vernichtung, Einsicht, Abruf).

Aufgrund der fortgeschrittenen Diskussion war es möglich, in einigen wichtigen Fragen Datenschutzvorkehrungen gesetzlich anzuordnen, die in Hessen zwar praktiziert werden, für die es aber noch keine ausdrücklichen Gesetzesbestimmungen gibt. So wird bei selbsttätiger Datenübermittlung eine Protokollierung von Empfänger, Zeit und Inhalt angeordnet. Die Behörden haben dem Datenschutzausschuß die Art der Daten, den Umfang ihrer Nutzung (nach Benutzerkreis, Benutzerzwecken und Programmen) sowie die zum Schutz zu erlassenden Dienstanweisungen mitzuteilen. Der Betroffene erhält ein Auskunftsrecht. Die Weitergabe von Daten an andere Träger öffentlicher Aufgaben ist, enger und präziser als im Regierungsentwurf eines Bundesdatenschutzgesetzes, nur insoweit zugelassen, „als dies zur Erfüllung gesetzlicher Aufgaben erforderlich ist", an andere Stellen, „soweit ... gesetzlich zugelassen".

In diesem und einigen anderen Punkten hat das Gesetz durchaus wegweisende Bedeutung. Leider hat man sich noch nicht dazu entschließen können, bei der Kontrollinstitution über einen aus nur nebenamtlich tätigen Abgeordneten (3) und Richtern oder Beamten (2) zusammengesetzten Ausschuß hinauszugehen. Der Landtag will diese Entscheidung jedoch später überprüfen.

2.1.4 Niedersachsen

Der noch unveröffentlichte Referentenentwurf eines Gesetzes über die Organisation der automatischen Datenverarbeitung in Niedersachsen – Stand Sept. 1973 – enthält Datenschutzregelungen, die von den bisher vorliegenden Länderentwürfen abweichen. An Stelle eigener materieller Vorschriften erklärt der Entwurf die Vorschriften des Bundesdatenschutzgesetzes in ihrer jeweils geltenden Fassung für die Landes- und Kommunalverwaltung auch insoweit für anwendbar, als diese nicht Bundesrecht ausführen. Die Überwachung des Datenschutzes wird dem Landesrechnungshof anvertraut, der dem Landtag in regelmäßigen Abständen berichten soll.

Der Runderlaß über den vorläufigen Datenschutz in den Rechenzentren des Landes (Nds. MBl. 1970, S. 1326, vgl. I, 2.1.4) soll überarbeitet werden. Der Referentenentwurf sieht vor, Maßnahmen des Datenschutzes und der Datensicherung künftig durch Verordnung vorzuschreiben. Unklar ist, ob sich der Datenschutz entsprechend der Zielsetzung des ADV-Gesetzentwurfs nur auf die automatische Datenverarbeitung oder infolge der Bezugnahme auf das Bundesdatenschutzgesetz auch auf konventionelle Verarbeitungsformen bezieht.

2.1.5 Baden-Württemberg

keine neuen Entwicklungen

2.1.6 Nordrhein-Westfalen

In Nordrhein-Westfalen hat der Landtag im Januar 1974 ein ADV-Organisationsgesetz beschlossen. Eine nahezu einstimmige Beschlußfassung war möglich, nachdem der ursprünglich umstrittene Regierungsentwurf einige Änderungen und Ergänzungen erfahren hatte. Hierzu gehören u. a. Vorschriften über das Informationsgleichgewicht zwischen den Verfassungsorganen. § 2 schreibt nunmehr vor, daß „durch den Einsatz der automatisierten Datenverarbeitung ... das Informationsgleichgewicht, insbesondere zwischen den Organen der gesetzgebenden und der vollziehenden Gewalt, nicht beeinträchtigt werden (darf)". Die Volksvertretungen des Landes und der Kommunen und ihre Fraktionen können von der Landesregierung und den obersten Landesbehörden bzw. dem Hauptverwaltungsbeamten im Rahmen ihrer Aufgaben Auskünfte auf Grund der von diesen im Landesinformationssystem oder sonst gespeicherten Daten verlangen. Die Landesdatenbank, die ausgewählte Daten für statistische Informationen, Planungs- und Entscheidungshilfe sowie zur Wirkungskontrolle enthält, steht jedermann für Auskünfte und Auswertungen nach Maßgabe der geltenden Vorschriften zur Verfügung. Der Landtag kann die Daten auch für den Aufbau eines eigenen Informationssystems benutzen (§§ 3, 13).

In einer Entschließung hat der Landtag die Regierung aufgefordert, möglichst noch vor der Sommerpause den Entwurf eines Landes-Datenschutzgesetzes vorzulegen, „das in weitgehender Übereinstimmung mit den zu erwartenden bundesgesetzlichen Regelungen einen wirksamen Schutz der Privatsphäre des Bürgers sicherstellt". Es besteht die Absicht, das Gesetz noch in der laufenden Legislaturperiode zu verabschieden.

2.1.7 Hamburg

keine neuen Entwicklungen

2.1.8 Berlin

Dem Abgeordnetenhaus liegt die Senatsvorlage eines Gesetzes über den Datenschutz in der Berliner Verwaltung vom 4. Mai 1974 vor (Abgeordnetenhaus-Drucks. 6/865). Der Entwurf liegt im wesentlichen auf der hessischen Linie, geht aber, ähnlich dem rheinland-pfälzischen Gesetz, an mehreren Stellen darüber hinaus. Er ist auf die automatische Datenverarbeitung beschränkt. Die Verwaltungen haben Art und Umfang der von ihnen gespeicherten Daten und den erfaßten Personenkreis im Amtsblatt zu veröffentlichen. Die Kontrolle obliegt einem Ausschuß, dem je ein Abgeordneter der Fraktionen im Abgeordnetenhaus sowie eine Dienstkraft des Rechnungshofes angehören sollen. Er überwacht die Datenverarbeitung auf die Einhaltung der Datenschutzvorschriften. Ebenso wie im hessischen Modell wird auch die Bedeutung der Datenverarbeitung für das staatlich-politische Gefüge erfaßt: Der Ausschuß soll die Auswirkungen der ADV auf die Arbeitsweise und Entscheidungsbefugnisse der Behörden dahingehend beobachten, „ob sie zu einer Beschränkung der Kontrollmöglichkeiten durch die Volksvertretung führen".

2.2 Gesetzgebungsstand im Bund

Auf Bundesebene sind im Berichtsjahr der angekündigte Entwurf eines Datenschutzgesetzes und ein geringfügig veränderter Bundesmeldegesetzentwurf (vgl. dazu II, 2.2.1) von der Regierung eingebracht worden. Von größerer Bedeutung für den Datenschutz ist auch das nunmehr verabschiedete Einführungsgesetz zum Strafgesetzbuch.

2.2.1 bis 2.2.2 Bundesdatenschutzgesetz und Bundesmeldegesetz

Die Regierungsentwürfe eines Bundesmeldegesetzes und eines Bundesdatenschutzgesetzes haben Bundesrat und Bundestag im ersten Durchgang passiert (vgl. Stenogr. Bericht vom 29. November 1973, S. 4017 ff.) und werden gegenwärtig in den Ausschüssen des Bundestages beraten (Bundesrats-Drucks. 390/73, 391/73, Bundestags-Drucks. 7/1059, 7/1027).

Der Innenausschuß führt Anfang Mai eine öffentliche Anhörung von Sachverständigen durch, an der auch der Datenschutzbeauftragte teilnimmt. Eine intensive Diskussion hat eingesetzt, in der die Regierungsentwürfe teilweise heftig kritisiert und überwiegend als nicht ausreichend bezeichnet werden (vgl. z. B. Simitis: Datenschutz, Notwendigkeit und Voraussetzungen einer gesetzlichen Regelung, in: Datenverarbeitung im Recht 1973, Heft 2/3, S. 138 ff.; Dammann/Karhausen/Müller/Steinmüller, Datenbanken und Datenschutz, Frankfurt/M. 1974, S. 20 ff., 27 ff., 132 ff., 150 ff., Tiedemann/Sasse, Delinquenzprophylaxe, Kreditsicherung und Datenschutz in der Wirtschaft, Köln u. a. 1973, S. 107 ff., Bühnemann, Datenschutz in nichtöffentlichem Bereich, Beilage 1/74 zum Betriebsberater, Heft 3/1974, Podlech, Datenschutz im Bereich der öffentlichen Verwaltung, Datenverarbeitung im Recht, Beiheft 1, Berlin 1973).

Nach Auffassung des Datenschutzbeauftragten sollten bei der Diskussion im weiteren Gesetzgebungsverfahren insbesondere die nachstehenden Grundsätze beachtet werden (vgl. ferner II. Anhang I):

a) Die Existenz einer externen Kontrollinstitution ist die Grundbedingung jedes wirksamen Datenschutzes. Der Regierungsentwurf führt lediglich für die geschäftsmäßige Datenverarbeitung nichtöffentlicher Stellen für Dritte (vierter Abschnitt) eine Anmeldepflicht ein und unterstellt sie einer behördlichen Aufsicht. Im weitaus größeren Berich der privaten Datenverarbeitung für eigene Zwecke (dritter Abschnitt) sieht er „insbesondere aus Gründen der Praktikabilität" von jeglicher Fremdkontrolle und Publizität ab und verfolgt „das Prinzip der Selbstverantwortlichkeit und einer abgestuften Selbstkontrolle" (Begründung, Bundestags-Drucks. 7/1027, S. 19). Dasselbe gilt im Prinzip für die Datenverarbeitung der öffentlichen Verwaltung. Dieser Lösung scheint die Annahme zugrundezuliegen, Selbst- und Fremdkontrolle seien grundsätzlich gegeneinander austauschbare Prinzipien. Dem ist zu widersprechen. Eine Pflicht zur Selbstkontrolle, nämlich zu allen erforderlichen innerorganisatorischen Vorkehrungen, ergibt sich ohne weiteres aus der Verbindlichkeit des Gesetzes. Ihre Erfüllung ist selbstverständlich und kann keinerlei Argument gegen oder Ersatz für eine externe Kontrolle abgeben. Die Erfahrungen des Datenschutzbeauftragten, wie sie in den bisherigen Tätigkeitsberichten vielfach zum Ausdruck kommen, haben immer wieder die dem hessischen Modell zugrundeliegende Auffassung bestätigt, daß die Interessen der Betroffenen nur die gebührende Beachtung finden, wenn sie einen fachkundigen und tatkräftigen institutionellen Fürsprecher besitzen, der sich rechtzeitig in die Entwicklung einschaltet. Dies gilt für den Regierungsentwurf um so mehr, als seine materiellen Schutzvorschriften in ungewöhnlichem Umfang auf Generalklauseln zurückgreifen, welche den speichernden und verarbeitenden Stellen große Möglichkeiten einer einseitigen Interpretation eröffnen. Es ist absehbar, daß – bei fehlendem institutionellen Gegengewicht – die Verwaltung im allgemeinen dazu neigen wird, den Effizienz- und Kostengesichtspunkten den Vorrang vor dem Schutz der Betroffenen zu geben, zumal, da diese von einer Verletzung ihrer Rechte mit nur geringer Wahrscheinlichkeit und wenn, so mit erheblicher Verzögerung, Kenntnis erhalten. Diese gerade für die Informations-

verarbeitung typische Gefahr wird offensichtlich verkannt, wenn statt gezielter institutioneller Vorkehrungen nur ein Hinweis auf den „Grundsatz der Rechtmäßigkeit allen Handelns, ... (die) Kontrolle der Parlamente und ihrer Einrichtungen sowie der unabhängigen Rechnungshöfe, ... (den) hierarische(n) Aufbau (der Behörden) mit parlamentarisch verantwortlichen Ministern an der Spitze, ... den lückenlosen Rechtsschutz ... und das Recht (des Bürgers), sich unmittelbar an das Parlament zu wenden" erfolgt (Begründung des Entwurfs a. a. O. S. 18).

Auch die Wissenschaft fordert einhellig und mit großem Nachdruck eine erweiterte Fremdkontrolle im öffentlichen wie im privaten Sektor, wobei die hessischen Erfahrungen sowie Gesetzgebungstendenzen im Ausland eine nicht geringe Rolle spielen.

b) Der Datenschutz muß lückenlos sein. Ein Bundesdatenschutzgesetz verfehlt seinen Zweck, wenn es, wie in § 2 Abs. 1 des Regierungsentwurfs vorgesehen, nur solche Daten erfaßt, die zur Weitergabe bestimmt sind. Ein Großteil der schutzbedürftigen Daten, auch im automatisierten Bereich, bliebe dabei ungeschützt. Auch der Bundesrat hat hier eine Erweiterung gefordert.

c) Die Berufs- und besonderen Amtsgeheimnisse, wie z. B. das ärztliche, das Steuer- und das Statistikgeheimnis, dürfen nicht untergraben werden. Der Regierungsentwurf zielt jedoch auf die Konstruktion eines Zweckverbundes, innerhalb dessen auch gesetzlich besonders geheimzuhaltende Daten frei weitergegeben werden dürfen. Wenn eine Stelle der öffentlichen Verwaltung solche besonders geschützten Daten, also etwa Gesundheitsdaten oder Angaben aus einer statistischen Befragung, für einen bestimmten Zweck erhalten hat, so darf sie sie an andere Verwaltungsstellen weiterreichen, wenn diese sie für den gleichen Zweck benötigen (§ 7 Abs. 1 Satz 1 des Entwurfs). Dem liegt die irrige Auffassung zugrunde, die bloße Gleichheit des Verwendungszweckes könne die weitere Weitergabe rechtfertigen. Soweit der Betroffene nicht zustimmt – und nur diese Fälle sind problematisch –, sollte aber allein der nach dem Gesetz Geheimhaltungspflichtige, also der Arzt, Statistiker usw., über die Weitergabe der geschützten Daten entscheiden. Er allein hat die besondere fachliche Kompetenz, die berufsethische Verantwortlichkeit und (meist) ein vitales Eigeninteresse an wirksamer Geheimhaltung und erfüllt hiermit die Voraussetzungen, die den Schutz der Betroffenen in der Praxis erst gewährleisten können. Da der Zweck einer Weitergabe meist nicht oder nur pauschal festgelegt wird, ist die Gleichheit des Zwecks zudem ein höchst unsicher anzuwendender Maßstab.

Auf die im Prinzip gleichen grundsätzlichen Einwände stoßen die §§ 8 Abs. 1 Satz 1 und 18 Abs. 1 Satz 1 des Entwurfs, die sinngemäß die nachfolgende Weitergabe gesetzlich besonders geheimzuhaltender Daten durch Verwaltungsstellen an Private bzw. durch Private zulassen, wenn „die gleichen Voraussetzungen gegeben sind, unter denen die zur Verschwiegenheit verpflichtete Person (sie) weitergeben dürfte". Auch hier wird die bisher eng begrenzten Berufsgruppen vorbehaltene Beurteilungs- und Entscheidungskompetenz auf einen unbeschränkten und unübersehbaren Personenkreis ausgeweitet, was zu einer unerträglichen Gefährdung der gesetzlich geschützten Geheimnisse führen müßte.

2.2.3 Einführungsgesetz zum Strafgesetzbuch mit Verpflichtungsgesetz

Das Einführungsgesetz zum Strafgesetzbuch (vgl. II, 2.2.4) ist kürzlich verkündet worden (BGBl. I S. 469) und wird am 1. Januar 1975 in Kraft treten. Der neue Straftatbestand der Verletzung von Privatgeheimnissen durch Amtsträger und gleichgestellte Personen (§ 203 Abs. 2), der die unbefugte Offenbarung von für die Aufgaben der öffentlichen Verwaltung erfaßten Einzelangaben über persönliche oder sachliche Verhältnisse eines anderen mit Strafe bedroht, auch soweit kein materielles Geheimnis vorliegt, ist im Verlaufe der Beratungen eingeschränkt worden. Er soll nach der endgültigen Fassung nicht mehr angewendet werden, soweit Angaben ohne materiellen Geheimnischarakter anderen Behörden oder sonstigen Stellen für Aufgaben der öffentlichen Verwaltung (unbefugt) bekanntgegeben werden. Mit Strafe bedroht ist danach nur noch die unbefugte Abgabe an Privatpersonen. Die Einschränkung in § 203 Abs. 2 EGStGB wurde vom Sonderausschuß des Bundestages für die Strafrechtsreform vorgenommen, „um der Befürchtung des Bundesrates zu begegnen, bei der im Entwurf vorgeschlagenen Formulierung könne die gegenseitige Unterrichtung von Verwaltungsbehörden künftig beeinträchtigt werden" (Bundestags-Drucks. 7/1261, S. 16).

Diese Argumentation bestätigt die vom Datenschutzbeauftragten von Anfang an vertretene Auffassung (I, 4.1.2, II, 4.1.1.1 b), daß die Erarbeitung präziser Regelungen für den Informationsaustausch innerhalb der öffentlichen Verwaltung, welche den allgemeinen Amtshilfegrundsatz konkretisieren und begrenzen, dringend geboten ist.

Im ersten und zweiten Tätigkeitsbericht ist verschiedentlich darauf hingewiesen worden, daß es um den Datenschutz besonders schlecht bestellt ist, wenn Daten in die Herrschaftsgewalt von Privatpersonen gelangen oder Private innerhalb des Organisationsbereichs der öffentlichen Verwaltung eingesetzt werden und dadurch Zugriff zu Daten erhalten. Hierzu gehören insbesondere die Vergabe von Erfassungs- oder Verarbeitungsaufträgen an private Service-Unternehmen, die Mitarbeit von Angestellten der Herstellerfirmen im Rechenzentrum und bei der Verfahrensentwicklung, die Heranziehung privater Handwerks- und Reinigungsfirmen, aber auch Gemeinschaftsprojekte zwischen Verwaltungsträgern und privaten Einrichtungen, etwa im Sozialsektor. Eine Lücke im Datenschutz bestand hier insofern, als spezielle Gesetze, insbesondere Strafvorschriften, die für die öffentliche Verwaltung und deren Bedienstete bestehen, auf die genannten privaten Personen und Einrichtungen nicht anwendbar sind.

Mit dem Gesetz über die förmliche Verpflichtung nichtbeamteter Personen, Art. 42 Einführungsgesetz zum Strafgesetzbuch vom 2. März 1974 (BGBl. I, S. 469), wird diese Lücke geschlossen. Danach können Personen förmlich auf die gewissenhafte Erfüllung ihrer Obliegenheiten verpflichtet werden, wenn sie bei einer Behörde der öffentlichen Verwaltung oder einer privaten Stelle, die Aufgaben der öffentlichen Verwaltung wahrnimmt oder ausführt, beschäftigt sind. Diese Verpflichtung hat zur Folge, daß der Verpflichtete ebenso wie ein Amtsträger nach § 203 Abs. 2 Nr. 2 StGB bestraft werden kann, wenn er unbefugt Einzelangaben über eine andere Person offenbart. Die bisher geübte Praxis, Hilfsunternehmen auf die für die Verwaltung selbst vorgeschriebene Geheimhaltungspflicht vertraglich zu verpflichten, konnte immer nur privatrechtliche, aber keine strafrechtlichen Konsequenzen haben.

2.3 Ausland

2.3.1 USA

In den Vereinigten Staaten bestand nach Erlaß des Fair Credit Reporting Act (vgl. I, 2.3.1) auf seiten der Bundesregierung eine deutliche Zurückhaltung gegenüber Forderungen nach weiteren legislativen Schritten. Beginnend mit der Vorlage einer umfangreichen Expertenstudie, die u. a. den Erlaß eines „Code of Fair Information Practice" vorschlägt, durch das Ministerium für Gesundheit, Erziehung und Wohlfahrt (U.S. Department of Health, Education and Welfare: Records, Computers and the Rights of Citizens, Report of the Secretary's Advisory Committee on Automated Personal Data Systems, July 1973, DHEW Publication No. [05] 73–94) hat sich dann seit Mitte 1973 ein allmählicher Meinungsumschwung vollzogen. Nunmehr liegt dem Kongreß der Entwurf eines Gesetzes zur Kontrolle von Kriminalinformationssystemen auf Staats- und Bundesebene vor (H. R. 9783), der allerdings weniger weit geht als das entsprechende Gesetz des Staates Massachusetts. Anfang des Jahres hat der amerikanische Präsident in seiner State of the Union Address auf die Bedrohung der Privatsphäre durch Datenbanken hingewiesen und ein rasches Handeln des Staates („We need action") für vordringlich erklärt. Ein neugebildeter Kabinettsausschuß (Domestic Council Committee on the Right of Privacy) unter Leitung von Vizepräsident Ford erhielt den Auftrag, binnen vier Monaten konkrete Vorschläge für gesetzgeberische und andere Maßnahmen zu entwickeln.

2.3.1.1 Massachusetts

Der amerikanische Bundesstaat Massachusetts hat als erster für sein Kriminalinformationssystem ein besonderes Datenschutzgesetz erlassen und damit eine Alternative zu der in den USA verbreiteten Freizügigkeit im Umgang mit Polizei- und Kriminaldaten aufgestellt (An Act Providing for the Establishment and Administration of a Criminal Offender Record Information System, July 19, 1972. The Commonwealth of Massachusetts, Acts 1972, Chap. 805, pp. 813–820). Das Gesetz legt genau fest, welche Daten in dem System gespeichert und welchen Stellen sie zugänglich gemacht werden dürfen. Durch ein Verbot der Speicherung ungesicherter oder unüberprüfbarer Daten („intelligence, analytical and investigative reports and files") soll die Mißbrauchsgefahr reduziert werden. Die Daten stehen außer den mit Strafverfolgung und -vollzug befaßten Behörden nur solchen Stellen offen, die hierzu besonders gesetzlich ermächtigt sind. Identität und Berechtigung der anfragenden Personen müssen besonders geprüft werden. Jedermann erhält das Recht auf Einsicht in die ihn betreffenden Daten und auf Aushändigung einer Kopie, soweit dies die Technik zuläßt. Bei ungenauen, unvollständigen oder falschen Daten kann er die Korrektur bzw. Löschung verlangen.

Beachtlich sind die institutionellen Vorkehrungen. Ein gemischter Ausschuß, in dem die mit Verbrechensbekämpfung, Strafverfolgung und Strafvollzug befaßten staatlichen Stellen sowie Berufsvereinigungen vertreten sind, überwacht die Datenverarbeitungs- und Datenübertragungssysteme. Er erläßt Vorschriften zur Sammlung, Speicherung, Weitergabe und Benutzung der Daten, zur laufenden Überprüfung ihrer Genauigkeit und Vollständigkeit, zur Gewährleistung einer rechtzeitigen Löschung und zur Gewährleistung der Einsichts- und Berichtigungsrechte der Betroffenen sowie zur Sicherung gegen unbefugten Zugriff. Er führt eine Liste der zugangsberechtigten Stellen und Personen. Dem Ausschuß steht ein beratendes Komitee zur Seite. Speziell für Fragen des Datenschutzes und der Datensicherung wurde außerdem der Security and Privacy Council geschaffen, der in der Mehrheit aus vom Gouverneur zu ernennenden Repräsentanten der Öffentlichkeit, der Verwaltung und der Strafverfolgung besteht. Der Rat überprüft ständig die Wirksamkeit aller Sicherheitsmaßnahmen und überwacht die Praxis des Datenschutzes. Bei Beschwerden von Bürgern führt er ein vorbereitendes Verfahren durch und legt dem Ausschuß einen Entscheidungsvorschlag vor. Der Rat arbeitet wie auch die anderen Gremien ehrenamtlich. Für seine Untersuchungen steht ihm die erforderliche büromäßige und sonstige Ausstattung zur Verfügung.

Der Staat Massachusetts hat es abgelehnt, sich dem National Crime Informations Center des FBI anzuschließen, ehe auch dort die notwendigen Garantien für die Rechte des einzelnen und ausreichende Mißbrauchssicherungen vorhanden seien. An dieser Entscheidung wurde auch festgehalten, als die Bundesregierung mit der Kürzung von Bundessubventionen und weiteren Nachteilen drohte und den Staat auf Anschluß an das NCIC verklagte. Die Tatsache, daß diese Klage später wieder zurückgenommen wurde, dürfte einen gewissen Klimaumschwung anzeigen.

2.3.1.2 Georgia

Im Staat Georgia wird ein Gesetzentwurf (H. B. No. 579) parlamentarisch beraten, der in erster Linie die Organisation des Georgia Crime Information Center regelt, darüber hinaus aber auch materielle, verfahrensmäßige und institutionelle Datenschutzvorkehrungen vorsieht.

2.3.2 Kanada

In mehreren Provinzen wurden Datenschutzgesetze für den Bereich der Kreditinformation erlassen.

2.3.3 Großbritannien

keine neuen Entwicklungen

2.3.4 Frankreich

keine neuen Entwicklungen.

2.3.5 Schweden

Schweden besitzt seit April 1973 ein umfassendes Datengesetz (Datalagen SFS 1973: 289, zum Inhalt vgl. II, 2.3.5). Mit der neu errichteten Kontrollbehörde, der data inspektionen, wurde ein Erfahrungsaustausch aufgenommen. Wesentliche neue Erkenntnisse über Praktikabilität und Auswirkungen der Überwachung sind nicht vor Ablauf des Jahres 1974 zu erwarten, da die Genehmigungspflicht von Datenbanken mit personenbezogenen Informationen ebenso wie die wesentlichen Aufsichtsrechte der Dateninspektion erst Mitte 1974 in Kraft treten.

Für das Gebiet des Kreditauskunfteiwesens ist ein Spezialgesetz in Vorbereitung. Der von einer königlichen Kommission vorgelegte Entwurf (SOU 1972: 79) macht die Betätigung auf dem Gebiet der Kreditauskunft genehmigungsbedürftig, ebenso die Veräußerung von Personen-Registern (Datensammlungen). Die Weitergabe von Daten darf den Betroffenen nicht ungebührlich in seiner persönlichen Integrität beeinträchtigen. Über Kriminalität, Alkoholmißbrauch, Krankheiten oder andere persönliche Verhältnisse besonders heikler Natur sowie über Fakten, die mehr als drei Jahre zurückliegen, darf deshalb nichts mehr mitgeteilt werden. Soweit ein Weitergabeverbot besteht, ist bereits die Sammlung entsprechender Daten verboten. Der einzelne hat das Recht, die Erteilung von Kreditauskünften zu seiner Person zu verbieten. Von der Erteilung negativer Auskünfte ist der Betroffene kostenlos zu informieren. Im übrigen besteht ein Auskunftsrecht über eigene Daten und über erteilte Auskünfte gegen eine angemessene Gebühr sowie ein Berichtigungsanspruch. Ein Kreditauskunftsausschuß, der aus neun von der Regierung zu ernennenden Mitgliedern bestehen soll, überwacht die Einhaltung des Gesetzes. Der Entwurf, der mit dem Datengesetz noch nicht abgestimmt ist, enthält ferner Haftungs- und Strafvorschriften.

2.3.6 Dänemark

In Dänemark hat eine Kommission unter Vorsitz des Präsidenten des obersten Gerichts im Juni 1973 den Entwurf eines Datenschutzgesetzes vorgelegt. Danach werden alle von privaten Stellen geführten systematischen Sammlungen und Aufzeichnungen von Informationen über die wirtschaftlichen Verhältnisse von Personen, Gesellschaften und Unternehmen sowie über persönliche und private Angelegenheiten der Kontrolle durch eine Verwaltungsbehörde, den sog. Registerausschuß, unterstellt. Betrieb und Veräußerung von Kreditauskünften sind anmeldepflichtig. Der Justizminister kann die Meldepflicht auf weitere Tatbestände ausdehnen. Auf Antrag des Betroffenen entscheidet der Registerausschuß endgültig bei Streitigkeiten über Berichtigungen.

Datenschutzregelungen für den öffentlichen Bereich sind in Vorbereitung.

2.3.7 Österreich

Ein Referentenentwurf eines Datenschutzgesetzes vom 1. August 1973 wurde vom österreichischen Bundeskanzleramt erarbeitet. Aus Kompetenzgründen bezieht er sich lediglich auf Dateien im Bereich der Bundesverwaltung. Die materiellen Regelungen sind weitgehend an den Entwurf des deutschen Bundesdatenschutzgesetzes angelehnt. Die Verarbeitung von Daten soll auf der Grundlage ausdrücklicher gesetzlicher Ermächtigungen zulässig sein, im übrigen nur, soweit sie zur Besorgung der gesetzlich übertragenen Aufgaben unbedingt notwendig ist. Für jede Datei ist eine Datei-Betriebsordnung aufzustellen. In dieser sind die erforderlichen Maßnahmen der Datensicherung vorzusehen und die Datenweitergabe in der Weise zu regeln, daß die begründeten Interessen der Betroffenen gewährleistet werden. Die Einhaltung des Datenschutzes soll ein Datei-Obmann überwachen. Jede Datenweitergabe im Wege der Rechts- oder Amtshilfe ist diesem mitzuteilen. Jeder Bundesminister soll jährlich eine Liste der von ihm eingerichteten Dateien unter Angabe der Datensätze im Amtsblatt veröffentlichen.

2.3.8 Schweiz

In der Schweiz hat die Regierung des Kantons Aargau den Entwurf eines Datengesetzes (Stand 8. Februar 1974) erarbeitet. Er lehnt sich an einige EDV-Organisationsgesetze der Länder der Bundesrepublik an. In der institutionellen Kontrolle des Datenschutzes folgt er dem hessischen Modell einer unabhängigen Instanz. Vom Datenschutzbeauftragten heißt es in der Begründung, man könne ihm skeptisch gegenüberstehen, „bessere Lösungen (seien) z. Z. aber nicht bekannt". In der Praxis seien mit dieser Institution bisher recht gute Erfahrungen gemacht worden. Was die Rechte des einzelnen betrifft, so folgt der Entwurf im großen und ganzen dem Bonner Datenschutzgesetzentwurf, sieht jedoch darüber hinaus eine Gefährdungshaftung vor.

2.3.9 Neuseeland

In Neuseeland hat eine Regierungskommission (Drayton Commission) im Oktober 1973 einen Untersuchungsbericht zum geplanten Kriminalinformationssystem vorgelegt (Government Caucus Committee Report on the Proposed Law Enforcement Information System). Darin wird vorgeschlagen, das System auf gesetzlicher Grundlage zu errichten. Im Gesetz sollen Organisation, Inhalt und Umfang des Systems festgelegt und die Datenschutzvorkehrungen vorgeschrieben werden. Die Kommissionsvorschläge folgen weitgehend dem oben erwähnten Gesetzentwurf des amerikanischen Bundesstaates Georgia.

Darüber hinaus empfiehlt die Kommission den Erlaß eines allgemeinen Datenschutzgesetzes (Preservation of Privacy Act 1973). Ein Datenschutzbeauftragter (Privacy Commissioner) soll die Computerinstallationen genehmigen und überwachen, Vorschläge zur Verbesserung des Schutzes der Privatsphäre machen und jährlich dem Generalgouverneur berichten. Der Entwurf enthält weiter detaillierte Vorschriften zum Schutz der Betroffenen.

2.4 Tendenzen der Datenschutzgesetzgebung

Im Ausland wie auch in der Diskussion in der Bundesrepublik hat sich die vom Datenschutzbeauftragten schon früher vertretene Auffassung durchgesetzt, daß die Datenschutzproblematik, auch wenn ein allgemeines Datenschutzgesetz in Kraft getreten ist, nur durch bereichsspezifische Regelungen, die den jeweiligen Interessen und Verhältnissen Rechnung tragen, befriedigend gelöst werden kann. In den Vereinigten Staaten, aber auch in einer Reihe anderer Länder, wie z. B. in Neuseeland, konzentrieren sich solche Bemühungen gegenwärtig stark auf die Regulierung und Kontrolle von Informationssystemen im Bereich der Strafverfolgung. Besonders kritisch ist auf diesem Sektor die Situation in Ländern, die kein institutionalisiertes Strafregister kennen. Auch in der Bundesrepublik ist die Lage jedoch nicht problemlos, da die Datenschutzvorschriften des Strafregisterwesens für sonstige Datensammlungen ähnlichen Inhalts, z. B. bei der Polizei oder in privater Hand, nicht gelten und auch nicht analog angewendet werden. Spezielle Schutzbestimmungen sind erforderlich. Die vom Standpunkt des Datenschutzes sauberste Lösung bestände darin, die Sammlung und Verwertung von Kriminaldaten ausschließlich durch die gesetzlich hierfür zuständigen staatlichen Stellen zuzulassen, wie es z. B. im neuen schwedischen Datengesetz bestimmt wird.

Ein weiteres Gebiet, das auf die Dauer nur spezialgesetzlich befriedigend reguliert werden kann, ist das der Kreditinformation sowie der Personalbeurteilung auf dem Arbeitsmarkt. Neben den in diesem und in früheren Berichten erwähnten einschlägigen Gesetzgebungsaktivitäten in den USA, in amerikanischen Einzelstaaten und in skandinavischen Ländern ist auf die von mehreren kanadischen Provinzen kürzlich erlassenen einschlägigen Schutzgesetze hinzuweisen.

Das Gesundheitswesen ist ein anderer Bereich, auf dem Informationssystem jenseits einer bestimmten Größenordnung oder organisatorischen Erstreckung zusätzlicher gesetzlicher Legitimierung und Kontrolle bedürfen. Zu diesem, in Hessen mit dem Hessischen Krankenhausgesetz von 1973 (vgl. 4.1.1.1) bereits eingeschlagenen Weg dürften sich bald auch andere Länder bekennen. Immerhin ist auch auf dem medizinischen Sektor die Verweigerung einer Teilnahme an Verbundprojekten bereits als Hebel zur Durchsetzung eines besseren Datenschutzes eingesetzt worden: In Großbritannien haben sich vier Krankenhäuser geweigert, an einem von der britischen Regierung geförderten Programm teilzunehmen, weil sie sich nicht berechtigt fühlten, die Daten ihrer Patienten aus ihrer unmittelbaren Kontrolle zu entlassen.

2.5 Datenfernverarbeitung und Datenkommunikation

Datenfernverarbeitung und Datenfernübertragung spielen bei der Automatisierung der Verwaltung erst in Teilbereichen eine Rolle wie z. B. bei der Kriminalpolizei und den Nachrichtendiensten. Es gibt aber Bemühungen, von den verschiedenen Einzelplanungen zu einer Gesamtplanung überzugehen und so ein universell einsetzbares Datenkommunikationsnetz zu schaffen. Diese Bestrebungen werden technologisch begründet: Einheitliche Grundsätze für Datenübertragung und Steuerungsverfahren lassen sich nachträglich nur unter hohen Kosten auf isoliert entwickelte Einzelprojekte aufsetzen; sie müssen deshalb im Rahmen einer breit angelegten Koordinierung den Teilprojekten bereits vorgegeben werden.

In den Vereinigten Staaten, in Kanada und in Japan wurden bereits Erfahrungen mit Fernverarbeitungs-Netzwerken gesammelt, die vor allem unter wirtschaftlichen Gesichtspunkten positiv bewertet werden. Die OECD rät deshalb ihren Mitgliedsländern, Planungen für umfassende elektronische Kommunikationssysteme aufzunehmen und mit hoher Priorität voranzutreiben. Im Entwurf eines Aktionsprogrammes der Kommission der Europäischen Gemeinschaften werden Vorplanungen für die Errichtung eines europäischen Informationsnetzes vorgeschlagen.

In der Bundesrepublik beschäftigen sich unter anderem der vom Bundespostministerium initiierte Ausschuß für Fragen der Datenfernverarbeitung und ein Arbeitskreis Datenfernverarbeitung des Kooperationsausschusses ADV Bund/Länder/Gemeinden mit grundsätzlichen Problemen der Planung von elektronischen Kommunikationsnetzen. Bisher ist in der öffentlichen Diskussion wiederholt und nicht ganz zu Unrecht betont worden, daß erst die Datenfernverarbeitung schwerwiegende Datenschutzprobleme mit sich bringe. Am Beginn entsprechender Globalplanungen muß nun mit Nachdruck dafür gesorgt werden, daß Datenschutz und Datensicherheit bei allen Überlegungen mit an vorderster Stelle zu rangieren haben. Hierauf hat die OECD wiederholt in begrüßenswerter Klarheit hingewiesen. Die Kommission der Europäischen Gemeinschaften hat Maßnahmen zum Schutz des Bürgers und die Regelung des Zugangs zu den gespeicherten Informationen als ein lebenswichtiges Problem und die Erstellung gemeinsamer Grundregeln auf der Basis einer breiten Meinungsbildung für erforderlich bezeichnet (vgl. Bundestags-Drucks. 7/1531).

Die zunehmenden internationalen Beziehungen in Staat und Wirtschaft verleihen der Problematik schon heute aktuelle Bedeutung. Die Freizügigkeit auf dem europäischen Arbeitsmarkt und die Heranziehung ausländischer Arbeitnehmer haben zu einem enormen Anstieg des internationalen Transfers von personenbezogenen Daten geführt. Schon im Bundesdatenschutzgesetz sollten deshalb Vorkehrungen zur Regulierung des grenzüberschreitenden Datenverkehrs getroffen werden. Darüber hinaus müssen internationale Vereinbarungen angestrebt werden, weil erst davon ein voll wirksamer Schutz zu erwarten ist.

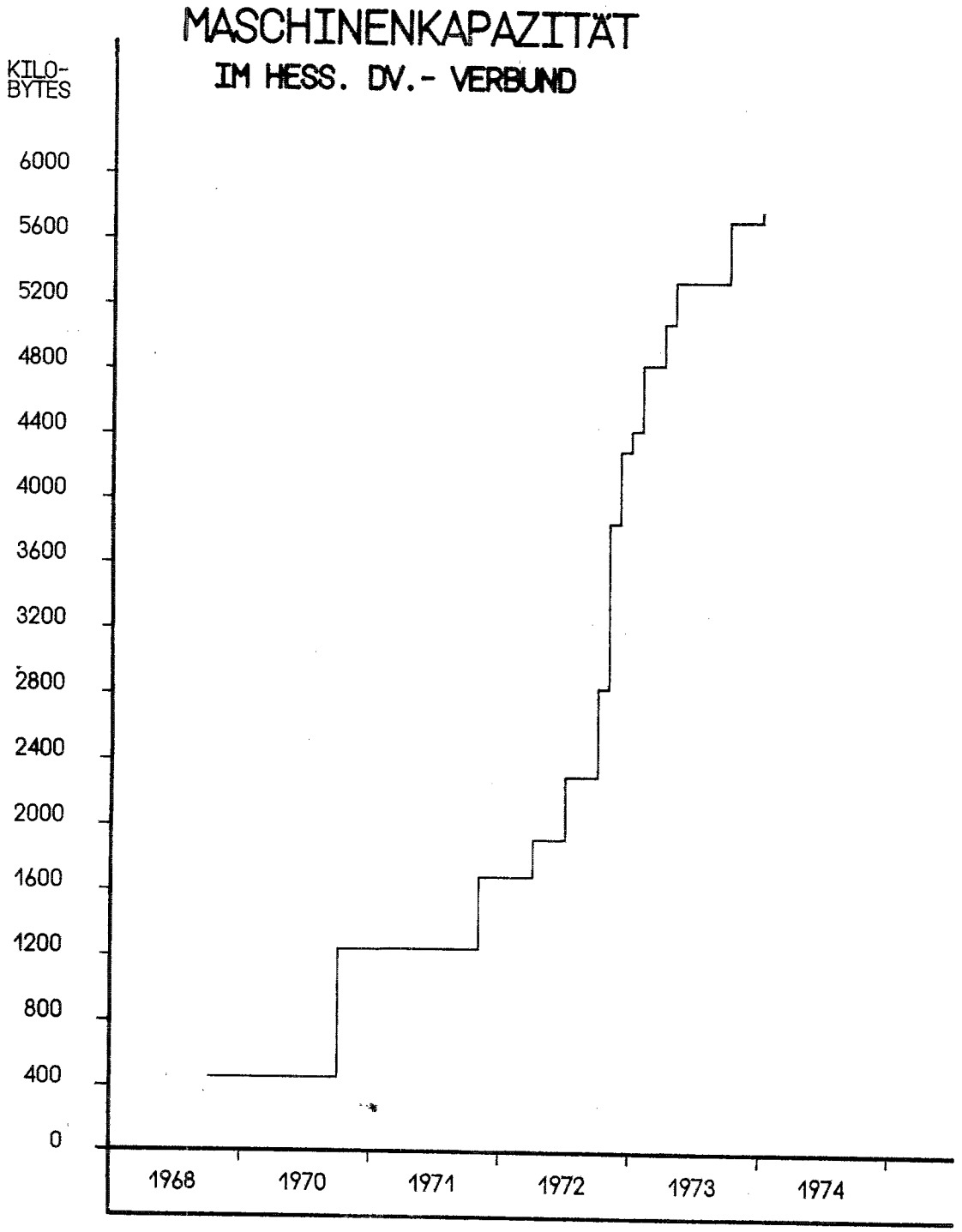
3. BESTANDSAUFNAHME

3. **Bestandsaufnahme**

Die Bestandsaufnahme über vorhandene EDV-Anlagen, über die zur Datenverarbeitung benutzten Erfassungsbogen und über die Datenschutzmaßnahmen bei den Behörden, Stellen und Körperschaften des öffentlichen Rechts wurde fortgeschrieben. Die im Berichtszeitraum eingegangenen Meldungen haben den Bestand nur unwesentlich verändert. Man kann davon ausgehen, daß die Beschaffung der Grundausstattung mit EDV-Anlagen in Hessen bei Behörden, Körperschaften des öffentlichen Rechts und anderen Stellen im großen und ganzen abgeschlossen ist. Es gibt auch nur noch wenige Gemeinden, die mit eigenen EDV-Anlagen rechnen oder die bei kommunalen Sparkassen rechnen lassen.

Zugenommen hat im Berichtsjahr die Zahl der Datenerfassungsstellen. Außer den schon länger bestehenden Kommunalen Datenerfassungszentralen in Hessen (KDH), die vom Hessischen Städte- und Gemeindebund getragen werden, wurden besonders von den größeren Gemeinden und Landkreisen im Raume Starkenburg 32 Datenerfassungsplätze eingerichtet, die sich zu einer Arbeitsgemeinschaft zusammengeschlossen haben.

Vor allem hat sich die Zahl der durch EDV bearbeiteten Fälle erhöht. Die Leistungssteigerung konnte durch Ausweitung der Maschinenkapazität erbracht werden. Waren in Hessen im Oktober 1968 bei den Landes- und Kommunalverwaltungen 10 Maschinensysteme mit einer Kapazität von insgesamt 520 K (Kilobyte) installiert, so sind es heute 16 Maschinensysteme mit einer Kapazität von insgesamt 5 776 K, 143 Platteneinheiten und 90 Bandeinheiten. Hinzu kommen noch die Maschinensysteme des Hessischen Landeskriminalamtes und des Statistischen Landesamtes.



(Quelle: Eigenerhebung DSB)

Die Grafik kann nur andeuten, welche Datenmengen verarbeitet und gespeichert werden. Nachstehende, nicht vollständige Übersicht soll verdeutlichen, auf welchen Gebieten bereits Einzelaufgaben in die automatische Datenverarbeitung einbezogen sind bzw. demnächst einbezogen werden.

4. AUFGABEN UND TÄTIGKEITEN DES DATENSCHUTZBEAUFTRAGTEN

4. Aufgaben und Tätigkeiten des Datenschutzbeauftragten

4.1 Der Schutz des Persönlichkeitsrechts

Die Aufgabe, die vertrauliche Behandlung der Angaben der Bürger und der über die einzelnen Bürger vorhandenen Unterlagen bei der maschinellen Datenverarbeitung zu überwachen (§ 10 Abs. 1 DSG), ist aufgrund der fortschreitenden Durchdringung der Datenschutzprobleme einerseits und der Entwicklung immer stärker integrierter Dateien oder Datenbanken andererseits stets von neuem zu analysieren. Mit den Begriffen der Privatsphäre oder der Intimsphäre kommt man, wie bereits im zweiten Tätigkeitsbericht (II, 4.1.2.1/2) dargelegt, nicht weiter. Diese Begriffe bleiben ebenso wie der Begriff des aus Art. 1 und Art. 2 GG abgeleiteten Persönlichkeitsrechts zu sehr im Allgemeinen.

In der Praxis ergibt sich jedoch immer wieder die Notwendigkeit, konkret zu bestimmen, ob eine Maßnahme der öffentlichen Verwaltung die Vertraulichkeit der Information des Bürgers wahrt oder ob und inwieweit sie sie verletzt. Fest steht nur, daß das Schutzbedürfnis personenbezogener Informationen in den vielfältigen Lebenslagen des Individuums durchaus verschieden ist. Welche Information vertraulich zu behandeln ist, kann allein aus dem Inhalt der Information nicht abgeleitet werden. Geschütztes Rechtsgut i. S. des Datenschutzgesetzes ist das Selbstbestimmungsrecht des einzelnen, d. h. das Recht jedermanns zu bestimmen, ob die Umwelt und wer von den Mitmenschen Informationen über ihn erhalten soll.

Die Ermittlung, Speicherung und Verarbeitung personenbezogener Daten durch den Staat kann schon ein Eingriff in das Persönlichkeitsrecht sein und bedarf daher der gesetzlichen Ermächtigung. Auch soweit der einzelne durch sein Verhalten, durch das Erscheinungsbild, das er in der Öffentlichkeit von sich entstehen läßt, Informationen über sich preisgibt oder soweit er freiwillig Auskünfte über sich gibt, kann im Bereich der öffentlichen Verwaltung auf eine gesetzliche Bindung der Behörden hinsichtlich der Erfassung und Verwertung solcher Informationen nicht verzichtet werden.

Welche Qualität eine Information hat, hängt weitgehend von dem Zusammenhang (Kontext) ab, in den sie gestellt, oder von dem Zweck, der mit ihrer Verwendung verfolgt wird. Auch die „Freiwilligkeit" der Auskunftserteilung ist eine unzulängliche Rechtfertigung für das Eindringen in die Privatsphäre, weil die Freiheit der Selbstbestimmung vielfach dadurch eingeschränkt ist, daß der einzelne durch den behördlichen Apparat und durch die Befürchtung von Nachteilen für den Fall der Auskunftsverweigerung verunsichert ist. Der Datenschutz ist im Bereich der öffentlichen Verwaltung als ein Mittel einer humanen Steuerung der immer stärker automatisierten Verwaltung zu betrachten, zumal mit der Einführung des Personenkennzeichens neue Impulse für eine „Verwaltung" des Bürgers gesetzt werden.

Daher muß gefordert werden, daß der Bürger, wenn er den Behörden Auskünfte über sich oder seine Familie geben soll, darüber aufgeklärt wird,

- für welchen Verwaltungszweck sie gebraucht werden,
- bei welchen Stellen sie gespeichert und
- an welche anderen Stellen sie weitergeleitet werden

und

- durch welche Maßnahme der Mißbrauch, die zweckwidrige Verwendung oder der Zugriff Unbefugter verhindert werden.

Diese Aufklärung ist insbesondere geboten, wenn der Bürger die Auskünfte mangels einer gesetzlichen Verpflichtung freiwillig geben soll. In diesen Fällen muß er auch darüber ausdrücklich unterrichtet werden, daß er nicht verpflichtet ist, die erbetene Information zu geben, und daß ihm aus der Verweigerung der Auskunft keine Nachteile entstehen. Aber auch der Gesetzgeber sollte, wenn er den Bürger zu Auskünften verpflichtet, die Behörden anweisen, den Bürger im vorstehenden Sinne aufzuklären.

4.1.1 Schutz medizinischer Daten

Der zweite Tätigkeitsbericht enthält die Feststellung, daß es beim Schutz medizinischer Daten weniger darauf ankommt, welche Daten gespeichert werden, als darauf, „sicherzustellen, daß diese Daten nicht oder nur mit Billigung der Patienten weitergegeben werden, es sei denn, daß die Weitergabe gesetzlich vorgeschrieben ist" (II, 4.1.2.3, S. 27). Dies wird damit begründet, daß aufgrund der vielfältigen Lebensumstände ohnehin nur unvollkommen durch den Gesetzgeber geregelt werden kann, welche Daten wann und von wem gespeichert werden dürfen und welche nicht.

Dieser Schutz durch Kontrolle der Datenweitergabe bedarf im medizinischen Bereich besonders strenger Maßstäbe. Diese bestehen vor allem in der Beachtung der Willensentscheidung des Patienten selbst; darüber hinaus aber in einer genauen Regelung des Zugriffsrechts auf medizinische Daten, in der Festlegung von Löschungsfristen und in der Anonymisierung (Verschlüsselung) von Daten.

Anlaß zur Verwirklichung dieser Grundsätze boten sich im Berichtsjahr auf medizinischem Gebiet in drei Teilbereichen, nämlich im Krankenhauswesen, beim Krankentransport und auf dem Gebiet medizinischer Datenbanken.

4.1.1.1 Krankenhauswesen

Die vom Hessischen Datenschutzbeauftragten erarbeitete „Formulierungshilfe" zum Datenschutz im Hessischen Krankenhausgesetz (vgl. zweiten Tätigkeitsbericht, Anlage 2) wurde – in wesentlichen Teilen wörtlich – als §§ 13 und 14 in das Hessische Krankenhausgesetz aufgenommen;

diese Datenschutzbestimmungen sind nunmehr geltendes Recht. Eine aufgrund von § 13 des Hessischen Krankenhausgesetzes vorgesehene Rechtsverordnung, die insbesondere die mit dem Krankenhaus-Verbund zusammenhängenden Probleme – auch solche des Datenschutzes – rechtlich regeln soll, befindet sich nach einer Auskunft des Hessischen Sozialministers gegenwärtig noch im Stadium der Vorbereitung.

4.1.1.2 Krankentransport

Aus der Anwendung der EDV im Krankentransportwesen ergeben sich folgende Probleme: Da sich das hessische Datenschutzgesetz nur auf die maschinelle Datenverarbeitung in der öffentlichen Verwaltung bezieht (vgl. § 1 DSG), war zunächst unklar, inwiefern beim Krankentransport durch private Organisationen (Rotes Kreuz, Arbeiter-Samariter-Bund, Johanniter Unfallhilfe und Malteser-Hilfsdienst) der Schutz medizinischer Daten gewährleistet ist.

Innerhalb des Hessischen Datenverarbeitungs-Verbundes (HZD/KGRZ) liegt der Abschlußbericht einer Aufgabenuntersuchung über Krankentransport und Rettungsdienst vor. Anregungen des Hessischen Datenschutzbeauftragten haben ihren Niederschlag gefunden in einer vom zuständigen Unterausschuß „Krankentransport und Rettungsdienst" formulierten Neufassung des Kapitels 5.26 „Datenschutz" dieses Abschlußberichtes:

„1. Die Auftraggeber (Krankentransportunternehmen, z. B. Rotes Kreuz usw.) haben alle medizinischen Daten zu vernichten, sobald das zuständige Rechenzentrum diese Daten als fehlerfrei erkannt und eingespeichert hat.

2. Die Berechtigung zum Zugriff auf personenbezogene Daten wird nur den Auftraggebern ermöglicht. Die Berechtigung zum Zugriff beschränkt sich auf personenbezogene Daten, die vom Auftraggeber ermittelt und erfaßt worden sind. Die Berechtigung zum Zugriff auf personenbezogene medizinische Daten ist ausgeschlossen.

3. Die Auftraggeber erhalten statistische Unterlagen, Daten und Ergebnisse nur im Rahmen der von ihnen ermittelten und erfaßten Daten.

4. Zum Zwecke der wissenschaftlichen, statistischen und sonstigen im öffentlichen Interesse liegenden Auswertungen dürfen die Rechenzentren mit schriftlicher Ermächtigung der Auftraggeber Daten (ohne Angabe personenidentifizierender Merkmale), Auswertungen, Ergebnisse und Statistiken an ausdrücklich zu benennende Empfänger weitergeben.

Um sicherzustellen, daß nicht vor der Verarbeitung der erfaßten Daten ein unberechtigter Zugriff ermöglicht wird, enthält die Erstausfertigung des Erfassungsbogens für medizinische Daten außer der Transportkennummer keine weiteren personenidentifizierenden Angaben."

4.1.1.3 Medizinische Datenbanken

Die Problematik medizinischer Datenbanken läßt sich an folgenden Beispielen erläutern, nämlich an den Planungen für einen Informations-Verbund mehrerer Krankenhäuser, für eine Datenbank zur Förderung des Leistungssports in der Schule und für eine Datenbank der Gesundheitsämter: Weil der durch die elektronische Datenverarbeitung angestrebte Rationalisierungserfolg nicht durch eine Beeinträchtigung des Persönlichkeitsrechts erkauft werden darf, müssen gleichzeitig und parallel mit der Entwicklung neuer EDV-Verfahren auch die entsprechenden Datenschutzverfahren und -maßnahmen festgelegt werden. Es genügt nicht, die Projekte aufzubauen und nach ihrer Fertigstellung noch ein paar Datenschutzmaßnahmen „anzuhängen". Nur wenn von vornherein jede Einzelmaßnahme und das Gesamtprojekt aus dem Blickwinkel des Datenschutzes kritisch betrachtet werden, ist es möglich, „Löcher" im Schutz zu verhindern.

Das erste Beispiel betrifft ein vom Bundesminister für Forschung und Technologie ausgeschriebenes Demonstrationsprojekt zur Planung eines „Datenverarbeitungseinsatzes zur Lösung überbetrieblicher Organisations- und Management-Aufgaben durch Integration des normierten Informationsflusses zwischen verschiedenen Einrichtungen des Gesundheitswesens" (DOMINIG). Von dem Projekt, das sich in zwei Teile gliedert, interessiert hier das Teilprojekt II, welches den Informationsverbund mehrerer Krankenhäuser unter Benutzung eines zentralisierten DV-Systems betrifft.

„Ziel dieses Teilprojektes ist es, eine Verbesserung der Informationserfassung, -speicherung und Informationsnutzung für die stationäre und halbstationäre Versorgung durch einen zentralisierten DV-Verbund mehrerer Krankenhäuser unter Berücksichtigung der Erfordernisse des Datenschutzes zu erreichen" (Bekanntmachung des BMFuT vom 3. 8. 1973, BAnz. Nr. 148 vom 10. 8. 1973). Hier wird schon in der Ausschreibung gleiches Gewicht auf die Erfordernisse der Wirtschaftlichkeit und des Datenschutzes gelegt.

Dies entspricht der hessischen Praxis, bei der schon im Stadium der Vorplanung neuer Projekte innerhalb der Automationsausschüsse (Land und Gemeinden) auch die Erfordernisse des Datenschutzes angesprochen werden. Dabei kommen den Planungen die bereits in über dreijähriger Praxis mit dem hessischen Datenschutzgesetz gewonnenen Erfahrungen zugute. Die Voraussetzungen zur Verwirklichung des DOMINIG-Projektes des Bundesministers für Forschung und Technologie sind dementsprechend in Hessen in besonderem Maße gegeben.

Die folgenden beiden Beispiele illustrieren die Gefahr, daß selbst dann, wenn bei der Planung des Einzelprojektes Datenschutzüberlegungen Berücksichtigung finden, der Datenschutz insgesamt zu kurz kommen kann. Dies ist dann möglich, wenn es sich bei den Einzelprojekten um Teile eines für später geplanten Gesamt-Informationssystems handelt. Um einen solchen Fall handelt es sich bei den Projekten „schulsportärztlicher Untersuchungsbogen" und „EDV im Gesundheitsamt": Wie aus den Aufgabenbeschreibungen beider Projekte hervorgeht, soll sowohl die sportärztliche Untersuchung wie auch die Dokumentation im Gesundheitsamt so ausgestaltet werden, „daß eine langfristige Weiterverwendung im Rahmen eines Gesundheitsinformationssystems möglich ist".

Die Zielsetzung der Projekte kann wie folgt umschrieben werden: Das mit dem Arbeitsbegriff „schulsportärztlicher Untersuchungsbogen" bezeichnete Projekt, das unter anderem dazu dient, „daß im Rahmen der Talentförderung mit Hilfe der Schule für alle Schüler und Schülerinnen, die in Leistungsgruppen oder einem Schulsportzentrum aufgenommen worden sind, die sportärztliche Überwachung gesichert ist", hat insbesondere zum Ziel, „erkennbares gesundheitliches Risiko durch Sport vom Sportler abzuwenden, den Sportler von konstitutionsbedingt ungünstigen Sportarten abzuhalten und zu günstigen hinzuführen". Der Entwurf des Projekts enthält erfreulicherweise in seinem Sollvorschlag auch bereits konkrete Bestimmungen über Datenschutz. Durch das Projekt „EDV im Gesundheitsamt" soll die „Verbesserung der gesundheitlichen Betreuung der Bevölkerung, insbesondere der Für- und Vorsorge und des medizinischen Umweltschutzes", erreicht werden; es soll darüber hinaus „Erkenntnisse zur Strukturverbesserung der Gesundheitsämter" erbringen und die „Bereitstellung von Planungsunterlagen" ermöglichen. Auch hier sind in einem besonderen Abschnitt Datenschutzbestimmungen vorgesehen.

Die schulsportärztliche Untersuchung, ihrerseits Teil einer geplanten Jugendgesundheitskarte" (die außerdem Neugeborenenuntersuchung, Kleinkinderuntersuchung, schulärztliche Untersuchung und Jugendarbeitsschutzuntersuchung umfassen soll), stell zusammen mit dem Impfwesen und der Dokumentation im Gesundheitsamt die z. Z. geplanten bzw. verwirklichten Teilbereiche eines späteren Gesundheitsinformationssystems dar. Ein solches Gesundheitsinformationssystem bringt die nahezu lückenlose Erfassung der medizinischen Daten eines Bürgers mit sich. Während heute die ständige ärztliche Überwachung nur bei bestimmten Krankheiten möglich ist und die Ausnahme darstellt, könnte sie nach Installation eines solchen Systems zur allgemeinen Regel werden.

Aus der Betrachtung der beiden geplanten Projekte kann folgendes entnommen werden: Obwohl bei der Planung von Anfang an Datenschutzfragen bewußt berücksichtigt wurden, zeichnet sich im Hinblick auf die Möglichkeiten der späteren Eingliederung in ein Gesamtinformationssystem eine für den Datenschutz unbefriedigende Entwicklung ab.

4.1.2 Personaldatenbanken

Der Hessische Datenschutzbeauftragte beobachtet sorgfältig die Entwicklung auf dem Gebiet der Planung von Personalinformationssystemen, wie sie gegenwärtig in verschiedenen Bundesländern zu erkennen ist. Auf diesem Gebiet besteht seit einiger Zeit eine Arbeitsgruppe „Personaldateien Bund/Länder/kommunaler Bereich", die gebildet wurde, um für Bund, Länder und Kommunalbereich Vorschläge für ein einheitliches Personalinformationssystem zu erarbeiten. Dieses System wurde zunächst so definiert, daß darin Dateien des Personalwesens, wie Personaldatei, Besoldungs-, Vergütungs- und evtl. Stellenplandatei ineinander integriert werden sollten. Infolge mangelnder Einigung über ein gemeinsames Konzept ist diese Gemeinschaftsarbeit jedoch wieder ins Stocken geraten: Die Vorstellungsbreite bewegte sich dabei zwischen einer „Personalstrukturdatei" für die Planung und einem „integrierten Personalinformationssystem", das in der Lage wäre, ein umfassendes Persönlichkeitsbild jedes einzelnen Bediensteten bereitzustellen. Während das Modell einer Personalstrukturdatei überwiegend mit aggregierten bzw. anonymisierten Daten auskommt und daher aus der Sicht des Datenschutzes keine wesentlichen Probleme erwarten läßt, wirft das Modell eines integrierten Personalinformationssystems in der öffentlichen Verwaltung eine ganze Reihe von Fragen des Datenschutzes auf.

In Hessen sind gegenwärtig Ansätze zur Entwicklung von Personaldatenbanken nur im Bereich des Kultusministers zu erkennen. Bisher wurde lediglich eine als Diskussionsentwurf bezeichnete Studie einer Schülerdatei für Hessen vorgelegt, die bisher noch nicht zu einem konkreten Verwaltungsprojekt geführt hat. Darüber hinaus existieren Vorversuche über die Einrichtung einer Lehrerindividualdatei. Wenngleich es im jetzigen Zeitpunkt noch zu früh für eine Stellungnahme ist, so erscheint doch aus der Sicht des Datenschutzes folgende Überlegung angebracht: Wie schon im Hinblick auf die Entwicklung medizinischer Datenbanken oben unter Ziffer 4.1.1.3 ausgeführt wurde, sollte die Planung solcher Dateien, die auch sensitive Daten enthalten (wie z. B. Examensnoten der Lehrer, Angaben in den Schülerdateien über „langfristige Heimaufenthalte" (Krankenhaus, Sanatorium, Heilpädagogisches Heim, Fürsorgeerziehung) sowie Vater- bzw. Mutterschaften von Anfang an zwei Ziele im Auge haben, nämlich neben dem angestrebten Rationalisierungserfolg den Schutz des Individuums vor Beeinträchtigung seines Persönlichkeitsrechts. Im Hinblick darauf stellt sich die Frage, ob nicht eine breite Diskussion mit den Betroffenen über Absicht und Zweck des Projektes, über die verschiedenen Stufen seiner Realisierung und über die Möglichkeiten seiner Verwirklichung der Erarbeitung eines Modells vorausgehen sollte. Wie aus Erfahrungen bei statistischen Erhebungen bekannt ist, ist nicht zuletzt die Mithilfe der Betroffenen eine wichtige Voraussetzung für das Funktionieren einer solchen Maßnahme der Verwaltungsrationalisierung.

Schließlich ist daran zu denken, daß ebenso wie beim Krankenhauswesen (§§ 13 und 14 des Hessischen Krankenhausgesetzes) eine Verrechtlichung, also der Erlaß spezieller Rechtsvorschriften über den Datenschutz bei Personaldatenbanken, ins Auge gefaßt werden sollte. Für diese rechtliche Normierung kämen beispielsweise folgende Fragen in Betracht: Zu welchem Zweck wird die Datenbank eingerichtet, sind die Angaben freiwillig oder nicht, wo werden sie gespeichert, wer hat Zugriff, zu welchem Zweck, und durch wen werden sie ausgewertet?

4.1.3 Einwohnerwesen

Im Einwohnerwesen wird gegenwärtig an der Entwicklung eines „Auskunftssystems" gearbeitet. Es soll die Meldeämter in den Stand setzen, über Datenstationen und Fernleitungen Daten aus der beim KGRZ installierten Einwohnerdatenbank abzurufen, um den Betroffenen so-

wie staatlichen und privaten Stellen Auskünfte erteilen zu können.

Aus der Sicht des Datenschutzes ergeben sich daraus die nachfolgenden technischen und organisatorischen Anforderungen:

a) Bei der Protokollierung von Abrufen aus der Datenbank sollen alle Tatsachen aufgezeichnet werden, die erforderlich sind, um nachträglich die Rechtmäßigkeit des Vorganges überprüfen zu können. Deshalb ist bei Auskünften an Privatpersonen zu protokollieren, auf Grund welcher berechtigten Interessen (im Sinne des künftigen Bundesmeldegesetzes) eine Auskunft erteilt worden ist. Der abrufende Bedienstete des Meldeamtes und der Auskunftsuchende bzw. die ersuchende staatliche Stelle müssen nachträglich zu ermitteln sein. Um Versuche einer mißbräuchlichen Inanspruchnahme des Systems entdecken zu können, ist die Aufzeichnung auch der abgelehnten Anfragen erforderlich.

b) Das System soll eine in sachlicher und regionaler Hinsicht möglichst flexible Festlegung von Zugriffs- und Verarbeitungsberechtigungen zulassen. Jeder zugriffsberechtigten Stelle und jedem Bediensteten darf jeweils nur der Teil der Daten zugänglich gemacht werden, den sie aufgrund ihrer Zuständigkeit benötigen.

c) Die Einführung des neuen Verfahrens wird bei vielen Gemeinden dazu führen, daß eine größere Anzahl von Daten für jeden Einwohner gespeichert wird. Dies gibt Anlaß, auch die Frage der Prüfung der Identität des Anfragenden durch den Meldeamtsbediensteten neu zu überdenken. Eine einheitliche Ausgestaltung der inhaltlichen und verfahrensmäßigen Anforderungen ist wünschenswert, damit einmal jeder Bürger weiß, wie stark seine Daten geschützt sind, und damit zum anderen auch der Datenschutzbeauftragte seine Kontrollfunktion wirksam wahrnehmen kann.

d) Bei maschinell erstellten Gruppenauswertungen erscheint eine Rückkontrolle auf seiten der Verwaltung angebracht, um festzustellen, ob die Datenschutzvorschriften, insbesondere etwa vorhandene Sperren, berücksichtigt worden sind.

e) Zu gegebener Zeit werden geeignete organisatorische und personelle Maßnahmen bei den Meldeämtern zu ergreifen sein, die ihrer veränderten Funktion und Bedeutung Rechnung tragen. Hierfür könnte eine Musterdienstanweisung erarbeitet werden.

4.1.4 Statistisches Landesamt und HZD

Die Hessische Zentrale für Datenverarbeitung (HZD) soll grundsätzlich alle im Bereich der Landesverwaltung anfallenden Aufgaben der maschinellen Datenverarbeitung durchführen. Eine Ausnahme von diesem Grundsatz bestand bisher u. a. für die amtliche Statistik. Das Statistische Landesamt unterhält z. Z. für seine Aufgaben ein eigenes Rechenzentrum. Aus Rationalisierungsgründen sowie zur Verbesserung der Ausgangsbedingungen für die Entwicklung eines funktionsfähigen Landesinformationssystems ist nunmehr vorgesehen, die maschinellen Abschnitte der statistischen Aufgabenerfüllung in die Organisation der HZD zu integrieren. Nach einer Übergangszeit soll das Rechenzentrum des Statistischen Landesamtes aufgelöst werden. Eine vergleichbare Abwicklung der statistischen Aufgaben gibt es schon bisher in einigen Bundesländern, in denen entweder Rechenzentren anderer Ressorts oder Rechenzentren mit eigener Rechtspersönlichkeit (Schleswig-Holstein) die statistischen Aufgaben maschinell erledigen.

Diese Lösungen sind nicht nur hinsichtlich der Rationalisierung und der Effektivität zu überprüfen. Ebenso muß der Datenschutz in die Überlegungen einbezogen werden.

Die Übernahme der maschinellen Datenverarbeitung der Statistik durch die HZD wird zu einer weiteren Konzentration empfindlicher personenbezogener Daten an einem Ort führen. Damit vergrößert sich die Gefahr, daß ein Zugriff auf eine große Menge von geschützten Daten an einer Stelle möglich wird, wenn es gelingt, dort in das Sicherheitssystem einzubrechen. Andererseits entspricht die Zusammenfassung dem Fort-Knox-Prinzip: Sie erlaubt eine Konzentration der Sicherheitsanstrengungen mit dem Ziel der Errichtung eines Sicherheitssystems von hoher Qualität.

Hierzu treten jedoch spezifische, gerade für die Statistik geltende Probleme: Nach § 12 Bundesstatistikgesetz dürfen „Einzelangaben auf dem Dienstweg" nur an die fachlich zuständigen obersten Bundes- und Landesbehörden oder die von ihnen bestimmten Stellen weitergeleitet werden, „wenn und soweit dies in den die Statistik anordnenden Rechtsvorschriften zugelassen und in den Erhebungsdrucksachen bekanntgegeben worden ist". Eine Zusammenfassung von Angaben mehrerer Auskunftspflichtiger ist keine Einzelangabe im Sinne des Statistikgesetzes. Danach ist die Weitergabe aggregierter Daten zulässig. Vom Datenschutz her ist dies so zu verstehen, daß die weitergegebenen Daten keine Rückschlüsse auf Einzelpersonen zulassen dürfen.

Die Überlassung statistischer Unterlagen an das Rechenzentrum einschließlich der Identifizierungsmerkmale (Name, Anschrift, Geburtsort und -datum) erscheint rechtlich daher nur dann zulässig, wenn man das Rechenzentrum nicht als eine „andere" Behörde oder Stelle betrachten könnte. Es dürfte die Verarbeitung nicht selbst als Körperschaft des öffentlichen Rechts übernehmen, so daß die Verantwortlichkeit für die Geheimhaltung seinen Organen zufiele. Vielmehr müßte vorausgesetzt werden, daß das Rechenzentrum nur seine technischen und personellen Einrichtungen dem statistischen Landesamt zur eigenverantwortlichen Verarbeitung des Datenmaterials überließe. Diese Lösung würde sehr komplexe Sicherungsvorkehrungen und eine strikte Abschottung der vom Statistischen Landesamt benutzten Einrichtungen von den übrigen Einrichtungen des Rechenzentrums erfordern. Weder die Organe des Rechenzentrums noch deren Bedienstete dürften Einfluß auf die Verarbeitung und deren Ablauf nehmen können. Deshalb ist diese Lösung kaum realisierbar.

Diese Beurteilung der Sach- und Rechtslage führt zu der Mindestforderung, die Identifizie-

rungsmerkmale von den Unterlagen der Statistischen Landesämter abzutrennen und zurückzubehalten, bevor die Unterlagen an die HZD weitergegeben werden (vgl. 4.2.3).

4.1.5 Besondere Informationssysteme

In den elektronischen Informationssystemen der Polizei und der Nachrichtendienste ist die Datenfernverarbeitung am weitesten entwickelt. In beiden Fällen handelt es sich um Verbundsysteme, die über Hessen hinausgehen. Von welch entscheidender Bedeutung die datenschutzmäßige Absicherung gerade dieser Systeme für die Freiheit des einzelnen ist, wird in Verwaltung und Öffentlichkeit erst allmählich erkannt*).

4.1.5.1 Umgang mit Daten im Polizei-Informationssystem (HEPOLIS, INPOL)

Im Berichtszeitraum ist der Aufbau des automatisierten **He**ssischen **Pol**izei-**I**nformationssystems – kurz HEPOLIS genannt – weiter fortgeschritten. Gegenüber der Darstellung im zweiten Tätigkeitsbericht haben sich folgende Veränderungen ergeben: Provisorisch wurde HEPOLIS über eine Datenabrufstation mit den automatisierten **I**nformations- und Auskunftssystemen für die gesamte **Pol**izei der Bundesrepublik – genannt INPOL – verbunden. Die erste Aufbauphase von HEPOLIS soll bis zum 1. Juli d. J. abgeschlossen sein. Dann kann jeder Polizeibeamte über die an die Zentrale in Wiesbaden angeschlossenen 32 Datenabrufstationen in den örtlichen Polizeidienststellen Angaben aus der 160 000 Personen umfassenden Personendatenfahndungsdatei abrufen.

Zu Beginn der 2. Aufbauphase soll HEPOLIS noch im 2. Quartal 1974 den Dialogverkehr mit INPOL aufnehmen. In dieser Phase wird auch der Aufbau der Dateien für die Sachfahndung, über Straftäter und Straftaten abgeschlossen werden. Damit stehen in dem polizeilichen Informationsverbundsystem in absehbarer Zeit Daten von einigen Millionen Personen zur Verfügung. Darunter befinden sich nicht nur Täterdaten, sondern auch die Daten von Opfern oder Zeugen von Straftaten.

Für eine präventive Verbrechensbekämpfung und eine wirksame Verfolgung von Straftätern benötigt die Polizei ohne Zweifel eine umfassende Datenbasis. Dabei ist es aber notwendig, daß der Zugriff zu diesen Daten durch Rechtsnormen abgegrenzt und festgelegt wird.

Eine rechtliche Normierung der Auskunfts- und Abrufberechtigung sowie der Löschung von Daten wurde deshalb bereits im zweiten Tätigkeitsbericht angeregt (II, 4.1.1.3 c und 5.3).

In ihrer Stellungnahme*) hat die Landesregierung bestätigt, daß „zusätzliche Überlegungen für den Datenschutz erforderlich" seien und die „Richtlinien für die Führung von Kriminalakten ... einer Überarbeitung bedürfen". Änderungen der geltenden Vorschriften und ihre Umwandlung in formelle Rechtsnormen müßten jedoch mit den anderen Ländern abgestimmt werden.

*) Vgl. Dammann/Karhausen/Müller/Steinmüller, Datenbanken und Datenschutz, Frankfurt/M. 1974, S. 33 ff., 41 ff.)

Obwohl sich eine Bund-Länder-Kommission mit diesen Fragen befaßt, ist eine bundeseinheitliche Regelung durch formelle Rechtsnormen in absehbarer Zukunft nicht zu erwarten. Solange aber diese bundeseinheitliche Regelung fehlt, muß es den Ländern überlassen bleiben, in ihrem Bereich neue Rechtsnormen für den Umgang mit Daten aus dem Kriminalbereich zu schaffen, wenn die geltenden als nicht mehr ausreichend angesehen werden. Das Land Hessen war das erste Land, das ein Datenschutzgesetz verabschiedet hat. Es hat damit der Gesetzgebung in Bund und Ländern und auch im Ausland wertvolle Anregungen gegeben. Jetzt könnte es durch die Erarbeitung klarer Rechtsnormen für die Auskunfts- und Abrufberechtigung sowie für die Löschungs- und Sperrfristen für Daten im Informationssystem der Polizei (und in dem des Verfassungsschutzes) erneut für die Entwicklung einer bundeseinheitlichen Regelung wichtige Anstöße liefern.

Einige Grundsätze für den Umgang mit erkennungsdienstlichen Unterlagen sind von der Rechtsprechung bereits entwickelt worden. Das Bundesverwaltungsgericht hat z. B. entschieden, daß eine Aufbewahrung nicht gerechtfertigt sei, wenn kein Anhaltspunkt dafür vorliegt, daß die erkennungsdienstlich behandelte Person zukünftig strafrechtlich in Erscheinung treten werde und die Unterlagen hierbei die Ermittlungen der Polizei fördern könnten. Nur wenn in einem mit Freispruch beendeten Strafverfahren die gegen den Angeklagten sprechenden schwerwiegenden Verdachtsmomente nicht ausgeräumt wurden, könne es notwendig sein, die erkennungsdienstlichen Unterlagen noch weiter aufzubewahren **).

Für die Notwendigkeit, durch Rechtsnormen verbindlich zu regeln, von wem, für wen und für welchen Zweck Informationen der Kriminalpolizei verwertet und verwendet werden dürfen, ergeben sich Maßstäbe aus dem Urteil des Bundesverfassungsgerichts vom 5. 6. 1973 (BVerfGE 35 202 – sogenanntes Lebach-Urteil).

> „Für die aktuelle Berichterstattung über schwere Straftaten verdient das Informationsinteresse der Öffentlichkeit im allgemeinen den Vorrang vor dem Persönlichkeitsschutz des Straftäters. Jedoch ist neben der Rücksicht auf den unantastbaren innersten Lebensbereich der Grundsatz der Verhältnismäßigkeit zu beachten; danach ist eine Namensnennung, Abbildung oder sonstige Identifikation des Täters nicht immer zulässig.
>
> Der verfassungsrechtliche Schutz der Persönlichkeit läßt es jedoch nicht zu, daß das Fernsehen sich über die aktuelle Berichterstattung hinaus, etwa in Form eines Dokumentarspiels, zeitlich unbeschränkt mit der Person eines Straftäters und seiner Privatsphäre befaßt (Leitsatz)."

Diese rechtsstaatlichen Erwägungen dürfen nicht durch den Abscheu vor der Tat der Verbrecher getrübt werden. Läßt man die Verwertung persönlicher Daten aus der Intimsphäre eines Beschuldigten oder eines Verurteilten auch nur in

*) LT-Drucks. 7/3511 vom 14. 6. 1973 — III/13.

**) BVerwG-Beschluß vom 18. 5. 1973 — IB 39/1973 in DÖV 1973, S. 752, ständige Rechtsprechung.

einem Falle, der wegen der besonderen Schwere des Verbrechens die Öffentlichkeit erregt hat, zu, so wird die Beachtung des Datenschutzes in diesem Bereich der willkürlichen Beurteilung durch den Beamten überlassen, der den Zugriff zu den Daten hat.

Dies gilt für die Verwendung von Informationen über einen Beschuldigten schlechthin, nicht nur in bezug auf das Fernsehen.

4.1.5.2 Weitergabe von Informationen des Verfassungsschutzes

Das Verfassungsschutzgesetz des Bundes in der Fassung vom 7. August 1972 (BGBl. 72/I, S. 1382) bestimmt, daß der Verfassungsschutz „bei der Überprüfung von Personen, denen im öffentlichen Interesse geheimhaltungsbedürftige Tatsachen, Gegenstände oder Erkenntnisse anvertraut werden" oder „die an sicherheitsempfindlichen Stellen ... beschäftigt sind" mitwirkt.

Die Ausführung des Gesetzes für die Weitergabe von Erkenntnissen des Verfassungsschutzes ist in Hessen durch Dienstanweisung geregelt. Die im zweiten Tätigkeitsbericht angeregte Verrechtlichung dieser Dienstanweisung sowie der Löschung bzw. Sperrung von Daten (vgl. II, 4.1.1.3 c und e und 5.3) hat bisher zu keinem Ergebnis geführt. Ebenso wie beim Polizeiinformationssystem soll eine bundeseinheitliche Regelung abgewartet werden. Solange diese aber fehlt, muß es auch hier den Ländern überlassen bleiben, die Amtshilfeverpflichtungen des Verfassungsschutzamtes in normativer Weise zu regeln, damit dem Bürger der größtmögliche Schutz gegen Mißbrauch der über ihn gespeicherten Informationen gewährt wird. Die nachrichtendienstliche Tätigkeit des Verfassungsschutzes braucht dadurch nicht beeinträchtigt zu werden. Das erfordert, daß die Generalklausel des § 2 DSG konkretisiert und im einzelnen bestimmt wird, wer im Sinne dieser Vorschrift befugt ist, Informationen vom Verfassungsschutzamt zu erhalten, wie die Information innerhalb der Verwaltung zu behandeln ist (Grad der Vertraulichkeit) und wie lange Informationen über den Bürger für den Zugriff oder für die Amtshilfe an andere Behörden vom Verfassungsschutzamt zur Verfügung gehalten werden. Wenn der Betroffene nach bestimmten Fristen nicht mehr in Erscheinung getreten ist, sollten die Daten gelöscht – d. h. physisch vernichtet – oder so gesperrt werden, daß der Zugriff nur aufgrund einer besonderen Anweisung zulässig ist.

4.1.6 Datenschutz im Verhältnis zwischen Staat und Kirche

Der im zweiten Tätigkeitsbericht (II, 4.1.1.3 f., S. 25) behandelte Fragenkomplex hinsichtlich der Wahrung des Steuergeheimnisses hat sich im Berichtszeitraum nur zum Teil erledigt.

Die Kirchen hatten ihre Forderungen nach einer möglichst umfassenden Einsichtnahme in staatliche Besteuerungsunterlagen damit begründet, daß sie ihr Recht, die Kirchensteuern zu stunden, zu erlassen oder niederzuschlagen, nur unter dieser Voraussetzung wahrnehmen könnten. Dieser Gesichtspunkt ist von den Kirchen in den weiteren Verhandlungen nicht mehr geltend gemacht worden.

Die Bedenken gegen die Einsichtnahme in Besteuerungsgrundlagen zum Zweck des sogenannten Finanzausgleichs zwischen Wohnsitzdiözese und Betriebsstättendiözese konnten in direkten Gesprächen mit dem Finanzministerium ausgeräumt werden.

4.1.7 Richtlinien für Verfahrensentwicklung

Das hessische Datenschutz-Modell bietet die rechtlichen und institutionellen Bedingungen für ein präventives Wirken. Der Datenschutzbeauftragte ist bestrebt, diese Chance zu nutzen, und ist um eine frühzeitige Beachtung des Datenschutzes bemüht. Er hat den Arbeitsausschüssen für die Automation der Verwaltungsaufgaben des Landes und der Gemeinden und Landkreise Vorschläge für eine verbesserte Behandlung des Datenschutzes im Rahmen der Verfahrensentwicklung vorgelegt. Um rechtzeitig eine ausreichende Informationsgrundlage zur Beurteilung der Schutzbedürftigkeit der Daten zu erhalten, hat er die Ausschüsse um Auskunft ersucht, welche Daten im Rahmen von geplanten Verfahren erfaßt, gespeichert sowie aus- und weitergegeben werden sollen. Soweit Daten für das zu automatisierende Verfahren routinemäßig von anderen Stellen der Verwaltung oder von Dritten bezogen werden, soll der Datenschutzbeauftragte auch hierüber sowie über die dafür maßgeblichen Rechtsvorschriften informiert werden.

Ferner wurde angeregt, bereits bei der Verfahrensgestaltung und -programmierung alle Vorkehrungen zur Anonymisierung vorzusehen, wenn eine Vergabe der Datenerfassung an private Serviceunternehmen in Betracht kommt (vgl. I, 1.3.2; II, 4.1.1.3 d). Schließlich hat der Datenschutzbeauftragte darauf hingewiesen, daß es der Datenschutz gebietet, bei jedem Verfahren die Fristen festzulegen, nach deren Ablauf die Daten zu löschen sind. Dabei wird nicht verkannt, daß hierbei Schwierigkeiten auftreten können, da neben der Anwendung der Vorschriften über Aufbewahrungsfristen auch der Informationsbedarf für Planungs- und Entscheidungshilfen nicht unberücksichtigt bleiben kann.

4.2 Erhaltung der Gewaltenteilung

Im Berichtszeitraum bildete der Hauptausschuß des Landtags eine Arbeitsgruppe EDV, die aus fünf Mitgliedern besteht. An ihren Sitzungen nehmen als Sachverständige Vertreter der Landesregierung, der HZD, des Landesrechnungshofs und der Datenschutzbeauftragte teil.

Der EDV-Referent des Landtags hatte bei Abschluß des Tätigkeitsberichts seine Arbeit noch nicht angetreten. Er wird nach seiner Einstellung ebenfalls an den Sitzungen der Arbeitsgruppe EDV teilnehmen.

4.2.1 Parlamentarische Informationsrechte

In der Arbeitsgruppe des Hauptausschuses für EDV-Fragen ist die Frage erörtert worden, welche „Zugriffsrechte" auf Daten dem Landtag nach § 6 Abs. 1 DSG zustehen und welche

Regeln für ihre Ausübung gelten sollten. Nach der Begründung zum Regierungsentwurf des Datenschutzgesetzes soll diese Vorschrift die Informationsmöglichkeit der parlamentarischen Körperschaften erweitern. „Ihnen wird der unmittelbare Zutritt zu den Stellen eröffnet, die Datenverarbeitungsanlagen betreiben. ... Die Exekutive kann damit durch den Betrieb von Datenverarbeitungsanlagen nicht mehr einen Informationsvorsprung vor den parlamentarischen Organen erlangen." Diese Zielsetzung, die auch in der amtlichen Überschrift der Vorschrift anklingt, steckt den Rahmen der Auskunftspflicht weit ab. „Auskünfte aufgrund der gespeicherten Daten" heißt nicht nur Auskünfte über die Art, den Umfang und die Qualität der gespeicherten Daten, sondern auch Auskunft über die Ergebnisse ihrer Verarbeitung, d. h. über die Information, welche die gespeicherten Datenarten beinhalten und aufgrund von Verknüpfungen (Verarbeitung) ergeben.

Die auskunftspflichtigen Behörden sind verpflichtet, die von ihnen gespeicherten Daten zu verarbeiten, wenn die vom Landtag (seinem Präsidenten oder seinen Fraktionen) gewünschten Auskünfte es erfordern und wenn Programme zur Auswertung vorhanden sind. Ob diese Voraussetzung vorliegt, wird im Einzelfall mit den auskunftspflichtigen Behörden zu klären sein. Hierfür sollten „Regeln" vereinbart werden, in denen auch die finanziellen Aufwendungen für die Herstellung von Auswertungsprogrammen zu berücksichtigen wären.

Die Eingrenzung der Auskunftspflicht auf aggregierte Daten im Sinne des § 5 Abs. 3 und auf die „Zuständigkeiten des Landtags" sollte dazu führen, daß innerhalb der Informationssysteme die Datenorganisation und die Datenstruktur sowie die Aufbereitungs- und Auskunftsprogramme von vornherein so gestaltet werden, daß ein Rückschluß auf Individuen ausgeschlossen ist.

Im Zusammenhang hiermit stellt sich die Frage, welches Geheimhaltungsbedürfnis bei den nach § 6 Abs. 1 DSG Auskunftsberechtigten besteht, wenn sie von den Landesbehörden, von der HZD oder den KGRZ Auskünfte aufgrund gespeicherter Daten verlangen. Dies gilt insbesondere, wenn die geforderten Informationen als Entscheidungshilfe bei der Vorbereitung von Initiativen, z. B. eines Gesetzentwurfs, einer Großen Anfrage oder dgl. von einer Fraktion gebraucht werden.

Der Regierung wird unter dem Gesichtspunkt der Gewaltenteilung (vgl. Urteil des Hess. StGH vom 24. 11. 1966, P.St. 414 – StAnz. 1966, S. 1612/1622) ein „Intern-Bereich" zugebilligt, welcher der Kontrolle des Parlaments entzogen ist. Auf den Landtag und seine Fraktionen kann diese Erwägung nicht übertragen werden, u. a. schon deswegen nicht, weil die Regierung keine Kontroll- und Auskunftsbefugnisse, deren Begrenzung aus dem Prinzip der Gewaltenteilung abzuleiten wäre, gegenüber dem Parlament besitzt.

Andererseits müssen Auskunftsersuchen des Landtags, vor allem der Fraktionen, vertraulich behandelt werden. Fraglich ist, ob die Amtspflicht der Behörden und Bediensteten zur Verschwiegenheit einen ausreichenden Schutz gewährt, insbesondere, wie die Grenze zu den „Mitteilungen im dienstlichen Verkehr" (§ 75 HBG) zu ziehen ist (vgl. II, 4.1.1.1 b). Dabei wird es einen Unterschied machen, ob sich das Auskunftsersuchen an eine – oberste oder nachgeordnete – Landesbehörde richtet oder ob Informationssysteme der HZD oder eines KGRZ benutzt werden. Vor allem in diesem Fall wird ein Bedürfnis nach vertraulicher Behandlung bestehen; denn solche Auskunftsersuchen können leicht Hinweise auf noch geheimhaltungsbedürftige politische Absichten, denen die Auskunft dienen soll, ergeben.

Daher müßte sichergestellt werden, daß die HZD und die KGRZ die Tatsache, daß Auskünfte gefordert worden sind, wer sie verlangt hat und welchen Inhalt sie haben, vertraulich und nicht als „Mitteilung im dienstlichen Verkehr" oder als eine sonst zulässige Amtshilfe behandeln. Die Organisation der HZD und der KGRZ als aus der Landesverwaltung und aus den Kommunalverwaltungen ausgegliederten Körperschaften des öffentlichen Rechts erleichtert eine solche Regelung, weil die Rechenzentren – anders als oberste Landesbehörden – neben ihren gesetzlichen Aufgaben keine anderen Interessen und Rücksichten zu wahren brauchen.

Ob das Recht, Auskünfte aufgrund der gespeicherten Daten zu verlangen, auch ein unmittelbares Zugriffsrecht auf Datenbestände der auskunftspflichtigen Behörden umfaßt, hängt von dem jeweiligen Stand der technischen Entwicklung der „Datenverarbeitungsanlagen" (vgl. § 6 Abs. 2 DSG) ab. Es würde weder der Materie der „maschinellen Datenverarbeitung", auf die es die Regelung abstellt, noch der Zielsetzung der Vorschrift entsprechen, den Begriff Auskunft im Sinne der herkömmlichen Auskünfte aus Akten oder manuell geführten Registern – d. h. also eng – auszulegen. Deshalb müßten hierfür bestimmte Regeln mit dem Auskunftspflichtigen – in erster Linie käme die HZD in Betracht – vereinbart werden. Im einzelnen wäre festzulegen, welche tatsächlichen Voraussetzungen gegeben und welche noch zu schaffen sind.

Mit diesem unmittelbaren Zugriffsrecht des Landtags (Auskunftsrecht gemäß § 6 Abs. 1 DSG) erhält das Parlament erstmals ein unmittelbares Auskunftsrecht auch gegenüber den Behörden, die den obersten Landesbehörden nachgeordnet sind oder ihrer Aufsicht unterstehen. Das parlamentarische Kontroll-Instrumentarium gegenüber der Regierung (Große und Kleine Anfrage, Fragestunde, Zitierrecht) wird um ein auf die EDV ausgerichtetes Mittel erweitert. Darin liegt seine verfassungsrechtliche und -politische Besonderheit.

4.2.2 Probleme der Verwirklichung

Inzwischen sind auch andere Länder dem hessischen Beispiel gefolgt und haben eine Überwachung der Rückwirkungen vorgesehen, die eine automatisierte Datenverarbeitung im Bereich der Exekutive auf die Wirksamkeit der parlamentarischen Kontrollfunktionen haben kann (vgl. 2.1.3, 2.1.6, 2.1.8 und 2.3.8). Ein Beschluß der Präsidenten der Landesparlamente vom 11. 10. 1973 verweist ebenfalls auf die besondere Bedeutung, die „das Zugriffsrecht des Parlaments und der Fraktionen auf staatliche und kommunale Datenbanken ... für die Wahrnehmung der Kontrollfunktion" besitzt.

Die Verwirklichung des in § 6 DSG normierten Rechts der Legislativen steht allerdings noch aus, u. a. auch weil die Informationssysteme der Regierungen, die den Exekutiven einen bedeutenden Informationsvorsprung gegenüber der Legislative verschaffen, sich noch im Aufbau befinden.

Gemäß seinem Auftrag, die sich anbahnende Entwicklung vorausschauend zu beobachten (§ 10 Abs. 2 DSG), informiert sich der Datenschutzbeauftragte fortlaufend bei der HZD und den KGRZ darüber, welche Datenbestände und Auswertungsprogramme bereits vorhanden sind, die für die Legislativen von Bedeutung sein könnten. Der Meinungsaustausch ergab stets Übereinstimmung darüber, daß es vor allem darauf ankomme, denkbare Wünsche der Volksvertretung kennenzulernen, damit deren Erfüllung schon bei der Entwicklung der Informationssysteme berücksichtigt werden kann.

4.2.3 Statistische Veröffentlichungen und Parlament

Bei der geplanten Übernahme der maschinellen Erledigung statistischer Aufgaben durch die HZD (vgl. 4.1.5) handelt es sich vordergründig um eine organisatorische Maßnahme der Regierung, die der Verwaltungsrationalisierung dient. Diese Maßnahme muß aber noch unter einem anderen Aspekt gesehen werden: Das Parlament insgesamt sowie seine Fraktionen und Mitglieder sind häufig auf die Veröffentlichung statistischer Ergebnisse des Landesamtes angewiesen, um die Regierungstätigkeit kontrollieren und um Initiativen ausarbeiten zu können. Sie müssen deswegen daran interessiert sein, daß die von der Regierung veranlaßten oder gesetzlich angeordneten statistischen Erhebungen rasch ausgewertet und umgehend veröffentlicht werden.

Die Übernahme der maschinellen Erledigung statistischer Aufgaben durch die HZD könnte eine schnelle Veröffentlichung der Ergebnisse gefährden. Denn im permanenten Prioritätskonflikt zwischen den Aufgaben des Verwaltungsvollzugs und der Statistik wird die Verwaltung im allgemeinen den Verwaltungsvollzug als die dringlichere Aufgabe ansehen. Vor allem aber muß, damit das Informationsrecht des Landtags nicht beeinträchtigt wird, gewährleistet sein, daß keine wie auch immer motivierte Beeinflussung den ordnungsmäßigen Ablauf des Verfahrens stören kann, etwa in der Absicht, das Bekanntwerden bestimmter statistischer Ergebnisse zu einem politisch unerwünschten Zeitpunkt zu verhindern.

4.3 Datensicherung

Seit jüngster Zeit nehmen auch in Deutschland die führenden Computerfirmen den Datenschutz und die Datensicherheit sehr ernst. Die neue Technologie kennzeichnet den Stand der Sicherheitsmöglichkeiten.

4.3.1 HZD und KGRZ

Die im zweiten Tätigkeitsbericht unter 4.3.1 dargestellten Maßnahmen (DASCH) wurden auf Empfehlung des Koordinierungsausschusses bei den Kommunalen Gebietsrechenzentren und der HZD zur Erprobung eingeführt.

Im Jahre 1973 wurden im Datenverarbeitungsverbund die Maschinensysteme, bis auf wenige Ausnahmen, durch DV-Anlagen der jüngsten Generation ersetzt. Die schon bisher in den Systemen gewährleistete Sicherheit wurde in den jetzt installierten DV-Anlagen durch die bessere Hardware-Ausstattung und durch den komplexeren Aufbau der Betriebssysteme wesentlich erhöht (z. B. durch sicherere Bauelemente, automatische Fehlererkennung und -korrektur, Prüfpunkt- und Wiederanlaufverfahren und ausreichenden Kernspeicherschutz). Die vollautomatische Steuerung und Überwachung des computerinternen Betriebsablaufs macht es auch dem erfahrenen EDV-Fachmann schwer, Programme oder Dateien zu manipulieren. Besondere Programme garantieren, daß jeder berechtigte oder unberechtigte Zugriffsversuch, ob mit oder ohne Erfolg, erkannt und automatisch protokolliert wird. Der Systembenutzer hat wenig Einfluß auf die Ablauf- und Verarbeitungssteuerung des Betriebssystems. Bei entsprechender Organisation kann er nur solche Operationen ausführen, die ihm vom System besonders bereitgestellt sind. Auch das steigende Maß an „eingebauter" Sicherheit kann aber nichts an dem grundsätzlichen Sachverhalt ändern, daß die Systeme letztlich doch von Menschen gesteuert werden und damit notwendigerweise auch mißbräuchlichen Zielen Raum geben. Wie notwendig deshalb gerade auch personelle Vorkehrungen bleiben, bestätigt ein Vorfall, der dem Datenschutzbeauftragten von einem Rechenzentrum gemeldet wurde. Dort hatte ein Außenstehender versucht, durch Bestechung eines Angestellten an gespeicherte personenbezogene Daten heranzukommen. Wenn auch in diesem Fall das Datenschutzbewußtsein des Mitarbeiters stärker war, so bleibt doch das Ziel der Datensicherung, möglichst weitgehend auszuschließen, daß der Schutz der Daten allein von der Integrität einer einzelnen Person abhängt.

4.3.2 Außerhalb des Datenverarbeitungsverbundes

Im Berichtsjahr hat der Datenschutzbeauftragte sich außerhalb des Verbundes schwerpunktmäßig über die Schutzmaßnahmen bei den hessischen Universitäten informiert. Hierbei wurde festgestellt, daß sich besonders bei den Verwaltungsstellen der Universität, die über keine eigenen DV-Anlagen verfügen und ihre Arbeiten auf Datenverarbeitungsanlagen im Bereich der Forschung erledigen, Unzulänglichkeiten ergeben. So mußte z. B. bei einer Stelle beanstandet werden, daß die Ablocharbeiten der Verwaltung (Erhebungsbogen für Neuimmatrikulierte und Belegscheine) im gleichen Raum vorgenommen werden, in dem auch die Studenten ihre Arbeiten erledigen. Es war also keine Gewähr dafür gegeben, daß Erhebungsbogen und Belegscheine von Unbefugten nicht eingesehen wurden.

Im allgemeinen ist aber zu berichten, daß im Bereich der Universitäten in eigener Verantwortung wirksame Schutzvorkehrungen getroffen wurden, die zum Teil eine unmittelbare Einschaltung der obersten Verwaltungsbeamten bei Einzelfragen bzw. die Einsetzung eines besonderen Beauftragten für Datenschutz vorsehen. Die an Ort und Stelle zu treffenden Entscheidungen

beziehen sich z. B. auf die Frage, welche Daten von Studenten gegebenenfalls für eine Stichprobe als Grundlage für empirische Arbeiten im Bereich der Sozialwissenschaften weitergegeben werden können und welche Auflagen bzw. Abschirmungen vorzusehen sind. Eine weitere konkrete Entscheidung bezog sich auf die Frage, ob und auf welche Weise dem Verlangen eines AStA entsprochen werden könnte, die Namen und Anschriften jener Studenten zu erfahren, deren Studienzeit sich über die übliche Semesterzahl hinaus erstreckt. Der AStA wollte diesen Studenten nach Auskunft der Universitätsleitung Hilfestellung bei der Wahrnehmung ihrer Interessen anbieten. Hier wurde eine Lösung angeboten, die die Weiterleitung der zur Verfügung gestellten Informationen an die ins Auge gefaßten Empfänger ermöglichen soll, ohne daß das Risiko einer Weiterverbreitung und evtl. einer Speicherung der Namen zur Langzeitverwendung eingegangen werden mußte.

4.3.3 Weiterentwicklung von Kontrollverfahren

Die Möglichkeiten der Kontrolle von Sicherheitsmaßnahmen durch den Datenschutzbeauftragten – aber auch durch die Verwaltung bzw. das Rechenzentrum selbst – sind begrenzt, soweit es sich um computerinterne Vorgänge handelt. Programmierte Schutzvorkehrungen, wie z. B. Zugriffstabellen, können am besten dadurch auf ihre Wirksamkeit geprüft werden, daß man in Form eines Planspiels Experten mit dem Versuch beauftragt, sie zu umgehen oder zu durchbrechen. Dagegen gibt es noch keine standardisierten Methoden und Verfahren, insbesondere keine Maschinenprogramme, mit denen sich die Wirksamkeit von Sicherungen routinemäßig überprüfen läßt. Deshalb läßt sich auch nie mit absoluter Sicherheit ausschließen, daß noch Manipulationsmöglichkeiten bestehen. Aus diesem Grund haben auch diejenigen Maßnahmen eine besondere Bedeutung, die darauf gerichtet sind, unbefugte oder verdächtige Aktivitäten möglichst frühzeitig zu entdecken und den Urheber zu identifizieren. Diese Aufgabe ist in erster Linie durch das EDV-System selbst zu organisieren. Das wichtigste Mittel ist die automatische Protokollierung aller sicherheitsrelevanten Aktivitäten, insbesondere derjenigen, die auf manipulative Absichten hindeuten, wie etwa Versuche, auf gesperrte Programme oder Daten zuzugreifen, unbefugt Programme einzusehen oder zu ändern oder die Protokollierung auszuschalten.

Während eine derartige Protokollierung selbst grundsätzlich keine technischen Schwierigkeiten bereitet, fehlt es wiederum an anwendungsfertigen Verfahren, die in erheblichen Mengen anfallenden Protokolldaten wirksam und zeitnah zu analysieren und in brauchbare Entscheidungsgrundlagen für Sofortmaßnahmen oder gezielte Nachforschungen umzusetzen. Die Entwicklung derartiger Prüf- und Anlayseprogramme ist jedoch gerade für einen präventiven Schutz von ausschlaggebender Bedeutung und sollte deshalb vorangetrieben werden.

5. Anregungen

Die in den ersten beiden Tätigkeitsberichten gegebenen Anregungen (I. 5.1–5.1.3 und II. 5.–5.4) sind weiterhin zum großen Teil noch aktuell. Bei der Einbeziehung des Datenschutzes in die Aus- und Fortbildung der im öffentlichen Dienst Beschäftigten, der Verbesserung der Datensicherheit, der Berücksichtigung der parlamentarischen Informationsbedürfnisse und der Vergabe von Forschungsaufträgen zur Untersuchung von Entwicklung und Konsequenzen der Datenverarbeitung handelt es sich um permanente Anliegen, deren Realisierung ständig überprüft werden muß.

Aufgrund der im Berichtszeitraum gemachten Erfahrungen wird im einzelnen angeregt:

5.1 Geltungsbereich des DSG und Service-Unternehmen

Der Datenschutzbeauftragte sollte seine – nach § 10 DSG auf die Behörden und Stellen des § 1 DSG – begrenzte Überwachungsfunktion auch gegenüber den privatrechtlichen Unternehmen ausüben können, denen die öffentliche Verwaltung Aufgaben ganz oder teilweise überträgt. Die Landesregierung sollte deshalb darauf hinwirken, daß dem Datenschutzbeauftragten gegenüber Unternehmen, die als Dienstleistungshelfer (Erfüllungsgehilfe) der öffentlichen Verwaltung tätig sind, Auskunfts- und Kontrollrechte eingeräumt werden, sei es durch vertragliche Vereinbarungen, sei es durch entsprechende Maßnahmen der Organe solcher privatrechtlichen Unternehmen, in denen die Landesregierung vertreten ist (vgl. 1.5.1 und II. 5.2).

5.2 Weitergabeverbot

Die Landesregierung sollte darauf hinwirken, daß im gesamten Bereich der öffentlichen Verwaltung im Sinne des § 1 DSG personenbezogene Daten von keiner Behörde oder Stelle für gewerbliche oder sonstige Zwecke an nichtöffentliche Stellen oder an Privatpersonen weitergegeben werden, es sei denn aufgrund einer gesetzlichen Verpflichtung oder wegen eines gegenüber dem Schutz des Persönlichkeitsrechts vorrangigen Interesses des Gemeinwohls (vgl. 1.5.6).

5.3 Konkretisierung des Amtshilfegebots

Das allgemeine Gebot der Amtshilfe, das für medizinische Informationen im Hessischen Krankenhausgesetz begrenzt worden ist, muß für weitere Bereiche der öffentlichen Verwaltung zum Schutz „empfindlicher" personenbezogener Daten einschränkend geregelt werden, und zwar in erster Linie dort, wo bereichsspezifische Regelungen der Datenverarbeitung und wo die Verrechtlichung von Verwaltungsanweisungen gefordert werden (vgl. 1.5.3, 1.5.4 und 2.2.3), z. B. für die Informationssysteme des Verfassungsschutzes, der Landeskriminalpolizei und auch des Personalwesens.

5.4 Verrechtlichung von Verwaltungsanordnungen

Die schon im zweiten Tätigkeitsbericht (II, 5.3) erhobene Forderung, die Auskunfts- und Abrufberechtigung sowie die Löschung von Daten in den Informationssystemen der Polizei und des Verfassungsschutzes in Rechtsnormen festzulegen, wird wiederholt. Die Notwendigkeit einer bundeseinheitlichen Regelung ist unbestritten. Solange diese aber fehlt, sollte es Aufgabe der

Landesregierung sein, neue Rechtsnormen für den Umgang mit Daten im Kriminal- und Verfassungsschutzbereich erarbeiten zu lassen, da die Landesregierung selbst die Ansicht vertritt, daß die z. Z. geltenden Bestimmungen „einer Überarbeitung bedürfen" (Vorlage der Landesregierung, Landtags-Drucks. 7/3511, III, 13). Es könnten damit der Entwicklung einer bundeseinheitlichen Regelung wichtige Anstöße gegeben werden (vgl. 4.1.5.1–4.1.5.3).

5.5 **Umgang mit medizinischen Daten**

Die besondere Schutzbedürftigkeit medizinischer Daten wurde bereits im Bereich des hessischen Krankenhausverbundes durch die Regelung in § 14 des Hessischen Krankenhausgesetzes berücksichtigt. Die dort niedergelegten Grundsätze sollten Allgemeingültigkeit überall dort erhalten, wo medizinische Daten von öffentlichen Verwaltungen verarbeitet werden, es sei denn, daß eine anderslautende gesetzliche Regelung oder ein dem Persönlichkeitsrechtsschutz vorrangiges Interesse des Gemeinwohls besteht (vgl. 4.1.1 ff.).

5.6 **Datenbankregister**

Die Landesregierung möge den Datenschutzbeauftragten beim Aufbau eines Datenbankregisters unterstützen, indem sie die erforderlichen Mittel zur Verfügung stellt. Die Verwaltung wäre anzuweisen, den Datenschutzbeauftragten laufend über Art und Zweck neuer Datenbanken und die Speicherung neuer Datenarten zu unterrichten und bei der Entwicklung neuer Automationsverfahren seine Informationsbedürfnisse zu berücksichtigen. Das Register soll dem Bürger Auskunft darüber geben, welche Datenarten oder Datengruppen von welchen Behörden oder Stellen erfaßt und gespeichert werden (vgl. 1.5.2).

5.7 **Vorschlagswettbewerb Datenschutz**

Ähnlich dem für die Landesbediensteten bestehenden ständigen Vorschlagswettbewerb über die Vereinfachung und Verbesserung der Verwaltung sollte die Landesregierung alle Bürger auffordern, sich an einem ständigen Vorschlagswettbewerb zur Verbesserung des Datenschutzes und der Datensicherung zu beteiligen. Dafür sollten Geldprämien ausgesetzt werden (vgl. 1.5.8).

5.8 **Zugriffsregelung für das Parlament**

Die Zugriffsrechte des Landtags zu den Daten aus dem Verwaltungsvollzug sollten im Sinne des § 6 Abs. 1 und unter Beachtung des in der Begründung des Regierungsentwurfs des Datenschutzes genannten „unmittelbaren Zugriff(s)" zu den datenverarbeitenden Stellen geregelt werden.

5.9 **Vergabe von Forschungsaufträgen**

Die Landesregierung möge Mittel für einen Forschungsauftrag bereitstellen, bei dem untersucht wird, in welcher Weise die automatische Datenverarbeitung dazu benutzt werden kann, bestehende Machtpositionen zu verfestigen, und welche Steuerungs- und Kontrollinstrumente dies verhindern können.

6. SCHLUSSBEMERKUNGEN

6. Schlußbemerkungen

Die jüngste Entwicklung auf dem Gebiet des Datenschutzes hat dazu geführt, daß der dritte Tätigkeitsbericht nicht nur die Arbeit des Datenschutzbeauftragten für das Land Hessen behandelt, sondern weiter ausholt. Die Situation ist dadurch gekennzeichnet, daß zwei weitere Länder den Datenschutz inzwischen gesetzlich geregelt haben – Rheinland-Pfalz und Schweden – und im Bund und in anderen Ländern Datenschutzgesetzentwürfe vorgelegt worden sind. Je mehr Länder sich zu einer gesetzlichen Regelung des Datenschutzes entschließen, um so breiter wird die Diskussion der dabei gewonnenen Erfahrungen, insbesondere dann, wenn unabhängige Überwachungsinstanzen vorgesehen sind, über deren Tätigkeit öffentlich berichtet wird. Damit wird die Voraussetzung dafür geschaffen, daß ein wechselseitiger Austausch zwischen Praxis und Wissenschaft entsteht, während bisher die Informatikwissenschaft weitgehend genötigt war, ohne Fühlung mit der Praxis zu arbeiten. Zwar sind sich Wissenschaft und Praxis einig über die Notwendigkeit, Datenverarbeitung für den Bürger transparent zu machen und ihm Abwehrrechte einzuräumen (vgl. §§ 10, 11, 20, 26, 30 EBDSG); jedoch würde die gegenseitige Durchdringung von Datenschutzpraxis und Wissenschaft eine wesentlich bessere Grundlage als bisher schaffen, um für bestimmte Bereiche, die durch allgemeine Normen nicht hinreichend abgedeckt werden, spezifische Datenschutzregelungen zu entwickeln. Beispiele hierfür sind das Gesundheitswesen, das Kreditauskunftswesen und die Risikoeinschätzung im Versicherungswesen.

Damit würde der fatalistischen Haltung entgegengewirkt, man könne gegen den Mißbrauch der EDV ja doch nichts unternehmen, der Computer werde letzten Endes doch dem „großen Bruder" zu seiner Überwachungsfunktion verhelfen.

Ein Mittel, um der Macht des Computers entgegenzuwirken, ist wiederum der Computer, indem man ihn zur Kontrolle des Computers einsetzt. Der Computer soll gleichsam den Computer zähmen. Die Eigenart der Datenverarbeitung bringt es nämlich notwendigerweise mit sich, die einzelnen Computeroperationen und ihre Reihenfolge im vorhinein festzulegen, damit das Verfahren ordnungsgemäß abläuft. Die Formalisierung der Computerarbeiten läßt keinen Raum für Entscheidungen und Maßnahmen, die von den vorgegebenen Vorschriften abweichen. Gerade solche Vorschriften, die dem Ermessen des Bearbeitenden Spielraum geben und damit Abweichungsmöglichkeiten zulassen, waren und sind bis heute vorherrschend. Der Formalisierungszwang, der vom Computer ausgeht, ist eine nicht zu unterschätzende Chance, die Freiheitsrechte des Bürgers zu schützen. Wenn dann durch eine unabhängige Instanz die öffentliche Diskussion der Problematik erzwungen wird und die Wissenschaft ihren Beitrag leistet, kann es gelingen, den technischen Fortschritt zu nutzen, ohne dabei die Freiheit zu riskieren.

Bedeutend weniger optimistisch darf man jedoch in bezug auf den möglichen Einsatz der EDV als Herrschaftsmittel sein. Die rigorose Auswertung des durch die EDV ermöglichten Informationsvorsprungs und der neuen Manipulationstechniken könnte die Stellung etablierter Machtgruppierungen in Staat und Gesellschaft in einem gefährlichen Ausmaß festigen. Diese Gefahr ist sehr ernst zu nehmen. Es muß zu den vordringlichsten Aufgaben unserer Wissenschaftler, Politiker und Publizisten gehören, diese Bedrohung näher zu analysieren und abwenden zu helfen.

SACHWÖRTERVERZEICHNIS

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

Adressenhandel II 1.3.2, III 1.5.6

Alarmpläne II 4.3.1

Allwissenheit des Staates I 1.2.1

Amtshilfe und Datenschutz I 4.1.2, II 4.1.1.1 b, III 1.5.5, III 5.3

Analyse (Ist- und Soll-) II 4.2.2

Anregungen I 5., II 5., III 5.

Arbeitsgruppe EDV des Landtags III 4.2

Anrufungsrecht des Bürgers (§ 11 DSG) I 4.1.4, I 5.10, II 4.1.4, III 1.3

Arbeiter-Samariter-Bund III 4.1.1.2

Ausbildung im Datenschutz I 5.8, II 4.2.2, III 5.

Auskunfteien II 1.3

Auskunftsersuchen des Parlaments I 4.2.3, III 4.2.1

Auskunft, Freiwilligkeit der — III 4.1

Auskunftspflicht II 1.3

Auskunftsrecht des Bürgers I 2.2.1, I 4.1.4, II 4.1.4, III 1.5

Auskunftssystem III 4.1.3

Automation, Nutzen der — I 1.2.2, I 1.2.3

Baader-Meinhof-Report III 1.2.2

Baden-Württemberg, Datenschutz in — I 2.1.5, I 4.2.1

Bankgeheimnis und Datenschutz I 4.1.1.3 d

Baskir, L. II 4.1.1.1.

Bayern, Datenschutz in — I 2.1.2, I 2.4.2

Benutzerfreundlich II 1.1

Bereich des Gesetzes I 4.1.3, II 4.1.3, III 1.5.1, III 5.1

Bereichsspezifische Regelung III 1.5.3

Berichtigungsanspruch des Bürgers I 2.2.1, III 1.5

Berlin, Datenschutz in — I 2.1.8, III 2.1.8

Bestandsaufnahme der Behörden und Stellen I 3.1, II 3.1, III 3.

Beurteilung der — I 3.2, II 3.2

— maschinellen Datenverarbeitung I 1.1

Bestechung III 1.3, III 4.3.1

Betroffenenfreundlich II 1.1

Betroffener
Rechte des — II 2.4.3
Benachrichtigung des — III 1.5
Einzelauskunft an — III 4.1.1.-2, II 4.1.1.3 g

Bistümer, kath. II 4.1.1.3 f

Bremen, Datenschutz in — I 2.1.8

Bühnemann III 2.2.1

Bund
Datenschutzgesetzgebungsstand im — I 2.2, I 5.1.1, III 2.2

Bundesangestelltentarif (BAT — § 9) II 4.1.1.1

Bundesanstalt für Arbeit II 4.1.1.1 b, II 4.1.1.2

Bundesausbildungsförderungsgesetz I 4.1.1.2

Bundesdatenschutzgesetz
— Initiativ-Entwurf I 2.2.2, I 2.4.7

— Regierungsentwurf I 2.2.3, II 1.3, II 2.4.1, II 4.1.1, III 1.2, III 1.4, III 2.2.1, III 2.2.2

Bundesgesetze und Datenschutz I 4.1.1.1, I 4.1.1.2, III 2.2.1.-2

Bundesmeldegesetz I 2.2.1, II 2.2.1, III 2.2.1.-2

Bundespost II 4.1.1.3 g

Bundesrecht, Kollision mit — I 1.3.2

Bundesregierung I 1.2.3, III 2.2.1.-2

Bundestag
Entschließung des — vom 21. 6. 1972 II 4.1.1.2

Bundesverfassungsgericht (Mikrozensus) I 1.2.3, III 1.2.2

— Ehescheidungsakten-Urteil II 4.1.1.6, III 1.5.5

— Lebach-Urteil III 4.1.5.1

Bußgeldvorschriften I 2.2.4, I 2.4.6

Bundeszentralregistergesetz II 4.1.1.3 c

Computerkriminalität I 4.3.2, III 1.3 III 4.3.1

Computermißbrauch-Versicherung II 1.3

DAMM III 1.2

Dammann/Karhausen/Müller/Steinmüller III 2.2.1

DASCH II 4.1.1.3, II 4.3.1 III 4.3.1

Daten

- Einwohner- I 2.2.1
- Grund- I 1.2.1
- „harmlose" — I 1.2.3
- Individual- I 1.2.1
- personenbezogene — (s. Personenbezogene Daten) III 1.5.1
- sachbezogene — I 4.1.3.2
- -weitergabe an andere Behörden I 2.2.1, I 5.4 III 1.5.5
- -weitergabe außerhalb der Verwaltung III 1.5.6
- — an Religionsgesellschaften II 4.1.1.3 f III 4.1.6
- medizinische — II 4.1.2.1, II 4.1.2.3 III 4.1.1
- -zweckentfremdung II 4.1.1.1 c

Datenaustausch II 1.3.2

Datenbanken I 1.2.1, I 1.2.3, II 4.1.1.1 c III 1.5.2

- Einwohnerwesen- III 4.1.3
- hochschulspezifische — I 4.1.1.1, I 4.1.1.2
- medizinische — III 4.1.1.3
- Personal- III 4.1.2
- register I 2.4.3, II 2.4.3, III 1.5.2, III 5.6
- statistische — I 4.1.1.1

Datenerfassung für die Unterlagen I 4.1.1.1

Datenfernverarbeitung I 1.2.3, III 2.5

Datengeheimnis II 4.3.1

Datenmißbrauch II 1.3.1, II 2.2.4 III 1.2.1

Datenschutz I 1.1, I 1.4.3,

- — außerhalb Hessens I 2., II 2., III 2.
- — im Ausland III 2.3
- Dänemark III 2.3.6
- Frankreich I 2.3.3, II 2.3.4
- Großbritannien, Kanada I 2.3.2, II 2.3.2, II 2.3.3, III 2.3.1.2
- Neuseeland III 2.3.1.9
- Österreich III 2.3.7
- Schweden II 2.3.5, III 2.3.5
- Schweiz III 2.3.8
- USA I 2.3.1, I 2.4.2, I 2.4.5, I 2.4.7, II 2.3.1, III 2.3.1

Datenverarbeitung ohne — I 1.2.3, I 4.1.1.3 e

Notwendigkeit und Problematik des — I 1.2.3, II 1.3, II 1.3.1, II 2.4

Regelung des — I 1.2.3

Überwachung des — I 2.4.7

Instrumente des — II 2.4, II 4.1.2.3

Inhalt des — II 4.1.2.1

— in der privaten Wirtschaft II 1.3

Mindestanforderung für — und Datensicherung II 4.3.1 III 4.3.1

Datenschutzbeauftragter

Unabhängigkeit des — I 1.4, II 1.1, II 1.4 III 1.4

Kontakt des — II 1.4 III 1.3

— und private Unternehmen II 4.1.1.3 d, II 4.1.3.1, II 4.1.3.2 III 1.5.1

Aufgaben des — II 4.1.2.1, III 4.1

Aufgabenbereich des — I 4.1.3, I 4.1.3.2

— und privatrechtliche Organisationen der öffentlichen Hand II 4.1.3.2, III 1.5.1 III 5.1

Datenschutzgesetz
hessisches — I 1.1, I 1.3, I 2.2.4, I 2.4, I 2.4.1, I 2.4.2, I 2.4.5, I 2.4.7, II 4.1.1, II 4.1.1.1 e, III 1.4
Anpassung des — III 1.5
— und Bundesgesetzgebung I 4.1.1.2, I 4.1.3, III 2.2.1
Geltungsbereich des — I 3.2, I 4.1.1.3 d, II 4.1.1.3, III 1.5.1, III 5.1
Datenschutzgesetzgebung
Tendenzen der — I 2.4, II 2.4, III 2.4
Datenschutzkommission II 2.1.1
Datenschutzmaßnahmen
Differenzierung der — II 2.4.1
Datenschutz-Technologie III 1.3
Datenschutzvorschriften
Anwendungsbereich der — (Privater Bereich, Öffentlicher Bereich) I 2.4.1, II 2.4.1
— im Krankenhausgesetz II 4.1.3.2, III 4.1.1.1
Datensicherung I 1.1, I 4.3, I 5.8, II 4.3, III 4.3
— außerhalb des hess. Datenverarbeitungsverbundes I 4.3.2, II 4.3.2, III 4.3.2
— im Einwohnerwesen I 4.3.2, III 4.1.3
— im hess. Datenverarbeitungsverbund I 4.3.1, II 4.1.1.3, II 4.3, III 4.3.1
— Weiterentwicklung von Kontrollverfahren III 4.3.3
Regelung der — I 1.2.3
Datensicherheit
Richtlinien für — II 5.4, III 4.3.1
Datenverarbeitung
— als Hilfsmittel der Verwaltung I 1.4.2, II 1.1, III 3.
— im Gesundheitsamt III 4.1.1.3
Ergebnisse der — I 1.3.2
— im Statistischen Landesamt I 4.1.1.3 b
— in der HZD und den KGRZ I 4.1.1.3 a
— in der öffentlichen Verwaltung I 3., II 1.3
integrierte — I 1.2.2, II 4.1.4, II 4.1.1.1 c
konventionelle — I 2.4.1
maschinelle — I 1.2.2, I 1.2.3, I 1.3.2, II 1.1, II 1.3
— ohne Datenschutz I 1.2.3
Tendenz der — zur Zentralisierung I 4.2.2
Unterausschuß für — II 5.1
Datenverarbeitungsanlagen II 1.1
Datenverarbeitungssysteme
integrierte — II 1.1, III 1.3
Datenverarbeitungsverbund
Koordinierungsausschuß des hessischen — I 4.2.2, I 4.3.1, II 4.1.1.3 c
Hessischer — II 4.1.1.3
— im Krankenhauswesen II 4.1.2.1, II 4.1.3.2, II 4.3.2
— Krankentransport III 4.1.1.2
Datenweitergabeverbot III 5.2
Demokratische Prinzipien I 1.2.1
DEVO II 4.1.1.2
DOMINIG III 4.1.1.3
DÜVO II 4.1.1.2

EDV im Gesundheitsamt III 4.1.1.3
Ehescheidungsakten II 4.1.1.1 b
Einführungsgesetz z. StGB III 2.2.3
Einwohnerinformationssystem I 2.2.1, III 4.1.3
Einwohnerwesen II 3.1, III 4.1.3
Enquête-Kommission
Zwischenbericht der — BT-Drucks. VI/3829 II 2.4.2
Entscheidungshilfe II 4.2.3
Erfahrungsvorsprung des Landes gegenüber den Kommunen II 4.2.4
Erfassung
Mehrfach- von Daten I 3.1, III 1.5.2
Erkennungsdienstliche Unterlagen III 4.1.5.1
Exekutive I 1.2.2, III 4.2.1

Fernabruf II 4.1.1.1
Fernübertragung
Daten- I 4.1.1.1, III 2.5
Finanzwesen II 3.1
Forschungsauftrag I 5.1.2, III 5.9
Freiwilligkeit der Auskunft III 4.1
Funktion
-trennung II 4.3.1
-verlagerung II 4.2.2

Gasölverwendungsgesetz I 4.1.1.3 e
Gebietsreform II 4.2.2
Geheimhaltungs-
-bestimmungen I 1.2.1, III 2.2.1
-vorschriften I 1.2.3
-pflicht II 2.2.4, III 4.2.1
Geheimnischarakter von Merkmalen I 1.2.3
Geltungsbereich des DSG III 1.5.1
Gemeindeplanungsdatei II 4.2.4
Generalklauseln
Konkretisierung der — II 4.1.2.1
Genscher, Bundesminister II 4.1.1.1 c, II 4.1.1.3 b
Gesetz über die Errichtung der Hessischen Zentrale für Datenverarbeitung und Kommunaler Gebietsrechenzentren (DVG) I 1.2.2, I 1.3.1
Gesundheits-
-amt III 4.1.1.3
-informationssystem III 4.1.1.3, III 2.4
-wesen III 4.1.1.3
Gewaltenteilung —
Auswirkungen von Planungs- und Entscheidungshilfen der Regierung auf die — I 4.2.1
Erhaltung der — I 4.2, III 4.2
Unterstützung der Funktionen der — I 2.4.1, III 4.2.1
Verschiebung in der — I 1.4.1, I 2.4.2
Graduiertenförderungsgesetz I 4.1.1.2
Grundrechte I 1.2.1

Hamburg
Datenschutz in — I 2.1.7, I 2.2.2, I 2.4.1
Hard- und Software III 1.3, III 4.3.1
HEPAS (siehe Hess. Planungs-informations- und Analysesystem)
HEPOLIS III 4.1.5.1
"Hessen '80 — Datenverarbeitung" I 1.2.2
Hessischer Gemeindetag II 4.1.1.3 d
Hessisches
— Beamtengesetz (HGB, § 75) II 4.1.1.1
— Planungsinformations- und Analysesystem (HEPAS) I 4.2.3, I 4.2.4, II 4.2.3, II 4.2.4
— Kommunal II 4.2.4
Hessische Zentrale für Datenverarbeitung (HZD) I 3.1, I 3.2, I 4.1.1.3, I 4.1.2, I 4.2.2, I 4.2.4, I 4.3.1, II 4.3.1, III 4.1.1.2, III 4.1.4
Hochschulstatistikgesetz I 4.1.1.2

Identifizierungsmerkmale I 1.2.3, I 4.1.1, I 4.1.1.1, I 4.1.1.2, I 4.1.1.3 b, I 5.1
getrennte Aufbewahrung der — I 5.2, III 1.5.1 b
Individualdaten
Statistik ohne — I 5.3, III 4.1.4
Individualinformation I 1.2.1,
Schutz vor Mißbrauch der — I 1.4
Information(s-)
empfindliche — I 5.2, III 4.1.2
-netz I 2.4.3, III 1.3, III 4.1.1.3, III 4.1.2, III 4.1.3
-qualität I 1.2.3
-struktur I 1.2.3, I 2.4.3
unbestätigte — III 1.2.2
Informationsbankensystem I 1.2.3
— des Bundes I 4.1.1.1
Informationsbedürfnis I 1.2.3
Informationsfluß I 1.2.1
Informationsgleichgewicht I 1.2.2, II 2.4.2, III 1.3, III 4.2
Informationsmißbrauch I 1.2.3, III 1.2.2

Informationsrechte
parlamentarische — I 4.2.3, II 4.2.3, III 4.2.1
Informationsstruktur
Eingriffe in die — II 2.4.1
Informationssystem I 1.2.3
allgemeines — I 1.2.3
Einwohner- I 1.2.3, III 4.1.3
Gesundheits- III 4.1.1.3
integriertes — I 1.2.1, I 1.2.2, I 1.2.3
parlamentarisches — I 4.2.1, III 4.2.1.-2
Personal- III 4.1.2
polizeiliches — I 4.1.1.3 c, II 4.1.1.3 c, III 4.1.5
Informationsverbund III 4.1.1.3
Informationsweitergabe
dysfunktionale — II 4.1.2.2
Infrastruktureinrichtungen
Planungsdatei für — II 4.2.4
Inkompatibilität I 1.4.2
— bei Übertragung der Datenschutzkontrolle auf Bundesminister I 2.4.7
INPOL III 4.1.5.1
Integration I 1.2.2, III 1.3
Intimsphäre I 1.2.3, I 4.1.1.3 c, I 4.1.2, I 5.4, III 4.1
Schutz der — II 2.2.1
IPEKS II 2.1.3

Johanniter Unfallhilfe III 4.1.1.2
Jugendgesundheitskarte III 4.1.1.3

Kamlah I 1.2.3
Katastrophenpläne II 4.3.1
Kirchen (s. auch Religionsgesellschaften) I 4.1.1.3 f, I 4.1.2
— und Datenschutz II 4.1.1.1 b, II 4.1.1.3 f, II 4.1.2.1, III 1.3, III 4.1.6
Kirchensteuergesetz — hess. II 4.1.1.3 f
Kommission der EG III 2.5
Kommunale
— Spitzenverbände II 4.2.2
— Vertretungsorgane I 1.3.1
Kommunales Gebiets-Rechen-Zentrum (KGRZ) I 3.1, I 3.2, I 4.1.1.3, I 4.1.2, I 4.2.2, II 4.3.1, III 1.5.6
Kommunen
Einfluß der EDV auf Verhältnis der — zum Land I 4.2.2
Erhöhung der Verwaltungskraft der — I 4.2.2
Kontrolle II 2.4.3, III 1.4, III 1.5.2, III 2.51 bis 2.2.2, III 2.4, III 4.2.1, III 4.3.5
demokratische — II 1.1
Kontrollverfahren, Weiterentwicklungen von — III 4.3.3, III 4.3.3
Kooperationsausschuß ADV Bund/Länder/Gemeinden III 1.2, III 2.5
Koordinierungsausschuß
— des hess. Datenverbundes II 4.1.1.3 a, III 4.3.1
— Hess. Statistischer II 4.1.1.3 b
Kostenfreiheit II 4.2.2
Krankenhausgesetz II 4.1.2.3, III 1.5.3, III 4.1.1.1
Krankenhauswesen III 2.4, III 4.1.1.1
Krankentransport III 4.1.1.2
Krankenversicherung II 4.1.1.2
Kriminalpolizei II 1.1
Informationssystem der — II 2.4.3, III 4.1.5.1
— Zusammenarbeit mit privaten Unternehmen II 4.1.1.3 d

Landesamt für Verfassungsschutz II 4.1.1.3 e, II 4.1.2.1, III 4.1.5.1
Landeskriminalamt I 1.2.3, I 4.1.1.3 c, II 4.1.1.3 c, II 4.1.1.3 d, II 4.1.2.1
Landesregierung I 1.1, I 1.2.2, I 1.3.1, III 4.1.5.1, III 4.2.1
Landesverwaltung I 1.2.2, II 4.1.1.3
Ausführung der Bundesgesetze durch die — I 4.1.1.2
Kontrolle der — durch DSB I 4.1.1.2, II 4.2.3, III 1.5.1, III 4.2.2

Landtag
- Arbeitsgruppe EDV des — III 4.2
- Informationsrecht des — I 1.3.1, II4.2.3, III 4.2.1, II 4.2.2
- Unterausschuß des — für EDV II 5.1
- Wahl des DSB durch den — I 1.4

Legislative I 1.2.2, III 4.2.2

Lehrerdatei III 4.1.2

Lehrstuhl III 1.5.7

Leistungssport III 4.1.1.3

Löschung von Daten II 4.1.1.3 c, II 4.1.1.3 e, III 4.1.7

Machtbalance zwischen Parlament und Regierung I 1.4

Malteser-Hilfsdienst III 4.1.1.2

Maschinenkapazität III 3

Massachusetts III 2.3.1.1

medizinische Daten II 4.1.2.3, III 4.1.1, III 5.5

medizinische Datenbanken III 4.1.1.3

Meldewesen I 2.2.1

Mikrozensus (s. Bundesverfassungsgericht) III 4.1.3

Mißbrauch von Informationen II 4.1.1.1 c

Müller, Paul J. II 4.1.2.2

Nachrichtendienste
- Informationssysteme der — (NADIS) II 1.1, II 2.4.3, II 4.1.1.3 e, III 4.1.5.2

Niedersachsen
- Datenschutz in — I 2.1.4, III 2.1.4

Nordrhein-Westfalen
- Datenschutz in — I 2.1.6, I 2.2.2, I 2.4.1, I 2.4.2, III 1.3, III 2.1.6

Normfindung III 1.5.7, III 6.

OECD III 2.5

Operatives Handeln I 1.2.1

Parlamente
- Auskunftsersuchen der — I 1.4.1, III 4.2.1
- Herausforderung der — durch Einsatz der EDV I 4.2.1
- Informationsrechte der — I 2.4.1, III 4.2.1
- — und Informationssysteme I 5,9, II 4.2.4
- — und Regierung I 4.2.1
- — und statistische Veröffentlichungen III 4.2.3

Personalakten
- Einsicht in — II 2.4, III 1.2.1

Personalwesen II 3.1

Personaldatenbanken III 4.1.2

Personalstrukturdatei III 4.1.2

Personenbezogene Daten I 1.2.3, I 3.1, I 4.1.1, I 4.1.2, II 3.1
- Erhebung — I 4.1.1.1, I 4.1.1.2
- Ermittlung — III 1.5.2
- — in der Landesverwaltung I 4.1.1.3
- — in der Bundesgesetzgebung I 4.1.1.2
- Umgang mit — I 4.1.1, II 4.1.1, III 1.3, III 1.5.1, III 1.5.5, III 1.5.6
- Weitergabe — III 4.1, III 1.5.6, III 5.2

Personalinformationssystem III 4.1.3

Personenkennzeichen I 2.2.1, III 4.1

Persönlichkeitsprofil II 1.3.2, II 4.1.1.1 c

Persönlichkeitsrecht I 1.2.3, III 1.5, III 4.1, III 5.5
- Eingriffe in das — in der Bundesgesetzgebung I 4.1.1.2
- Gefährdung des — II 4.1.1.1 c
- Schutz des — I 4.1, I 4.1.1.1, II 4.1, II 4.1.1.1 c, III 4.1

Persönlichkeitsschutz I 1.4, I 2.4.1, II 2.4.2

Planerisches Handeln I 1.2.1

Planung
- -bürokratie I 4.2.1
- — und Entscheidungshilfe I 4.2.1
- integrierte — I 4.2.1
- kommunale — II 4.2.4

Planungsinformation politische — II 4.2.4

Polizei-Informations-System III 4.1.5.1

Podlech II 4.1.1.1, III 2.2.1

Praxis
Wissenschaft und — III 1.5.7
Private Unternehmen I 1.3.2, II 4.1.3, III 1.5.1
Hilfe durch — bei Verwaltungsaufgaben I 4.1.2.3 d, II 4.1.1.3 d, II 4.1.3.1, II 4.1.3.2
Zusammenarbeit mit — II 5.2, III 5.1
Privatrecht
Regelung im Bereich des — I 1.3.2
Privatsphäre I 1.2.1, I 1.2.3, I 1.3.1, III 4.1
Beschränkungen der Datenschutzvorschriften auf den Schutz der — I 2.4.2
Eindringen in die — I 4.1.1.2, I 4.1.1.3 c
Schutz der — im Verhältnis zur Kirche I 4.1.1.3 f, III 4.1.6
Interpretation der — II 4.1.2.2
Programme für Datenschutz II 1.3.1, III 4.3.1
Programm-Manipulation III 4.3.1, III 4.3.3
Protokolle über Datenabruf I 2.2.1, III 4.1.3 a
Protokollierung
automatische — I 2.4.4, II 2.4.3 bis II 2.4.5, III 4.3.1, III 4.3.3
Prüf- und Analyseprogramme III 4.3.3

Rationalisierung der Verwaltung I 1.2.2
Rechnungshof für das Land Hessen II 4.3.1
Religionsgesellschaften
öffentlich-rechtl. — II 2.2.1, II 4.1.1.3 g
Rentenauskunftsverfahren II 4.1.1.3 g
Rentenversicherung II 4.1.1.2
Rheinland-Pfalz
Datenschutz in — I 2.1.3, I 2.4.2, II 2.1.3, III 1.3, III 2.1.3
Einwohnerinformationssystem in — I 1.2.3
Rotes Kreuz III 4.1.1.2

Saarland
Datenschutz im — I 2.1.8
Schleswig-Holstein
Datenschutz in — I 2.1.1, II 2.1.1
Schülerdatei III 4.1.2
Schulsportärztlicher Untersuchungsbogen III 4.1.1.3
Schutzmaßnahmen II 4.3.2
Schweigegebot
Aufhebung des — I 1.4
Schweigepflicht
ärztliche — II 4.1.2.3
Seidel II 4.1.1.1
Service-Unternehmen I 1.3.2, I 4.1.2.3. d, II 4.1.1.3 d, II 4.1.3.1, II 4.1.3.2, II 5.2, III 5.1
Sicherheitsbestimmungen I 1.2.1, II 4.3.1
Simitis I 1.2.3, III 2.2.1
Sozialarbeiterin III 1.2.1
Sozialversicherungen und Datenschutz I 4.1.1.3 d, II 4.1.1.2
Sparkassen- u. Giroverband III 1.5.1
Sperren
— gegen Abruf I 2.2.1, III 4.3.3
— gegen Privatauskünfte I 2.2.1
Sphärentheorie I 1.2.3, II 4.1.2.1
Staatsgerichtshof — Urteil v. 27. 10. 65 — I 4.1.1.3 f
Stadtplanung III 1.5.1 c
Statistik I 4.1.1.1, III 4.2.3
Bundes- I 4.1.1.2
— ohne Individualdaten I 5.4
gesetzliche Verankerung der — II 4.1.1.3 b
Scheidungs- I 4.1.2
Statistisches Bundesamt I 4.1.1.1, I 4.1.2
Statistisches Landesamt I 4.1.1.3, I 4.1.2, II 4.1.1.3 b, III 4.1.4, III 4.2.3
Steinmüller I 1.2.3
Strafvorschriften I 2.2.4, I 2.4.6, II 2.2.4

Tätigkeitsbericht
parlamentarische Behandlung des — II 1.1, III 4.2
Tiedemann/Sasse III 2.2.1
Transparenz II 2.4.3, II 4.1.4

Universitäten III 4.3.2
Universitätsklinik III 1.5.7
Unterlagen für die Zwecke der maschinellen Datenverarbeitung I 1.3.2, I 3.2
Unterlassungsanspruch des Bürgers I 2.4.5

Untersuchungsbogen III 4.1.1.3
Urmaterial der Erfassung I 4.1.1.1
Verantwortung für Datenschutz I 5.6, II 4.1.1.3 d, II 4.1.3.2
Verfahrensentwicklung
Prioritätensetzung bei der — II 4.2.2
Verfassungsschutz III 4.1.5.2
Verkehrsordnungswidrigkeiten II 4.2.2
Verkehrsplanung III 1.5.1 b
Verkehrsverbund III 1.5.1 b
Verpflichtungsgesetz III 2.2.3
Verrechtlichung von Verwaltungsvorschriften II 4.1.1.3 c, II 4.1.1.3 e, II 5.3, III 1.5.4, III 5.4
Verschwiegenheitspflicht I 1.4, I 4.1.1.1, I 4.1.2, II 4.1.1.1
Verschwiegenheitsvorschriften I 1.2.3
Versicherungsvertreter III 1.2.1
Vertraulichkeit der Angaben des Bürgers I 4.1.1.1, II 4.1.1.1 c, II 4.1.2.2, II 4.1.2.3
Verwaltung
öffentliche — I 1.2.3, I 1.3.2, I 4.3, II 4.2.2 III 1.5.1
-aufbau II 4.2.2
-verfahren II 4.2.2
Volksvertretung
kommunale — II 4.2.4
Initiativfunktion und Kontrollfunktion der — II 4.2.4
Vorschlagswettbewerb III 1.5.8 III 5.7
Wahlrechtskartei II 4.1.1.1 c
Westin, Alan F. I 2.4.2
Wiederherstellungsanspruch des Bürgers I 2.4.5
Wissenschaft und Praxis
Zusammenarbeit von — III 1.5.8
Wohngeld
Auszahlung des — mittels EDV -daten I 4.1.1.3 d II 4.2.3
Wohnungsstichprobengesetz
Entwurf eines — I 4.1.1.2
Zielkonflikt
„Datenschutz-Datenverarbeitung" II 2.4.3
Zugang zu Daten I 4.2.2
Zugriff auf Datenbestände I 1.2.3, I 4.1.2, I 5.4
Zugriffsrecht I 1.2.3 III 1.5.6
Zusammenarbeit der Verwaltung und privater Stellen I 4.1.1.3 d, I 5.5, II 4.1.1.3 d