9. Wahlperiode

Drucksache **9/4032**

HESSISCHER LANDTAG

23. 12. 80

Neunter Tätigkeitsbericht des Hessischen Datenschutzbeauftragten

Mit Schreiben vom 23. Dezember 1980 legt der Datenschutzbeauftragte gemäß § 29 des Hessischen Datenschutzgesetzes vom 31. Januar 1978 dem Landtag folgenden Tätigkeitsbericht vor:

Eingegangen am 23. Dezember 1980 - Ausgegeben am 24. Februar 1981

Druck und Auslieferung: Kanzlei des Hessischen Landtags - Postfach 3240 - 6200 Wiesbaden 1

INHALTSVERZEICHNIS

Seite

1. **Schwerpunkte und Entwicklungstendenzen** ... 5

2. **Aufgaben der nächsten Jahre** ... 11

2.1 **Direktzugriff und Rechnerverbund - Entwicklung der Informationstechnik und Datenschutz** ... 11

2.1.1 Direktverbindung zwischen Polizei und Kfz.-Zulassungsstelle ... 11

2.1.2. Datenschutz in der Datenfernverarbeitung ... 11

2.2 **Schutz von Patientendaten im Krankenhaus und in der medizinischen Forschung** ... 17

2.2.1 Neuregelung des Datenschutzes im Hessischen Krankenhausgesetz (HKG) ... 17

2.2.2 Krebsregister ... 24

2.3 **Datenbedarf von Planung und Statistik - Implikationen des Datenschutzes** ... 25

2.3.1 Datenzugang für die Landesplanung - Die Problematik der Rechtsgrundlage ... 25

2.3.2 Funktionswandel der Statistik, Informationsgleichgewicht und die Notwendigkeit einer bereichsspezifischen Regelung ... 26

2.3.3 Datenschutz und alternative Formen der Erhebung für statistische Zwecke - Das Beispiel "Mikrozensus" ... 27

2.4 **Datenverarbeitung durch den Verfassungsschutz - Notwendigkeit und Grundsätze einer gesetzlichen Regelung** ... 28

3. **Konsequenzen der Bundesgesetzgebung** ... 30

3.1 **Das Melderechtsrahmengesetz und die Novellierung des Landesmelderechts** ... 30

3.2 **Bundespersonalausweisgesetz - Anforderungen an das Herstellungsverfahren** ... 36

3.3 **Sozialdatenschutz bei Leistungsträgern auf Landes-, Kreis- und kommunaler Ebene - Zum neuen 10. Buch des Sozialgesetzbuchs (SGB X)** ... 37

4. **Datenschutzprobleme - Erfahrungen und Beispiele** ... 38

4.1 **Personaldatenschutz im öffentlichen Dienst** ... 38

4.1.1 Zum Stand der Automatisierung der Datenverarbeitung in der Personalverwaltung in Hessen 38

4.1.2 Personaldatensystem des Hessischen Landesamtes für Straßenbau ... 39

4.1.3 Automatisierte Speicherung und Auswertung von Telefongesprächen ... 39

4.1.4 Datenschutz und das Verhältnis zwischen Dienststelle und Personalvertretung ... 40

4.2 **Übermittlungsgrenzen bei Informationsaustausch zwischen Behörden** ... 41

4.2.1 Amtshilfe der Justiz für die Exekutive - Akteneinsichtsrecht für Sicherheitsbehörden? ... 41

4.2.2 Amtshilfe von Hochschulen gegenüber dem Landesamt für Verfassungsschutz (LfV) ... 42

4.2.3 Einschränkung der "Mitteilungen in Strafsachen" (MiStra) ... 43

4.3 **Datenschutz im Hochschulbereich - Exemplarische Darstellung und Konsequenzen einer Prüfung gem. § 23 HDSG** ... 44

4.4 **Schutz von Wählerdaten - Beispiel: Die neue Hessische Kommunalwahlordnung (KWO)** ... 48

4.5 **Berichtigung - Konsequenzen für die Verwaltung** ... 49

4.6 **Datensicherung - Forderungen an Automationsvorhaben der Verwaltung** ... 49

5. **Dateienregister** ... 51

6. **Materialien** ... 52
Erklärung zum Datenschutz und zu der Verwendung personenbezogener Daten für Forschungszwecke (verabschiedet von der Generalversammlung der European Science Foundation am 12. November 1980)

1. Schwerpunkte und Entwicklungstendenzen

1.1 Zehn Jahre nach der Verabschiedung des ersten Hessischen Datenschutzgesetzes hat die Diskussion über den Datenschutz nichts von ihrer Aktualität verloren. Die Vorzeichen haben sich freilich geändert. Im Vordergrund steht nicht mehr die Forderung, generelle, gesetzlich abgesicherte Vorkehrungen gegen die Gefahren einer Verarbeitung personenbezogener Daten zu treffen. Datenschutzgesetze gibt es mittlerweile fast überall. Die Diskussion wird vielmehr von der Aufgabe beherrscht, die in den Datenschutzgesetzen enthaltenen allgemeinen Aussagen in konkrete, auf die unterschiedlichsten Problemfälle umgemünzte Anforderungen umzusetzen. So wichtig allgemeine Verarbeitungsbedingungen auch sein mögen, so wenig geht es an, sich mit ihnen zufriedenzugeben. Von einem wirklich ebenso wirksamen wie überzeugenden Datenschutz kann erst die Rede sein, wenn beispielsweise feststeht, welche Konsequenzen er genau für die Verarbeitung von Gesundheitsdaten hat, wie er sich auf die Informationserwartungen der Sicherheitsbehörden auswirkt, welche Schutzvorkehrungen im Rahmen der wissenschaftlichen Forschung zu treffen sind, wo die Grenzen bei der Verarbeitung von Arbeitnehmerdaten zu ziehen sind.

Die publizistische Attraktivität des Datenschutzes mag darunter leiden. Es ist nun einmal leichter, globale Forderungen aufzustellen, und über eine allgemein gehaltene Kritik läßt sich unstreitig sehr viel einfacher reden. Wo es hingegen darum geht, sich mit den besonderen Aspekten einzelner Konflikte auseinanderzusetzen und sorgfältig differenzierende Lösungen auszuarbeiten, fällt es wesentlich schwerer, den Stand und die Ziele des Datenschutzes zu verdeutlichen. Noch einmal aber: Zuverlässige Aussagen über den Datenschutz lassen sich nur machen, wenn feststeht, ob der Bürger in den konkreten, ihn unmittelbar berührenden Situationen von den Formularen der Meldebehörde bis zu der Verarbeitung seiner Daten bei einem Krankenhausaufenthalt mit einer Regelung rechnen kann, die Verarbeitung nicht hinnimmt, sondern gezielt zu steuern sucht und damit seine Chance, Fragenbogen abzulehnen und Antworten zu verweigern, ebenso festigt wie für verbindliche Verarbeitungsbedingungen und wirksame Kontrollvorkehrungen sorgt.

1.2 Der Schwerpunkt des diesjährigen Tätigkeitsberichts ist damit bereits angedeutet. Er will vor allem auf Bereiche hinweisen, für die eine gesetzliche Regelung dringend notwendig ist, wenn die Verarbeitung personenbezogener Daten auch weiterhin keine Erscheinung sein soll, der sich der Bürger fügen muß, sondern die nur solange hingenommen werden darf, wie ihre Ziele offengelegt und ihre Konsequenzen gesehen und präzise geregelt werden. Direktzugriff und Rechnerverbund, Krankenhäuser, Planung sowie Verfassungsschutz sind die Bereiche, auf die sich der Tätigkeitsbericht konzentriert. Jeder von ihnen ist freilich nur eines von vielen möglichen Beispielen für die Notwendigkeit einer Regelung. Sie sind deshalb keineswegs die einzigen in Betracht kommenden Anknüpfungspunkte, an die man im Zusammenhang mit der Aktivität des Gesetzgebers denken kann und muß. Wenn aber gerade diese Bereiche für den Tätigkeitsbericht ausgewählt worden sind, so weil sowohl die Erfahrungen der vergangen Jahre als auch die Diskussion über die weitere Entwicklung und die Defizite des Datenschutzes sich in ganz besonderem Maße auf sie konzentrieren.

1.3 Die Geschichte des Datenschutzes ist durch den Wandel der Informationstechnik bestimmt. Vom Datenschutz wird erst in dem Augenblick gesprochen, in dem die automatische Datenverarbeitung aufkommt. Es sind ihre Konsequenzen, die den Blick für die gesellschaftlichen und politischen Auswirkungen der Datenverarbeitung geschärft haben, und es ist ihre Nutzung durch die staatliche Verwaltung, die den Gesetzgeber des Landes Hessen veranlaßt hat, die Auseinandersetzung mit der Automatisierung auch als Verpflichtung zu verstehen, den Bürger vor den Gefahren einer Verarbeitung seiner Daten zu schützen. Die technische Entwicklung dürfte auch in den kommenden Jahren den Gesetzgeber vor seine wichtigste Aufgabe stellen. Die Überlegungen zu den technischen Aspekten des Datenschutzes reduzieren sich nicht, wie es immer wieder heißt, auf eine Verbesserung der Datensicherung. Zwar kommt es ohne Zweifel darauf an, die vorhandenen Sicherungssysteme zu verfeinern, also wirksamere technische Hindernisse für den Zugang und die Verwendung der Daten aufzubauen. Weitaus wichtiger ist aber die Feststellung, daß der technische Hintergrund, auf dem die Datenschutzgesetzgebung konzipiert und formuliert wurde, überholt ist. Mehr und mehr setzt sich der direkte Zugriff durch. Der Tätigkeitsbericht bringt das Beispiel des direkten Anschlusses der Polizeibehörden an die Dateien der Kraftfahrzeugzulassungsstellen. Damit wird der erste Schritt in eine Richtung vollzogen, die Organisation und Struktur der Datenverarbeitung radikal verändert. Die Behörden erhalten die Möglichkeit, die jeweils von ihnen benötigten Daten zu bekommen, ohne das Rechenzentrum oder diejenige Stelle, die über die Angaben konkret verfügt, einschalten zu müssen. Verwendungsbarrieren, die bislang noch bestanden, werden damit hinfällig. Die technischen Voraussetzungen, um jederzeit an alle dem Staat zugängliche Daten heranzukommen, sind geschaffen (siehe 2.1.1).

Damit sind aber zugleich die vom Gesetzgeber festgeschriebenen Grundsätze des Datenschutzes in Frage gestellt. Ganz gleich, ob man die strikte Zweckbindung der Verarbeitung, die Notwendigkeit, den konkreten Verwendungszusammenhang zu beachten, oder die Verpflichtung, auf die Erforderlichkeit der Daten im Einzelfall Rücksicht zu nehmen, in den Mittelpunkt stellt, jeder dieser Grundsätze ist unter ganz anderen technischen Voraussetzungen entstanden. Sie sind deshalb die rechtliche Reaktion auf eine technische Wirklichkeit, die in dieser Form nicht mehr besteht. Was in der Diskussion über das Personalausweisgesetz kurz angesprochen wurde, gewinnt durch den fortschreitenden Übergang zum on-line-Zugriff konkrete Gestalt: Erleichterte Zugänglichkeit und technische Verbindung der Daten machen es möglich, andere, ungemein gefährlichere Verwendungsbedingungen zu verwirklichen. Nie zuvor war die Chance so groß, so schnell und so zuverlässig den gesamten staatlichen Informationsbestand auszuwerten; nie zuvor hat deshalb auch der Satz des Bundesverfassungsgerichts, daß eine uneingeschränkte Sammlung und Auswertung von Informationen über den Einzelnen dem Grundgesetz widerspricht, einen solchen Realitätsgehalt gehabt.

Die Datenschutzgesetzgebung kann sich deshalb nicht mehr mit ihren bisherigen Anknüpfungspunkten zufriedengeben. Sie muß auf die veränderten technischen Strukturen mit einem neuen Regelungskonzept reagieren. Man kann sich dieser Forderung nicht durch den Hinweis entziehen, letztlich ginge es doch auch beim on-line-Zugriff nur darum, die Arbeitsbedingungen der Verwaltung zu verbessern und ihr damit auch die Möglichkeit zu geben, ihren Aufgaben konsequenter gerecht zu werden. Eine solche Argumentation hat einen fatalen Beigeschmack. Schon einmal waren es scheinbar rein arbeitstechnische Überlegungen, die zum Aufbau von Datenbanksystemen führten, und zwar auch und gerade ohne Rücksicht auf die gesellschaftlichen und politischen Folgen der Informationsaufbereitung. Weder in der Bundesrepublik noch anderwo hat sich der Datenschutz in einem Zug mit dem Übergang zur automatischen Datenverarbeitung entwickelt. Der Gesetzgeber hat die notwendigen Steuerungsinstrumente erst sehr viel später formuliert, und bis heute leidet der Datenschutz unter der Tatsache, daß eine ganze Reihe von Verarbeitungsvorgängen ohne die notwendige Kontrolle und ohne die erforderliche Bindung an bestimmte Verarbeitungsbedingungen eingeleitet worden sind. Dieser Fehler darf sich nicht wiederholen.

So wünschenswert der on-line-Zugriff unter administrativen Gesichtspunkten deshalb auch erscheinen mag, er darf nicht verwirklicht werden, solange die rechtliche Grundlage für die veränderte Informationsstruktur nicht geschaffen worden ist. Entscheidend ist nicht die Erleichterung der Arbeit, sondern einzig und allein die Frage, ob und in welchem Umfang die neue Verarbeitungstechnik noch mit den in der Datenschutzgesetzgebung akzeptierten Grundsätzen vereinbar ist. Daran ändert sich auch dann nichts, wenn es sich um "Pilotprojekte" handelt. Allzuoft haben in der Vergangenheit "Pilotprojekte" Realitäten geschaffen, die der Gesetzgeber dann unter dem Druck eines vermeintlichen Sachzwangs akzeptieren mußte. Ausnahmen für Pilotprojekte darf es deshalb nicht geben. Auch mit solchen Projekten darf erst begonnen werden, wenn zuvor den Anforderungen des Datenschutzes Rechnung getragen worden ist (siehe 2.1.2).

1.4 Auf einer ganz anderen Ebene liegen die Überlegungen zu der Notwendigkeit, die Verarbeitung medizinischer Daten zu regeln. Der Hessische Gesetzgeber hat auch hier sehr viel früher als andere Gesetzgeber für eine erste rechtliche Reaktion gesorgt. So begrüßenswert die Vorschriften des Hessischen Krankenhausgesetzes auch waren, so wenig helfen sie weiter. Eine detaillierte bereichsspezifische Regelung ist längst erforderlich. Nicht von ungefähr hat gerade dieses Problem den Hessischen Landtag beschäftigt. Ebensowenig überrascht es, wenn der bayerische Gesetzgeber und der Datenschutzbeauftragte des Saarlandes hier einen wichtigen Ansatzpunkt für eine bereichsspezifische Datenschutzregelung gesehen haben. Der Tätigkeitsbericht greift die wichtigsten Punkte der bisherigen Diskussion auf und versucht, die für eine rechtliche Regelung entscheidenden Punkte zu formulieren. Dabei geht es einerseits um Verarbeitungsbedingungen, die auf die spezifische Situation im Krankenhaus Rücksicht nehmen und andererseits um die Gewährleistung der auch ansonsten vom Gesetzgeber geforderten Information des Betroffenen und seiner Möglichkeit, die Verarbeitung seiner Daten zu kontrollieren und zu korrigieren. Der Betroffene muß nicht deshalb eine Verkürzung seiner Rechte hinnehmen, weil die ärztliche Behandlung im Vordergrund steht. Es geht um eine auf seine Person bezogene Behandlung und deshalb auch um Daten, die mit ihm unmittelbar zusammenhängen. Sein Anspruch, den Verarbeitungsprozeß nachvollziehen zu können, darf deshalb nicht geschmälert werden.

Ganz in diesem Sinne hat sich die Rechtsprechung unabhängig vom Datenschutz bereits wiederholt und nachdrücklich für eine Information des Patienten ausgesprochen. Der Datenschutz greift insoweit die von der Rechtsprechung anerkannten Grundsätze auf und präzisiert sie im Hinblick auf die Verarbeitung der Patientendaten. Sicherlich kann und darf nicht außer acht gelassen werden, daß es Situationen gibt, in denen die Interessen des Patienten einer Offenlegung der zu seiner Person verarbeiteten Angaben entge-

genstehen. Die Behandlung psychischer Krankheiten ist das wohl beste Beispiel dafür. Der vom Patienten gewollte Behandlungserfolg könnte durch die Offenlegung gefährdet werden. Keine Datenschutzregelung kann sich deshalb der Notwendigkeit entziehen, Ausnahmen vorzusehen. Nur gilt es, nicht zu übersehen, daß diese Ausnahmen nichts an der für den Regelfall bestehenden Verpflichtung ändern, den Patienten genauso wie jeden anderen von der Verarbeitung Betroffenen zu behandeln, seinen Anspruch auf Information also voll und ganz zu respektieren. Die Verarbeitung medizinischer Daten steht insofern ebenso unter dem Vorzeichen der Transparenz wie auch die Verwendung aller anderen personenbezogenen Angaben. Nicht minder wichtig sind Vorkehrungen, die eine Verarbeitungskontrolle sichern. Gerade weil es unter Umständen auch Ausnahmen von der Auskunftsverpflichtung geben muß, kommt es besonders darauf an, einen Kontrollmechanismus vorzusehen, der dem Patienten die Gewißheit vermittelt, daß die Ausnahme nicht zum bequemen Umgehungsmittel des Datenschutzes werden kann (siehe 2.2.1).

Die Verarbeitung medizinischer Daten gehört schon vom Umfang her zu den wichtigsten Verarbeitungsfällen. Sie betrifft zudem Angaben, die zu den sensibelsten zählen. Der Gesetzgeber darf eine Regelung daher nicht weiter hinausschieben. Sowohl im Interesse der Patienten als auch in dem der Ärzte und Krankenhäuser kommt es darauf an, möglichst bald Verarbeitungsregeln festzuschreiben, die sich an den konkreten, für die Verwendung medizinischer Daten bezeichnenden Konflikten orientieren und deshalb Lösungen bereitstellen, die den Besonderheiten dieser Konflikte Rechnung tragen. Einen besonderen Verarbeitungsfall betrifft das Krebsregister. Die Krebsforschung ist unstreitig auf die Kenntnis der Patientendaten angewiesen; genausowenig läßt sich aber der hohe Sensibilitätsgrad der verwendeten Angaben übersehen. Die Verarbeitung setzt deshalb in ganz besonderem Maß einen wirksamen Datenschutz voraus. Der Tätigkeitsbericht enthält deshalb sowohl Vorschläge für eine gesetzliche als auch Überlegungen zu einer möglichen Übergangsregelung (siehe 2.2.2).

1.5 Der Sechste Tätigkeitsbericht hatte bereits auf die Notwendigkeit besonderer Datenschutzbestimmungen für staatliche Planungsaktivitäten hingewiesen. Die Erfahrung der letzten Jahre hat diese Forderung nachdrücklich bestätigt. Die Planungsinstanzen des Landes sehen sich beim Zugang zu den für ihre Tätigkeit erforderlichen Angaben in zunehmendem Maße mit Schwierigkeiten konfrontiert. Sie ergeben sich einmal aus den mit dem Statistikgeheimnis verbundenen Verwendungsgrenzen. Angaben, die zu statistischen Zwecken erhoben worden sind, dürfen eben nicht ohne weiteres für andere Ziele genutzt werden. Die Kehrseite der vom Gesetzgeber der Statistik gegenüber verlangten Offenheit ist die strikte Begrenzung des Zugangs zu den Daten, die den statistischen Ämtern zur Verfügung stehen. Die Schwierigkeiten folgen aber auch aus dem für einen wirksamen Datenschutz unverzichtbaren Grundsatz, daß immer nur die für eine ganz bestimmte Aufgabe wirklich erforderlichen Angaben verarbeitet werden dürfen. Selbst wenn also gewisse Angaben der öffentlichen Verwaltung durchaus zur Verfügung stehen, sind sie nicht beliebig verwendbar. Dabei bleibt es auch, wenn es um die Planung geht. Sie findet im Rahmen der staatlichen Tätigkeit statt und muß sich daher an die für diese Tätigkeit vorgesehenen Verarbeitungsregeln halten.

Will man deshalb den Zugang der Planungsinstanzen zu den von ihnen benötigten Daten ermöglichen, dann muß zuvor für eine strenge Abschottung der Planungsbehörden gesorgt werden. Ähnlich wie für den Bereich der wissenschaftlichen Forschung gilt auch hier der Satz: Angaben, die für Planungszwecke überlassen werden, sind nur für diese Zwecke zu benutzen, mag ihre Verwendung für andere Ziele noch so wünschenswert erscheinen. Solange es an einer solchen Abschottung fehlt, riskiert die Planung, den Datenschutz in Frage zu stellen. Die Zugangsschwierigkeiten sind insofern auch eine Absicherung des Datenschutzes. Der Gesetzgeber kann aber nicht umhin, den Widerspruch zu lösen, der sich aus der gleichzeitigen Bereitschaft, die Planung zu fördern und den Datenschutz zu gewährleisten, ergibt. Mag sein, daß die Planungsinstanzen zu einem Zeitpunkt entstanden sind, zu dem die Konsequenzen des Datenschutzes noch nicht klar abzusehen waren. Erst recht folgt aber daraus, daß mit der Verwirklichung des Datenschutzes auch die Frage beantwortet werden muß, wie die als notwendig angesehenen und institutionell abgesicherten Planungsaufgaben erfüllt werden können (siehe 2.3).

1.6 Über die Sicherheitsbehörden ist gerade unter Datenschutzgesichtspunkten sehr viel diskutiert worden. An der Notwendigkeit bereichsspezifischer Regelungen besteht mittlerweile kein Zweifel. Ebensowenig läßt sich bestreiten, daß erste entscheidende Schritte in diese Richtung erfolgt sind. Im Vordergrund haben aber bisher, ganz gleich, ob man die Richtlinien für die kriminalpolizeilichen Sammlungen oder die Überlegungen zu den verschiedenen Dateien nimmt, die Polizeibehörden gestanden. Der Datenschutz kann und darf sich aber nicht in einer Regelung der Verarbeitung personenbezogener Daten für polizeiliche Zwecke erschöpfen. Vielmehr kommt es genauso darauf an, die Verarbeitungsbedingungen für alle anderen Sicherheitsbehörden festzulegen. Ganz in diesem Sinn enthält der Tätigkeitsbericht Überlegungen zu der Verarbeitung im Bereich des Verfassungsschutzes.

Der Gesetzgeber kann sich dieser Aufgabe schon deshalb nicht entziehen, weil es gegenwärtig für den Landesbereich an einer rechtlichen Regelung fehlt, aus der sich die Zulässigkeit der Verarbeitung durch das Landesamt für Verfassungsschutz ergeben könnte. Es geht also keineswegs nur darum, die Einzelheiten der Verarbeitung näher zu bestimmen, sondern vor allem anderen um eine gesetzliche Grundlage für die Verarbeitung. Für den Verfassungsschutz gilt ebenso wie für jede andere Behörde des Landes die Verpflichtung, den Anforderungen des Datenschutzes zu genügen. Die im Hessischen Datenschutzgesetz formulierten Zulässigkeitsvoraussetzungen sind aber im Falle des Verfassungsschutzes nicht erfüllt. Solange es daher an einer klaren, die Befugnisse des Verfassungsschutzes im Verarbeitungsbereich festlegenden Norm fehlt, bewegt sich die Verarbeitung außerhalb des vom Gesetzgeber selbst abgesteckten Rahmens.

Ziel der gesetzlichen Regelung muß es zunächst sein, für eine klare Trennung der Aufgaben von Verfassungsschutz und Polizeibehörden und damit auch der jeweiligen Informationssysteme zu sorgen. Die Verarbeitung ist stets nur solange zulässig, wie sie durch die konkreten, gesetzlich abgesicherten Aufgaben gerechtfertigt wird. Verfassungsschutz und Polizeibehörden mögen zwar Sicherheitsaufgaben wahrnehmen. Hinter diesem gemeinsamen Nenner verbergen sich aber höchst unterschiedliche Ziele, die auch eine getrennte und nach verschiedenen Grundsätzen zu beurteilende Aktivität zur Folge haben. Unter diesem Gesichtspunkt gilt es, die Verarbeitung zu beurteilen und ihre Grenzen abzustecken. Mag sein, daß es durchaus Fälle gibt, in denen ein Informationsaustausch zwischen Verfassungsschutzämtern und Polizeibehörden notwendig erscheint. Es ist aber Sache des Gesetzgebers, diese Fälle offenzulegen und die Voraussetzungen für eine Informationsübermittlung zu schaffen.

Der Tätigkeitsbericht weist aber auch darauf hin, daß eine gesetzliche Regelung für klare Verarbeitungsbedingungen und eindeutige Kontrollrechte des Betroffenen sorgen muß. Die Diskussion über den Datenschutz im polizeilichen Bereich hat zu einer Korrektur der ursprünglichen Einstellung des Gesetzgebers zur Auskunft an den Betroffenen geführt. Sie hat zugleich gezeigt, wie wenig globale Aussagen für oder gegen die Auskunft angebracht sind. Auch für den Verfassungsschutz muß deshalb gelten: Die Verarbeitung personenbezogener Daten hat grundsätzlich die Verpflichtung zur Folge, dem anfragenden Bürger eine vollständige und korrekte Auskunft zu geben. Dem Auskunftsrecht sind sicherlich Grenzen gesetzt. Ihre Notwendigkeit ist aber kein Argument gegen die grundsätzliche Anerkennung des Auskunftsrechts. Sie verpflichtet den Gesetzgeber lediglich dazu, von Anfang an festzulegen, welche Schranken zu beachten sind. Als Ansatzpunkt bietet sich wiederum die für den polizeilichen Bereich getroffene Regelung. Zu den aus der Perspektive des Datenschutzes wichtigsten Vorkehrungen gehört schließlich die Löschung der für die jeweilige Aufgabe nicht mehr gebrauchten Angaben. Der Datenschutz fordert klare Fristen, die letztlich allein die Gewißheit verschaffen, daß es zu keinem beliebigen Rückgriff auf die einmal erhobenen Angaben kommt. Personenbezogene Angaben sind eben kein jederzeit verwertbares Informationsmaterial, sondern sie dürfen immer nur zu ganz bestimmten Zwecken und innerhalb eines ebenso feststehenden zeitlichen Rahmens genutzt werden (siehe 2.4).

1.7 Der zweite Schwerpunkt des Tätigkeitsberichts ist durch die Entscheidungen des Bundesgesetzgebers bedingt. Der Bundestag hat im Berichtszeitraum eine Reihe für den Datenschutz wichtiger Regelungen verabschiedet. Das Melderechtsrahmengesetz zählt ebenso dazu wie das Personalausweisgesetz und die Ergänzung des Sozialgesetzbuches. In jedem dieser Fälle hat der Bundesgesetzgeber versucht, bereichsspezifische Antworten auf die Datenschutzfragen zu geben. Jeder von ihnen stellt aber zugleich den Landesgesetzgeber und die Landesbehörden vor neue Aufgaben.

1.8 Wohl am deutlichsten ist dies beim Melderechtsrahmengesetz der Fall. Sein Inhalt war lange umstritten, und die Kontroverse um manche seiner Bestimmungen dürfte sich auch nach der Verabschiedung fortsetzen. An der Intention des Gesetzes läßt sich dennoch nicht zweifeln. Es will der Meldebehörde eine genau umrissene Aufgabe zuweisen und lehnt damit zugleich jeden Versuch entschieden ab, die Meldebehörden als Datendepots der öffentlichen Verwaltung auszugeben. Der Verarbeitung von personenbezogenen Daten sind damit enge Grenzen gezogen. Für den Landesgesetzgeber folgt daraus, daß er sich bei seiner Entscheidung auch an den durch die Aufgaben der Meldebehörde festgelegten Rahmen halten muß. Speicherbar sind infolgedessen grundsätzlich nur Angaben, mit deren Hilfe die Identität festgestellt und die Wohnung nachgewiesen werden kann. Das Gesetz erkennt zwar ausdrücklich das Recht der Länder an, den Datenkatalog mit Rücksicht auf bestimmte von ihnen zu erfüllende Aufgaben zu erweitern. Sie sind aber deshalb nicht berechtigt, den Umfang der Verarbeitung beliebig zu variieren. Zulässig kann und darf immer nur eine Erweiterung sein, die sich mit der vom Gesetz festgelegten Aufgabe der Meldebehörden vereinbaren läßt. Das gilt auch und gerade dann, wenn die Meldebehörden bislang Aufgaben wahrgenommen haben, die darüber hinausgehen. Der Datenschutz zwingt die Verwaltung, ihre Aufgaben

zu überprüfen und die Konsequenzen aus seinen Anforderungen zu ziehen. Für den Meldebereich bedeutet diese Feststellung, daß ein wirksamer und den Intentionen des Gesetzgebers entsprechender Schutz nur zu erzielen ist, wenn sich die Tätigkeit der Meldebehörden strikt nach ihrer im Gesetz selbst definierten Aufgabe richtet.

Daraus folgt freilich nicht, daß sich die Länder darauf beschränken müssen, das Melderechtsrahmengesetz zu übernehmen. Sie sind vielmehr verpflichtet, zu prüfen, ob es nicht möglich ist, den Datenschutz auszubauen und manche mißverständliche gesetzliche Bestimmung durch klare, die Verarbeitung begrenzende Aussagen, zu ersetzen. Dies gilt für die regelmäßigen Übermittlungen im öffentlichen Bereich ebenso wie für die Weitergabe von Informationen innerhalb einer Gemeinde oder die Auskunft aus dem Melderegister. In jedem dieser Fälle werden die Verwendungsmöglichkeiten der Daten des Bürgers erweitert, gewinnt also auch die Notwendigkeit, die Verarbeitung sorgfältig einzuschränken, eine ganz besondere Bedeutung (siehe 3.1).

1.9 Beim Personalausweisgesetz, dem zweiten im Tätigkeitsbericht für die Auswirkungen einer bundesgesetzlichen Regelung angeführten Beispiel, geht es dagegen nicht um eine Entscheidung des Landesgesetzgebers. Im Vordergrund steht vielmehr die Auseinandersetzung über das Verfahren für die Herstellung der Ausweise. Auf den ersten Blick eine rein technische Frage, die scheinbar, jedenfalls unter Datenschutzgesichtspunkten, keine weitere Beachtung verdient. Der Eindruck täuscht freilich. Das Gesetz hat sich im Interesse eines wirksamen Datenschutzes für ein Speicherungsverbot der bei der Ausstellung des Ausweises verwendeten Angaben ausgesprochen. Das vorgesehene Herstellungsverfahren unterläuft diese Anforderung. Die Daten werden eben doch bei der Bundesdruckerei gespeichert, wenn auch nur vorläufig und aus Gründen, die mit der Herstellung zusammenhängen. Der Gesetzgeber hat aber keine Ausnahme zugelassen. Er fragt nicht nach den Gründen für die Speicherung, sondern spricht sich generell gegen sie aus, und zwar mit Rücksicht auf die besonderen Gefahren, die sich aus der Konzentration der Daten bei der Bundesdruckerei ergeben. Dieser Erwartung des Gesetzgebers muß auch entsprochen werden. Technische Sachzwänge, die eine andere Lösung rechtfertigen könnten, gibt es nicht. Das Gesetz enthält eine verbindliche Vorlage für die Herstellungstechnik. Sie hat sich deshalb nach seinen Anforderungen zu richten. Daß dies durchaus möglich ist, zeigen die von mir unterbreiteten Vorschläge. Sie mögen nicht die einzig denkbaren und vertretbaren sein; sie sind aber zumindest eine Aufforderung, über gesetzeskonforme Verfahren nachzudenken und nur Lösungen zu akzeptieren, die mit dem Gesetz in Einklang stehen (siehe 3.2).

1.10 Beim Sozialgesetzbuch schließlich hat sich der Bundesgesetzgeber zu einer eingehenden Datenschutzregelung entschlossen. Manche der Bestimmungen konnte im Laufe des Gesetzgebungsverfahrens verbessert werden. Dennoch bringt das Gesetz, so begrüßenswert es im übrigen auch ist, Komplikationen mit sich. Sie liegen in erster Linie im Bereich der Abgrenzung der verschiedenen Datenschutzregelungen. Hier wird es vor allem darauf ankommen, Wege zu finden, die es einerseits den Sozialleistungsträgern ermöglichen, mehr und mehr mit den spezifischen Datenschutzanforderungen des Sozialgesetzbuches vertraut zu werden, und andererseits rechtzeitig die Unsicherheit ausschalten, die sich aus dem Nebeneinander verschiedener Regelungen ergeben könnten (siehe 3.3).

1.11 Der letzte größere Teil des Tätigkeitsberichts greift Erfahrungen aus dem vergangenen Jahr auf. Sie geben einen Ausschnitt aus der Arbeit des Datenschutzbeauftragten wieder und sind ausschließlich unter dem Gesichtspunkt ausgewählt, weitere Anregungen für die Verbesserung des Datenschutzes zu vermitteln. Das gilt ganz besonders für den Personaldatenschutz. Sowohl im öffentlichen als auch im privaten Bereich spielt die Diskussion über die Verarbeitung von Arbeitnehmerdaten eine immer wichtigere Rolle. Personalinformationssysteme und Kontrollrechte der Arbeitnehmervertretung sind nur zwei der aktuellsten Stichworte. Der Bericht bringt Beispiele für entstehende Personalinformationssysteme und weist unter anderem auf die Bedeutung der Mitwirkung des Personalrats bei der Verwirklichung von Datensicherungsmaßnahmen hin (siehe 4.1).

Mit der Verabschiedung der Datenschutzgesetze ist zugleich die Notwendigkeit sichtbar geworden, den Informationsaustausch im staatlichen Bereich an feste, strikt aufgabenorientierte Voraussetzungen zu binden. Der Staat ist keine Informationseinheit, innerhalb derer personenbezogene Angaben grundsätzlich frei zirkulieren können. Der Tätigkeitsbericht weist auf eine Reihe von Fällen hin, die deutlich zeigen, wie sehr es darauf ankommt, die Grenzen einer Übermittlung von Informationen näher zu bestimmen. Das gilt für das Verhältnis der Justiz zur Exekutive genauso wie für den Zugriff des Verfassungsschutzes auf Daten, die den Hochschulen zur Verfügung stehen. Die ebenfalls in diesem Zusammenhang angeführten "Mitteilungen in Strafsachen" gehören zu den Informationsinstrumenten, die lange vor dem Datenschutz bestanden haben, die aber in der überlieferten Form nicht mehr hingenommen werden können. Der

Datenschutz verlangt nun einmal eine konsequente Überprüfung aller bislang akzeptierten Übermittlungsformen. Der Gesetzgeber hat mit seiner Entscheidung für den Datenschutz die Prioritäten anders als bisher formuliert; nicht die Verbesserung der Übermittlung von Informationen steht im Vordergrund, sondern die Verpflichtung, jeden Übermittlungsfall auf seine Konsequenzen für den Betroffenen hin zu kontrollieren (siehe 4.2).

Der Tätigkeitsbericht geht schließlich in diesem Teil ausführlich auf die besonderen Probleme ein, die mit der Prüfung einer Hochschule verbunden sind. Die Hochschule ist gleichsam Schnittpunkt überaus verschiedener Verarbeitungszusammenhänge. Sie verarbeitet Personal- ebenso wie Studenten-, Patienten- und Forschungsdaten, um nur die wichtigsten Beispiele zu nennen. So sehr es aber gerade deshalb darauf ankommt, den Datenschutz sicherzustellen, so wenig können die Konsequenzen übersehen werden, die sich beispielsweise aus der Verpflichtung ergeben, die verfassungsrechtlich garantierte Freiheit der Forschung zu respektieren. In den früheren Tätigkeitsberichten war auf dieses Problem und seine in Hessen angestrebte Lösung wiederholt hingewiesen worden. Der Bericht über die Prüfung der Verarbeitung im Rahmen einer Hochschule macht noch einmal die Schwierigkeiten klar, bestätigt aber deutlich die Notwendigkeit, auch im Bereich der Hochschule konsequente Datenschutzmaßnahmen zu treffen (siehe 4.3).

1.12 Manche der im letzten Tätigkeitsbericht angesprochenen Fragen hat auch im Berichtszeitraum eine wichtige Rolle gespielt. Ein bezeichnendes Beispiel dafür ist die Forderung nach Datenschutzvorschriften für den polizeilichen Bereich. Die Diskussion im Rahmen der Länder über die Vorschriften für kriminalpolizeiliche Sammlungen ist inzwischen abgeschlossen. Der Innenausschuß des Hessischen Landtags hat sich ausdrücklich dafür ausgesprochen, sie so bald wie möglich auch für Hessen in Kraft zu setzen. Zu ihren wichtigsten Merkmalen gehört die Anerkennung der Forderung nach einem Auskunftsrecht des Bürgers. Bei der nunmehr erforderlichen Konkretisierung der zwischen den Ländern vereinbarten Vorschriften für den Bereich des Landes Hessen wird ganz besonders darauf zu achten sein, ob und in welchem Umfang es möglich ist, weitere Verbesserungen der Datenschutzvorschriften zu erzielen.

Wie wenig allerdings davon die Rede sein kann, daß mit den Vorschriften über die kriminalpolizeilichen Sammlungen die Datenschutzanforderungen im polizeilichen Bereich erfüllt sind, zeigt sich an der Rasterfahndung. Weder das Bundesdatenschutzgesetz noch die Strafprozeßordnung bieten genügend Anhaltspunkte für eine überzeugende rechtliche Regelung. Zu den vordringlichsten Aufgaben der nächsten Monate wird es daher gehören, die Bedingungen zu formulieren, unter denen ein Zugriff auf personenbezogene Daten im Rahmen polizeilicher Fahndungsaktionen, die in diese Richtung zielen, überhaupt in Betracht kommt. Die Datenschutzbeauftragten der Länder und des Bundes haben sich übereinstimmend für eine klare rechtliche Regelung ausgesprochen. Sowohl der Bundes- als auch der Landesinnenminister haben ihre Bereitschaft dazu erklärt. Die Regelung kann und darf nicht wieder aufgeschoben werden.

1.13 Die Schwerpunkte des Tätigkeitsberichts sind auch bezeichnend für die Verteilung der Arbeit im Berichtszeitraum. Sie war und ist zu einem großen Teil Beratung des Gesetzgebers; Melderechtsrahmen-, Personalausweisgesetz und Sozialgesetzbuch sind durch die vom Hessischen Datenschutzbeauftragten vorgelegten Vorschläge entscheidend beeinflußt worden. Sie war und ist aber auch Beratung der mit den Problemen des Datenschutzes konfrontierten öffentlichen Stellen; der Personaldatenschutz ist ebenso bezeichnend dafür wie die Diskussion über das Krebsregister. Sie war und ist schließlich aktive Beteiligung an Fortbildungsveranstaltungen zum Datenschutz.

Nach wie vor steht aber im Vordergrund aller Anstrengungen des Datenschutzbeauftragten die Verbindung zum Bürger. Seinen Fragen wird deshalb der unbedingte Vorrang gewährt. Die Zahl der Fälle, in denen die ausführliche Auseinandersetzung mit konkreten Verarbeitungssituationen auf die Initiative betroffener Bürger zurückgeht, hat erneut zugenommen. Wiederum hat sich daher bestätigt, daß die Fragen aus allen Teilen der Bevölkerung kommen und sich keineswegs nur auf einen ganz bestimmten Aspekt der staatlichen Tätigkeit konzentrieren. Dennoch ist noch lange nicht der Punkt erreicht, der es rechtfertigen würde, von einer ausreichenden Beteiligung der Bürger an der Kontrolle des Datenschutzes und einer überzeugenden Wahrnehmung ihrer Rechte zu sprechen. Die Verpflichtung, die Beziehung zum Bürger zu verbessern, ihm bewußt zu machen, daß es um die Verarbeitung seiner Daten und die Verwirklichung seiner Rechte geht, zählt daher immer noch zu den vordringlichsten Aufgaben des Datenschutzbeauftragten.

2. Aufgaben der nächsten Jahre

2.1 Direktzugriff und Rechnerverbund - Entwicklung der Informationstechnik und Datenschutz

2.1.1 Direktverbindung zwischen Polizei und Kfz-Zulassungsstelle

Das Problem des sogenannten "on-line"-Zugriffs einer Behörde auf Dateien einer anderen Behörde kann an Hand des folgenden Beispiels demonstriert werden, das in diesem Jahr akut wurde: Als "Pilotprojekt" ausgewiesen, besteht eine direkte Zugriffsmöglichkeit des Polizeipräsidenten in Darmstadt auf die automatisierten Dateien der Kraftfahrzeugzulassungsstellen Darmstadt/Darmstadt-Land beim Kommunalen Gebietsrechenzentrum (KGRZ) Starkenburg. Der Zugriff erfolgt über ein Bildschirm-Terminal, über das ein Teil der Daten jedes Kfz-Halters bzw. Fahrzeugs abgerufen werden kann. Weder das Rechenzentrum noch die Zulassungsstellen müssen hierbei organisatorisch eingeschaltet werden. Dieses Projekt soll einen geplanten weitergehenden Rechnerverbund zwischen den Rechenzentren und dem Landeskriminalamt (d.h. dem polizeilichen Informationssystem -HEPOLIS-) vorbereiten.

In meiner Stellungnahme habe ich den Hessischen Minister des Innern zur Überprüfung der Rechtslage aufgefordert und darauf hingewiesen, daß nach meiner Auffassung schon das bestehende Projekt mit der geltenden Rechtslage nicht in Einklang steht. Nach § 26 Abs. 5 der Straßenverkehrszulassungsordnung (StVZO) kann eine Auskunft über Fahrzeuge, Halter und Versicherungen durch die Zulassungsstelle an eine andere Behörde nur **auf Antrag** und **im Einzelfall** erteilt werden. Wenn das Gesetz einen Antrag fordert, so bedeutet dies, daß die Zulassungsstelle die Übermittlung prüfen muß. Sie muß somit eine Möglichkeit der Kontrolle des Übermittlungsvorgangs haben. Die Beschränkung auf den Einzelfall ist Ausdruck des Grundsatzes der Funktionstrennung beider Behörden. Dieser letztere Grundsatz ist ein wesentlicher Bestandteil des Rechts der Amtshilfe wie auch eine notwendige Grundlage für einen funktionsfähigen Datenschutz. Schon im "Pilotprojekt" kann die Polizei prinzipiell genauso unbeschränkt auf den Datenbestand der Kfz-Zulassungsstellen zugreifen wie diese selbst. Eine Überprüfung durch die Zulassungsstelle, ob die Übermittlung an die Polizei erfolgen darf, findet somit nicht statt. Auch erfolgt keine Beschränkung der Übermittlung auf den "Einzelfall", wie es das Gesetz fordert. Die gesetzliche Beschränkung steht im Widerspruch zu einer prinzipiell direkten und unkontrollierbaren Anbindung der Polizeibehörden an die genannten Dateien. Zwar kann auch "im Einzelfall" einmal die Überprüfung einer Reihe von Daten verschiedener Halter oder Fahrzeuge erfolgen. Eine ständige Anbindung der Polizeidienststellen an die Rechner im Gebietsrechenzentrum ohne jeden Bezug auf einen konkreten Fall überschreitet jedoch sicher die Grenzen des "Einzelfalles". Diese Überlegung gilt sowohl für den Datenzugriff zu präventiv-polizeilichen Zwecken (§§ 1, 2 des Hessischen Gesetzes über die öffentliche Sicherheit und Ordnung -HSOG-) als auch für die Strafverfolgung.

Ebenso ist zu berücksichtigen, daß eine "Übermittlung" von Daten aus dem Kommunalen Gebietsrechenzentrum nach § 2 Abs. 2 Ziff. 2 Hessisches Datenschutzgesetz schon dann vorliegt, wenn die Daten "zur Einsichtnahme, namentlich zum Abruf bereitgehalten werden." Schon die Bereithaltung zum Abruf für die Polizeibehörden gilt demnach als "Übermittlung". Im Lichte dieser Norm halte ich die Bereitstellung des gesamten gespeicherten Datenbestandes der Kfz-Zulassungsstelle rund um die Uhr für rechtlich nicht zulässig.

Die gleiche rechtliche Bewertung gilt - in noch stärkerem Ausmaß - für den geplanten **Rechner**zugriff seitens des Landeskriminalamtes, da dann die Daten nicht nur abgerufen, sondern in beliebiger Reihenfolge oder Auswahl mit den Datensätzen des Hessischen Polizeiinformationssystems (HEPOLIS) abgeglichen werden können. Die hier dargestellte Konstellation wirft ein Schlaglicht auf die komplexen Fragen, die die Entwicklung der Informationstechnik in Richtung auf "on-line"-Anschlüsse und den Rechner-Rechner-Verbund aufwirft. Mir erscheint es daher notwendig, im folgenden umfassender auf Stand und Entwicklung der Datenfernverarbeitung einzugehen und ihre Konsequenzen für den Datenschutz aufzuzeigen.

2.1.2 Datenschutz in der Datenfernverarbeitung

Bereits in meinem Achten Tätigkeitsbericht habe ich Datenschutzprobleme dargestellt, die im Zuge des verstärkten Einsatzes von Techniken der Datenfernverarbeitung entstehen (vgl. 1.3.3, 2.4.5.3).

Die Landesregierung hat in ihrer Stellungnahme zu meinem Achten Tätigkeitsbericht dazu ausgeführt: "Die Bedenken des Datenschutzbeauftragten gegen die Dezentralisierung der Datenverarbeitung widersprechen der bisher vorherrschenden Meinung, daß gerade abgeschottete dezentrale Systeme einen größeren Datenschutz gewährleisten als die Verarbeitung in Universalrechenzentren. Im Prinzip ist von jeder Datenstation aus die Möglichkeit gegeben, auf alle in einem Universalrechenzentrum gespeicherten Daten zuzugreifen, soweit dies nicht durch programmtechnische Maßnahmen eingeschränkt wird. Bei

dezentralen Systemen ist das Prinzip nicht möglich, **es sei denn durch Rechnerkopplung - d.h. die Zusammenschaltung selbständiger DV-Anlagen - wird ein Druchgriff auf die dezentral gespeicherten Daten eigens ermöglicht.**" Die Rechnerkopplung wird hier als mögliche Gefahrenquelle innerhalb der Datenfernverarbeitung erwähnt. Wenn die Kommunikation zwischen verschiedenen Rechnern vor einigen Jahren noch als "in absehbarer Zeit nicht realisierbar erschien" (s. Abschlußbericht "Grundstufe Kfz-Zulassungswesen" Ziffer 11.3.3) - zumindest galt diese Aussage mit Ausnahme einiger polizeispezifischer Anwendungen für die Datenfernverarbeitung im öffentlichen Bereich - soll, wie unter 2.1.1 dargelegt, ein weiterer Rechnerverbund verwirklicht werden. Ähnliche Überlegungen werden auch für polizeiliche Zugriffe auf kommunale Einwohnerdateien angestellt. Weitere Einzelheiten über eingeleitete und angestrebte Datenfernverarbeitungsaktivitäten ergeben sich aus den Protokollen und Arbeitsunterlagen des Gemeinsamen Unterausschusses Datenfernverarbeitung.

Sachzwänge und ihr Einfluß auf Automationsvorhaben

Wer sich heute mit Datenfernverarbeitung befaßt, wird von DV-Geräteherstellern und -anwendern mit einer Flut von Argumenten - pro und contra - überschüttet. Er sieht sich mit Begriffen konfrontiert, die für den Laien im Bereich der ADV nicht oder nur schwer verständlich sind. Hinzu kommt, daß sich die Computerindustrie der üblichen Marketingstrategien und Werbemethoden bedient. Typisch sind Schlagworte wie "bürgerfreundliche Verwaltung durch DV-Intelligenz am Arbeitsplatz" oder die Aussage der Hessischen Landesregierung aus dem Jahr 1978: "Die zukünftigen Entwicklungen in der Datenverarbeitung gehen dahin, daß die Computerleistung für den Sachbearbeiter am Arbeitsplatz verfügbar und leichter handhabbar gemacht wird und damit örtlich und zeitlich in die Aufgabenerfüllung integriert werden kann." Die Firma Siemens führt in ihrer Untersuchung "Datenerfassung und -fernverarbeitung; Modellstudie für Hessen" aus: "Die Datenfernverarbeitung bietet die Möglichkeit, dem unterschiedlichen Stand und den verschiedenen Bedürfnissen der Anwender Rechnung zu tragen. Eine engere Kommunikation zwischen Fachverwaltung und Datenbank wird erreicht."

Die Vielfalt der angebotenen Techniken und Systeme läßt dagegen dem einzelnen Anwender kaum noch die Möglichkeit, aussagefähige Preis-Leistungsvergleiche anzustellen. Datenschutzanforderungen, wie z.B. sichere Zugriffstechniken u.ä., werden nach meinen Erfahrungen kaum in Betracht gezogen. Selbstverständlich soll hier nicht eine Technik kritisiert werden, die die Verwaltung aus bekannten Sachzwängen herausführen könnte. Die Ärgernisse, die mit der Konzentration von Verwaltungsaufgaben auf einige wenige Universalrechenzentren verbunden sind, sind nur zu gut bekannt. Welcher Bürger hätte sich noch nicht über die endlose Bearbeitungsdauer von Anträgen, komplizierten Formalismus und bis zur Abstraktion unverständliche "DV-gerechte" Bescheide beschwert? Eines kann man sicher feststellen: Wenn die Datenfernverarbeitung - insbesondere Dialogtechniken - dem einzelnen Mitarbeiter wieder direkten Zugang zu seinen Daten ermöglicht und ihm damit wieder die sofortige Möglichkeit der Information des vorsprechenden Bürgers eröffnet wird, ist allein aus psychologischer Sicht ein Schritt in die propagierte Richtung der "bürgerfreundlichen Verwaltung" getan. Umso mehr stellen sich für den Datenschutz die Fragen nach Risiken und Grenzen dieser Entwicklung.

Technische Entwicklung von Maschinen und Programmen

Begann der "Vater der ADV", der US-Amerikaner Hermann Hollerith, schon 1880 mit dem Einsatz des nach ihm benannten Hollerith-Verfahrens auf der Basis von Lochkarten, so folgten 1934 bis 1941 der Deutsche Konrad Zuse mit den Rechnern Z1 bis Z3 und 1939 bis 1944 der Amerikaner Howard A. Aiken mit dem Rechner Howard Mark I. Allen Geräten gemeinsam war die Verwendung rein mechanischer Elemente und Speicher.

Die **erste Generation** der EDV basierte auf der Verwendung von Elektronenröhren (etwa von 1944 bis 1955). Ab 1955 bis etwa 1964 folgte die **zweite Generation** auf der Basis der Transistortechnik. Die **dritte Generation** wurde ab 1965 auf den Markt gebracht. Bedeutende Vertreter dieser Maschinengeneration - die den Übergang vom Magnetkern (Ferrit)-Speicher zum monolithischen Schaltkreis (Chip) brachte - sind z.B. IBM '360, '370, '303X; Univac 9000, 1100; Siemens 4004, 7500 und andere. Von einer **vierten Generation** wird erst zu sprechen sein, wenn neue Speicherelemente wie chemische Speicher oder Blasenspeicher - die unter Laborbedingungen bereits funktionieren - kommerziell genutzt werden können.

Die Rechner der zweiten Generation hatten für heutige Begriffe unvorstellbar kleine Speichergrößen (z.B. 4000 byte bei der damals weit verbreiteten IBM 1401) und auf die räumlich nächste Umgebung zum Rechner beschränkte Anschlußgeräte wie Drucker, Kartenleser, Kartenstanzer und Bandgeräte. Komplexe Verwaltungsabläufe mußten in viele Einzelschritte zerlegt werden, um sich den geringen Speicherkapazitäten der Rechner anzupassen. Daten wurden in der Regel auf empfindlichen und umständlich zu handhabenden Datenträgern wie z.B. Lochkarten gespeichert. Zahlreiche Fehlerquellen waren die Folge.

Die dritte Generation der Rechenanlagen verwirklichte dann bereits Programmtechniken zur besseren Ausnutzung der hohen internen Rechengeschwindigkeit der Rechner im Verhältnis zu den langsamen Anschlußgeräten. Durch sog. "Multiprogramming" konnten verschiedene Verwaltungsaufgaben gleichzeitig im Rechner bearbeitet werden, da ein Maschinensteuerprogramm - das sog. Betriebssystem - die Zuordnung aller Maschinenkomponenten nach deren Leistungsfähigkeit übernahm. Weiterentwickelte Betriebssystemprogramme ermöglichten die sog. Echtzeit- oder Dialogverarbeitung, d.h. den direkten Zugriff auf Daten und Programme und schufen Zugangsmöglichkeiten für einen größeren Kreis von externen Benutzern durch die Einführung sog. "Zeitscheibenverfahren" - besser unter dem Begriff "time sharing" bekannt. Dabei wird in regelmäßigen chronologischen Intervallen die gesamte Rechnerleistung einem Benutzer zugeordnet. Dieser kann dann alle Betriebsmittel des Systems nutzen, um Programme zu schreiben, zu testen und auch ablaufen zu lassen. Die schnelle Folge der Zeitscheiben läßt ihn bei normalem Ablauf nicht spüren, daß er mit vielen anderen gleichzeitig im System arbeitet.

Zur Zeit sind folgende Datenfernverarbeitungstechniken im Einsatz:

- **Stapelübertragung:** Datenstapel - etwa eine Folge von Datensätzen - werden aufeinanderfolgend zum Rechenzentrum übertragen und dort zur Weiterverarbeitung zwischengespeichert.
- **Stapelfernverarbeitung:** Von einem Datenendgerät, welches an einen Rechner angeschlossen ist, werden vollständige Bearbeitungsaufträge zur direkten Abarbeitung durch das Betriebssystem gesendet, die Arbeitsergebnisse dann zum Anwender rückübertragen.
- **Dialogverkehr:** Der Dialogverkehr ist die heute komfortabelste Art des direkten, wechselseitigen Datenaustauschs zwischen Großrechner und Anwender. Auf jede Einzelanfrage folgt unmittelbar eine Antwort des Rechners. Man spricht hier auch von direkter Datenfernverarbeitung bzw. Echtzeitverarbeitung.

Schien bis vor kurzem der Dialogverkehr das Non-plus-ultra zu sein, wenn man nicht teure Insellösungen mit eigenen Rechnern anstreben wollte, so hat der Preisverfall auf dem Computermarkt hier neue Möglichkeiten eröffnet. Von der Kostenseite her ist es jetzt durchaus interessant, direkt bei einzelnen Anwendern Rechenanlagen mittlerer Größe zu installieren, die mit eigenen Programmen und Daten Verwaltungsaufgaben erfüllen können und nur bei Erreichen ihrer Leistungsgrenze - z.B. bei umfangreichen Jahresabschlußarbeiten - auf mit ihnen verbundene Großrechenzentren zugreifen.

Der Stand der Technik läßt heute mit Sicherheit folgende Aussagen zu:

- Verteilte Datenverarbeitung durch kleine, preisgünstige, aber in der Leistungsklasse der Rechner aus den frühen 70er Jahren liegende Geräte wird in Kürze auch im Bereich der öffentlichen Verwaltung realisierbar.
- Die technischen Probleme des Zugriffs dieser Anlagen auf die Daten und Programme der Großrechenzentren werden kurzfristig gelöst.
- Der Verbund von Rechenzentren unter Ausnutzung öffentlicher Datenübertragungsnetze wie Datex-P der Deutschen Bundespost steht unmittelbar bevor.
- Die mit dem Einsatz dieser Vernetzungstechniken verbundenen möglichen Datenschutz- und Datensicherungsprobleme sind heute zwar zu erahnen, keinesfalls aber endgültig definiert.

Probleme für Datenschutz und Datensicherung

Die heute realisierbaren Möglichkeiten der Verknüpfung von Rechnern zu Rechnernetzen auf den verschiedensten Ebenen der öffentlichen Verwaltung wirft aus der Sicht des Datenschutzes eine Vielzahl von technischen und organisatorischen Fragen auf. Bei Einsatz der Datenfernverarbeitung erreicht der Datenschutz aufgrund der folgenden Faktoren neue Dimensionen:

- Der enge Rahmen der Universal-Rechenzentren wird beliebig erweitert.
- Die Zahl derjenigen, die auf die Betriebsmittel (Maschinen, Daten, Programme) zugreifen können, wird vergrößert.
- Komponenten des Rechners wie Prozessoren-, Speicher- und Datenendeinrichtungen sind oft über größere räumliche Entfernungen verteilt und durch Leitungen, die über Grundstücke Dritter gehen, sich öffentlicher Netze bedienen oder ins Ausland führen, verbunden.

Die Verwaltung als "Herr der Daten" muß sich mithin die Frage stellen, ob sie es zulassen will, daß in einem Netzverbund ihre Daten an beliebigen Stellen verarbeitet werden dürfen. Ich habe aus vielen Gesprächen den Eindruck gewonnen, daß es hier nicht zuletzt aus dem Gefühl heraus, endlich von zeitraubender Verwaltungsarbeit befreit zu werden - z.B. bei besonders aufwendigen Auskunftsverfahren im Wege der Amtshilfe wie im Einwohnerwesen, bei der Kfz-Zulassung - noch oft am nötigen Problembewußtsein mangelt.

Sicherlich kann z.B. eine verteilte Datenhaltung zu verringerten Verlustrisiken führen. Bei einem Rechnerverbund entstehen aber völlig neue Zugriffsrisiken, da hinter Zugriffen nicht mehr in jedem Fall lediglich ein Datenendgerät steht, sondern auch ein Verbundrechner mit allen zusätzlichen Möglichkeiten eines Betriebssystems einschließlich sensitiver Dienstprogramme des Herstellers sowie eigenen Anwendungsprogrammen stehen kann.

Bekannt ist auch, daß es nur mit großem Aufwand möglich (und deshalb unüblich) ist, nachzuweisen, mit welcher Programmversion wann welche Daten verarbeitet wurden. Dokumentationsprogramme der DV-Hersteller, die den gezielten Nachweis von Programmänderungen oder Programm-Manipulationen erbringen - dies gilt ganz besonders für die interaktive Programmierung im Dialog mit dem Rechner -, sind nach Aussage von Marktkennern nicht bekannt. Die bei Programmveränderungen anfallenden Umwandlungslisten sind für diese Zwecke ungeeignet.

Gleiches gilt für die Sicherung von Programmbibliotheken gegen unbefugtes Benutzen. Selbst aufwendige Datenschutzprogramme (wie z.B. RACF) schützen Programme gegen unberechtigten Aufruf nur auf Bibliotheksebene, d.h. jeder, der legitimen Zugang zu einer bestimmten Programmbibliothek hat, kann mit **allen Programmen** dieser Bibliothek arbeiten. Der Hinweis auf die "umfangreiche Protokollierung" hilft hier auch nicht weiter. Protokolle, die wegen Zeitmangels nicht ausgewertet werden, haben keinen Kontrolleffekt.

Um Mißverständnisse zu vermeiden, möchte ich noch einmal unterstreichen: Die Suche nach wirksamen Vorkehrungen der Datensicherung bei der Datenfernverarbeitung impliziert keineswegs ein Mißtrauen gegen die bei der Datenverarbeitung Beschäftigten. Sie setzt vielmehr - und dies ist mein Anliegen - eine Schärfung des Problembewußtseins bei allen Beteiligten voraus.

Maßnahmen nach § 10 (Anlage) HDSG

Die Forderung nach einfachem Zugang zu Datenverarbeitungsleistungen bei hohem Sicherungsstandard der Daten führt unweigerlich zu einem Zielkonflikt. Die Lösung ist deshalb so schwierig, weil bei Datenfernverarbeitung in einem Netzwerk Geräte, die unterschiedlich leistungsfähig sind und von den verschiedensten Herstellern stammen, in einem System zusammenarbeiten. Datenschutz- und Datensicherungsmaßnahmen müssen, wenn sie effektiv sein sollen, bereits in der eingesetzten hard- und software realisiert werden und ihren Niederschlag in Benutzerregelungen finden. Dies gilt in verstärktem Maße, wenn künftig Datenübertragungen in öffentlichen - d.h. jedem zugänglichen - Netzen, wie z.B. DATEX-P der Deutschen Bundespost, erfolgen. Die Schwierigkeit besteht darin, daß auf der einen Seite die zu treffenden Maßnahmen ein Höchstmaß an Datenschutz und Datensicherung garantieren müssen, auf der anderen Seite aber ein solches Kommunikationssystem durch administrative Maßnahmen nicht bis zur Funktionsunfähigkeit eingeschränkt werden darf. Anhand der in der Anlage zu § 10 HDSG aufgeführten Kontrollarten sollen hier Beispiele für Sicherungsmaßnahmen beim Einsatz von Datenfernverarbeitung dargestellt werden; dabei werden nur für diese Form der Datenverarbeitung typische Kontrollformen erwähnt.

- Zugangskontrolle

Datenstations- bzw. Konzentratorräume sind abzuschließen; Terminals sind mit Schlüsselschaltern auszurüsten (dies gilt auch für Telefone, soweit sie zur Datenübertragung eingesetzt werden); Modems und Schnittstellenvervielfacher gehören in abschließbare Schränke bzw. verschließbare Räume.

- Abgangskontrolle

Diese Kontrolle ist zwar für die Datenfernverarbeitung nicht typisch. Erwähnung verdient aber, daß es Datenendeinrichtungen gibt, die gegen die unbefugte Entnahme von magnetisierbaren Datenträgern oder auch Druckerprotokollen geschützt sind.

- Benutzerkontrolle

Terminal-Identifikationen sind gerätemäßig oder über Programm (z.B. TP-Monitor) zu realisieren. Werden zwischen Terminal und Rechenzentrum fest geschaltete Verbindungen, d.h. Standleitungen, verwendet, so treten im allgemeinen keine Identifikationsprobleme auf. Bei der Verwendung von Wählleitungen empfiehlt sich der Einsatz automatischer Wähleinrichtungen vom Rechenzentrum zum Anwender bzw. der automatisierte Rückruf.

Wichtig ist auch, daß nach dem Zustandekommen der physischen Verbindung eine logische Identifizierung des Teilnehmers erfolgt. Dies kann z.B. durch den Einsatz von Passworten geschehen, die den Anwender gleichzeitig auf erlaubte Aktivitäten beschränken. Das Problem der mißbräuchlichen Benutzung eines eingeschalteten Datenendgerätes ist am günstigsten organisatorisch zu lösen, indem man von gemeinsamen Terminalräumen möglichst absieht und die Geräte direkt zu den befugten Sachbearbeitern

stellt. Auch sollte jeder Benutzer darauf hingewiesen werden, daß er auch bei kurzfristigem Verlassen seines Arbeitsplatzes das Gerät bei dem System "abmeldet".

Allgemein gesagt sollten alle Möglichkeiten der durch die Hersteller gelieferten Betriebssysteme zum Schutz von Programmen und Daten ausgenutzt werden. Bei Großrechenzentren empfiehlt sich darüber hinaus der Einsatz besonderer Datenschutzprogramme, die in der Lage sind, nicht nur Zugriffe auf ihre Zulässigkeit hin zu prüfen, sondern auch unberechtigte Zugriffe zu protokollieren.

- Zugriffskontrolle

Die im vorigen Abschnitt für die Benutzerkontrolle geschilderten Maßnahmen gelten auch für die Zugriffskontrolle. Zu regeln ist der Zugang zu sensitiven Programmen und kritischen Systemfunktionen.

- Übermittlungskontrolle

Innerhalb eines Rechnernetzes vorgesehene Verkehrsbeziehungen sind schon bei der Einrichtung festzuhalten und nachweisbar zu gestalten.

- Transportkontrolle

Verfahren der Datenübertragung müssen ausreichend gesichert werden. Dies geschieht am besten durch Einsatz höherer Datenübertragungsprozeduren (z.B. HDLC), die weitentwickelte Transportsicherungen enthalten und einen automatischen Wiederanlauf bei Fehlern ermöglichen. Außerdem können Transportprotokolle gewonnen werden, die festhalten, welche Datenstationen eine Meldung erhalten haben. Bei der Übertragung besonders sensitiver Daten ist von Fall zu Fall zu untersuchen, ob Verschlüsselungsverfahren zu verwenden sind.

- Organisationskontrolle

Den höchsten Schutzeffekt zu erreichen setzt voraus, daß alle Maßnahmen aufeinander abgestimmt werden. So verhilft die sorgfältige Abgrenzung von Berechtigungen der mit dem System arbeitenden Mitarbeiter zur größeren Wirksamkeit eingeplanter Datenschutzmaßnahmen. Beispiele dafür sind die Restriktion privilegierter Befehle für Maschinenbediener und Systemverwaltung sowie das "Vier-Augen-Prinzip".

Datenfernverarbeitung in Hessen

Stand: 1979/80

Verfahren	Stapelübertragung Ein-gabe	Rück-gabe	DFV Dia-log	RJE	ST.	LK	KF	KA	GE	R
Einwohnerwesen										
-Erfassung			x				x	x	x	
-Abfrage			x							
Komm. Finanzwesen										(LKA)
-Erfassung	x	x	(x)			x	x	x	x	
-Abfrage	x	x	x			x	x	x	x	
Personalwesen	x		(x)		x	x	x	x	x	
Personal-inform.Syst.			(x)		x					
Krankenhauswes.	x	x	(x)		x	x	x	x		Uni-RZ
Sozialwesen	x		(x)			x	x	x		
Anwendungen in Schulen	(x)			(x)		x	x			
Schulinformationssystem			x		x					
Bibliothekswesen	x	x	(x)		x	x	x	x	x	
Wirtschaftl. Unternehmen	x	x	(x)				x	x	x	
Ordnungswidrigkeiten	x				x	x	x			KBA/VZR
Kfz.-Zulassung			(x)			x	x			(LKA)KBA
Vermessungswesen	(x)	(x)		(x)	x	x	x			
Straßenwesen			x	x	x		x			
Baustatik			(x)	(x)	x		x			
Hochbau			(x)	(x)	x		x			
Dokumentationssysteme (Landtag, HIBS, HDSB)			x		x					
Gemeindeplanungsdatei	(x)	(x)		(x)		x	x	x	x	
Wahlen und Abstimmungen	x		x		x	x	x	x	x	
Staatl. Finanzw.										
-Erfassung	x	(x)			x					
-Abfrage			x		x					
Forstwirtschaft				(x)	x					
Umweltüberwachung	(x)	(x)	(x)	(x)	x					
Statistik (StaLa)				x	x					

Erläuterungen:

Anwenderkreis: ST.=staatl. Verwaltung, LK-Landkreis, KF-kreisfr. Stadt, KA-kreisang. Stadt, GE=Gemeinde

Rechnerverbund: R /LKA=Landeskriminalamt (HEPOLIS), Uni-RZ=Universitätsrechenzentrum, KBA=Kraftfahrtbundesamt, VZR=Verkehrszentralregister

Stand der Maßn.: (x)=geplant, in Vorbereitung, x=in Betrieb (auch als Pilotprojekt)

(nach Unterlagen des UA-Datenfernv. u.a.

2.2 Schutz von Patientendaten im Krankenhaus und in der medizinischen Forschung

2.2.1 Neuregelung des Datenschutzes im Hessischen Krankenhausgesetz (HKG)

2.2.1.1 Derzeitige Rechtslage und Notwendigkeit der Novellierung des § 14 HKG

Der Datenschutz für Patientendaten im Krankenhausbereich ist derzeit nur unbefriedigend geregelt. Einerseits bestehen zahlreiche Vorschriften nebeneinander. Zu erwähnen sind hier § 14 des Hessischen Krankenhausgesetzes (HKG), das BDSG, das HDSG, die Datenschutzregelungen des Sozialgesetzbuchs (SGB) sowie die Vorschriften über die ärztliche Schweigepflicht. Die Feststellung, welche Regelungen im Einzelfall anzuwenden sind, bereitet in der Praxis erhebliche Schwierigkeiten.

Zum anderen ist der Inhalt dieser Vorschriften vielfach unklar. Selbst wenn es gelingt, das jeweils anzuwendende Recht zu ermitteln, führen Generalklauseln und unbestimmte Rechtsbegriffe zu Rechtsunsicherheit.

Zur Datenschutzbestimmung des § 14 HKG ist folgendes zu bemerken: Zum Zeitpunkt der Entstehung des Hessischen Krankenhausgesetzes ging der Gesetzgeber davon aus, daß mit der Einführung von Verbundsystemen in der medizinischen Datenverarbeitung in absehbarer Zeit zu rechnen sei. Hieraus erklärt sich die in § 13 HKG enthaltene Ermächtigung, Aufgaben aus dem Bereich der Krankenhausversorgung in ein Verbundsystem einzubeziehen.

Entsprechend knüpft die Datenschutzvorschrift in § 14, die nach § 8 HKG nur für in den Krankenhausbedarfsplan aufgenommene Krankenhäuser gilt, am Begriff "Datenverbundsystem" an. Da entgegen den früheren Erwartungen ein solcher Datenverbund in Hessen nicht geschaffen wurde und zumindest mittelfristig allenfalls in Ansätzen zu erwarten ist, läuft die Vorschrift praktisch leer. Jedenfalls gilt dies hinsichtlich der in § 14 Abs. 1 HKG vorgeschriebenen Bekanntgabe und wohl auch bezüglich des ebenfalls dort geregelten Auskunftsrechts, das nach seinem systematischen Standort ein Datenverbundsystem voraussetzt.

Darüber hinaus ist die Regelung des § 14 HKG lückenhaft. So fehlt etwa eine Vorschrift über die Zulässigkeit der Speicherung. Weiterhin ist Abs. 2 nicht den inzwischen geltenden Vorschriften des BDSG und des HDSG angepaßt. So wird eine Verschlüsselung der Daten verlangt. Die in diesem Zusammenhang naheliegende Anonymisierung ist nicht vorgeschrieben.

§ 14 hat somit derzeit wenig praktische Relevanz. Es kann kein Zweifel bestehen, daß die Vorschrift novellierungsbedürftig ist. Bei der erforderlichen Neufassung gilt es eine Vielzahl von rechtlichen Aspekten einzubeziehen, etwa

- die Problematik der Einbeziehung von Krankenhäusern in kirchlicher Trägerschaft
- die Abstimmung mit Terminologie und Grundsätzen der Datenschutzgesetze
- die einschlägigen Regelungen des ärztlichen Standesrechts usw.

Diese Gesichtspunkte wurden eingehend geprüft; sie sind in dem folgenden Regelungsvorschlag berücksichtigt.

2.2.1.2 Einzelheiten einer bereichsspezifischen Regelung

Eine bereichsspezifische Regelung sollte für eine möglichst große Zahl von Krankenhäusern anwendbar sein. Sie sollte also sowohl für öffentlich-rechtliche als auch für private und frei-gemeinnützige Krankenhäuser gelten. Am sinnvollsten erscheint daher eine Regelung im Hessischen Krankenhausgesetz.

Der nachstehend wiedergegebene Vorschlag einer bereichsspezifischen Regelung für den Datenschutz im Krankenhausbereich ist so konzipiert, daß er als neugefaßter § 14 in das HKG übernommen werden könnte. Im folgenden wird dann auf die einzelnen Absätze des Novellierungsvorschlags Bezug genommen.

I. 1) Alle Patientendaten im Bereich von Krankenhäusern unterliegen unabhängig von ihrer Verarbeitung in einer Datei dem Datenschutz.

2) Soweit dieses Gesetz nichts Abweichendes vorschreibt, gelten das Bundesdatenschutzgesetz und das Hessische Datenschutzgesetz entsprechend.

3) §§ 1 Abs. 2 Satz 2 BDSG und HDSG finden keine Anwendung.

II. 1) Die Erhebung und Speicherung ist zulässig

1. im Rahmen der Zweckbestimmung eines Vertragsverhältnisses oder vertragsähnlichen Vertrauensverhältnisses.
2. soweit eine andere Rechtsvorschrift sie erlaubt oder
3. soweit der Betroffene eingewilligt hat.

2) Für die Form der Einwilligung gelten §§ 3 Satz 2 BDSG, 7 Satz 2 HDSG entsprechend.

3) Der Betroffene ist schriftlich über Art und Zweck der Erhebung oder Speicherung aufzuklären.

4) Dem Betroffenen dürfen aus der Verweigerung der Einwilligung keine Rechtsnachteile entstehen.

III. 1) Die im Krankenhaus Beschäftigten dürfen Patientendaten nur für den zur jeweiligen rechtmäßigen Aufgabenerfüllung gehörenden Zweck einsehen, verarbeiten oder sonst nutzen.

2) Insbesondere ist sicherzustellen, daß die Einsichtnahme oder Nutzung durch die Krankenhausverwaltung nur erfolgt, soweit dies zur verwaltungsmäßigen Abwicklung der Behandlung erforderlich ist.

3) Die Ausführung der in Satz 1 und 2 genannten Anforderungen ist durch geeignete technische und organisatorische Maßnahmen zu gewährleisten.

IV. 1) Die Übermittlung ist nur mit Einwilligung des Betroffenen zulässig, es sei denn, daß sie gesetzlich zugelassen ist.

2) II Satz 2 bis 4 gelten entsprechend.

3) Nach Satz 1 übermittelte Daten dürfen nur unter den dort genannten Voraussetzungen weiter übermittelt werden.

V. 1) Der Patient hat ein Recht auf schriftliche Auskunft über die ihn betreffenden Daten sowie über die Personen und Stellen, an die solche Daten übermittelt werden.

2) Über medizinische Daten darf Auskunft nur vom behandelnden Arzt erteilt werden.

3) Die Auskunft kann eingeschränkt werden, soweit dies zum Schutz der Gesundheit des Betroffenen zwingend geboten ist.

VI. 1) Patientendaten können für bestimmte Forschungsvorhaben im Rahmen unabhängiger wissenschaftlicher Forschung verarbeitet oder sonst genutzt werden, wenn besondere Rechtsvorschriften dies zulassen oder der Betroffene eingewilligt hat.

2) II Satz 2 bis 4 gelten entsprechend.

3) Läßt das Forschungsvorhaben die Einholung der Einwilligung nicht zu oder kann die Einwilligung aus anderen zwingenden Gründen nicht eingeholt werden, und ist die Nutzung der Daten zu wissenschaftlichen Zwecken unerläßlich, so ist sie für Forschungsvorhaben gemäß Satz 1 zulässig, wenn schutzwürdige Belange des Betroffenen, insbesondere durch die Art der Nutzung der Daten, nicht beeinträchtigt werden.

4) Eine Übermittlung nach Satz 3 ist von öffentlich-rechtlichen Krankenhäusern dem Hessischen Datenschutzbeauftragten, von privatrechtlichen Krankenhäusern der Aufsichtsbehörde gemäß § 30 BDSG zu melden; für den Inhalt der Meldung gilt § 75 Abs. 2 Satz 3 SGB X entsprechend.

5) Satz 3 gilt nicht für die Übermittlung an zentrale Register.

6) Satz 1 bis 3 gelten nicht, wenn der Forschungszweck auf andere Weise, insbesondere durch die Verwendung nicht personenbezogener Daten, erreichbar ist.

7) Nach Satz 1 bis 3 übermittelte Daten dürfen nur mit Einwilligung des Betroffenen weiter übermittelt werden.

VII. 1) Jedes Krankenhaus hat einen Datenschutzbeauftragten schriftlich zu bestellen.

2) §§ 28 Abs. 2 bis 4, 29 BDSG gelten entsprechend.

- Anwendungsbereich

Die vorgeschlagene Regelung gilt für alle Patientendaten im Bereich der ihr unterliegenden Krankenhäuser (I.1). Dabei spielt es keine Rolle, ob die Daten in Dateien gespeichert sind. Insoweit gilt das gleiche wie für vergleichbare bereichsspezifische Regelungen (z.B. die Vorschriften des SGB über das Sozialgeheimnis).

Die Beschränkung der Datenschutzgesetze auf Dateien führt gerade im Krankenhausbereich zu erheblichen Abgrenzungsschwierigkeiten. So ist etwa bei den vielfach in Form von Hängemappen geführten Archiven mit Patientenunterlagen je nach dem Grad der Formalisierung oft außerordentlich schwer zu entscheiden, ob es sich um eine Datei oder eine Akte handelt.

Von den Abgrenzungsproblemen abgesehen, führt die Beschränkung auf die in Dateien gespeicherten Daten auch zu nicht sachgerechten Ergebnissen. Dieser aus anderen Bereichen bekannte Sachverhalt ist gerade im Krankenhausbereich untragbar, da hier äußerst sensitive personenbezogene Daten verarbeitet werden.

Weiterhin gilt die Regelung nach I.3 auch für solche Daten, die **nicht** zur Übermittlung an Dritte bestimmt sind ("interne Daten"). Dadurch werden nicht nur die Abgrenzungsschwierigkeiten bei der Auslegung der entsprechenden Ausnahmeklauseln in § 1 Abs. 2 Satz 2 BDSG und HDSG vermieden. Entscheidend ist, daß ein Schutzbedürfnis des Patienten auch dort besteht, wo Daten nicht an Dritte weitergegeben werden. So ist etwa nicht einzusehen, warum der Patient insoweit keinen Auskunftsanspruch hinsichtlich der ihn betreffenden Daten haben sollte. Ähnlich wie nach dem im Arbeitsrecht geltenden "materiellen Aktenbegriff" müssen die Schutznormen zugunsten der Betroffenen für alle sie betreffenden Daten gelten, unabhängig davon, in welchem Kontext sie geführt werden.

Auf die Art der Daten kann es nicht ankommen. Entsprechend der Systematik des Datenschutzgesetzes sind alle personenbezogenen Daten ohne Rücksicht auf ihre Sensitivität einzubeziehen, unabhängig davon, ob sie zu Zwecken der ärztlichen Behandlung oder aus administrativen Gründen erhoben werden.

Die vorgeschlagene Novellierung bedient sich der in den Datenschutzgesetzen verwendeten Begriffe. Da darüber hinaus schon aus Gründen des Umfangs der Vorschriften eine abschließende Regelung nicht möglich ist, gelten das HDSG und das BDSG entsprechend, soweit nichts Abweichendes vorgeschrieben ist (I.2).

- Erhebung und Speicherung (II.)

- - Einbeziehung der Erhebung

Regelungsbedürftig ist nicht nur die Speicherung von Daten. Vielmehr ist im Interesse der Vermeidung von Lücken im Datenschutz die der Speicherung zeitlich vorgeschaltete Phase der Erhebung, d.h. des Beschaffens von Daten, einzubeziehen. Dies liegt zwar bereits in der Konsequenz des Verzichts auf den Dateibegriff, sollte aber dennoch klargestellt werden, zumal die Datenschutzgesetze die Erhebungsphase grundsätzlich nicht einbeziehen (vgl. aber §§ 9 Abs. 2 BDSG, 11 Abs. 2 HDSG).

- - Speicherung im Rahmen der Zweckbestimmung eines Vertragsverhältnisses

In der Praxis entstehen Unklarheiten dadurch, daß der hier in der Regel anzuwendende § 23 BDSG die Speicherung zuläßt, "soweit es zur Wahrung berechtigter Interessen der speichernden Stelle erforderlich ist und kein Grund zur Annahme besteht, daß dadurch schutzwürdige Belange des Betroffenen beeinträchtigt werden". Durch die Vermeidung dieser unbestimmten Rechtsbegriffe werden die bisherigen Auslegungsschwierigkeiten nicht unerheblich reduziert. Daten, deren Erhebung nicht vom Vertragszweck erfaßt wird, können dann nur noch auf Grund der Einwilligung des Betroffenen verarbeitet werden.

Es ist zwar nicht zu erkennen, daß auch die Grenzen der Zweckbestimmung des Vertragsverhältnisses oft schwer zu bestimmen sind. Eine präzisere Regelung erscheint jedoch nicht möglich. Insbesondere können die Daten, die für die ärztliche Behandlung erforderlich sind, nicht näher umschrieben werden. Bei bestimmten (z.B. psychischen) Erkrankungen können Daten von Bedeutung sein, die bis weit ins soziale Umfeld hineinreichen. Jede Form eines Datenkatalogs - und sei es in der Form eines Negativkatalogs - verbietet sich hier. Eher möglich wäre eine solche Lösung für diejenigen Daten, die für die Klinikverwaltung benötigt werden. Doch auch hier scheinen präzisere Regelungen wegen der Vielgestaltigkeit der einzelnen rechtlichen Beziehungen nicht praktikabel.

In diesem Zusammenhang ist darauf hinzuweisen, daß die Anknüpfung am Vertragszweck deswegen problematisch sein könnte, weil vor allem bei Kassenpatienten die Rechtsnatur ihrer Beziehungen mit dem Krankenhaus dogmatisch unklar ist. Die wohl herrschende Ansicht geht von einem Vertrag zugunsten Dritter zwischen Leistungsträger und Krankenhaus aus. Unabhängig davon kommt jedoch in der Praxis zwischen Krankenhaus und Patient ein Vertrag zustande, der meist als "Krankenhausaufnahmevertrag" bezeichnet wird. Dabei werden häufig Formulare verwendet, die gleichzeitig der Datenerhebung für administrative Zwecke dienen (u.a. Grunddaten des Betroffenen, Angaben über Kostenträger, einweisenden Arzt). Der strittigen Frage, inwieweit ein öffentlich-rechtliches oder privatrechtliches Benutzungsverhältnis vorliegt, braucht in diesem Zusammenhang nicht weiter nachgegangen zu werden, da jedenfalls vertragliche Beziehungen bestehen, an die für die Zulässigkeit der Speicherung angeknüpft werden kann.

- - Speicherung aufgrund anderer Rechtsvorschriften

Entsprechend der Systematik der Datenschutzgesetze ist die Speicherung auch aufgrund anderer Rechtsvorschriften zulässig. Hier kommt z.B. bei Zwangseinweisungen das Hessische Freiheitsentziehungsgesetz in Betracht.

- Einwilligung

Die Speicherung ist außerdem zulässig, soweit der Betroffene in sie eingewilligt hat. Zwar ist gerade bei Patientendaten die Einwilligung als Zulässigkeitsvoraussetzung problematisch. Der Betroffene befindet sich oft in einer psychischen Zwangslage, wenn er in ein Krankenhaus eingeliefert wird. Es erscheint hier noch fraglicher als in anderen sozialen Bereichen, von einer Freiwilligkeit der Einwilligung auszugehen.

Dennoch ist die Einwilligung als Zulässigkeitsvoraussetzung für die Speicherung insoweit nicht gänzlich verzichtbar, als eine Reihe von Fällen weder durch den Vertragszweck noch durch spezielle Rechtsvorschriften abgedeckt sind. Dies gilt z.B. bei Datenerhebungen für Forschungsvorhaben oder für Dienstleistungen, die vom Krankenhaus außerhalb der eigentlichen Behandlung angeboten werden (z.B. Beratung durch Sozialarbeiter).

Entsprechend dem Grundsatz des "informed consent" sieht II.3 eine Aufklärungspflicht hinsichtlich Art und Zweck der Erhebung bzw. Speicherung vor. Im gleichen Sinne werden zwar überwiegend die geltenden Vorschriften über die Einwilligung im HDSG und BDSG interpretiert. Angesichts der erheblichen Diskrepanz zur Praxis und wegen der großen Bedeutung der Einwilligung empfiehlt sich jedoch eine Klarstellung.

Vorschläge, der Zwangssituation des Patienten bei Einlieferung ins Krankenhaus dadurch Rechnung zu tragen, daß die Einwilligung zu einem späteren Zeitpunkt nachgeholt wird, erscheinen jedenfalls als generelle Lösung nicht praktikabel. In den Fällen der Ausnutzung einer Zwangssituation sollte geprüft werden, ob ein Widerruf oder eine Anfechtung der Einwilligung in Betracht kommt.

Verweigert der Patient trotz der erwähnten schwierigen Situation die Einwilligung, so stellt II.4 entsprechend der Regelung in § 11 Abs. 2 Satz 2 HDSG klar, daß ihm daraus keine Nachteile entstehen dürfen. Dies gilt z.B., wenn der Patient die Mitteilung von Daten verweigert, die nicht für seine Behandlung erforderlich sind, sondern allein Forschungszwecken dienen. Im übrigen hat der Patient ohnehin nach Maßgabe des HKG einen Anspruch auf ärztliche und pflegerische Versorgung.

Hinsichtlich der Form der Einwilligung wird in II.2 auf die Regelungen im BDSG und HDSG verwiesen, um Mißverständnisse auszuschalten.

Um die Regelung nicht zu sehr mit Einzelheiten zu überfrachten, wurde auf besondere Vorschriften für den Fall verzichtet, daß der Patient nicht zu Willensäußerungen in der Lage ist.

- Interne Zulässigkeitsschranken (III.)

Adressat der Regelung des Entwurfs ist das einzelne Krankenhaus. Hier besteht ein struktureller Unterschied gegenüber den Regelungen der Datenschutzgesetze, die jedenfalls für den öffentlichen Bereich eine funktionelle Auslegung des Begriffs "speichernde Stelle" zulassen, so daß Adressat der Regelungen die Fachabteilung ist. Dies gilt allerdings nicht für private Krankenhäuser, da hier nach § 22 BDSG der Rechtsträger, d.h. das Krankenhaus insgesamt, speichernde Stelle ist.

Eine bereichsspezifische Regelung kann die interne Datenverarbeitung nicht ungeregelt lassen. Hier ist zu beachten, daß die ärztliche Schweigepflicht auch gegenüber Ärzten und sonstigen Beschäftigten gilt. Daraus folgt, daß das Krankenhaus keine Informationseinheit sein kann.

Zwei Möglichkeiten bieten sich hier an. Zum einen können eigene Schranken für die Datenverarbeitung innerhalb des Krankenhauses festgelegt werden. Andererseits können die Vorschriften über die Übermittlung für anwendbar erklärt werden für Fälle der Datenweitergabe zwischen Fachabteilungen. Auf die letztere Möglichkeit wird in dem Entwurf verzichtet. Vielmehr wird für die Übermittlung eine sehr restriktive Regelung getroffen (IV.). Sie dürfte sich aus Praktikabilitätsgründen nicht auf die Kommunikation zwischen Fachabteilungen eines Krankenhauses übertragen lassen, da das Erfordernis einer Einwilligung für jeden Einzelfall zu weit gehen dürfte.

III.1 sieht eine an den Funktionen orientierte interne Bearbeitungsregelung vor. Die eingangs erwähnten Regelungen der ärztlichen Schweigepflicht können hier zur Interpretation herangezogen werden.

Besonders wichtig ist die Funktionentrennung zwischen Krankenhausverwaltung und ärztlichem Bereich. Freilich läßt sich eine Abschottung nicht in der Weise vornehmen, daß die Verwaltung keinen Zugang zu medizinischen Daten hat. Da die Verwaltung die Abrechnung mit den Kostenträgern durchführt, ist eine Kenntnisnahme der hierfür erforderlichen Daten unumgänglich. Bei stationären Kassenpatienten ist die Abrechnungsweise insofern datenschutzfreundlich, als allein nach Tagessätzen abgerechnet wird, d.h. die Kasse braucht nur zu wissen, wie lange der Patient in Behandlung war. Allerdings werden aufgrund von Rahmenverträgen zwischen den Landesverbänden der Krankenhäuser (§ 372 RVO) auch die Entlassungsdiagnosen mitgeteilt. Bei ambulanten Kassenpatienten - also in der Mehrzahl der Fälle - wird nach den jeweils gewährten Leistungen abgerechnet. Aus der Art der Leistungen sind Rückschlüsse auf die Krankheit möglich.

Die Wahrung der internen Zulässigkeitsbeschränkungen ist durch Datensicherungsmaßnahmen zu gewährleisten. Werden Daten automatisiert verarbeitet, so sind abgestufte Zugriffsregelungen erforderlich. Ein Beispiel bilden die Zugriffskategorien im Rahmen des Informationssystems mehrerer Krankenhäuser in der Region Groß-Stockholm (vgl. im einzelnen den Sechsten Tätigkeitsbericht, 3.2.4.2).

- Übermittlung
  Übermittelt werden Daten u.a. an
- Krankenkassen für Abrechnungszwecke. Eine ausdrückliche gesetzliche Grundlage fehlt bisher (vgl. aber den Gesetzentwurf für das 3. Kapitel des SGB X, § 106, Bundesratsdrucksache 526/80). Mitgeteilt werden die Einweisungsdiagnose (für die Kostendeckungszusage), bei stationären Patienten die Entlassungsdiagnose, bei ambulanten Patienten die gewährten Leistungen (s.o. 2.3).
- Unfallversicherungsträger. Diesem muß der Arzt nach § 1543 d RVO Auskunft erteilen.
- Privatversicherer. Hier darf der Arzt nur Auskunft geben, soweit er von der Schweigepflicht entbunden ist.
- Arbeitgeber. Hier darf nur das Ergebnis der Untersuchung nach Maßgabe des Erforderlichkeitsgrundsatzes bzw. spezialgesetzlichen Bestimmungen mitgeteilt werden.
- Gesundheitsamt. Besondere Meldepflichten greifen in einer Reihe von Fällen ein. Entsprechende gesetzliche Regelungen sind in §§ 4 Bundesseuchengesetz, 12 Geschlechtskrankheitengesetz enthalten.
- Gerichte. Der als Zeuge vor Gericht geladene Arzt hat gemäß §§ 383 ZPO, 53 Abs. 1 Nr. 3 StPO ein Zeugnisverweigerungsrecht. Eine Verpflichtung zur Aussage besteht nur, soweit er von dem Patienten von der Schweigepflicht entbunden ist.
- Strafverfolgungsbehörden. Hinsichtlich der in § 138 StGB genannten Verbrechen ist auch der Arzt anzeigepflichtig.
- Finanzamt. Von der grundsätzlich auch Dritte treffenden Auskunftspflicht steuererheblicher Sachverhalte (§ 93 AO) sind die Ärzte durch § 102 Nr. 3 a AO ausgenommen.
- Verkehrsbehörden. Ein Arzt ist nach § 34 StGB berechtigt (nicht verpflichtet), die Verkehrsbehörde zu benachrichtigen, wenn ein Patient trotz abmahnenden Zuredens ein Kraftfahrzeug führt, obwohl er krankheitsbedingt dazu nicht in der Lage ist.
- Erziehungsberechtigte. Nach § 46 Jugendarbeitsschutzgesetz hat der Arzt den Eltern oder dem Vormund des Jugendlichen das wesentliche Ergebnis der Untersuchung schriftlich mitzuteilen.

Die Bestandsaufnahme zeigt, daß die ärztliche Schweigepflicht heute vielfach durchlöchert ist. Umso wichtiger ist es, klare Regelungen zu treffen, die der Bedeutung der Vertrauensbeziehungen zwischen Arzt und Patient gerecht werden. Sollen die Unsicherheiten, die durch die unpräzisen Regelungen in den Übermittlungsvorschriften der Datenschutzgesetze stehen, vermieden werden, so muß auf unbestimmte Rechtsbegriffe verzichtet werden.

Dies kann nur dadurch erreicht werden, daß die Übermittlung auf die Fälle beschränkt wird, in denen sie spezialgesetzlich zugelassen wird oder der Betroffene seine Einwilligung erteilt. Eine entsprechende Regelung ist in § 6 Abs. 2 des rheinland-pfälzischen Datenschutzgesetzes enthalten.

Zwar bestehen gegen die Einwilligung als Zulässigkeitsvoraussetzung die bereits im Zusammenhang mit der Speicherung dargestellten Vorbehalte. Immerhin kann auch die faktische Zwangssituation, in der sich der Patient befindet, durch die Anwendung des Benachteiligungsverbots in II.4 gemildert werden. Geht man davon aus, daß unbestimmte Rechtsbegriffe vermieden werden sollen, so dürfte es gegenüber der Einwilligung keine Alternative geben.

Was die Übermittlung an andere Ärzte betrifft, so ist IV. restriktiver als die geltenden Regelungen über die ärztliche Schweigepflicht. Danach ist die Einwilligung zwar grundsätzlich dann erforderlich, wenn Daten an Ärzte weitergegeben werden sollen, die der Patient nicht konsultiert hat. Dagegen ist sie entbehrlich, wenn mehrere Ärzte gleichzeitig oder nacheinander denselben Patienten untersuchen oder behandeln. In diesem Fall sind sie "untereinander von der Schweigepflicht soweit befreit, als der Patient nicht etwas anderes bestimmt" (Teil I, § 2 Abs. 6 der Berufsordnung für die Ärzte in Hessen). Diese Regelung ist insofern problematisch, als damit die Übermittlung grundsätzlich zulässig ist. Dies mag allenfalls angehen, wenn ein Arzt den Patienten an einen anderen Arzt überweist und der Patient anschließend diesen aufsucht. Grundsätzlich ist es jedoch vorzuziehen, wenn die Last des Tätigwerdens nicht beim Patienten besteht. Sollte es zunehmend zur Speicherung von Patientendaten in zentralen Informationssystemen kommen, so erscheint eine Einwilligungslösung ohnehin unabdingbar. Insoweit ist die gesetzgeberische Zielsetzung bei § 14 Abs. 2 KHG zutreffend.

IV.3 stellt klar, daß der Empfänger übermittelter Daten diese nur unter den in IV.1 genannten Voraussetzungen weiter übermitteln darf. Diese Regelung ist mit § 76 Abs. 1 SGB X abgestimmt, der für den Fall der Übermittlung an Sozialleistungsträger die gleichen Einschränkungen vorsieht.

- Auskunft an den Betroffenen

- - Voraussetzungen und Umfang des Auskunftsanspruchs

In Rechtsprechung und Literatur wird das Auskunftsrecht des Patienten hinsichtlich der seine Person betreffenden Daten auch unabhängig von den Anwendungsvoraussetzungen der Datenschutzgesetze zunehmend anerkannt. Neben vertraglichen Anspruchsgrundlagen kommt hier § 810 BGB in Betracht. Hintergrund dieser Entwicklung ist zum einen die zunehmende Anerkennung der Bedeutung des Selbstbestimmungsrechts des Patienten. Die daraus abgeleitete Aufklärungspflicht ist von der Rechtsprechung stark ausgeweitet worden. Eine umfassende Information des Patienten, die ihm sinnvolle Entscheidungen erst ermöglicht, bedeutet freilich nicht nur die mündliche Mitteilung von Behandlungsrisiken. Nicht weniger wichtig kann die genaue Erkenntnis gespeicherter Daten (z.B. Laborwerte) sein. Zwar ist einzuräumen, daß die meisten Patienten ärztliche Unterlagen kaum verstehen. Sie werden jedoch in die Lage versetzt, sich vom behandelnden oder auch einem anderen Arzt präzise aufklären zu lassen.

Die Bedeutung gerade einer **schriftlichen** Auskunft zeigt sich, wenn die ärztliche Behandlung fehlgeschlagen ist. Im Kunftfehlerprozeß ist es für den Patienten unumgänglich, daß er für seine Beweisführung die ärztlichen Unterlagen zur Verfügung hat. Inzwischen ist im übrigen von der Rechtsprechung anerkannt worden, daß die Verpflichtung des Arztes "über die in Ausübung seines Berufes gemachten Feststellungen und getroffenen Maßnahmen hinreichende Aufzeichnungen zu fertigen" (§ 11 der Berufsordnung für die deutschen Ärzte von 1976) jedenfalls auch im Interesse des einzelnen Patienten besteht (vgl. BGH NJW 1978, 2377).

Trotz der aufgezeigten Tendenzen dürfte sich der Auskunftsanspruch des Patienten in der Praxis noch nicht voll durchgesetzt haben. Deshalb und wegen der unklaren Fassung der Auskunftsregelung in den Datenschutzgesetzen ist eine bereichsspezifische Regelung dringend geboten.

V. erstreckt den Auskunftsanspruch generell auf die Empfänger übermittelter Daten und geht damit über § 26 BDSG hinaus, der dies nur im Fall regelmäßiger Übermittlungen im Rahmen automatisierter Verfahren vorsieht. Diese verbesserte Transparenz erscheint gerade bei medizinischen Daten im Hinblick auf deren besondere Sensitivität und den potentiellen Schaden für den Betroffenen geboten. Eine Konzeption, nach der die Übermittlung medizinischer Daten im Hinblick auf die Vertrauensbeziehungen zwischen Arzt und Patient die Ausnahme bilden soll, erfordert eine präzise Information des Patienten über diese Ausnahmen. Anderenfalls kann der Eindruck einer unregulierten Datenproliferation entstehen.

Was die Form der Auskunftserteilung angeht, so sieht V. im Hinblick auf die erforderliche präzise Information sowie die Beweissicherungsfunktion der Auskunft deren Schriftlichkeit vor. Auf unklar gefaßte Ausnahmetatbestände wie in § 26 Abs. 2 Satz 2 BDSG ("besondere Umstände") wird verzichtet. Daß der Patient sich mit einer mündlichen Auskunft begnügen **kann**, erscheint selbstverständlich und bedarf keiner ausdrücklichen Regelung im Gesetz.

- - Erteilung der Auskunft durch den behandelnden Arzt (V.2)

Die Auskunft über administrative Daten kann von der Krankenhausverwaltung erteilt werden. Dagegen dürfen medizinische Daten - auch soweit sie bei der Verwaltung gespeichert sind -, nur vom behandelnden Arzt mitgeteilt werden. Dies ist schon deshalb erforderlich, weil nur der Arzt beurteilen kann, ob eine Ausnahme nach V.3 Satz 3 vorliegt (vgl. auch § 25 Abs. 2 SGB X). Darüber hinaus kann allein er im Einzelfall erforderliche Erläuterungen geben.

- - Ausnahmeregelung

In den Datenschutzgesetzen ist nicht klar geregelt, ob die Auskunft im Einzelfall verweigert bzw. eingeschränkt werden kann. Hinsichtlich des § 26 BDSG wurde in der Literatur teilweise darauf verwiesen, daß der Gesetzgeber bewußt davon absah, eine spezielle Regelung einzufügen, die die Ärzte zur Auskunftsverweigerung berechtigt hätte (vgl. die Nachweise bei Mallmann in Simitis/Dammann/Mallmann/Reh, BDSG § 26 Rdnr. 68). Dennoch wird ganz überwiegend anerkannt, daß der Patient dann nicht über seinen Gesundheitszustand informiert werden muß, wenn diese Unterrichtung schwerwiegende gesundheitliche Schäden verursachen könnte; die Begründung ist allerdings umstritten.

Eine bereichsspezifische Regelung sollte zwar mithin grundsätzlich einen uneingeschränkten Auskunftsanspruch vorsehen. Die Tendenz in der modernen Medizin geht dahin, Patienten auch bei lebensbedrohenden Krankheiten aufzuklären. Dennoch bleiben Einzelfälle, in denen dies im Hinblick auf die psychische Konstellation des Betroffenen - z.B. Suizidneigungen - nicht möglich ist (vgl. auch den Siebenten Tätigkeitsbericht, 8.3). Von den gleichen Anforderungen geht im übrigen auch die Rechtsprechung des BGH zur ärztlichen Aufklärungspflicht aus, die nur unter sehr engen Voraussetzungen eine Ausnahme zuläßt (BGH NJW 1959, 814). Sollten Ärzte die Ausnahmeklausel allzu extensiv auslegen oder gar zur Verdeckung von Behandlungsfehlern mißbrauchen, so bleibt dem Betroffenen der Weg zu Datenschutz-Kontrollbehörden und Gerichten.

- Nutzung von Daten für Forschungszwecke (VI.)
Das Problem "Datenschutz und Forschung" wird vor allem im medizinischen Bereich intensiv diskutiert. Vorwürfe, der Datenschutz behindere die medizinische Forschung, sind zwar einseitig. Es geht hier nicht allein um die im Grundgesetz garantierte Wissenschaftsfreiheit. Dem Persönlichkeitsrecht des Patienten kommt kein geringerer Stellenwert zu.

Unzweifelhaft ist jedoch, daß die derzeitige Rechtslage gerade hinsichtlich der Verwendung personenbezogener Daten für Forschungszwecke in zahlreichen Punkten unklar ist. Vielfach entsteht gerade zu Unrecht der Eindruck, Datenschutz behindere die Forschung.

Besonders wichtig erscheint es somit, eine eindeutige Regelung zu treffen. Dies auch deswegen, weil § 14 HKG für die Universitätskliniken gilt. VI. läßt eine Nutzung personenbezogener Daten für Forschungszwecke grundsätzlich nur auf Grund besonderer Rechtsvorschriften oder der Einwilligung des Betroffenen zu. Im übrigen knüpft die Regelung an § 15 HDSG an. Danach kann nicht der weite Wissenschaftsbegriff des Art. 5 Abs. 3 GG gelten, da dieser keine praktikable Eingrenzung ermöglicht. Vielmehr ist die Verarbeitung nur zulässig für bestimmte Forschungsvorhaben im Rahmen unabhängiger wissenschaftlicher Forschung.

Das Erfordernis der Einwilligung ist im übrigen in den Regelungen über die ärztliche Schweigepflicht enthalten. Nach Teil I § 2 Abs. 7 der Berufsordnung der Ärzte in Hessen dürfen der Schweigepflicht unterliegende Tatsachen und Befunde nur soweit mitgeteilt werden, als dabei die Anonymität des Patienten gesichert ist oder dieser ausdrücklich zustimmt.

Freilich wird gerade diese Regelung in der Praxis oft nicht eingehalten. So ist es vielfach üblich, Patientenunterlagen an Doktoranden zu übergeben, ohne daß die Daten anonymisiert werden oder der Patient einwilligt.

Immerhin sind Fälle denkbar, in denen die Einwilligung nicht eingeholt werden kann. Dies ist z.B. in den Ausnahmefällen möglich, in denen der Arzt den Patienten zum Schutz seiner Gesundheit nicht bzw. nicht in vollem Umfang über die Art seiner Erkrankung aufklärt. Das Erfordernis einer Einwilligung könnte hier zu Rückschlüssen seitens des Patienten führen. Nach VI.3 kann deshalb unter engen Voraussetzungen von der Einwilligung abgesehen werden. Die Formulierung lehnt sich an die Regelung in § 14 Abs. 2 Satz 3 BDSG über gesperrte Daten an: Die Nutzung ist nur zulässig, wenn sie zu wissenschaftlichen Zwecken unerläßlich ist. Dies bedeutet, daß ein überwiegendes Interesse an der konkreten Nutzung zu wissenschaftlichen Zwecken bestehen muß. Es muß also eine Abwägung zwischen den Interessen des Betroffenen und denjenigen an der Nutzung der Daten vorgenommen werden. Darin liegt kein unzulässiger Eingriff in die Wissenschaftsfreiheit, da es hier (auch) um das gleichrangige Grundrecht auf Wahrung der persönlichen Integrität des Patienten geht. Im Rahmen der Abwägung ist zu prüfen, ob schutzwürdige Belange des Betroffenen, insbesondere durch die Art der Verwendung der Daten, beeinträchtigt werden. Hier kommt es vor allem auf ausreichende technische und organisatorische Maßnahmen an. Abweichend von § 15 HDSG stellt VI.3 nicht auf eine fehlende Beeinträchtigung schutzwürdiger Belange wegen der Art der Daten oder ihre Offenkundigkeit ab, da diese Fälle bei medizinischen Daten in der Regel ausscheiden.

Um einen Mißbrauch der Ausnahmeregelung in VI.3 zu verhindern, sieht VI.4 eine Meldepflicht an den Hessischen Datenschutzbeauftragten bzw. die Aufsichtsbehörde für den nicht-öffentlichen Bereich vor. Eine vergleichbare Regelung enthält § 75 SGB X für die Forschung im Sozialleistungsbereich, der allerdings insofern weitergeht, als er eine Genehmigungspflicht statuiert.

VI.5 stellt klar, daß VI.3 keine Übermittlung von Patientendaten an zentrale Register (z.B. Krebsregister) ermöglicht. Die Übermittlung von Daten an solche Register und die Speicherung durch sie ist nur auf Grund eines Spezialgesetzes zulässig, das die Modalitäten der Führung des Registers im einzelnen regelt.

Eine Nutzung von personenbezogenen Daten für Forschungszwecke kann nicht in Betracht kommen, wenn der Forschungszweck auf andere Weise, insbesondere durch Verwendung anonymisierter Daten erreichbar ist. Diese Einschränkung findet sich auch in § 75 Abs. 1 Satz 2 SGB X. Die Regelung VI.6 ist insoweit weitergehend, da unter den geannten Voraussetzungen auch die Einwilligung nicht die Verarbeitung personenbezogener Daten ermöglicht. VI.7 macht die weitere Übermittlung durch Datenempfänger von der Einwilligung des Betroffenen abhängig. Dies entspricht der Regelung in § 15 Abs. 2 HDSG.

- Bestellung eines Datenschutzbeauftragten (VII.)
Nach der derzeitigen Rechtslage sind nur die dem 3. Abschnitt des BDSG unterfallenden Krankenhäuser verpflichtet, einen Datenschutzbeauftragten zu bestellen. Für öffentlich-rechtliche Krankenhäuser erscheint ein entsprechendes Erfordernis aus den gleichen Gründen zweckmäßig.

2.2.2 Krebsregister

Auf Grund eines Beschlusses des Landtags vom 28.11.1979 prüft die Landesregierung gegenwärtig die Errichtung eines Krebsregisters in Hessen. Nach dem derzeitigen Stand der Überlegungen soll zunächst ein regional begrenztes Inzidenzregister beim Klinikum der Universität Gießen aufgebaut werden. Ziel einer solchen Einrichtung ist es vor allem, Erkenntnisse über die Zahl jährlicher Neuerkrankungen an verschiedenen Krebsformen und die Ursachen dieser Erkrankungen zu gewinnen. Zu einem späteren Zeitpunkt soll das Register zu einem kombinierten Inzidenz- und Nachsorgeregister erweitert werden.

Vorgesehen ist die namentliche Meldung an Krebs erkrankter Patienten an das Register. Eine personenbezogene Übermittlung wird auch in dem vom "Bund/Länder-Arbeitskreis Krebsregister" vorgelegten Gutachten (Bundestagsdrucksache 8/3556, Anlage I) im Hinblick auf ein exaktes "Record Linkage", individuelle Verlaufskontrolle und Eliminierung von Mehrfachmeldungen des gleichen Falles für erforderlich gehalten. In Betracht kommen für die Abgabe der Meldung pathologische Institute, Krankenhäuser und niedergelassene Ärzte, wobei an eine Meldepflicht nicht gedacht ist.

Zu den damit angeschnittenen datenschutzrechtlichen Fragen habe ich im Rahmen meiner Beratungskompetenz gegenüber dem Hessischen Sozialminister Stellung genommen und die Erforderlichkeit einer spezialgesetzlichen Regelung wie folgt begründet:

Die Zulässigkeit der Datenverarbeitung richtet sich nach den im Einzelfall anzuwendenden datenschutzrechtlichen Bestimmungen. Im Anwendungsbreich des HDSG, d.h. für öffentliche Stellen (z.B. Städtische Krankenhäuser) ist nach § 7 HDSG eine Übermittlung an das Register nur zulässig, wenn dieses Gesetz oder eine andere Rechtsvorschrift es erlaubt oder der Betroffene eingewilligt hat. Entsprechendes gilt nach § 3 BDSG für nichtöffentliche Stellen (z.B. private Krankenhäuser, niedergelassene Ärzte).

Weder die Übermittlungsvorschriften des HDSG noch diejenigen des BDSG bieten eine Grundlage für die Übermittlung von personenbezogenen Daten durch Krankenhäuser und sonstige in Frage kommende Stellen an ein Krebsregister. Was § 24 Abs. 1 BDSG angeht, so liegt die Übermittlung nicht im Rahmen der Zweckbestimmung des mit dem Patienten abgeschlossenen Vertrages bzw. eines vertragsähnlichen Vertrauensverhältnisses. Auch die dritte Alternative des § 24 Abs. 1 BDSG läßt keine Übermittlung zu. Zwar kann im Hinblick auf die vordringliche Bedeutung einer wirksamen Krebsforschung und -behandlung von berechtigtem Interesse der Allgemeinheit ausgegangen werden. Andererseits ist jedoch zu berücksichtigen, daß Daten über Krebserkrankungen zu den sensitivsten überhaupt gehören. Dem Betroffenen kann durch eine Kenntnisnahme Dritter ein nicht wieder gutzumachender Schaden entstehen. Geht man hiervon aus und berücksichtigt man darüber hinaus, daß die dritte Alternative des § 24 Abs. 1 BDSG eine eng auszulegende Ausnahmevorschrift darstellt, so bedeutet dies, daß eine Übermittlung schutzwürdige Belange des Betroffenen beeinträchtigen würde.

Nichts anderes kann für die Auslegung der Übermittlungsvorschriften des HDSG gelten, soweit diese im Einzelfall anzuwenden sind (§§ 12, 15, 16 HDSG). Hinsichtlich der Beeinträchtigung schutzwürdiger Belange ist von den gleichen Überlegungen auszugehen wie im Rahmen des § 24 BDSG. Weiterhin dient eine Übermittlung schon deshalb nicht der **rechtmäßigen** Aufgabenerfüllung, weil sie einen Eingriff in das Persönlichkeitsrecht des Betroffenen bedeuten würde.

Unzulässig ist eine Übermittlung schließlich nach den Vorschriften über die ärztliche Schweigepflicht (Berufsordnung für Ärzte in Hessen, Teil I § 2). Danach dürfen Daten grundsätzlich nur an andere behandelnde Ärzte weitergegeben werden (§ 2 Abs. 6 Berufsordnung). Auch für Forschungszwecke ist eine Übermittlung personenbezogener Daten im Hinblick auf die in § 2 Abs. 7 Berufsordnung vorgeschriebene Anonymisierung nicht möglich. Die genannten Vorschriften sind vor allem dann von Bedeutung, wenn Daten nicht aus Dateien übermittelt werden und die Datenschutzgesetze somit für die Übermittlung nicht anzuwenden sind.

Die Übermittlung von Patientendaten an ein Krebsregister setzt mithin, soweit nicht im Einzelfall eine Einwilligung des Patienten vorliegt, eine spezialgesetzliche Regelung voraus. Hiervon ging im übrigen auch der saarländische Gesetzgeber aus, der mit dem Gesetz über das Krebsregister vom 17.1.1979 eine eigene Rechtsgrundlage für das dortige Register geschaffen hat. Eine derartige spezialgesetzliche Regelung muß insbesondere Vorschriften über die Art der zu übermittelnden Daten, ihre Anonymisierung, die Zugriffsberechtigung auf die im Register gespeicherten Daten sowie über Trägerschaft und Aufgabenstellung des Registers enthalten.

Angesichts der Bedeutung einer wirksamen Bekämpfung der Krebskrankheit stellt sich die Frage einer Übergangslösung. Wenn es gelingt, Bedingungen für die Errichtung des Krebsregisters zu schaffen, die einen wirksamen Datenschutz sicherstellen, so kann das Fehlen einer spezialgesetzlichen Grundlage für eine kurze Übergangszeit hingenommen werden. Dies kommt freilich nur insoweit in Betracht, als die zu übermittelnden Daten anonymisiert und ausschließlich zu wissenschaftlichen Zwecken genutzt werden.

Dabei kann von einem vom Institut für medizinische Statistik und Dokumentation der Universität Gießen vorgelegten, auf dem Prinzip der sog. "file-Trennung" basierenden "Konzept für den Aufbau eines Tumorregisters für die Region Mittel- und Nordhessen" ausgegangen werden, das die Führung eines reinen Inzidenzregisters vorsieht. Präzise festgelegt werden muß insbesondere, wer auf die in den beiden zu errichtenden Dateien - d.h. die Namensdatei und die verschlüsselte Datei mit den medizinischen Angaben - enthaltenen Daten Zugriff erhält. Eine Nutzung von personenbezogenen Patientendaten - auch zu wissenschaftlichen Zwecken - muß in jedem Fall ausgeschlossen sein. Im Interesse einer wirksamen Aufsicht über das Register sollte sich dieses in öffentlich rechtlicher Trägerschaft befinden.

Die Errichtung eines Nachsorgeregisters zur weiteren Behandlung von Krebskranken ist im Hinblick auf die dann erfolgende personenbezogene Auswertung äußerst sensitiver Daten nach der oben dargelegten Rechtslage erst dann möglich, wenn eine spezialgesetzliche Grundlage vorliegt. Solange diese nicht besteht, ist eine Übermittlung von Patientendaten an ein Nachsorgeregister nur mit Einwilligung des Betroffenen zulässig.

2.3. Datenbedarf von Planung und Statistik - Implikationen des Datenschutzes

2.3.1 Datenzugang für die Landesplanung - die Problematik der Rechtsgrundlage

Zehn Jahre nach dem Inkrafttreten des ersten Hessischen Datenschutzgesetzes besteht ausreichend Anlaß, um über die künftige Entwicklung nachzudenken, wahrscheinlich auftretende Konfliktfelder zu prognostizieren und politische wie rechtliche Lösungen zu formulieren..
Dem dient eine Rückbesinnung auf die Motive des hessischen Gesetzgebers, zur damaligen Zeit das erste Datenschutzgesetz der Welt zu verabschieden. Neben der rapiden Ausdehnung der automatischen Datenverarbeitung war die zunehmende Informationsverarbeitungskapazität im Rahmen eines sozialstaatlichen Aufgabenzuwachses unmittelbarer Anlaß zu dieser Regelung. Die Verabschiedung des Datenschutzgesetzes stand mit anderen Worten in einem untrennbaren Zusammenhang mit der umfassenden Konzeption der Landesentwicklungsplanung Hessen` 80, die auf computergestützte Planungs- und Analysesysteme aufbaut. Dieser offensichtliche Zusammenhang zwischen zunehmender Planungstätigkeit des Staates und Datenschutz ist allerdings im Laufe der vergangenen zehn Jahre immer mehr aus dem Blickfeld geraten.

Die Schwierigkeiten, die sich heute für die Landesplanung ergeben, was den Zugang zu administrativen, insbesondere aber statistischen Daten betrifft, haben ihre Ursache in Unterlassungen des Gesetzgebers, in mangelnder Beachtung der rechtlichen Rahmenbedingungen von Planung überhaupt. Wenn heute der Hessische Minister für Landesentwicklung, Umweltschutz, Landwirtschaft und Forsten den Grund für eine unzureichende Datenbasis der Landesentwicklungsplanung, etwa bei der Gemeindedatei, am Datenschutz festzumachen versucht; so ist dies allenfalls teilweise zutreffend. Von Anfang an mußte nämlich jedem, der mit Landesplanung zu tun hat, klar sein, daß das Statistikgeheimnis des § 12 des Bundesstatistikgesetzes von 1953 eine unübersteigbare Barriere für den Zugang zu Mikrodaten - "Einzelangaben", wie das Statistikgesetz formuliert - darstellt. Diese Tatsache ist bei der Novellierung des Bundesstatistikgesetzes - in der Fassung von 1980 - lediglich konstruktiv verdeutlicht worden. Danach sind statistische Einzelangaben grundsätzlich geheimzuhalten. Sie dürfen nur im Ausnahmefall weitergeleitet werden und dann auch nur aufgrund einer speziellen Rechtsvorschrift, in der die jeweilige Statistik angeordnet wird. Im Interesse eines weitgehenden Schutzes des Einzelnen ist es damit nicht der Verwaltung, sondern dem Gesetzgeber überlassen, bei jeder neuen Statistik eine Abwägung zwischen den Interessen der Befragten an der Geheimhaltung ihrer Angaben und den Wünschen der Planer und anderer Interessenten an einer weiteren Verwertung des gewonnenen statistischen Einzelmaterials vorzunehmen.

Daher erfordert der Eingriff in die private Rechtssphäre des Einzelnen, wie er durch eine allgemeine statistische Auskunftspflicht begründet wird, eine Information des Auskunftspflichtigen, inwieweit und zu welchem Zweck seine persönlichen und sachlichen Angaben verwertet werden. Im Interesse einer besseren Kontrollmöglichkeit durch den Betroffenen und einer größeren Transparenz des statistischen Datenflusses ist es deshalb notwendig, daß der Kreis der Empfänger statistischer Einzelangaben, die Art der Angaben und ihre Verwendung in der die Statistik anordnenden Rechtsvorschrift angegeben werden, wie es auch bisher schon regelmäßig in den betreffenden Einzelgesetzen geschehen ist. Im Übrigen ist bei der Abfassung der einzelnen Statistikgesetze darauf zu achten, daß sie sich an den Standards der Datenschutzgesetze orientieren, d.h. natürlich mindestens nicht hinter deren Schutzbestimmungen zurückbleiben.

Das Statistikgeheimnis hatte mithin von Anfang an ein grundsätzliches Datenmonopol der statistischen Ämter für Einzelangaben, soweit sie aus Bundesstatistiken stammen, zur Folge. Das Statistische Landesamt ist im Rahmen von Bundesstatistiken lediglich befugt, Einzelangaben zu übermitteln, die so anonymisiert sind, daß die Auskunftspflichtigen oder Betroffenen nicht mehr zugeordnet werden können. Der Gesetzgeber hat hiermit zu der bisher umstrittenen Frage Stellung genommen, ob anonymisierte Mikroda-

ten als Einzelangaben im Sinne des § 11 Abs. 1 Bundesstatistikgesetz geheimzuhalten sind. Diese Regelung würde auch die Einrichtung sog. "public use-files" erlauben, die als öffentliche automatisierte statistische Datenbank neben die klassischen Mittel der Veröffentlichung amtlicher Statistiken treten kann. Eine statistische Datenbank mit anonymisierten Einzelangaben und institutionalisierten Zugangsrechten für grundsätzlich jedermann ist ein von mir seit langem angeregtes und im Ausland zum Teil diskutiertes, zum Teil bereits eingeführtes Konzept des Informationszugangs, das vor allem für Forschung, Planung, Politikberatung sowie praktische Politikvorbereitung von eminenter Bedeutung ist. Es würde in Hessen einen wesentlichen Schritt in Richtung auf ein gesellschaftliches Informationsgleichgewicht bedeuten. Allerdings muß bei Anonymisierungsmaßnahmen immer mitbedacht werden, welches Zusatzwissen beim Empfänger von anonymisierten Daten vorhanden ist. Diese Forderung ist in der Praxis durch das Statistische Landesamt schwieriger zu verwirklichen als die Aggregation, d.h. die Zusammenfassung mehrerer Einzelangaben (vgl. § 11 Abs. 6 BStatG).

Die sich aus dem Statistikgeheimnis ergebende Einschränkung des Datenzugangs für die Landesentwicklungsplanung besagt andererseits noch nichts über die Zulässigkeit des Aufbaus von Planungsdatenbanken überhaupt. Weil aber die "Vorratsspeicherung" von personenbezogenen Angaben zu unterschiedlichen Planungszwecken nach dem Hessischen Datenschutzgesetz rechtlich bedenklich ist, habe ich schon im Sechsten Tätigkeitsbericht - in meinem dort vorgelegten Musterentwurf für ein Hessisches Datenschutzgesetz - eine bereichsspezifische Regelung für planerische und statistische Datenbanken gefordert. Immerhin enthielt ja das erste Hessische Datenschutzgesetz von 1970 diese Spezialvorschrift in § 5 fast gleichlautend. Die Landesregierung hat diese Planungsnorm bei der Novellierung des Hessischen Datenschutzgesetzes als nicht erforderlich und sachdienlich gestrichen und damit die Ursache für jenes Informationsdefizit sozialstaatlicher Landesentwicklungsplanung gesetzt, das mit meinem Vorschlag gerade verhindert werden sollte.

Die rechtliche Begründung der Einrichtung derartiger Datenbanken mit der allgemeinen Zulässigkeitsnorm des § 11 Abs. 1 HDSG muß an der Unbestimmtheit des Planungszwecks und der strukturellen Vielfältigkeit von Planung scheitern. Die Sammlung einer unbestimmten Vielzahl von Daten zu dem Zweck unbestimmter möglicher Auswertung ist durch die Gesetzesformel "zur Aufgabenerfüllung erforderlich" nicht gedeckt. Diese Formulierung, die vornehmlich auf die Bedingungen des Verwaltungsverfahrens zugeschnitten ist, wird mit anderen Worten dann zu unbestimmt und mithin verfassungsrechtlich problematisch, wenn damit Informationssammlungen für noch nicht näher definierte Aufgaben und Zwecke legitimiert werden sollen. Der Bundesgesetzgeber hat mit gutem Grund bei der Regelung des Sozialgeheimnisses und des Schutzes der Sozialdaten im neuen 10. Buch des Sozialgesetzbuchs die Notwendigkeit anerkannt, die Voraussetzungen der Informationsverarbeitung für die Planung zu normieren (vgl. § 75 SGB X).

Eine Novellierung des HDSG wäre für Landesregierung und Landtag die Gelegenheit zu dokumentieren, welchen Stellenwert sie der Datenverarbeitung, zu Planungszwecken und damit sozialstaatlicher Planung überhaupt, einräumen. Allerdings würde eine entsprechende bereichsspezifische Norm im HDSG noch keine Legitimation für eine Übermittlung von Einzelangaben aus Datenbeständen der Bundesstatistik, die sich beim Hessischen Statistischen Landesamt befinden, an andere Behörden bedeuten. Diese kann nur durch spezifizierte Regelungen in statistischen Bundesgesetzen geschaffen werden (vgl. §11 Abs. 3 Bundesstatistikgesetz). Dabei geht es im Grunde darum, die notwendige rechtliche und funktionale Bestimmung des Verhältnisses von Planungs- und statistischen Informationssystemen vorzunehmen.

2.3.2 Funktionswandel der Statistik, Informationsgleichgewicht und die Notwendigkeit einer bereichsspezifischen Regelung

Durch die Diskussion um den Datenzugang staatlicher Planung zu statistischer Information wird auch die veränderte Funktion der amtlichen Statistik sichtbar. War diese traditionell retrospektiv ausgerichtet, führte sie mehr oder weniger ein Schattendasein in der Ecke der fiskalischen Hilfsmittel der öffentlichen Verwaltung mit der Aufgabe, vollzogene Entscheidungen zu rechtfertigen oder zu kritisieren und zukünftige Steuereinnahmen zu schätzen, bietet die heutige amtliche Statistik in ihrer Komplexität ein völlig anderes Bild, ohne daß Organisation und Rechtsgrundlage sich geändert hätten.

Der Aufbau statistischer Datenbanken schreitet voran; das Bundesstatistikgesetz schreibt die Einrichtung und Führung der "Allgemeinen Statistischen Datenbank des Bundes" vor (§ 3 Abs. 1 Ziff. 8). Der Einsatz der automatischen Datenverarbeitung aktualisiert die amtliche Statistik und macht sie zu einer gültigen, jederzeit mit den Datenbeständen aller Einzelstatistiken verknüpfbaren Datenbasis, die wiederum jederzeit verfügbar ist und nach verschiedensten Gesichtspunkten ausgewertet werden kann. Die Segmentierung einzelner Bundes- und Landesstatistiken, wie sie sich noch in den Statistikgesetzen oder anderen Rechtsvorschriften im Sinne von thematisch und gegenständlich getrennten Erhebungsprogrammen darstellt, wird in einem universellen Datenbankkonzept tendenziell aufgehoben; der Datenbestand wird "multifunktional".

Aktualität, Verfügbarkeit und Validität der Daten lassen die amtliche Statistik immer attraktiver werden für Informationsbegehren staatlicher Planung und wissenschaftlicher Forschung. Der Einsatz der ADV macht im Gegensatz zur "handverlesenen" Statistik das Mikrodatum, die statistische Einzelangabe überhaupt erst nutzbar. Die Forschungsmethoden der Sekundäranalyse und der mikroanalytischen Simulation finden hier eine methodische aufbereitete Datenbasis, die in Art und Umfang einzigartig ist.

Um so bedeutsamer ist angesichts dieser Entwicklung die Feststellung, daß es der Verarbeitung personenbezogener Daten durch das Statistische Landesamt, soweit sie nicht durch eine gesetzlich angeordnete Bundesstatistik legitimiert ist, d.h. also für die Erstellung von Landesstatistiken, an einer gesetzlichen Grundlage fehlt. Die allgemeine Norm des § 11 Abs. 1 HDSG mit der Zulässigkeitsvoraussetzung "zur Aufgabenerfüllung erforderlich" wird der Bedeutung und der gewandelten Funktion der amtlichen Statistik auf Landesebene kaum gerecht. Dieser Funktionswandel - Statistik als Institution für Bürgerinformation - erfordert ein Gesetz, das eine Rechtsgrundlage für die Verarbeitung personenbezogener Daten schafft und Zugangsrechte für grundsätzlich jedermann - im Rahmen der notwendigen Geheimhaltung - statuiert. Ansonsten ist nicht auszuschließen, daß aufgrund der gesteigerten Funktionsfähigkeit der amtlichen Statistik durch automatische Datenverarbeitung ein Informationsmonopol der Landesexekutive entsteht, das zu Lasten des Parlaments und der kommunalen Gebietskörperschaften geht. Ein Landesstatistikgesetz, das Datenschutz und Informationsfreiheit gleichzeitig gewährleistet, könnte jenen Zusammenhang wieder herstellen, den der hessische Gesetzgeber von 1970 bei der Verabschiedung des ersten HDSG noch mitbedacht hat. Jede Politik zur Verbesserung des Datenschutzes muß - so die Konsequenz - gleichzeitig als aktive Informationspolitik definiert werden.

2.3.3 Datenschutz und alternative Formen der Erhebung für statistische Zwecke - das Beispiel "Mikrozensus"

Datenschutz problematisiert nicht nur die Auswertung, sondern bereits bestimmte Formen der Erhebung statistischer Information. Die gesetzlich angeordnete jährliche "Mikrozensus"-Befragung stellt die wohl "intimste" Erhebung statistischer Angaben beim Bürger dar. Dementsprechend zahlreich sind die Beschwerden von Betroffenen, die eine Verletzung ihrer Privatsphäre rügen. Immerhin weigerte sich im Jahr 1979 etwa ein Zehntel der ca. 22.000 befragten Haushalte in Hessen, dem vom Hessischen Statistischen Landesamt beauftragten Interviewer die Fragen zum Mikrozensus zu beantworten. Ungefähr 120 Haushalte haben auch nach Belehrung des Statistischen Landesamtes über die gesetzliche Auskunftspflicht oder sogar schriftliche Bitten die Erhebungsbogen unbeantwortet gelassen; nicht einmal die Androhung von Bußgeldverfahren konnte ihre Auskunftsbereitschaft erhöhen.

Die mit der Auskunftspflicht verbundene Bußgeldandrohung verstärkt vielmehr die Ängste und Befürchtungen jener Bürger, die dieser äußerst "peinlichen" Befragung ohnehin skeptisch gegenüberstehen. Diese Befürchtungen sind auch keineswegs so unbegründet, wie dies von den Statistikämtern immer wieder unter ständigem Hinweis auf das Statistikgeheimnis beteuert wird: Immerhin werden Name und Anschrift auf den Erhebungsbögen erfaßt; diese werden drei Jahre lang aufbewahrt. Auch wenn der Name nur zur Rücklaufkontrolle erforderlich ist und nicht auf automatischen Datenträgern zur weiteren Verwendung gespeichert wird, muß der kritische Beobachter fragen, ob nicht Alternativen zu dieser Methode der Repräsentativstatistik bestehen. Erfahrungen aus anderen westlichen Industriestaaten mit vergleichbarer Gesellschafts- und Wirtschaftsstruktur beweisen dies. An einem ersten von mir angeregten informellen Expertengespräch, das demnächst in anderem Rahmen fortgesetzt werden soll, nahmen Vertreter ausländischer Statistikämter, Wissenschaftler und Statistiker aus Behörden (u.a. der Präsident des Hessischen Statistischen Landesamts) teil, um in aller Offenheit über Perspektiven des Datenschutzes in der amtlichen Statistik zu diskutieren. Im Rahmen dieses Gesprächs wurde auf Lösungswege hingewiesen, die mir auch im Hinblick auf den Mikrozensus plausibel und wünschenswert erscheinen.

Die Bundesrepublik Deutschland ist der einzige Staat in der westlichen Welt, der bei einer Repräsentativstatistik die Auskunftspflicht des Bürgers mit einer Strafsanktion verbindet; bis auf Kanada hält man in anderen Ländern selbst die Auskunftspflicht als solche für entbehrlich. An die Stelle der Strafdrohung tritt dort die Aufklärung der Öffentlichkeit über Sinn und Zweck der Statistik, um die Auskunftsbereitschaft der Bevölkerung zu erreichen. Ich würde es begrüßen, wenn in diesem Sinne die Landesregierung das Hessische Statistische Landesamt beauftragte, die Betroffenen in einer umfassenden Kampagne über Zweck und Notwendigkeit des Mikrozensus zu informieren und zugleich zu erklären, daß auf die Einleitung von Ordnungswidrigkeitsverfahren verzichtet wird. Alle Experten prognostizieren nach Erfahrungen in Schweden und Kanada eine erhöhte Teilnahmebereitschaft der Bevölkerung, validere Ergebnisse und damit bessere und solidere Grundlagen für Planungen und Entscheidungen der Exekutive. Ein solches Aktionsprogramm könnte zugleich Erkenntnisse für zukünftige Regelungen der Auskunftsverpflichtung in statistischen Gesetzen vermitteln.

Noch einmal: Ein gesicherter Zusammenhang besteht zwischen Auskunftsbereitschaft, Aufklärung des Betroffenen und Statistikgeheimnis; Sanktionen dagegen sind aus der Sicht des Datenschutzes höchst bedenklich, um Informationen vom Bürger über sich zu erzwingen, führen vielmehr potentiell zu falscher Information der Regierung und der Öffentlichkeit.

Angesichts der Möglichkeiten der Informationstechnologie und der verfeinerten Methodik von Repräsentativerhebungen habe ich angesichts der neueren Rechtssprechung des Bundesverfassungsgerichts zum allgemeinen Persönlichkeitsrecht seit dem "Mikrozensusurteil" und den gesetzlichen Entwicklungen im Bereich des Datenschutzes Zweifel, ob die Durchführung der Mikrozensus-Statistik in ihrer heutigen Form einer verfassungsgerichtlichen Überprüfung noch standhalten würde.

2.4 Datenverarbeitung durch den Verfassungsschutz - Notwendigkeit und Grundsätze einer gesetzlichen Regelung

Die Aufgabe des Verfassungsschutzes besteht nach § 3 Abs. 1 des Gesetzes über die Zusammenarbeit des Bundes und der Länder in Angelegenheiten des Verfassungsschutzes -BVerfSchG- vom 27. September 1950 i.d.F. vom 7.8.1972 in der "Sammlung und Auswertung von Auskünften, Nachrichten und sonstigen Unterlagen" über verfassungsfeindliche Bestrebungen (Ziff. 1), sicherheitsgefährdende und geheimdienstliche Tätigkeiten für eine fremde Macht (Ziff. 2) bzw. der Gefährdung auswärtiger Belange der Bundesrepublik Deutschland durch Anwendung von Gewalt (Ziff. 3). Darüber hinaus wirken die Ämter für Verfassungsschutz in bestimmten Fällen bei der Überprüfung von Personen mit, die zu geheimhaltungsbedürftigen Informationen Zugang haben oder an sicherheitsempfindlichen Stellen beschäftigt sind oder werden sollen, § 3 Abs.2 Ziff. 1, 2 BVerfSchG. Schließlich sind ihnen Aufgaben bei der technischen Sicherung bestimmter Anlagen übertragen, § 3 Abs. 2 Ziff. 3. Im Bundesgesetz wird auch die Aufgabe der Verfassungsschutzbehörden der Länder im einzelnen festgelegt. Daher fehlt im Gesetz über die Errichtung eines Landesamtes für Verfassungsschutz vom 19. Juli 1951 (GVBl. I S. 43 -HessVerfSchG-) eine ausdrückliche Aufgabenbeschreibung für das Landesamt für Verfassungsschutz. Eine Novellierung allerdings sollte sich nicht mit diesem pauschalen Hinweis begnügen, sondern die Aufgabenzuweisung zur Klarstellung in die Gesetzesformulierung mit einbeziehen.

Die Novellierung der Verfassungsschutzgesetze - insoweit ist auch das Bundesverfassungsschutzgesetz betroffen - ist aber vor allem aus einem anderen Grund notwendig: Die Aufgabe des Verfassungsschutzes bedingt in erheblichem Umfang die Verarbeitung personenbezogener Daten. Beide Gesetze enthalten aber weder eine ausreichende Befugnisnorm - d.h. eine Rechtsvorschrift, die die Zulässigkeit einer Verarbeitung personenbezogener Daten begründet - noch sonstige Datenschutzbestimmungen. § 3 Abs. 3 S. 1 BVerfSchG spricht zwar gegenüber den Verfassungsschutzbehörden das Verbot aus, polizeiliche Befugnisse oder Kontrollbefugnisse auszuüben - dem entspricht § 2 HessVerfSchG. Weiterhin überträgt § 3 Abs. 3 S. 2 BVerfSchG den Verfassungsschutzbehörden die Befugnis, zur Erfüllung ihrer Aufgaben "nachrichtendienstliche Mittel anzuwenden". Eine entsprechende Vorschrift im HessVerfSchG fehlt hingegen. Aber auch eine ausdrückliche Zuweisung dieses Inhalts kann nicht als ausreichende Rechtsgrundlage für die Verarbeitung personenbezogener Daten angesehen werden. Dafür wäre bzw. ist sie zu unbestimmt. Ebensowenig folgt aus der Aufgabenbeschreibung, welche Befugnisse den Verfassungsschutzämtern im einzelnen zustehen. So könnten die Aufgaben durch eine Vielzahl höchst unterschiedlicher Befugnisse wahrgenommen werden. Aus diesem Grund kann die fehlende bereichsspezifische Norm über die Datenverarbeitung auch nicht durch einen Rückgriff auf die Regelungen der §§ 9 Abs. 1 BDSG bzw. 11 Abs. 1 HDSG ersetzt werden, nach denen das Speichern und das Verändern personenbezogener Daten zulässig ist, "wenn es zur rechtmäßigen Erfüllung der in der Zuständigkeit der speichernden Stellen liegenden Aufgaben erforderlich ist".

Die Befugnisnorm eines Verfassungsschutzgesetzes muß vielmehr konkret festlegen, unter welchen Voraussetzungen Daten erhoben, gespeichert und verändert werden dürfen, wem und zu welchem Zweck die Verfassungsschutzbehörden diese Daten übermitteln dürfen, von wem ihnen Daten übermittelt werden und wann diese Daten zu berichtigen bzw. zu löschen sind.

Im einzelnen muß die Novellierung insbesondere folgenden Gesichtspunkten Rechnung tragen:

- Soweit die Verfassungsschutzbehörden zur Erfüllung ihrer Aufgaben Informationen sammeln, werden diese - von Ausnahmen abgesehen - personenbezogene Daten enthalten. Die Befugnisnorm hat deshalb die damit verbundene Datenverarbeitung allgemein in der Terminologie des Datenschutzes zu regeln, d.h. insbesondere unter Verwendung der Begriffe des "Speicherns", "Übermittelns", "Berichtigens" und "Löschens". Nur auf diesem Wege ist es möglich, das bereits entwickelte Rechtssystem des Datenschutzes zur Anwendung zu bringen und dem Bürger eine weitgehende Sicherung seiner Rechte zu gewähren.

- Soweit der Begriff des "nachrichtendienstlichen Mittels" ohne eine Konkretisierung der einzelnen Methoden in die Befugnisnorm aufgenommen wird, bedarf es einer Eingrenzung sowohl hinsichtlich des Grundes für ein Tätigwerden überhaupt als auch hinsichtlich der Wahl der Mittel. "Nachrichtendienstliche Mittel", die über das offene Sammeln von Informationen hinausgehen, sollten nicht zur Erfüllung von Mitwirkungsfunktionen, insbesondere bei der Personenüberprüfung herangezogen werden, sondern sich auf den Bereich der originären Aufgaben der Verfassungsschutzbehörden im Sinne des § 3 Abs. 1 BVerfSchG beschränken. Sie sollten nur dann zum Einsatz kommen, wenn tatsächliche Anhaltspunkte für den Verdacht verfassungsfeindlicher Bestrebungen oder Tätigkeiten vorliegen. Die Anwendung und die Auswahl des jeweiligen Mittels ist an das verfassungsrechtlich begründete Verhältnismäßigkeitsprinzip zu knüpfen. Zu prüfen ist, ob nicht im gleichen Sinne wie nach § 5 Abs. 5 des Gesetzes zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses vom 19. Juli 1975 (BGBl. I, S. 1921) dem Betroffenen nach Abschluß einer Maßnahme der Vorgang mitzuteilen ist, wenn eine Gefährdung des Zwecks des Eingriffs ausgeschlossen werden kann (so auch § 4 Abs. 2 a.E. des Entwurfs eines Gesetzes zur Änderung des Gesetzes über den Verfassungsschutz im Lande Bremen - Antrag der Fraktion der SPD, Landtagsdrucksache 10/367 vom 13.11.1980).

- Die Verarbeitung der personenbezogenen Daten von Minderjährigen bedarf einer besonderen Regelung. Dabei ist im einzelnen festzulegen, welche verfassungsfeindliche Tätigkeit oder Bestrebung zu einer Speicherung führen kann. Auch die Frage, ob nicht gespeicherte Daten über diesen Personenkreis kürzeren Löschungsfristen unterliegen können, ist zu prüfen.

- Ein besonderes Problem ist die Frage der Löschungsfrist. Die intensiven Diskussionen über eine allgemeine Festlegung von Löschungsfristen für die Speicherung personenbezogener Daten im Bereich der Polizei, wie sie im Arbeitskreis II der Innenministerkonferenz und in der "Arbeitsgruppe Datenschutz" der Konferenz der Landesbeauftragten und des Bundesbeauftragten für den Datenschutz stattgefunden haben, zeigen die erhebliche Bedeutung, die der Festlegung einer Löschungsfrist gerade im Bereich der Sicherheitsbehörden zukommt. Hierbei geht es nicht um das Problem der Löschung unrichtiger oder unzulässigerweise gespeicherter Daten, sondern von solchen, die zur Aufgabenerfüllung nicht mehr erforderlich sind (vgl. §§ 19 Abs. 3 HDSG, 14 Abs. 3 BDSG). Der Einwand, solche Löschungsfristen könnten nicht generell bestimmt werden, überzeugt nicht. Wie schon bei der Neuformulierung der Bestimmungen über die kriminalpolizeilichen personenbezogenen Sammlungen (KpS) kann auch hier, wenn nicht eine Löschungsfrist, so doch eine Überprüfungsfrist festgelegt werden. Nach Ablauf dieser Überprüfungsfrist - die dem Erfahrungswert der im Normalfall notwendigen Registrierungsdauer entspricht - muß über die Löschung entschieden werden. Ist die Datenspeicherung zur rechtmäßigen Aufgabenerfüllung nicht mehr erforderlich, sind die Daten zu löschen, anderenfalls ist für diesen Fall eine neue Prüffrist festzulegen.

- Die Übermittlung personenbezogener Daten von anderen Behörden an die Verfassungsschutzbehörden ist näher zu regeln. Das Auskunftsrecht der Verfassungsschutzämter ist dabei einzugrenzen durch ihre Aufgabenstellung, entgegenstehende gesetzliche Vorschriften und den Grundsatz der Erforderlichkeit.

- Die Übermittlung von Daten durch die Verfassungsschutzämter an andere öffentliche Stellen bedarf ebenfalls einer eingehenden Regelung. Es reicht nicht aus, daß eine Übermittlung zur Erfüllung der Aufgabe der Verfassungsschutzbehörde oder einer anderen staatlichen Stelle erforderlich ist. Sie muß auch verhältnismäßig sein, gemessen an den Rechten des betroffenen Bürgers.

  Insbesondere ist festzulegen, unter welchen Voraussetzungen an die Strafverfolgungsbehörden übermittelt werden darf. Der Grundsatz der Trennung von Polizei und Verfassungsschutz muß auch hier zu einer Einschränkung der Übermittlung führen. Dabei ist die Art der Tat ein gewichtiger Grund der Differenzierung (§ 6 Abs. 2 Ziff 1 des zitierten "Bremer Entwurfs" knüpft beispielsweise an § 7 Abs. 3 des Gesetzes zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses an. Danach dürfen Erkenntnisse, die aus Maßnahmen der Brief-, Post- und Fernmeldeüberwachung gewonnen werden, nur zur Erforschung und Verfolgung bestimmter schwerwiegender Delikte verwertet werden). Weiterhin sollte die Datenübermittlung durch die Verfassungsschutzbehörden an private Dritte wie z.B. im Staatsauftrag tätige Unternehmen nur zulässig sein, soweit dies zur Wahrnehmung der Aufgaben des Verfassungsschutzes unerläßlich ist. Wirken die Ämter nach § 3 Abs. 2 BVerfSchG bei der Überprüfung von Personen mit, dürfen zudem nur die Ergebnisse der Überprüfung mitgeteilt werden.

- Die Übermittlung von Daten aus dem Bereich der Verfassungsschutzämter nach außen sollte ausschließlich über die zuständige Aufsichtsbehörde, den Minister des Innern, erfolgen. Dadurch wäre ein Amtshilfeverkehr unmittelbar mit den Verfassungsschutzbehörden ausgeschlossen. Diese Regelung

würde der starken Beeinträchtigung Rechnung tragen, die für den Betroffenen in der Übermittlung seiner im Bereich des Verfassungsschutzes gespeicherten Daten an andere Stellen liegen kann. Sie würde andererseits die Verwendung dieser Angaben unmittelbar in die parlamentarische Verantwortung des Innenministers rücken.

- Für beide Richtungen der Übermittlung ergibt sich die Notwendigkeit einer klaren Trennung der Informationssysteme der Polizei einerseits und der Verfassungsschutzämter andererseits. Eine allgemeine Zugriffsberechtigung auf Datenbestände des jeweils anderen darf es nicht geben. Informationen dürfen nur im Einzelfall nach Prüfung der Erforderlichkeit zur Aufgabenerfüllung des Landesamtes für Verfassungsschutz von diesem und an dieses weitergegeben werden. Der Bundesminister des Innern hat den von seiten der Datenschutzbeauftragten vielfach geäußerten Bedenken Rechnung getragen und die Zugriffsberechtigung des Bundesamtes für Verfassungsschutz auf den Fahndungsbestand von INPOL und auf den Teilbereich Terrorismus in dem Informationssystem PIOS des Bundeskriminalamtes eingestellt.
- Die gebotene Novellierung muß sich mit den Rechten der Betroffenen befassen. Eine generelle, für die Sicherheitsbehörden vorgesehene Ausnahme von der Auskunftspflicht gegenüber dem Bürger (§ 18 Abs. 2 HDSG) ist - wie ich bereits in meinem letzten Tätigkeitsbericht dargelegt habe - nicht gerechtfertigt. Auch im Bereich der Verfassungsschutzbehörden könnte in einer großen Zahl von Fällen dem anfragenden Bürger mitgeteilt werden, daß er dort nicht gespeichert ist, ohne daß dadurch die Arbeit des Verfassungsschutzes gefährdet würde. Die Auskunftsregelung - von der auch die Geltendmachung weiterer dem Bürger zustehender Rechte wie Berichtigung, Sperrung und Löschung abhängt - sollte ähnlich wie in den KpS-Richtlinien in der Weise getroffen werden, daß die Behörde in jedem Einzelfall abwägen muß, ob ihr Interesse an einer Geheimhaltung der Daten das Auskunftsinteresse des Bürgers überwiegt. Nur wenn dies der Fall ist, kann die Auskunft verweigert werden, anderenfalls ist sie zu erteilen. Schließlich ist dem Bürger ein Rechtsanspruch auf Berichtigung unrichtiger Daten und Löschung unzulässig gespeicherter oder zur Aufgabenerfüllung nicht mehr erforderlicher Daten einzuräumen.

3. Konsequenzen der Bundesgesetzgebung

3.1 Das Melderechtsrahmengesetz und die Novellierung des Landesmelderechts

Am 23. August 1980 trat das Melderechtsrahmengesetz (MRRG) in Kraft (Bundesgesetzblatt I S. 1429). Nach fast zehnjährigen Vorarbeiten gelang es damit, dem Einwohnerwesen eine gesetzliche Grundlage zu verschaffen, in der die Forderung nach einem wirksamen, bereichsspezifischen Datenschutz weitgehend berücksichtigt wird. Die Länder sind nun aufgefordert, innerhalb von zwei Jahren nach Inkrafttreten des Gesetzes ihr Melderecht dem MRRG anzupassen und innerhalb des vorgegebenen Rahmens eigene Meldegesetze zu verabschieden.

3.1.1 Rückblick

Das Melderecht des 19. Jahrhunderts bis hin zu der Reichsmeldeordnung vom 13.1.1938 (Reichsgesetzblatt I S. 13) verstand sich weitgehend als Sicherheitsrecht, d.h. als Maßnahme gegen Gefahren, die der Allgemeinheit drohen und als Mittel zur Bekämpfung von Straftaten. Noch die Ländergesetze der Jahre 1949 und 1950 übernahmen die Reichsmeldeordnung fast wörtlich. Nur die spezifisch nationalsozialistisch beeinflußten Normen wurden gestrichen. Die Durchführungsvorschriften zur Meldeordnung hatten in der Zeit des Nationalsozialismus mit der Erfassung von immer mehr Daten zu einer ungeahnten Ausweitung der Datenerfassung und -verarbeitung mit dem Ziel einer möglichst lückenlosen Überwachung der Bürger geführt. Mit nur geringfügigen Korrekturen wurde das Prinzip eines möglichst umfassenden Informationssystems auch in dem Musterentwurf und den auf diesen folgenden Ländermeldegesetzen der Jahre 1959/60 beibehalten. Das Ziel lautete: Vom Einwohnermeldewesen zum Einwohnerwesen. Die Funktion des Melderegisters als Grunddatei, aus der unter anderem an Personenstands-, Paß- u. Personalausweis-, Staatsangehörigkeits-, Wehr-, Ausländer-, Gesundheits- und Justizbehörden regelmäßig übermittelt wird, begründete ein großes Bedürfnis nach einer möglichst umfangreichen Datenerfassung. Die klassische polizeirechtliche Funktion des Meldewesens trat damit zwar in den Hintergrund. Die Einbeziehung des Meldewesens in ein umfassend gedachtes Verwaltungsinformationssystem bewahrte jedoch die alten Strukturen vor einer grundlegenden Veränderung. Es war nur folgerichtig, daß der Bundestag in seinen Entwürfen zu einem Bundesmeldegesetz in der 6. und 7. Wahlperiode (Bundestagsdrucksache VI/2654 bzw. 7/1059) den Ausbau eines verwaltungsinternen Datenverbunds vor allem an den durch die Entwicklung der elektronischen Datenverarbeitung entstandenen Möglichkeiten maß und ein entsprechendes System auch anstrebte. Die in den Entwürfen vorgesehene Einführung eines einheitlichen Personenkennzeichens für jeden Bürger versprach zwar eine qualitativ wesentliche Verbesserung bei der Verarbeitung

der Einwohnerdaten aus der Sicht der Verwaltung. Gleichzeitig standen diesem Vorschlag zu Recht erhebliche datenschutzrechtliche Bedenken entgegen. Wenn auch nicht beabsichtigt, so wäre mit der Realisierung dieses Vorschlags ein wesentlicher Schritt in Richtung auf den in seinen persönlichen Lebensäußerungen weitgehend kontrollierbaren "gläsernen Menschen" vollzogen worden. Es ist dem Einfluß der mit dem Datenschutz befaßten Stellen, nicht zuletzt dem Hessischen Datenschutzbeauftragten, gelungen, in einer Vielzahl von Stellungnahmen den Bundestag zu einer Revision dieser Zielsetzung zu bewegen und auf das Personenkennzeichen als einheitlichen Ordnungsbegriff im Meldewesen zu verzichten.

Der in der 8. Legislaturperiode des Bundestags neu eingereichte Entwurf brachte eine für den Datenschutz bedeutsame Tendenzwende. Das Inkraftreten des Bundesdatenschutzgesetzes am 1.1.1978 zeigte insofern deutliche Auswirkungen. Das Einwohnermeldewesen wurde nun vor allem als Aufgabe des bereichsspezifischen Datenschutzes verstanden, hinter der die Funktion als Verwaltungsinformationssystem zurückzutreten hatte. Der Hessische Datenschutzbeauftragte beteiligte sich in den verschiedenen Phasen des Gesetzgebungsverfahrens an der Ausarbeitung einer möglichst datenschutzfreundlichen Lösung.

Nachdrücklich zu begrüßen ist die Ankündigung der Landesregierung, im Laufe des Jahres 1981 einen Gesetzentwurf für ein Landesmeldegesetz beim Landtag einzubringen.

3.1.2 Notwendige Überlegungen aus der Sicht des Datenschutzes

- Umfang der Speicherung von Daten
  § 2 Abs. 1 MRRG sieht einen Katalog von Daten vor, die im Meldregister zur Erfüllung des Meldezwecks gespeichert werden dürfen. Es fällt auf, daß für den dem Wortlaut nach identischen Meldezweck, nämlich für die Identitätsfeststellung und den Wohnungsnachweis nach § 2 Abs. 1 neunzehn Datenarten, nach § 10 Abs. 5 MRRG aber offensichtlich ein verminderter Datensatz für erforderlich gehalten wird. Nach letzterer Vorschrift hat der Landesgesetzgeber die Aufgabe, den Datensatz festzulegen, der nach dem Wegfall der Meldepflicht etwa durch Wegzug oder Tod eines Einwohners weiter erforderlich bleibt. Diese Ermächtigung hat nur einen Sinn, wenn im Unterschied zu dem nach § 2 Abs. 1 bzw. der Parallelvorschrift in dem jeweiligen Landesgesetz zu speichernden Satz sich der Satz nach § 10 Abs. 5 MRRG auf die effektiv zur Erfüllung des genannten Meldezwecks erforderlichen Daten reduziert. Demnach gibt § 2 Abs. 1 nur den Maximalsatz der zur Erfüllung des Meldezweckes vorgesehenen Datenarten an. Er kann bei der Konzipierung der Landemeldegesetze eingeschränkt werden, ohne daß dies die Erfüllung des Meldezwecks beeinträchtigen würde.

  Der Charakter des Bundesgesetzes als Rahmennorm verpflichtet somit zu einer Überprüfung der Frage, ob alle diese Daten zur Erfüllung des Meldezwecks notwendig sind oder ob nicht schon ein geringerer Datensatz hierfür ausreicht.

- Umfang der Speicherung von Daten für die Erfüllung von Aufgaben der Länder
  Nach dem Wortlaut von § 2 Abs. 3 kann durch Landesgesetz ohne erkennbare Einschränkung bestimmt werden, daß für die Erfüllung von Aufgaben der Länder weitere Daten gespeichert werden dürfen. Diese Auslegung widerspräche jedoch der Konzeption des Melderechtsrahmengesetzes. Demnach dient das Melderegister in erster Linie und vor allem dem genannten Meldezweck. Wenn es darüber hinaus zur Erfüllung auch anderer öffentlicher Aufgaben herangezogen wird, so kann dies nur in engen Grenzen geschehen. So wurde bei der Konzipierung des § 2 Abs. 2 MRRG, der die Speicherung für die Erfüllung von Aufgaben des Bundes im einzelnen regelt, eine in zweifacher Hinsicht restriktive Regelung getroffen. Zum einen werden dort nur die traditionellen Aufgaben genannt, bei denen die Meldebehörde Unterstützungsfunktionen zugunsten anderer Behörden wahrnimmt. Diese sind die Erstellung der Wahlregister zum Bundestag und Europäischen Parlament, die Ausstellung von Lohnsteuerkarten, die Mitwirkung im Ausweiswesen sowie in der Wehr- oder Zivildienstüberwachung. In allen diesen Bereichen hat sich der Bundesgesetzgeber auf den absolut notwendigen Datensatz beschränkt. Dies kommt darin zum Ausdruck, daß für den Fall von Wahlausschlußgründen, Paßversagungsgründen, Anordnungen nach § 2 Abs. 2 Personalausweisgesetz sowie die Wehr- oder Zivildienstüberwachung jeweils nur die Tatsache an sich gespeichert werden darf, nicht aber die Gründe. Damit wird die Entscheidung des Gesetzgebers deutlich, eine Datenspeicherung außerhalb des Meldezwecks so eng wie möglich zu halten. Eine Speicherung von Daten für die Erfüllung von Aufgaben der Länder wird sich an diesem Grundsatz ausrichten müssen. Der Meldezweck nach § 1 Abs. 1 läßt nur eine Speicherung von Daten zu, die auch in einem engen Bezug zu den Aufgaben der Meldebehörden stehen. Auch die traditionell von diesen wahrgenommene Verarbeitung personenbezogener Daten zur Erfüllung von Aufgaben der Länder muß daraufhin überprüft werden, ob sie der Entscheidung des Rahmengesetzes für ein Einwohnermeldewesen und gegen ein umfassendes Einwohnerinformationssystem gerecht wird.

Soweit es den Ländern überlassen bleibt, festzulegen, welche Angaben zum Nachweis der Richtigkeit der erhobenen Daten im Melderegister zu speichern sind, sollten sie dieselbe restriktive Haltung einnehmen.

- Sicherstellung der Zweckbindung der Daten
  Die Zweckbindung der Daten soll sicherstellen, daß jeder der eben genannten Datensätze nur im Rahmen seines Zwecks und getrennt von den anderen gespeichert und verarbeitet wird. Die Regelung in § 3 Satz 3 sieht vor, daß die für Bundes- oder Landeszwecke gespeicherten Daten nur insoweit mit den eigentlichen Meldedaten verarbeitet werden dürfen, "als dies zur rechtmäßigen Erfüllung der jeweiligen Aufgabe erforderlich ist". Das Landesrecht wird im einzelnen festzulegen haben, welche der nach § 2 Abs. 2 gespeicherten Daten in Verbindung mit den nach § 2 Abs. 1 und nach § 2 Abs. 3 gespeicherten Daten gemeinsam verarbeitet werden dürfen. In diesem Zusammenhang ist zu fordern, daß die nach § 2 Abs. 3 zu speichernden Daten einer genau definierten Landesaufgabe zugeordnet werden.

- Datenerhebung bei der An- oder Abmeldung
  Keineswegs alle der erwähnten Daten müssen bei der An- oder Abmeldung eines Einwohners über die dabei verwendeten Formulare erhoben werden, § 4 Abs. 1. Die Bürgerfreundlichkeit des Formulars wird hierbei nicht unbedingt daran zu messen sein, wie kurz es ist und wieviel Zeit den Bürger das Ausfüllen kostet. Ein wesentliches Anliegen ist auch die Richtigkeit der gespeicherten Daten. Hierbei ist zu berücksichtigen, daß ein einen größeren Datensatz erhebendes Formular ein Mehr an Datenschutz bedeuten kann. Auf diese Weise kann die Behörde leichter und ohne den Umweg über eine vom Bürger erst auf anderen Wegen festzustellende Fehlverarbeitung den gespeicherten Datensatz kontrollieren.

- Meldegeheimnis
  Nicht zuletzt aufgrund der dezidierten Stellungnahme des Hessischen Datenschutzbeauftragten hat der Gesetzgeber in § 5 das "Meldegeheimnis" eingeführt, das sich direkt an die Bediensteten der Meldebehörden, aber auch an etwaige in einem privatrechtlichen Auftragsverhältnis die Daten der Meldebehörde verarbeitenden Personen wendet. Ihnen und auch dem betroffenen Bürger wird durch diese Norm verdeutlicht, daß das Meldegesetz dem bereichsspezifischen Datenschutz zuzuordnen ist. Dem Landesrecht obliegt es, das Nähere über Zeitpunkt und Form der Verpflichtung auf das Meldegeheimnis zu regeln. Dies sollte in Anlehnung an die bereits vorhandenen Vorschriften etwa zum Hessischen Datenschutzgesetz geschehen. Wichtig ist, daß in diesem Zusammenhang auch bestimmt wird, mit welchen Sanktionen Verstößen gegen das Meldegeheimnis zu begegnen ist.

- Verfahren der Weiterverwendung nicht mehr zur Aufgabenerfüllung erforderlicher Daten
  Das Melderechtsrahmengesetz regelt ausführlich die Ansprüche des betroffenen Einwohners hinsichtlich der Berichtigung unrichtiger Daten, der Löschung unzulässiger Daten und der Einrichtung von Übermittlungssperren, § 6 ff. Dabei räumt es dem Landesrecht einen wesentlichen Spielraum hinsichtlich der Daten von Einwohnern ein, die insbesondere aufgrund Wegzugs oder Todes nicht mehr meldepflichtig sind. § 10 Abs. 2 bis 5 sieht für diese Daten zwei Kategorien vor: einmal die für die Identitätsfeststellung und den Wohnungsnachweis sowie für Wahlzwecke weiterhin erforderlichen Daten, zum anderen die übrigen Daten. Schon oben wurde betont, daß, auch wenn man in der Ermächtigung an den Landesgesetzgeber die Zuweisung eines Regelungsspielraumes sieht, hier auf jeden Fall ein im Vergleich zu § 2 Abs. 1 erheblich verminderter Datensatz vorgesehen ist. Nur die Daten sollen nicht gelöscht werden, die absolut unerläßlich für die genannten Zwecke sind. Konkret ist festzustellen, daß einige der in § 2 Abs. 1 angesprochenen Daten, etwa die Angaben Nr. 8: erwerbstätig/nicht erwerbstätig, Nr. 9: gesetzliche Vertreter (Vor- und Familienname, akademische Grade, Anschrift, Tag der Geburt), Nr. 10: Staatsangehörigkeit, Nr. 11: rechtliche Zugehörigkeit zu einer Religionsgemeinschaft sowie die Angaben zu den Familienangehörigen, nämlich Nr. 15: Ehegatte und Nr. 16: minderjährige Kinder, nicht zu den Daten gehören, die unbedingt für die Identitätsfeststellung oder den Wohnungsnachweis bzw. für Wahlzwecke erforderlich sind. Dem Landesgesetzgeber ist es damit aufgegeben, jedes einzelne Datum insoweit zu überprüfen. Die weiterhin für diese Zwecke erforderlich angesehenen Daten sind nach einer vom Landesgesetzgeber zu bestimmenden Frist gesondert aufzubewahren und besonders zu sichern. Eine Weiterverarbeitung darf nur zu wissenschaftlichen Zwecken, zur Behebung einer bestehenden Beweisnot, zur rechtmäßigen Aufgabenerfüllung der Sicherheitsbehörden oder für Wahlzwecke erfolgen bzw. wenn der Betroffene schriftlich einwilligt. Besonders die Weiterverarbeitung zu wissenschaftlichen Zwecken wird durch Landesrecht im einzelnen zu regeln sein. Dabei sind vor allem die Anforderungen an den Forschungsträger, das Forschungsvorhaben, die Art der Daten und die im Forschungsverfahren beschäftigten Personen zu regeln. Auch hier muß mit aller Deutlichkeit darauf hingewiesen werden, daß es bisher an einer befriedigenden Regelung des bereichsspezifischen Datenschutzes bei der wissenschaftlichen Forschung mangelt. Zu begrüßen wäre es, wenn der Landesgesetzgeber außerhalb des Rahmens eines Landesmeldegesetzes hier zu einer umfassenden Regelung kommen könnte.

Die nicht für diese Zwecke weiter verwendbaren Daten sind prinzipiell zu löschen. Das Landesrecht kann jedoch in zwei Fällen von einer Löschung absehen: Einmal, wenn die Löschung wegen der besonderen Art der Speicherung im Melderegister nicht oder nur mit unverhältnismäßig hohem Aufwand möglich ist (§ 10 Abs. 4), zum anderen, wenn ausdrücklich durch Landesrecht bestimmt wird, daß die Daten vor ihrer Löschung dem zuständigen Archiv zur Übernahme angeboten werden. Diese Lösung ist auch für die zur Identitätsfeststellung und dem Wohnungsnachweis schließlich gesondert aufzubewahrenden Daten eine mögliche Alternativlösung (§ 10 Abs. 5 Satz 2).

Wie für die wissenschaftliche Forschung, so ist auch für das Archivwesen eine bereichsspezifische Datenschutznorm bisher noch nicht ergangen. Hier zeigt sich in gleicher Weise, daß das Melderecht ohne einen Ausbau des bereichsspezifischen Datenschutzes in einer Reihe von anderen Gebieten überfordert ist. Der Gesetzgeber bleibt aufgefordert, diesem Mangel unverzüglich abzuhelfen.

Im Melderecht hingegen sind Frist und Art der gesonderten Aufbewahrung sowie die Sicherung der in begrenztem Maße weiterhin erforderlichen Daten zu regeln.

- Allgemeine Meldepflicht
  § 11 Abs. 2 sieht vor, daß eine Abmeldepflicht des Einwohners entfallen kann, wenn nach Landesrecht der Einwohner sich anschließend in demselben Land anmeldet und sich dort auch anzumelden hat. Die technische Infrastruktur in Hessen läßt derzeit einen Verzicht auf die Abmeldung allenfalls innerhalb der Grenzen eines Kommunalen Gebietsrechenzentrums zu. Nur in diesem Rahmen besteht ein Datenverbund aller beteiligten Meldebehörden. § 11 Abs. 2 könnte Anlaß für den Versuch eines landesweiten Datenverbundes sein. Gegen ein derartiges Landesadreßregister äußerte der Hessische Datenschutzbeauftragte schon mehrfach Bedenken. Der Gesichtspunkt der Bürgerfreundlichkeit kann nicht dazu führen, daß die berechtigten Anliegen des Datenschutzes mit dem Argument zurückgewiesen werden, es sei dem Bürger nicht zuzumuten, bei einem Umzug in das Gebiet eines anderen Gebietsrechenzentrums sich abmelden zu müssen. Jede Veränderung muß hier von einer sorgfältigen Prüfung begleitet werden.
- Mitwirkungspflicht des Wohnungsgebers bei der An- oder Abmeldung
  Das Melderechtsrahmengesetz legt prinzipiell nur eine Mitwirkungspflicht des Wohnungsgebers bei den melderechtlichen Vorgängen vor. Bisher besteht in Hessen eine Pflicht des Wohnungsgebers, einen meldepflichtigen Vorgang bei der Behörde anzuzeigen, wenn der Wohnungsnehmer seiner Meldepflicht nicht genügt. Der Wohnungsgeber konnte aber auch bisher nicht den Wohnungsnehmer selbständig anmelden. Davon wird auch im Hinblick auf ein neues Landesmeldegesetz auszugehen sein.
- Meldepflicht in Beherbergungsstätten
  Das Gesetz überläßt es in § 16 Abs. 2 dem Landesrecht, mitreisende Ehegatten und minderjährige Kinder sowie Teilnehmer von Reisegesellschaften von der Meldepflicht in Beherbergungsstätten auszunehmen. Diese Möglichkeit sollte ausgenützt werden. Der Verzicht auf diese Daten entspricht dem datenschutzrechtlichen Grundsatz, nur die Daten zu erheben, die für eine bestimmte Aufgabenerfüllung unerläßlich sind. Der genannte Personenkreis kann nicht Gegenstand einer besonderen Kontrolle durch die Sicherheitsbehörden sein. Der Grundsatz der Erforderlichkeit und Verhältnismäßigkeit sollte auch dazu führen, daß die Leiter der Beherbergungsstätten oder ihre Beauftragten die ausgefüllten Meldevordrucke für die zuständige Behörde lediglich bereithalten, nicht aber übermitteln müssen, § 16 Abs. 2 Satz 3. Soweit nach § 16 Abs. 4 Satz 2 diese Daten nicht nur zu Zwecken der Gefahrenabwehr oder Strafverfolgung sowie der Aufklärung der Schicksale von Vermißten und Unfallopfern ausgewertet und verarbeitet werden dürfen, ist auf einer Anonymisierung der Daten zu bestehen. Andere öffentlich-rechtliche Stellen wie Fremdenverkehrseinrichtungen können diese Daten auch sinnvoll verwenden, wenn der direkte Personenbezug weggefallen ist.
- Datenübermittlung zwischen den Meldebehörden
  Nach § 17 ist grundsätzlich zwischen der neuen Meldebehörde und der früheren Meldebehörde nur ein begrenzter Datensatz zur Feststellung der Richtigkeit der gemeldeten Daten auszutauschen. § 17 Abs. 1 Satz 2 sieht vor, daß, soweit Meldebehörden desselben Landes beteiligt sind, durch Landesrecht weitergehende Regelungen getroffen werden können. Von dieser Ermächtigung sollte kein Gebrauch gemacht werden. Der gleiche Zweck wird erreicht, wenn bei der Anmeldung nach § 4 der Einwohner einen entsprechend umfangreichen Datensatz in seinem Formular zur Verfügung stellt. Das Problem der fehlerhaften Übermittlung entsteht dadurch nicht in dem Ausmaß.

- Datenübermittlungen von der Meldebehörde an andere öffentliche Stellen
Am ausführlichsten regelt das Gesetz die sogenannte Einzelübermittlung von der Meldebehörde an andere öffentliche Stellen in § 18 Abs. 1. Die Ländergesetze haben insoweit einen nur sehr eng begrenzten Spielraum. So zählt das Gesetz im einzelnen die Auswahl der nach § 2 Abs. 1 erhobenen Daten auf, die an andere Behörden übermittelt werden darf. Das Landesrecht kann demnach nicht vorsehen, daß im Regelungsbereich des § 18 Abs. 1 etwa die Merkmale "erwerbstätig/nicht erwerbstätig" oder "rechtliche Zugehörigkeit zu einer Religionsgemeinschaft" übermittelt werden. In jedem Fall hat die Meldebehörde die Befugnis zu überprüfen, ob die Übermittlung des jeweiligen Datums zur rechtmäßigen Erfüllung ihrer eigenen Aufgaben oder der Aufgaben des Empfängers dient. Die übrigen im Melderegister gespeicherten Daten dürfen nach Abs. 2 nur bei Vorliegen besonderer Gründe und Voraussetzungen übermittelt werden. Dieser Fall liegt dann vor, wenn der Empfänger ohne Kenntnis der Daten zur Erfüllung einer ihm durch Rechtsvorschriften übertragenen Aufgabe nicht in der Lage wäre und die Daten beim betroffenen Einwohner nur mit unverhältnismäßig hohem Aufwand erheben könnte oder von einer Datenerhebung nach der Art der Aufgabe, zu der die Daten erforderlich sind, abgesehen werden muß.
- Datenübermittlungen von der Meldebehörde an die Sicherheitsbehörden
Eine Sonderregelung gilt für die Sicherheitsbehörden. Zunächst erfolgt die Übermittlung an die Sicherheitsbehörden im Einzelfall nach Abs. 1. Die Meldebehörde hat insofern auch zu überprüfen, ob die Übermittlung zur rechtmäßigen Erfüllung der in der Zuständigkeit der Sicherheitsbehörden liegenden Aufgaben erforderlich ist. Nach § 18 Abs. 1 Satz 2 dürfen an die Sicherheitsbehörden auch die Ausstellungsbehörde, das Ausstellungsdatum und die Gültigkeitsdauer von Personalausweis und Paß übermittelt werden. Bei den übrigen als sensitiver angesehenen Daten entfällt nach Abs. 3 eine Überprüfung, wie sie eigentlich gemäß Abs. 2 zu erfolgen hätte. An Stelle dieser Prüfung treten zwei Vorgänge: Zum einen hat die Meldebehörde im Fall der Übermittlung dieser "sensitiveren" Daten auch zu prüfen, ob die Übermittlung zur rechtmäßigen Erfüllung der in der Zuständigkeit der Sicherheitsbehörde liegenden Aufgabe dient, zum zweiten ist diese Übermittlung bei der Sicherheitsbehörde mit Namen und Anschrift des Betroffenen unter Hinweis auf den Anlaß der Übermittlung aufzuzeichnen. Diese Aufzeichnungen sind gesondert aufzubewahren und am Ende des der Aufzeichnung folgenden Kalenderjahres zu vernichten.

  Für die Sicherheitsbehörden gilt somit im Ergebnis auch im Bereich der "sensitiveren" Daten § 18 Abs. 1, ergänzt durch die erwähnte Protokollierungspflicht. Unbeschadet der Einstufung der gewünschten Daten muß die Sicherheitsbehörde der Meldebehörde im Einzelfall und nicht nur pauschal eine Begründung für ihr Ersuchen geben.

  Die Bedeutung dieser Vorschrift muß vor dem Hintergrund der Bestrebungen gesehen werden, durch sog. "on-line"-Verbindungen einzelner Sicherheitsbehörden zu den Dateien anderer Behörden wie Melde- oder Kfz-Zulassungsstellen den Zugriff auf die Dateien dieser Behörden technisch auszuweiten (s. auch 2.1.1). Die Prüfungskompetenz und -pflicht der Meldebehörde bezieht sich jedoch auf jeden einzelnen Übermittlungsvorgang. Sie steht im Gegesatz zu Bestrebungen, durch bei den Sicherheitsbehörden installierte Bildschirmterminals diesen faktisch den gesamten Bestand der Meldedateien zu überlassen. Umso mehr ist ein Rechner-Rechner-Verbund mit weiterreichenden technischen Möglichkeiten ausgeschlossen.

  Die Protokollierungspflicht dient der datenschutzrechtlichen Kontrolle. Sie hat zur Konsequenz, daß sowohl die Datenschutzinstanzen der Behörden als auch der Bundes- und die Landesdatenschutzbeauftragten die Übermittlungspraxis an die Sicherheitsbehörden verstärkt zu kontrollieren haben.
- Regelmäßige Datenübermittlungen von der Meldebehörde an andere öffentliche Stellen
Betrafen die genannten Vorschriften des § 18 Abs. 1-3 Einzelübermittlungen, so sieht § 18 Abs. 4 einen Rahmen für regelmäßige Datenübermittlungen vor. Letztere sollen zulässig sein, wenn durch Bundes- oder Landesrecht unter Festlegung des Anlasses und des Zweckes der Übermittlungen der Datenempfänger und der zu übermittelnden Daten die Voraussetzungen festgelegt sind. Außerdem gilt für diese Fälle das Gebot der Zweckbindung, § 18 Abs. 5. Der Empfänger darf die Daten nur für den Zweck verwenden, zu dessen Erfüllung sie ihm übermittelt wurden. Das Rahmengesetz fordert mit diesen Vorschriften den Bundes- und Landesgesetzgeber zu einem weiteren Ausbau des bereichsspezifischen Datenschutzes auf. Folgende Überlegungen sollten dabei bedacht werden: In jedem Fall müssen Anlaß, Zweck der Übermittlung, Datenempfänger und die zu übermittelnden Daten im einzelnen genau festgehalten werden. Regelmäßige Datenübermittlungen werden ohne eine Prüfung der Rechtmäßigkeit der Übermittlung im Einzelfall vorgenommen, vgl. auch § 6 Satz 2 MRRG. Umso mehr Gedanken muß sich der Gesetzgeber machen, legt er den Datenfluß gesetzlich fest. Dabei darf wiederum nicht

verkannt werden, daß das Melderegister nicht die Grundlage eines umfassenden Einwohnerinformationssystems sein darf. Das Melderechtsrahmengesetz hat sich bewußt auf die Regelung des Einwohnermeldewesens beschränkt. Es entspräche nicht der Zielsetzung des Gesetzes, würde der Gesetzgeber diese Beschränkung über großzügige Übermittlungsregelungen wieder aufheben. So, wie der Landesgesetzgeber nach § 2 Abs. 3 MRRG die Speicherung weiterer Daten zur Erfüllung seiner eigenen Aufgaben an der traditionellen Funktion des Melderegisters und am Zweck des Gesetzes ausrichten muß, gelten ähnliche Beschränkungen auch für neue Regelungen der regelmäßigen Datenübermittlung.

- Übermittlungen innerhalb der Gemeinde
§ 18 Abs. 6 verankert den im Datenschutzrecht entwickelten Grundsatz des sog. funktionalen Behördenbegriffs auch im Meldewesen. Danach darf die Meldebehörde an andere Stellen innerhalb der Gemeinde die sog. Grunddaten nach § 2 Abs. 1 sowie die mit diesen verbundenen Hinweise weitergeben, wenn dies zur rechtmäßigen Erfüllung der in der Zuständigkeit der Empfängereinheit liegenden Aufgaben erforderlich ist. Konkret heißt das, daß das Meldeamt bei Weitergabe von Daten zum Beispiel an das Sozialamt derselben Gemeinde prüfen muß, ob die zu übermittelnden Daten von der Sozialbehörde nach deren Aufgabenstellung benötigt werden. Der "Selbstbedienung" aus dem Melderegister innerhalb der Gemeinde als organisatorischer Einheit ist damit eine Absage erteilt. In gleicher Weise gilt für die sog. sensitiveren Daten nach § 2 Abs. 2 die genannte Schranke nach § 18 Abs. 2. Für das Landesmelderecht stellt sich hier die Aufgabe, konkrete und praktizierbare Regelungen zu treffen.
- Übermittlungen an öffentlich-rechtliche Religionsgemeinschaften
Das Melderechtsrahmengesetz gesteht den öffentlich-rechtlichen Religionsgemeinschaften eine Übermittlung sowohl der Daten ihrer Mitglieder als auch der Daten zu, die deren zum Teil andersgläubige Familienangehörige betreffen, § 19. Dies ist keineswegs unproblematisch und durch ein Sperrecht des betroffenen Angehörigen nach § 19 Abs. 2 Satz 3 nur unzureichend abgemildert. Danach kann der Betroffene verlangen, daß seine Daten nicht übermittelt werden; er ist hierauf bei der Anmeldung hinzuweisen. In vielen Fällen wird der betroffene Familienangehörige bei der Anmeldung gar nicht anwesend sein. Füllt sein der öffentlich-rechtlichen Religionsgemeinschaft zugehöriger Familienangehöriger das Formular aus, so wird der Betroffene ohne besondere Vorkehrungen von diesem Sperrecht nicht Kenntnis nehmen können. Es wird zu prüfen sein, ob in diesem Fall im Landesrecht nicht eine ausdrückliche schriftliche Benachrichtigungspflicht seitens der Meldebehörde verankert werden muß. Keinesfalls sollte von der in § 19 Abs. 2 Satz 2 festgelegten Ermächtigung Gebrauch gemacht werden, von dem andersgläubigen Familienangehörigen mehr als nur Vor- und Familienname, Tag der Geburt, Zugehörigkeit zu einer öffentlich-rechtlichen Religionsgemeinschaft, Übermittlungssperren und Sterbetag zu übermitteln. Für das Merkmal "Zugehörigkeit zu einer öffentlich-rechtlichen Religionsgemeinschaft" muß es genügen, wenn das Landesrecht hier eine Antwort: ja/nein vorsieht. Dies folgt aus der bedenklichen Einschränkung der negativen Bekenntnisfreiheit durch diese Vorschrift.

  Immerhin sieht das Gesetz vor, daß Datenübermittlungen nur dann zulässig sind, wenn sichergestellt ist, daß bei dem Datenempfänger (der öffentlich-rechtlichen Religionsgemeinschaft) ausreichende Datenschutzmaßnahmen getroffen sind. Es ist dem Landesgesetzgeber aufgegeben, hier Konkretes zu bestimmen. Angesichts der sehr weitreichenden Übermittlungsmöglichkeiten nach § 19 muß der Landesgesetzgeber sich hier am Ziel eines möglichst intensiven Datenschutzes orientieren. Dabei ist zu berücksichtigen, daß über die traditionellen christlichen Konfessionen hinaus in den Genuß dieser Regelung auch religiöse Gesellschaften kommen könnten, denen trotz der Verleihung eines öffentlich-rechtlichen Status nicht unbedingt ein der Verfassung entsprechendes Verständnis von Datenschutz zueigen ist.

  Erfahrungen mit dem bisherigen Melderecht in den Ländern haben gezeigt, daß Übermittlungen nicht nur an die Kirchen und ihre örtlichen Gemeinden, sondern auch an einzelne kirchliche Werke, Stiftungen o.ä. wiederholt zu Bedenken Anlaß gaben, ob die Empfänger die notwendigen datenschutzrechtlichen Voraussetzungen erfüllen. Da diese Einrichtungen sich an ihre jeweilige Kirche wenden können, sollte eine direkte Übermittlung durch die staatlich/kommunalen Meldestellen an diese Institutionen im Rahmen des § 19 ausgeschlossen werden.

- Melderegisterauskunft
Das Hessische Meldegesetz hat mit seinem unter Mitarbeit des Hessischen Datenschutzbeauftragten entstandenen § 16 a bereits Erfahrung auf dem Gebiet der Melderegisterauskunft sammeln können. § 21 MRRG unterscheidet sich nicht in der Konzeption aber in Details von § 16 a Hessisches Meldegesetz. Neu ist, daß die sog. einfache Melderegisterauskunft, nach der Vor- und Familiennamen, akademische Grade und Anschriften einzelner bestimmter Einwohner an Dritte übermittelt werden können, ohne jegliche Voraussetzung zu gewähren ist. Ein berechtigtes Interesse ist glaubhaft zu machen, soweit die

erweiterte Melderegisterauskunft gewünscht wird. Sie umfaßt Tag und Ort der Geburt, frühere Vor- und Familiennamen, Familienstand, beschränkt auf die Angabe ob verheiratet oder nicht, Staatsangehörigkeit, frühere Anschriften, Tag des Ein- und Auszugs, gesetzliche Vertreter, Sterbetag und Sterbeort. Es ist zu begrüßen, daß der Betroffene von der Erteilung einer erweiterten Melderegisterauskunft über seine Daten an einen Datenempfänger unverzüglich zu unterrichten ist. Dies gilt nicht, wenn der Datenempfänger ein rechtliches Interesse, insbesondere zur Geltendmachung von Rechtsansprüchen, glaubhaft gemacht hat. Diese Vorschrift dient dem Gläubigerschutz. In ihr wird deutlich, daß das Melderegister, das von seiner Konzeption her kein öffentliches Register ist, zum Teil auch andere Funktionen wahrnehmen soll. Der Landesgesetzgeber hat hier nur geringe Möglichkeiten zur eigenen Gestaltung. Wie schon im bisherigen Recht, ist ihm nun auch ausdrücklich der Auftrag erteilt worden (§ 21 Abs. 3), die Voraussetzungen für eine Gruppenauskunft, das heißt eine Auskunft über eine Vielzahl nicht namentlich bezeichneter Einwohner, zu regeln. Für diese Gruppenauskunft ist Voraussetzung das Vorliegen eines öffentlichen Interesses. Der Landesgesetzgeber wird nicht umhin können, sowohl das öffentliche Interesse genauer zu spezifizieren als auch gemäß § 21 Abs. 3 Satz 2 festzulegen, nach welchen Kriterien die Daten einer vorgegebenen Personengruppe dem Melderegister entnommen werden können. Diese Regelung wird im einzelnen durch eine intensive Diskussion vorbereitet werden müssen.

- Regelung der Sperre einer Auskunft aus dem Melderegister nach § 21 Abs. 5 und 6 MRRG
  Abgestuft nach dem Nachweis eines berechtigten Interesses oder aber der Glaubhaftmachung einer Gefahr für Leben, Gesundheit, persönliche Freiheit oder ähnliche schutzwürdige Belange kann der betroffene Einwohner die Melderegisterauskunft nur der sog. sensitiveren Daten nach § 21 Abs. 2 oder aber auch der Melderegisterauskunft überhaupt verlangen. Diese Regelung ist als begrüßenswerte Fortentwicklung der Norm im Hessischen Meldegesetz anzusehen. Das Landesrecht kann bestimmen, daß die Auskunftssperre befristet wird. Auch diese Möglichkeit ist zu begrüßen; sie löst aber nicht die Grundfrage, welcher Rechtscharakter einer Sperre zukommt, und ob es möglich ist, diese wieder aufzuheben. Eine Lösung dieser Frage bedarf der eingehenden Diskussion.
- Melderegisterauskünfte an Parteien und Wählergruppen sowie in den Fällen der Alters- oder Ehejubiläen
  Eine einfache Melderegisterauskunft ist wie bisher nach dem Hessischen Melderecht schon in den besonderen Fällen der Partei- und Wähleraktionen vor Wahlen (Stichwort: Jungwählerlisten bzw. Seniorenlisten) gemäß § 22 zulässig. Ebenso kann eine einfache Melderegisterauskunft über ein Alters- oder Ehejubiläum von Einwohnern einschließlich des Tages und der Art des Jubiläums gegeben werden. Das Landesrecht kann vorsehen, daß der Betroffene diese Auskunft sperrt. Diese Möglichkeit sieht schon heute das Hessische Meldegesetz vor. An ihr sollte festgehalten werden.
- Übergangsvorschriften
  Eine Reihe von Datenschutzbeauftragten, darunter der Hessische Datenschutzbeauftragte, haben sich dagegen gewandt, daß für die Zeit bis zum 31. Dezember 1985 durch Landesgesetz es dem Polizeivollzugsdienst weiter gestattet sein soll, in bestimmten Fällen Einsicht in die bei der Meldebehörde gespeicherten Daten zu nehmen (§ 24 MRRG). Die Einsichtnahme tritt dabei an die Stelle der Übermittlung, wie sie in § 18 Abs. 1 und 2 festgelegt ist. In diesem Verfahren ist es schwer, an dem Grundsatz festzuhalten, daß nur die für die Aufgabenerfüllung der empfangenden Stelle notwendigen Daten übermittelt werden.
  Wie schon in den Überlegungen zu § 18 Abs. 3 dargelegt wurde, kommt der im Amtshilferecht begründeten Prüfungskompetenz der Meldebehörde vor jeder Übermittlung an eine andere Behörde große Bedeutung zu. Die derzeitige Praxis entspricht damit zentralen Erfordernissen des Datenschutzes nicht. Auch insoweit sollte die Frist in den Landesgesetzen nicht voll ausgeschöpft werden. Eine Frist von drei Jahren muß für die Umstellung ausreichen.

3.1.3 Zusammenfassung

Es kann festgestellt werden, daß das Melderechtsrahmengesetz im wesentlichen eine zu begrüßende Regelung des bereichsspezifischen Datenschutzes enthält. Die Phase der Umsetzung in das Landesrecht birgt jedoch eine Reihe von Gefahren. Nur eine konsequente, die datenschutzrechtliche Substanz des Melderechtsrahmengesetzes berücksichtigende und fortentwickelnde Umsetzung in das Landesmelderecht wird zu einer befriedigenden Lösung führen.

3.2 Bundespersonalausweisgesetz - Anforderungen an das Herstellungsverfahren

Die grundsätzlich positive Beurteilung des Personalausweisgesetzes in meinem Achten Tätigkeitsbericht (vgl. Ziff. 1.2.2) war unmißverständlich geknüpft an die Gesetzmäßigkeit des Herstellungsverfahrens und an bereichsspezifische Datenschutzregelungen im Melderechtsrahmengesetz und für die Dateien der Si-

cherheitsbehörden. Meine schon damals geäußerten Bedenken gegenüber dem Herstellungsverfahren des maschinenlesbaren Personalausweises bei der Bundesdruckerei haben sich zwischenzeitlich bestätigt. In der vorgesehenen Form unterläuft es diejenigen Datenschutzregelungen, die vornehmlich aufgrund der Initiative der Hessischen Landesregierung im Gesetz über Personalausweise verankert worden sind.

Entgegen dem eindeutigen gesetzlichen Verbot des § 3 Abs. 3 Satz 2 Bundespersonalausweisgesetz sollen weitere Angaben als die Seriennummer bei der Bundesdruckerei gespeichert werden.

Angesichts der Bedeutung, die dem Speicherungsverbot von Personalausweisangaben bei der Bundesdruckerei in der öffentlichen Diskussion, den parlamentarischen Beratungen und in den Überlegungen der Hessischen Landesregierung beigemessen worden ist, kann ich bei allem Verständnis für die Wünsche der Verwaltungspraxis ein solches Herstellungsverfahren nicht tolerieren. Hinzu käme die Gefahr, die Legaldefinition der Speicherung in den Datenschutzgesetzen tendenziell aufzulösen.

Ich habe daher sowohl dem Bundesminister des Innern als auch dem Hessischen Innenminister eine Reihe von Vorschlägen unterbreitet, die dem Speicherungsverbot Rechnung tragen. Diese Vorschläge sind unter Hinweis auf den "nicht zu verkraftenden Mehraufwand" und die angestrebte "Fälschungssicherheit" des Personalausweises abgelehnt worden. Diese Argumentation überzeugt nicht. Die geringeren Kosten des bisher angestrebten Verfahrens sind lediglich darauf zurückzuführen, daß man sich zwar für eine möglicherweise praktikablere, nicht aber den gesetzlichen Erfordernissen entsprechende Lösung entscheidet. Der Grundsatz der Gesetzmäßigkeit der Verwaltung läßt eine Differenzierung zwischen Praktikabilität und Gesetzmäßigkeit nicht zu. Vielmehr gehört es zu den politischen Kosten des Rechtsstaats, daß Aufgaben in rechtmäßiger Weise nur durch zuweilen umständlichere Verfahren erfüllt werden können, die mit einem Mehraufwand verbunden sind. Über finanzielle Mehrbelastung läßt sich m.a.W. nur innerhalb vorgegebener gesetzkonformer Alternativen streiten. Das Argument der Fälschungssicherheit steht im Zusammenhang mit der Verwendung eines Aufklebers auf der Rückseite des Personalausweises; das Problem stellt sich allerdings ohnehin auch im geplanten Verfahren bei sich ändernden Wohnungsangaben.

Immerhin hat der Bundesminister des Innern aufgrund meiner Einwände eine modifizierte Version des geplanten Herstellungsverfahrens vorgelegt. Im wesentlichen handelt es sich dabei um eine Verringerung der Speicherungszeit für den Datensatz, der zur Herstellung der Vorderseite des Ausweises gespeichert wird. Der Datensatz, welcher zur Produktion der Rückseite dienen sollte, bleibt dagegen unverändert über einen längeren Zeitraum gespeichert. Das Herstellungsverfahren verstößt mithin - auch nach übereinstimmender Meinung der Datenschutzbeauftragten der Länder und des Bundes - noch immer gegen das Gesetz.

3.3 Sozialdatenschutz bei Leistungsträgern auf Landes-, Kreis- und kommunaler Ebene - Zum neuen 10. Buch des Sozialgesetzbuchs (SGB X)

Herausragendes Ereignis - was den Datenschutz im Sozialwesen angeht - war im abgelaufenen Berichtsjahr die Verabschiedung des 10. Buches des Sozialgesetzbuchs (BGBl. I, Nr. 51/80, S. 1469). Es stellt eine wichtige Aufgabe des Hessischen Datenschutzbeauftragten dar, auf Anforderung von Ministerien an der Formulierung der hessischen Position auch zu Bundesgesetzen, die datenschutzrechtliche Aspekte tangieren, mitzuarbeiten. Dies gilt insbesondere, wenn - wie es beim SGB X der Fall ist - erhebliche Auswirkungen auf Behörden, Körperschaften und Anstalten auf Landes- und Gemeindeebene zu erwarten sind. Im Gesetzgebungsverfahren zum SGB X hat eine intensive Zusammenarbeit meiner Dienststelle mit dem Hessischen Sozialminister und der Staatskanzlei stattgefunden, bei der ich zahlreiche Anregungen und Textvorschläge eingebracht habe.

Das 2. Kapitel des SGB X, das am 1. Januar 1981 in Kraft tritt, enthält eine ausführliche Regelung über den Schutz des Sozialgeheimnisses und der Sozialdaten bei der Datenverarbeitung durch die Sozialleistungsträger. Sie geht von dem Prinzip aus, daß eine Offenbarung personenbezogener Daten nur dann zulässig ist, wenn und soweit der Betroffene im Einzelfall schriftlich eingewilligt hat oder die Voraussetzungen eines abschließend gefaßten Katalogs von gesetzlichen Offenbarungsbefugnissen vorliegen (z.B. zur Erfüllung der Aufgaben der Sozialleistungsträger, für die Durchführung des Arbeitsschutzes usw).

Von besonderer Bedeutung ist die in § 75 enthaltene Regelung über die Offenbarung von Sozialdaten zu Zwecken der Forschung und Planung angesichts der in der öffentlichen Diskussion immer wieder aufgeworfenen Problematik des Verhältnisses von Forschung und Datenschutz. Ich halte diese Vorschrift für in mehrfacher Hinsicht nicht geglückt. Eine von mir erarbeitete und vom Hessischen Kultusminister im Einvernehmen mit dem Sozialminister in die Ausschußberatungen eingebrachte veränderte Fassung dieser Bestimmung konnte jedoch angesichts der Knappheit der Zeit am Ende der Legislaturperiode und ohne ausreichende Erörterung keine Mehrheit mehr finden.

Als einheitliche bereichsspezifische Datenschutzvorschrift für den gesamten Sozialleistungsbereich gilt das SGB X (2. Kapitel) auch für diejenigen Träger, die unter der Aufsicht des Landes stehen (z.B. die Landesversicherungsanstalt) oder Ämter der Kommunen sind (z.B. das Sozialamt). Für problematisch halte ich allerdings in diesem Zusammenhang die Regelung des § 79, nach der künftig bei den Sozialbehörden der Länder, Kreise und Gemeinden neben dem SGB statt der jeweiligen Landesdatenschutzgesetze das Bundesdatenschutzgesetz anzuwenden ist. Sie hat zur Konsequenz, daß bei größeren Verwaltungseinheiten, in die Sozialleistungsträger integriert sind (z.B. Stadtverwaltung mit Sozialamt), unterschiedliches Datenschutzrecht Anwendung findet, was die Rechtsklarheit für Bedienstete und Betroffene wesentlich erschwert. Das vom Gesetzgeber für die Gesetz gewordene Lösung angeführte Argument der notwendigen Einheitlichkeit des Datenschutzrechts bei allen Sozialleistungsträgern vermag diesen erheblichen Nachteil nicht aufzuwiegen.

Trotz der genannten kritischen Einwände zu einzelnen Bestimmungen begrüße ich grundsätzlich die Verabschiedung dieser weittragenden Neuregelung; viele der Fragen, die auf Grund eines erfreulicherweise zunehmenden Datenschutzbewußtseins von Sozialbehörden im vergangenen Jahr an mich gerichtet wurden, werden künftig durch die Bestimmungen des SGB X beantwortet. Hauptproblem für die nahe Zukunft wird es sein, den Inhalt der neuen Vorschriften in den betroffenen Behörden intensiv bekanntzumachen, damit ihre Einhaltung nicht durch Unkenntnis gefährdet wird. Ich habe gegenüber dem Landespersonalamt, das für die Fortbildung in der Landesverwaltung zuständig ist, und gegenüber dem Hessischen Sozialminister meine Bereitschaft erklärt, durch Teilnahme meiner Mitarbeiter an einschlägigen Informations- und Schulungsveranstaltungen an der Bewältigung dieser Aufgabe mitzuwirken.

4. Datenschutzprobleme - Erfahrungen und Beispiele

4.1 Personaldatenschutz im Öffentlichen Dienst

4.1.1 Zum Stand der Automatisierung der Datenverarbeitung in der Personalverwaltung in Hessen

Die Verwendung der automatischen Datenverarbeitung (ADV) im Personalwesen des Landes Hessen ist durch folgende Entwicklung gekennzeichnet:
Vorstellungen der Landesregierung, ein umfassendes Hessisches Personalinformationssystem (HEPIS) zur Erfassung aller Landesbediensteten zu schaffen, sind bisher nicht realisiert worden. HEPIS befindet sich noch immer in der ersten Ausbaustufe, in der in erster Linie statistische bzw. aggregierte Auswertungen aus Datenbeständen vorgenommen werden, die bei der Hessischen Besoldungskasse (für die Beamten) und bei der Zentralen Vergütungs- und Lohnstelle (für die Angestellten und Arbeiter) vorhanden sind. Die Darstellung, die der Hessische Minister des Innern in seiner Antwort auf die Kleine Anfrage der Abgeordneten Korn, Demke u.a. im Dezember 1977 (Landtags-Drucksache 8/5382) gegeben hat, gibt mithin in dieser Frage noch immer im großen und ganzen den derzeitigen Stand wieder.

Dagegen ist die Automatisierung der Datenverarbeitung in Teilbereichen der Personalverwaltung im Berichtszeitraum weiter fortgeschritten. Zu nennen wäre die Komplettierung der vom Hessischen Institut für Bildungsplanung und Schulentwicklung (HIBS) in Wiesbaden betreuten Lehrer-Individualdatei (LID), in der inzwischen persönliche Daten nahezu aller - über 40.000 - hessischen Lehrer gespeichert sind. Im Hessischen Ministerium für Wirtschaft und Technik ist für die über 5.000 Bediensteten des ihm unterstellten Hessischen Landesamtes für Straßenbau ein Personaldatensystem in Vorbereitung (dazu unten 4.1.2). Dort soll ein Verfahren übernommen werden, das die Hessische Zentrale für Datenverarbeitung (HZD) entwickelt hat und für ihre eigenen Mitarbeiter anwendet. In diesen Zusammenhang gehört auch die Einführung der automatisierten Gesprächsdatenerfassung in der Telefonzentrale des Regierungspräsidenten in Darmstadt (dazu unten 4.1.3).

Bei den Kommunen zeichnet sich ein zunehmender Trend zur Datenfernverarbeitung im Personalwesen ab. Als Beispiel zu nennen ist die Stadt Wiesbaden, die in Zusammenarbeit mit dem KGRZ Wiesbaden an der "On-line"-Erfassung für ihre Besoldungs- und Versorgungsverfahren arbeitet.

Angesichts der intensiven datenschutzrechtlichen Diskussion über Personalinformationssysteme, wie sie vor allem für den Bereich der Privatwirtschaft geführt wird, verfolge ich derartige Projekte bei Behörden und sonstigen öffentlichen Stellen des Landes Hessen mit besonderer Aufmerksamkeit. Gerade für den Bereich des Personalwesens lege ich besonderen Wert auf das Prinzip, daß der Hessische Datenschutzbeauftragte frühzeitig, d.h. im Planungsstadium von Automatisierungsvorhaben eingeschaltet wird, um die datenschutzrechtlichen Fragen vor der Vorlage von Berichten an den Landesautomationsausschuß abzuklären; dies ist im abgelaufenen Jahr nicht immer geschehen.

Ungeachtet dieser Ansätze zur Automatisierung im Personalwesen wird auf absehbare Zeit die herkömmliche Personalakte vorrangiges Mittel der Personalverwaltung bleiben. Zwar gelten für Akten die Datenschutzgesetze nicht, doch finden sich in zahlreichen anderen Vorschriften Regelungen, die den Schutz von Personaldaten bezwecken. Zu ihnen gehört - um nur ein Beispiel zu nennen - die Regelung über die Aufbewahrung und Vernichtung von Personalakten. Bei meiner Kontrolltätigkeit sowie bei Schulungsveranstaltungen muß ich jedoch immer wieder feststellen, daß der einschlägige gemeinsame Erlaß der Hessischen Landesregierung ("Aufbewahrungsbestimmungen für Akten und sonstiges Schriftgut der Dienststellen des Landes Hessen" vom 10.8.1978, Staatsanzeiger 35/1978, S. 1706) bei den personalführenden Stellen nicht hinreichend bekannt ist.

4.1.2 Personaldatensystem des Hessischen Landesamtes für Straßenbau

Anhand dieses Vorhabens hat der Hessische Datenschutzbeauftragte in den Gesprächen mit Vertretern des Wirtschaftsministeriums sowie des Landesamtes selbst exemplarisch deutlich gemacht, welche Maßnahmen aus der Sicht des Datenschutzes bei der Installierung von Personalinformationssystemen zu treffen sind:

1. eine klare Festlegung des zur Speicherung vorgesehenen Datenkatalogs unter Beschränkung auf Angaben, die im Rahmen der Zweckbestimmung der Dienst- oder Arbeitsverhältnisse liegen;
2. eine eindeutige Regelung der Zugriffsberechtigung zur Personaldatei, die auch innerhalb der Behörde das Datengeheimnis wahrt und die Tatsache berücksichtigt, daß der sog. "funktionale Behördenbegriff" der Datenschutzgesetze auch innerhalb von Verwaltungseinheiten sowie zwischen über- und nachgeordneten Behörden Übermittlungsbeschränkungen mit sich bringt;
3. Vorkehrungen für die Löschung und Sperrung nicht mehr benötigter Personaldaten;
4. eine wirksame Datensicherung, die sich auch auf die von der EDV-Anlage gefertigten Ausdrucke, Listen usw. erstrecken muß;
5. die Gewährleistung der Benachrichtigung und der Auskunftserteilung an die betroffenen Beschäftigten.

Die genannten Anforderungen gelten zwar für jede Personalverwaltung, auch wenn sie mit manuell geführten Dateien arbeitet, gewinnen allerdings bei der automatisierten Datenverarbeitung besondere Bedeutung.

4.1.3 Automatisierte Speicherung und Auswertung von Telefongesprächen

In Hessen wächst wie anderswo die Zahl der Behörden, die die Installierung automatisierter Telefongebühren-Abrechnungssysteme planen, bei denen - auch zur Kontrolle der Mitarbeiter - Angaben über die Benutzung der einzelnen dienstlichen Telefonapparate registriert werden. Diese Entwicklung bringt, wie ich mehrfach feststellen konnte, Konfliktpotential für das Verhältnis zwischen Dienststellenleitungen, Personalvertretungen und den Bediensteten selbst mit sich. Zu den datenschutzrechtlichen Problemen der Speicherung und Auswertung von Daten über dienstliche oder private Telefongespräche, die Beschäftigte von ihren Dienstapparaten aus führen, habe ich bereits in meinem Siebenten Tätigkeitsbericht (unter 7.3) Stellung genommen. Die vorgesehene Umstellung der Telefonzentrale des Regierungspräsidiums in Darmstadt, an der weitere 31 Dienststellen und in der Endausbaustufe ca. 1.700 Apparate angeschlossen sind, gibt mir Gelegenheit, die dort aufgestellten Grundsätze zu ergänzen und zu aktualisieren.

Aus gegebenem Anlaß folgendes vorweg: Es wäre unangebracht, die ohne Zweifel wichtigen Ziele der Wirtschaftlichkeit und Sparsamkeit der öffentlichen Verwaltung und den Datenschutz in diesem Zusammenhang gegeneinander auszuspielen. Die Einhaltung des Datenschutzrechts zu fordern bedeutet nicht, unberechtigtes Telefonieren im öffentlichen Dienst zu ermöglichen oder zu erleichtern.

Die rechtliche Problematik wird deutlich, wenn - wie in der Anlage beim Darmstädter Regierungspräsidenten vorgesehen - nicht nur pro Telefonat der benutzte Nebenanschluß, Datum, Zahl der Einheiten und Höhe der Gebühr aufgezeichnet werden, sondern auch die Telefonnummer des außenstehenden Angerufenen, und dies auch für - ausdrücklich als solche angemeldete - Privatgespräche gilt; wenn also die Möglichkeit besteht, zur Feststellung privat geführter, aber als dienstlich deklarierter Gespräche Kontrollanrufe bei dem registrierten Teilnehmer durchzuführen. Das Fernmeldegeheimnis schützt nämlich nicht nur den Inhalt, sondern auch die näheren Umstände eines Telefongesprächs, insbesondere die Tatsache seines Zustandekommens sowie die Identität der Beteiligten, den Ort, den Zeitpunkt usw. In der bisherigen Diskussion steht die Frage nach Umfang und Grenzen der Einschränkung des Telefongeheimnisses durch das öffentliche Dienstrecht im Vordergrund, angeregt nicht zuletzt durch zwei widersprüchliche Urteile

des VG und des OVG Bremen (VG Bremen, Neue Juristische Wochenschrift 1978, S. 66 und OVG Bremen, NJW 1980, S. 606). Andere Gesichtspunkte, die die Zulässigkeit der Speicherung von Telefondaten berühren, sind noch zu wenig beachtet worden: Beispielsweise unterliegt auch die bloße Tatsache, daß ein Bürger Sozialleistungsempfänger ist und als solcher mit dem Sozialamt in Kontakt steht, dem Sozialgeheimnis, das auch gegenüber anderen Ämtern derselben Behörde zu wahren ist. Was vor allem nottut, ist ein gründliches Überdenken der "Erforderlichkeit" der Registrierung und Auswertung einzelner Telefonnebendaten im Rahmen des verfassungsrechtlich Zulässigen.

So dient beispielsweise die Datenerfassung bei privaten Telefongesprächen von Bediensteten, die z.B. durch Benutzung einer abweichenden Vorwahlnummer ausdrücklich als privat erkennbar sind, ausschließlich der Sicherstellung der Gebührenabrechnung; eine Kontrolle durch die Dienststellenleitung kommt selbstverständlich nicht in Betracht. Zu diesem Zweck genügt es aber, den Namen oder die Nebenstellennummer des gesprächsführenden Bediensteten und den Betrag oder die Gebühreneinheiten aufzuzeichnen. Alle anderen Angaben sind allenfalls für eine Überprüfung durch den Beschäftigten selbst notwendig, dürfen mithin nur mit seiner Einwilligung festgehalten werden. Die Erforderlichkeit als Maßstab der Zulässigkeit der Speicherung (§§ 3 Abs. 4 HDSG i.V.m. § 23 BDSG) zwingt aber auch bei Dienstgesprächen - was die Verhinderung unberechtigter Telefonate angeht - zur Suche nach Verfahrensweisen, die zu einer Datenaufzeichnung im geringstmöglichen Umfang führen. Die einschlägigen "Fernsprechvorschriften für die staatliche Verwaltung im Lande Hessen" (StAnz. 29/1975, S. 1283) lassen - ungeachtet der Tatsache, daß sie gegenüber den Datenschutzgesetzen unterrangiges Recht darstellen - gerade bei der automatischen Gebührenaufzeichnung ausreichenden Spielraum (vgl. dort unter 3.4.2).

Um die Einhaltung dieser Rechtslage sowie der Prinzipien des Siebenten Tätigkeitsberichts bei dem im Regierungspräsidium Darmstadt geplanten Vorhaben sicherzustellen, habe ich mein positives Votum von einer entsprechenden Ergänzung des vorgelegten Vorberichts an den Landesautomationsausschuß sowie der Vorlage einer amtsinternen Hausverfügung abhängig gemacht, in der insbesondere die Fragen der Zugriffsberechtigung und -kontrolle sowie der Datenlöschung nach erfolgter Abrechnung zu präzisieren sind.

4.1.4 Datenschutz und das Verhältnis zwischen Dienststelle und Personalvertretung

In Anfragen und auf Informationsveranstaltungen bin ich zu wiederholten Malen um Stellungnahme zu der Frage gebeten worden, welchen Einfluß die Datenschutzgesetze auf die Weitergabe persönlicher Daten zwischen Dienststelle und Personalrat haben. Sicherlich gehören die durch die Überschneidung von Personalvertretungs- und Datenschutzrecht aufgeworfenen Rechtsfragen zu den umstrittensten der jüngeren Diskussion um den Datenschutz. Ich nehme daher die Gefahr ernst, daß der Datenschutz unnötige Auseinandersetzungen in die gesetzlich geforderte vertrauensvolle Zusammenarbeit zwischen Behördenleitung und Vertretung der Beschäftigten trägt; entsprechende Vorfälle sind mir mehrfach zur Kenntnis gekommen. Mögliches Konfliktpotential kann jedoch entschärft werden, wenn folgende Grundsätze berücksichtigt werden:

- Die Personalvertretungen sind Teil der "speichernden Stelle", nicht aber "Dritte" im Sinne der Datenschutzgesetze. Die Frage, welche personenbezogenen Daten der Personalrat von der Dienststellenleitung verlangen kann, richtet sich ausschließlich nach den Bestimmungen des Hessischen Personalvertretungsgesetzes (HPVG) und den dort abschließend umschriebenen Aufgaben der Personalvertretung; nicht aber sind die datenschutzrechtlichen Vorschriften über die Übermittlung (§ 3 Abs. 4 HDSG i.V.m. § 24 BDSG) heranzuziehen.
- Soweit der Personalrat persönliche Angaben selbst in Dateien speichert, löscht oder aus Dateien übermittelt, muß er sich grundsätzlich an die Vorschriften der Datenschutzgesetze halten.
- In diesen Zusammenhang gehört auch die Frage der Mitbestimmung des Personalrats bei der Einführung der nach § 10 HDSG vorgesehenen Maßnahmen der Datensicherung. Dazu hat sich bereits im letzten Jahr das Verwaltungsgericht Kassel geäußert (Az. L 25/79). Gegenüber der bei mir anfragenden Leitung eines KGRZ habe ich meine Position wie folgt dargelegt: Da § 10 HDSG nur allgemein die notwendigen technischen und organisatorischen Maßnahmen der Datensicherung umschreibt, entfallen die Beteiligungsrechte des Personalrats nach § 61 HPVG nicht. Allgemeiner formuliert: Bei der Entscheidung über die verschiedenen Möglichkeiten der Datensicherung hat der Personalrat das gesetzlich vorgesehene Beteiligungsrecht.

4.2 Übermittlungsgrenzen beim Informationsaustausch zwischen Behörden

4.2.1 Amtshilfe der Justiz für die Exekutive: Akteneinsichtsrecht für Sicherheitsbehörden?

Besondere Rechtsprobleme wirft - wegen der verfassungsrechtlich gewährleisteten besonderen Stellung der Gerichte - die Amtshilfe der Justiz für die Exekutive auf, soweit es um die Weitergabe personenbezogener Daten geht. Als Beispiel greife ich in diesem Zusammenhang die Frage auf, unter welchen spezifischen Voraussetzungen den Verfassungsschutzbehörden ein Einsichtsrecht in Gerichtsakten zusteht. Dazu habe ich auf Ersuchen des Hessischen Sozialministers anläßlich eines Vorkommnisses beim Arbeitsgericht Frankfurt eine gutachtliche Stellungnahme abgegeben. Die allgemeinere und grundsätzliche Bedeutung dieser Frage veranlaßt mich, im folgenden die wesentlichen Argumentationslinien dieser Stellungnahme wiederzugeben:

Die Frage der Rechtsgrundlage für die Einsicht in Gerichtsakten durch Behörden ist in Rechtsprechung und Literatur umstritten. Für die Arbeitsgerichte wird teils § 46 Abs. 2 ArbGG i.V.m. § 299 Abs. 2 ZPO, teils Art. 35 GG herangezogen. Welcher Auffassung zu folgen ist, braucht für die hier interessierende Problematik nicht entschieden zu werden, da beide Meinungen zum gleichen Ergebnis führen: Geht man mit der überwiegenden Ansicht von Art. 35 GG aus, so ist zu beachten, daß es sich hierbei um eine bloße Rahmenvorschrift handelt, die über Umfang und Grenzen der Amtshilfe nichts aussagt. Das gleiche muß für § 3 des hessischen Gesetzes über die Errichtung eines Landesamtes für Verfassungsschutz gelten. Auch aus dieser Vorschrift läßt sich nicht präzise entnehmen, welche Auskünfte im Wege der Amtshilfe zu erteilen sind. Amtshilfeverpflichtungen bestehen selbstverständlich - was auch für das Landesamt für Verfassungsschutz gilt - nicht voraussetzungs- und schrankenlos. Dies ergibt sich zunächst aus Verfahrensvorschriften, die für die ersuchende und ersuchte Behörde gelten. Dabei können §§ 4 ff. des Hessischen Verwaltungsverfahrensgesetzes (HessVwVfG), auch wenn diese Regelungen hier nicht unmittelbar anwendbar sind, herangezogen werden, da sie Ausdruck allgemeiner Rechtsgrundsätze sind. Nach § 5 Abs. 2 HessVwVfG **darf** die ersuchte Behörde - also hier das Arbeitsgericht - u.a. dann keine Amtshilfe leisten, wenn sie aus rechtlichen Gründen dazu nicht in der Lage ist, oder wenn es sich um Vorgänge handelt, die nach einem Gesetz oder ihren Wesen nach geheimgehalten werden müssen. Weiterhin **braucht** die ersuchte Behörde unter den Voraussetzungen des § 5 Abs. 3 HessVwVfG nicht Amtshilfe zu leisten. In der Literatur dürfte Einigkeit bestehen, daß die ersuchte Behörde insoweit zur Prüfung verpflichtet (bezüglich § 5 Abs. 2) bzw. berechtigt (bezüglich des § 5 Abs. 3) ist. Die umstrittene Frage, ob die ersuchte Behörde darüber hinaus berechtigt ist, die Voraussetzungen des § 5 Abs. 1 HessVwVfG zu prüfen, kann in diesem Zusammenhang dahingestellt bleiben.

Ist somit die ersuchte Behörde zur Prüfung **verpflichtet**, ob Rechtsgründe oder Geheimhaltungspflichten der Amtshilfe entgegenstehen - z.B. weil das Persönlichkeitsrecht eines Prozeßbeteiligten durch die Akteneinsicht verletzt würde -, so benötigt sie auch die zu dieser Prüfung erforderlichen Tatsachen. So kann etwa die Einhaltung des in diesem Zusammenhang zu berücksichtigenden Grundsatzes der Verhältnismäßigkeit nur geprüft werden, wenn von der ersuchenden Behörde mitgeteilt wird, zu welchem Zweck im einzelnen zu benennende tatsächlichen Angaben benötigt werden.

Dem entspricht die Regelung in § 7 Abs. 2 S. 2 HessVwVfG, nach der die ersuchte Behörde für die Durchführung der Amtshilfe verantwortlich ist. Zwar trägt die ersuchende Behörde im Innenverhältnis gegenüber der ersuchten Behörde die Verantwortung für die Rechtmäßigkeit der zugrunde liegenden Maßnahmen. Dies läßt jedoch die Prüfungspflicht der ersuchten Behörde hinsichtlich der Rechtmäßigkeit der Amtshilfe unberührt. Die ersuchte Behörde kann sich im übrigen auch deswegen nicht auf eine Prüfung durch die ersuchende Behörde verlassen, weil bei rechtswidriger Durchführung der Amtshilfe Ersatzansprüche Dritter **nur** gegen die ersuchte Behörde bestehen.

Im Rahmen der Prüfung des Amtshilfeersuchens hat das Arbeitsgericht die Grundsätze zu berücksichtigen, die das Bundesverfassungsgericht in seinen Entscheidungen zur Zulässigkeit der Übersendung von Ehescheidungsakten herausgearbeitet hat (BVerfGE 27, 344; 34, 205). Insbesondere ist der Grundsatz der Verhältnismäßigkeit zu beachten. Dieser verlangt neben der generellen Abwägung zwischen dem Schutz der Privatsphäre und dem öffentlichen Interesse, daß die Maßnahme zur Erreichung des angestrebten Zwecks geeignet und erforderlich ist und daß der mit ihr verbundene Eingriff nicht außer Verhältnis steht. Hierbei ist auch zu prüfen, ob in die Akten insgesamt oder teilweise (z.B. Urteil) Einsicht gewährt werden kann. Die danach gebotene Abwägung setzt voraus, daß die ersuchende Behörde mitteilt, zu welchem Zweck sie welche Tatsachen benötigt. Der bloße Hinweis auf die gesetzliche Aufgabenstellung ermöglicht noch keine Abwägung. Für den Verfassungsschutz kann hier schon deswegen nichts anderes gelten, da es um die Einhaltung von Grundrechten geht.

Diese Grundsätze sind nicht nur im Einzelfall, sondern generell anzuwenden. Eine schrankenlose Amtshilfe wäre mit dem Persönlichkeitsrecht des Betroffenen unvereinbar. Die vom Bundesverfassungsgericht entwickelten Grundsätze betreffen keineswegs nur Fälle, in denen es um den Kernbereich der Intimsphäre geht. In diesem Zusammenahng ist darauf hinzuweisen, daß arbeitsgerichtliche Akten (z.B. in Kündigungsschutzprozessen) vielfach sensitive und potentiell diskriminierende Angaben enthalten. Zu berücksichtigen ist weiterhin, daß eine Behörde im Anwendungsbereich der Datenschutzgesetze personenbezogene Daten nur soweit zur rechtmäßigen Erfüllung der Aufgaben einer anderen Behörde - auch des Landesamts für Verfassungsschutz - weitergeben darf, als die Übermittlung hierfür erforderlich ist (vgl. z.B. § 12 Abs. 1 S. 1 HDSG). Die Übermittlung dient nicht der rechtmäßigen Aufgabenerfüllung, wenn das Persönlichkeitsrecht des Betroffenen durch sie verletzt würde. Die Verantwortung für die Zulässigkeit der Übermittlung trägt die übermittelnde Behörde (vgl. auch die Strafvorschrift in § 32 HDSG). Es ist nicht einsichtig, warum die Rechtslage anders sein sollte, wenn Daten nicht aus Dateien, sondern aus Akten übermittelt werden. Die Übermittlungsvorschriften der Datenschutzgesetze tragen vielmehr der Tatsache Rechnung, daß die Übermittlung personenbezogener Daten einen Eingriff in die Rechtsphäre des Betroffenen darstellt.

Die oben entwickelten Grundsätze gelten generell für die Behandlung von Amtshilfeersuchen durch Behörden. Eine Besonderheit ergibt sich daraus, daß im vorliegenden Fall ein Gericht um Amtshilfe ersucht würde. Zu beachten ist die verfassungsmäßige Stellung der Gerichte, die diese aufgrund des Gewaltenteilungsprinzips und der ihnen garantierten Unabhängigkeit innehaben. Dem Bürger, der sich an ein unabhängiges Gericht wendet, muß Vertrauensschutz gewährt werden. Er darf sich grundsätzlich darauf verlassen, daß die ihn betreffenden Informationen zweckgebunden, d.h. nur für die Abwicklung des Gerichtsverfahrens verwendet werden. Amtshilfe in Form der Weitergabe personenbezogener Daten aus Gerichtsakten kann demnach nur in Ausnahmefällen in Betracht kommen.

Freilich geht es nicht nur um die Prozeßparteien. Auch die Stellung des Richters ist tangiert. Er kann nicht gezwungen werden, etwa vor einer anstehenden Beweisaufnahme, Dritten Einblick in die Akten zu gewähren. Der Bundesgerichtshof hat aufgrund dieser Überlegungen zu Recht entschieden, daß jedenfalls in schwebenden Verfahren die Entscheidung darüber, ob im Wege der Amtshilfe Auskünfte aus den Gerichtsakten zu erteilen sind, richterliche Tätigkeit ist und der Unabhängigkeitsgarantie unterfällt (BGHZ 51, 193). Der Gerichtsvorstand ist deshalb insoweit auch nicht allein zur Entscheidung befugt, sondern er bedarf der Zustimmung des mit dem Fall befaßten Richters oder Spruchkörpers.

Sieht man die Grundlage für die Anforderung von arbeitsgerichtlichen Akten durch Behörden in § 46 Abs. 2 ArbGG i.V.m. § 299 Abs. 2 ZPO, so finden die gleichen Grundsätze Anwendung. Die Notwendigkeit einer umfassenden Abwägung ergibt sich hier aus dem glaubhaft zu machenden "rechtlichen Interesse". Dieses ist zu verneinen, wenn die Einsichtnahme das Persönlichkeitsrecht des Betroffenen verletzen würde.

4.2.2 Amtshilfe von Hochschulen gegenüber dem Landesamt für Verfassungsschutz (LfV)

Eingaben und Beschwerden haben mich veranlaßt, die Praxis der Amtshilfe zwischen hessischen Hochschulen und dem Landesamt für Verfassungsschutz zu überprüfen. Dabei habe ich festgestellt, daß offenbar keine einheitliche Praxis besteht. Die Universität Frankfurt am Main berief sich insoweit noch immer auf einen - nur ihr gegenüber ergangenen - Erlaß des Hessischen Kultusministers aus dem Jahre 1974, obwohl dessen Rechtsgrundlagen zumindest seit dem Inkrafttreten des zweiten Hessischen Datenschutzgesetzes von 1978 nicht mehr gegeben waren. Der Erlaß regelte die Übermittlung von Namen, akademischen Graden, Geburtsdaten und Anschriften von Studenten an das LfV und erklärte sie für generell zulässig.

Ich habe in einer gemeinsamen Besprechung mit Vertretern des Hessischen Kultusministers und des Hessischen Innenministers angeregt, den Erlaß formell aufzuheben und die Datenübermittlung im Wege der Amtshilfe gegenüber dem LfV in einem neuen Erlaß zu regeln, der den Anforderungen des Datenschutzrechts genügt. Der Hessische Kultusminister war dazu nicht bereit; in einem neuen Erlaß aus diesem Jahr traf er lediglich die lapidare Anweisung, zwar wie bisher zu verfahren, aber bei der Auslegung des Erlasses von 1974 von der geänderten Rechtslage auszugehen.

Damit gewinnt allerdings weder die Universitätsverwaltung hinreichende Klarheit darüber, nach welchen Vorschriften sie sich richten muß, noch ist den Voraussetzungen des HDSG genügt. Wie im vorigen Abschnitt (4.2.1) stellt sich auch in dieser Konstellation die prinzielle Problematik des Verhältnisses von Datenschutzrecht und Amtshilfe mit personenbezogenen Angaben. Aus diesem Grund erscheint es mir geboten, auch für diesen Fall meine Rechtsposition klarzustellen.

Die Übermittlungsvorschrift des § 12 HDSG findet Anwendung, da Verfassungsschutz und Polizei um die Übermittlung von Studentendaten ersuchen, die bei den Hochschulen in Dateien verarbeitet werden. Die allgemeinen Amtshilfe-Bestimmungen der § 4 ff. Hessisches Verwaltungsverfahrensgesetz (HVwVfG) sind (nur) insoweit anwendbar, als § 12 HDSG keine spezielle Regelung für die Weitergabe personenbezogener Daten enthält. Zwar obliegt grundsätzlich der anfragenden Behörde die Prüfung und Entscheidung, welche Daten zur Erfüllung der ihr obliegenden Aufgabe erforderlich sind. Ohne Zweifel bedeutet diese Verantwortlichkeit aber nicht, daß eine öffentliche Stelle - unter Berufung auf die allgemeine Pflicht zur Amtshilfeleistung - die Übermittlung persönlicher Daten aller Art verlangen kann und die übermittelnde Behörde von jeder Prüfungspflicht entbunden wäre. Allgemeiner ausgedrückt: Die Amtshilfepflicht als solche ist keine Legitimation für eine Datenübermittlung. Eine Verpflichtung der um Auskunft gebetenen Hochschule zur Mitprüfung ergibt sich vielmehr bereits aus § 5 Abs. 2 und Abs. 3 HVwVfG. Diese Auffassung wird bestätigt durch die ständige Rechtsprechung des Bundesverfassungsgerichts, nach der im Einzelfall abzuwägen ist zwischen dem Schutz der Privatsphäre und dem öffentlichen Interesse an der Weitergabe der Daten. In dem von ihm entschiedenen Fall (BVerfGE 27, 344, 353 f) fordert das Gericht, daß die um Information ersuchende Stelle ihr Begehren substantiiert und mit Tatsachen erhärtet darlegt. Zu prüfen hat der Adressat mithin nicht nur, ob überhaupt, sondern auch, ob alle angeforderten Angaben übermittelt werden müssen. Ich verkenne nicht, daß Belange der öffentlichen Sicherheit im Einzelfall einer substantiierten Darlegung des Auskunftsbegehrens entgegenstehen können. Dies bedeutet aber keineswegs, daß für die Sicherheitsbehörden die von den Datenschutzgesetzen aufgestellten Voraussetzungen für für die Übermittlung nicht gelten. Eine generelle Anweisung an die Hochschule, zumal in einer Selbstverwaltungsangelegenheit wie der Studentenverwaltung, zur Weitergabe eines festgelegten Datensatzes im Wege der Amtshilfe an Polizei und Verfassungsschutz entspricht mithin den Anforderungen von § 12 HDSG nicht. Hinzu kommt ein weiterer rechtlicher Gesichtspunkt: Nicht endgültig geklärt ist die Frage, ob Studentendaten nicht aufgrund der § 15 Abs. 3 Hochschulstatistikgesetz i.V.m. § 11 Bundesstatistikgesetz dem Statistikgeheimnis unterliegen und damit "amtshilfefest" sind, d.h. auch im Wege der Amtshilfe nicht herausgegeben werden dürfen.

Im Hinblick auf die geschilderte Rechtslage unterstreiche ich daher noch einmal meine Aufforderung an den Kultusminister, den neuen Erlaß so zu präzisieren, daß kein Anlaß zur Beanstandung wegen Verstoßes gegen datenschutzrechtliche Bestimmungen besteht.

4.2.3 Einschränkung der "Mitteilungen in Strafsachen" (MiStra)

Nach der "Anordnung über die Mitteilung in Strafsachen" informieren Gerichte und Staatsanwaltschaften eine Vielzahl anderer öffentlicher Stellen (z.B. öffentliche Arbeitgeber, Kammern, Hochschulen, Bundeswehr) über die Einleitung von Ermittlungsverfahren und Verurteilungen von Bürgern. Die MiStra regelt somit - in den Kategorien des Datenschutzes - die Übermittlung personenbezogener Daten aus Akten über einzelne Ermittlungs- oder Strafverfahren.

Die Mitteilung, deren Anordnung dem Richter oder dem Staatsanwalt obliegt, hat zwar zu unterbleiben, "wenn ihr im Einzelfall erhebliche Bedenken entgegenstehen" (vgl. Justizministerialblatt für Hessen Nr. 23 vom 1. Dezember 1977 Nr. 108 - Neufassung der Anordnung über Mitteilung in Strafsachen (MiStra) - und Erlaß des Ministers der Justiz vom 15. November 1977 (1431 - III/6 - 345/77, Justizministerialblatt S 667). Nach Auffassung des Hessischen Justizministers, die auch der seither geäußerten Meinung des Bundesministers der Justiz entspricht, kann, was die strafrechtliche Geheimhaltungsbestimmung des §203 StGB angeht, bei den in der Anordnung ausdrücklich vorgesehenen Mitteilungen an andere Behörden anders als bei sonstigen Mitteilungen (z.B. an Außenstehende) meist "von einem Überwiegen des öffentlichen Interesses ausgegangen werden". Im übrigen sei nicht als Geheimnis anzusehen, was Gegenstand einer öffentlichen Gerichtsverhandlung war.

Nach übereinstimmender Ansicht der Datenschutzbeauftragten des Bundes und der Länder bedarf die MiStra dringend der Überprüfung auf die Notwendigkeit der zahlreichen Mitteilungspflichten. Die Anknüpfung an die Bestimmung der strafrechtlichen Vorschrift über den Geheimnisschutz (§ 203 StGB) genügt hierfür nicht. Zwar betrifft diese Norm Geheimnisse, die im Verlauf eines Strafverfahrens den Beteiligten bekannt werden, erstreckt sich jedoch nach allgemeiner Meinung nicht auf die Tatsache, daß Dritte von einem Strafverfahren als solchem erfahren. Für die Weitergabe persönlicher Daten nach der MiStra sind vielmehr die Grundsätze der Übermittlungsregelung in den Datenschutzgesetzen heranzuziehen. Danach ist die einzelne Mitteilungspflicht daran zu messen, ob die Information für die empfangende Behörde zur rechtmäßigen Erfüllung der in ihrer Zuständigkeit liegenden Aufgabe erforderlich ist - konkreter: ob sie ihr zu Maßnahmen Anlaß geben könnte. Dieses datenschutzrechtliche Prinzip findet nicht zuletzt deshalb Anwendung, weil zum einen die Speicherung der erhaltenen Nachricht bei der empfangenden Stelle der gleichen Zulässigkeitsvoraussetzung unterliegt, zum anderen dieser Grundsatz einen Ausfluß des Verfassungsprinzips der Gesetzmäßigkeit der Verwaltung darstellt.

Vor allem aber hält die von den Landesjustizverwaltungen und dem Bundesminister der Justiz als Verwaltungsvereinbarung getroffene MiStra wichtigen Grundentscheidungen des Gesetzgebers und des Bundesverfassungsgerichts nicht mehr stand. Mit bzw. aufgrund der Datenschutzgesetzgebung des Bundes und der Länder sowie einschlägigen Gesetzen gerade für den Bereich des Strafverfahrens (Bundeszentralregistergesetz) haben Bundesverfassungsgericht und Gesetzgeber unmißverständlich verdeutlicht, daß prinzipiell jede Stelle der öffentlichen Verwaltung mit jenem Minimum an Daten auskommen muß, das zur Aufgabenerfüllung unbedingt benötigt wird.

Die Konsequenz daraus lautet: Da jede Mitteilung in Strafsachen einen - im übrigen erheblichen - Eingriff in die nach Art. 2 Abs. 1 i.V.m. Art. 1 GG geschützte Rechtssphäre des Betroffenen darstellt, bedarf ein solcher Eingriff einer gesetzlichen Grundlage. Zweifellos sind mehrere Mitteilungspflichten, die in den MiStra noch einmal konkretisiert werden, ohnehin gesetzlich geregelt und insofern in diesem Zusammenhang unproblematisch. Andere dagegen haben ihre Grundlage allein in dieser internen Verwaltungsvereinbarung, die mithin als Rechtsgrundlage allein nicht in Betracht kommt. Die Justizminister werden daher zu prüfen haben, ob insoweit für die Mitteilung in Strafsachen eine gesetzliche Grundlage geschaffen werden muß; ihre Absicht, die MiStra aus datenschutzrechtlicher Sicht zu überprüfen, begrüße ich. Dies gilt vor allem für die Anregung des Bundesjustizministers, den Umfang der bisherigen Urteilsmitteilungen zu reduzieren und das Regel-Ausnahmeverhältnis in Nr. 6 Abs. 2 umzukehren, d.h. grundsätzlich nur die Urteilsformeln, die Urteilsgründe jedoch nur in Ausnahmefällen weiterzugeben. Auch die Löschungsvorschriften der Datenschutzregelungen - wie sie sich in entsprechender Weise in den Dateienrichtlinien des BKA bzw. denen über die kriminalpolizeilichen Sammlungen (KpS) wiederfinden - müssen in eine Neuregelung der MiStra Eingang finden. Gleiches gilt für die Unterrichtungspflichten gegenüber dem Betroffenen über erfolgte Mitteilungen.

Meine Initiative aus dem Jahre 1979 hat zu einer breiten Diskussion im Kreise der Datenschutzbeauftragten der Länder und des Bundes und schließlich zu einer Empfehlung geführt, in der die vorstehenden Punkte enthalten sind. Für die nächste Zukunft geht es darum, die konkreten Mitteilungspflichten in der Praxis auf ihre Relevanz im Einzelfall hin zu überprüfen. Diese Überprüfung, die auf meine Anregung hin arbeitsteilig von den Datenschutzbeauftragten der Länder und des Bundes vorgenommen wird, ist noch nicht abgeschlossen.

4.3 Datenschutz im Hochschulbereich - exemplarische Darstellung und Konsequenzen einer Prüfung gemäß § 23 HDSG

4.3.1 Motiv und Ziel der Prüfung

Die Datenverarbeitung in Universitäten und sonstigen Hochschulen ist aus mehreren Gründen für den Datenschutzbeauftragten von besonderem Interesse: Die komplexe Organisationsstruktur der Selbstverwaltungskörperschaft Universität mit der relativen Autonomie der Fachbereiche hat besondere Probleme für den Datenschutz als Organisationsaufgabe zur Folge, die bei hierarchisch geordneten Behörden nicht auftreten. Hinzu kommt die vielfältige Aufgabenstruktur der Hochschule, die Forschung und Lehre, Verwaltung sowie die Dienstleistungsaufgaben des Klinikums integriert. Aber auch quantitativ gesehen gehören die Hochschulen zu den größten "Datenverarbeitern" in Hessen. Diese Faktoren haben mich veranlaßt, bei der Universität Frankfurt am Main eine datenschutzrechtliche Prüfung gemäß § 23 HDSG durchzuführen. Mit Rücksicht auf den exemplarischen Charakter dieses Kontrollbesuchs erscheint mir eine ausführliche Wiedergabe des abschließenden Prüfungsberichts angebracht. Dies mag anderen Hochschulen mit den gleichen Mängeln und Schwierigkeiten helfen, ihre Datenschutzprobleme zu lösen.

Die Prüfung der Johann Wolfgang Goethe-Universität hat im Mai 1980 stattgefunden und erstreckte sich auf die Verwaltung der Universität, das Klinikum und einige Fachbereiche, wobei diejenigen außer Betracht blieben, deren Forschungsinteresse sich nicht auf personenbezogene Daten richtet.

Ziel der Prüfung der Johann Wolfgang Goethe-Universität war die Feststellung, inwieweit die Bestimmungen des Hessischen Datenschutzgesetzes sowie andere Vorschriften über den Datenschutz eingehalten werden. Maßstab der Prüfung war der Katalog der "Maßnahmen zur Durchführung des Hessischen Datenschutzgesetzes durch die Behörden und sonstigen öffentlichen Stellen des Landes" (vgl. Erlaß des Hessischen Ministers des Innern vom 2.10.1978 - II A 4 - 3 d 10-15; Staatsanzeiger 41/1978 S. 2011). Mittel der Prüfung waren vom Hessischen Datenschutzbeauftragten entwickelte standardisierte Checklisten für Rechenzentren und Datenendgeräte, die Besichtigung des Hochschulrechenzentrums, der Anwenderräume und der ausgewählten Abteilungen und Institute, Interviews mit Anwendern, den Datenschutzbeauftragten und anderen verantwortlichen Mitarbeitern der Universitätsverwaltung und des Klinikums.

4.3.2 Organisation und Ablauf der Prüfung

Jede sinnvolle Kontrolle des Datenschutzes hat zur Grundlage, daß die Organisationsstrukturen und die Informationsströme detailliert dargestellt werden können. In diesem Zusammenhang schreibt das Hessische Datenschutzgesetz vor, daß eine Übersicht über die Art der gespeicherten personenbezogenen Daten und über die Aufgabe, zu deren Erfüllung die Kenntnis der Daten erforderlich ist, sowie deren regelmäßige Empfänger zu führen ist (vgl. § 5 Satz 2 Ziff. 1 HDSG). Die von der Universität vorgelegte Übersicht war jedoch nicht vollständig. Sie enthielt lediglich diejenigen Dateien der Verwaltung und der Universitätsklinik, die bereits zum Register des Hessischen Datenschutzbeauftragten gemeldet worden waren. Dagegen bestand kein Überblick über die Forschungsdateien, in denen personenbezogene Daten enthalten sind, bis auf diejenigen des Fachbereichs Medizin, die aus dem Dateienregister ersichtlich sind. So sind z.B. verschiedene Projekte in sozialwissenschaftlichen Fachbereichen, mit denen der Hessische Datenschutzbeauftragte durch Bürger- oder Behördenanfragen befaßt worden ist, der Universitätsverwaltung als für den Datenschutz verantwortliche Institution offensichtlich nicht bekannt gewesen.

Eine weitere wesentliche Voraussetzung für eine effektive Kontrolle des Datenschutzes ist ein Überblick über die gesamte Hardwareausstattung einschließlich der Peripheriegeräte, die in der Universität installiert sind. Eine vollständige Inventarliste der eingereichten Datenverarbeitungsanlagen lag jedoch zum Zeitpunkt der Prüfung nicht vor. Der Kultusminister hat jedoch zugesichert, Anfang 1981 einen vollständigen Ausstattungsplan vorzulegen. Allerdings bleibt anzumerken, daß sich die Verpflichtung, Ausstattungspläne aufzustellen und fortzuschreiben, bereits aus §§ 18 Abs. 2 Ziff. 8, 23, 24 Abs. 2 Hessisches Hochschulgesetz ergibt. Der Einwand der Hochschule und des Kultusministers, eine vollständige Liste sei auch nicht sinnvoll, da nicht auf jeder Anlage personenbezogene Daten verarbeitet werden, ist bei näherer Betrachtung wenig stichhaltig. Dem Datenschutzbeauftragten muß es unbenommen bleiben, die gesamte Informationsverarbeitungskapazität des zu prüfenden Teils der öffentlichen Verwaltung daraufhin zu untersuchen, ob in ihm unbefugt oder befugt personenbezogene Daten verarbeitet werden. Effektive Kontrolle kann sich daher nicht auf diejenige Datenverarbeitungsanlage beschränken, die von der zu prüfenden Organisation als Anlage definiert wird, auf der ausschließlich personenbezogene Daten verarbeitet werden dürfen. Ich sehe mich daher auch in Zukunft bei jeder Prüfung veranlaßt, eine unvollständige Liste der installierten Hardware zu beanstanden.

Darüber hinaus konnte die Universität bis auf die von der zentralen Datenverarbeitung angewandten Programme keine Programmbibliothek vorlegen (vgl. § 5 Satz 2 Ziff. 2 HDSG). Zwar ist der Einwand der Universität in ihrer Stellungnahme zum Bericht nicht von der Hand zu weisen, daß Forderungen nach einer vollständigen Dokumentation aller an den Anlagen eingesetzten Programme nicht realistisch sind. Sie führt dazu das Beispiel des Programmierkurses mit 100 Studenten innerhalb einiger Wochen an, in dem je Student jeweils 10 bis 20 Programme geschrieben werden mit der Folge, daß nicht für jedes dieser Programme das Verfahren vollständiger Programmdokumentation durchgehalten werden kann. Eine solche Forderung ist auch durch den Hessischen Datenschutzbeauftragten nicht aufgestellt worden. Vielmehr kommt es darauf an, daß außer den administrativen Programmen der Hochschule auch diejenigen dokumentiert werden müssen, mit Hilfe derer zu Forschungszwecken personenbezogene Daten verarbeitet werden. Hierbei muß noch einmal deutlich gemacht werden, daß bei der Bewertung der Maßnahmen nach § 10 HDSG die "Dienstanweisung zur Gewährleistung des Datenschutzes und der Datensicherung im Hessischen Datenverarbeitungsverbund" (DASCH) nicht schematisch als Prüfungsgrundlage herangezogen wurde, da die besonderen Bedingungen eines Hochschulrechenzentrums durchaus auch bei den Prüfungsmaßstäben Berücksichtigung gefunden haben. Nicht zuletzt deshalb waren auch der Datenschutzbeauftragte der Universität und die Leitung des Hochschulrechenzentrums der Ansicht, daß diese Dienstanweisung die besonderen Bedingungen des Forschungsrechenzentrums nicht berücksichtige und infolgedessen auch nicht anwendbar sei; vorrangige Aufgabe für das Hochschulrechenzentrum sei vielmehr, den Benutzern aus Forschung und Lehre Datenverarbeitungskapazität anzubieten und Hilfe bei der Implementierung und Entwicklung von Programmen zu leisten. Dementsprechend befaßten sich die mir bekanntgewordenen Verfahrensrichtlinien und Anweisungen der Universität hauptsächlich mit Maßnahmen, die einen möglichst reibungslosen technischen Ablauf im Rechenzentrum sicherstellen. Datenschutzmaßnahmen spielten hierbei eine untergeordnete Rolle.

Die Freiheit von Forschung und Lehre bedingt zwar einerseits möglichst große Offenheit des Zugangs zu allen Einrichtungen. Dies darf aber nicht dazu führen, daß gesetzlich geschützte Belange Dritter beeinträchtigt werden. Immerhin muß auch die Konzeption des Hochschulrechenzentrums als sog. Multi-user-Anlage sich daraufhin befragen lassen, welchen Datensicherungsstandard es angesichts der Tatsache anzubieten gedenkt, daß z.B. das Zentrum für Psychiatrie im Hochschulrechenzentrum der Universität Frankfurt personenbezogene Daten höchst sensitiver Art verarbeitet. Da diese Daten u.a. der ärztlichen Schweigepflicht unterliegen, die über § 203 StGB strafrechtlich bewehrt ist, darf deren Verarbeitung nur

unter der Voraussetzung einer optimalen Datensicherung erfolgen, wie sie auch in den DASCH-Richtlinien für den Hessischen DV-Verbund festgeschrieben sind. Dies muß umso mehr gelten, als im Rechenzentrum auch über ein Datenendgerät alle Personal- und Beschäftigtendaten der Universität in Kommunikation mit dem Hochschulverbundrechenzentrum in Darmstadt verarbeitet werden. Nicht zuletzt an diesen Tatsachen zeigt sich die Komplexität der Datenschutzkonzeption einer Universität als Organisationsaufgabe. Vorhandene Organisationsmängel und Informationsdefizite aber wirken sich notwendig auf die Effektivität des Datenschutzes aus. Dies heißt in der Konsequenz - neben einer Verbesserung der technischen und baulichen Datensicherungsmaßnahmen -, daß die Universität einen effektiven Datenschutz nur gewährleisten kann, wenn die jeweils Verantwortlichen wissen, was, wann, auf welcher Anlage und mit welchem Programm verarbeitet wird.

Die Prüfung hat zwar eindeutig ergeben, daß das Hochschulrechenzentrum bemüht ist, Maßnahmen der Datensicherung und des Datenschutzes zu ergreifen. Allerdings hängt deren Realisierung weitgehend von der Mitwirkung der Benutzer ab. Niemand außer dem jeweiligen Benutzer, ob Student oder Hochschullehrer, ist darüber informiert, welche Daten mit welchen Programmen auf den dortigen Anlagen verarbeitet werden, es sei denn, er beantragt eine Sonderrechennummer, die die Verarbeitung personenbezogener Daten erlaubt. Die zuständigen Instanzen und Gremien der Universität wissen bis auf die jeweils verwandte Rechnerzeit nicht, was auf ihren Rechenanlagen geschieht. Dies gilt weitgehend auch für die im Hochschulrechenzentrum tätigen Mitarbeiter. Die Verarbeitung personenbezogener Daten im Hochschulrechenzentrum ist angesichts dieser Sachlage für die für den Datenschutz Verantwortlichen weitgehend nicht überschaubar. Auch die Gebäudesicherung des Hochschulrechenzentrums gab Anlaß zur Kritik, obwohl die baulichen Maßnahmen nicht Gegenstand eingehender Prüfung waren. Darüber hinaus läßt die Organisation des Hochschulrechenzentrums ebenfalls zu wünschen übrig, da klare Funktionstrennungen nicht erkennbar waren. Ein sog. closed-shop-Betrieb, der zwar angestrebt ist, ist unter den gegebenen baulichen Bedingungen kaum zu verwirklichen. Anlaß zur Kritik gab weiter die Zugangsregelung, das Datenträgerarchiv und die Zulassung von Benutzern zum Rechnerbetrieb, so daß die Datensicherungsmaßnahmen des Hochschulrechenzentrums beanstandet werden müssen. Allerdings wurde in einem Gespräch mit der Universitätsverwaltung und Vertretern des Kultusministers vereinbart, daß unter Beteiligung des Hessischen Datenschutzbeauftragten für die Bedingungen der Forschungsdatenverarbeitung Richtlinien und Empfehlungen erarbeitet werden sollen, die für den Hochschulrechnerverbund angemessene Sicherungsstandards enthalten.

4.3.3 Datenschutz in Forschungseinrichtungen

Der Informationsstand über und die Sensibilisierung für den Datenschutz im Bereich wissenschaftlicher Forschung sind sehr unterschiedlich. Besonders hervorzuheben war hierbei die Bemühung des Sonderforschungsbereichs III (SPES-Projekt), der eine vorbildliche Datenschutzkonzeption für seine Forschungsdateien entwickelt und implementiert hat. Weit über die rechtlichen Anforderungen hinaus wird ein Dateienhandbuch in Lose-Blatt-Form geführt, das in seiner Differenziertheit richtungsweisend ist. Neue Mitarbeiter werden im Rahmen eines jährlich veranstalteten Kolloquiums über die Grundprobleme des Datenschutzes in der wissenschaftlichen Forschung informiert. Dieses Beispiel zeigt, daß die Verwirklichung des Datenschutzes und der Datensicherung auch im Bereich der wissenschaftlichen Forschung ohne Beeinträchtigung für Forschungsziele und -methoden zu verwirklichen ist. Im Gegensatz dazu ist in anderen Fachbereichen Datenschutz noch nicht einmal als Problem definiert, selbst dort, wo eigene Rechner betrieben werden.

Diese Situationsanalyse kann einschneidende Folgen für die wissenschaftliche Forschung haben. So werden angesichts dieser Sachlage Klagen über mangelnden und schleppenden Datenzugang zu personenbezogenen Daten von Behörden und anderen Institutionen wenig glaubhaft, wenn sich die um Datenübermittlung für Forschungszwecke ersuchte öffentliche oder private Stelle darüber im klaren ist, daß die Hochschulen und die Einrichtungen unabhängiger Forschung selbst den Datenschutz für die übermittelten personenbezogenen Daten nicht gewährleisten können. Es liegt daher im eigenen Interesse der Hochschule, die Datenverarbeitung mit personenbezogenen Daten zu Forschungszwecken betreiben will, ausreichenden Datenschutz und Datensicherung sicherzustellen. Universitätsverwaltung und Fachbereiche müssen sich daher der Tatsache bewußt werden, daß ohne die Implementierung eines effektiven Datenschutzes eine der wichtigsten Ressourcen für empirische Forschung potentiell abgeschnitten wird: der Zugang zu vorhandenen personenbezogenen Daten bei öffentlichen wie privaten Stellen.

4.3.4 Datenschutzprobleme in den Abteilungen der Universitätsverwaltung

Die Prüfung umfaßte folgende Auswahl von Verwaltungsabteilungen der Universität: Studentenabteilung, Akademisches Auslandsamt, Wahlamt, Personalabteilung, Lohn- und Gehaltsabteilung. Sie ergab, daß Problembewußtsein und Interesse der Mitarbeiter für Datenschutz und Datensicherung vielfach

vorhanden sind, daß aber in einer Reihe von Punkten Verbesserungen möglich und notwendig sind. Dies sind insbesondere die Verpflichtung auf das Datengeheimnis (§ 9 HDSG), die Löschung und Archivierung personenbezogener Daten und die Organisation der Amtshilfe. Ein übergreifendes Problem der Organisation ist das unzureichend definierte Verhältnis von jeweiliger Fachabteilung und EDV-Abteilung. Ich konnte feststellen, daß Fachabteilungen keinen Überblick über alle Phasen der Verarbeitung der ihrer Verantwortung unterliegenden personenbezogenen Daten haben, obwohl sie nach dem Datenschutzgesetz "speichernde Stelle" im Sinne des "funktionellen Behördenbegriffs" sind. Ihre datenschutzrechtliche Verantwortlichkeit kann eine Verwaltungsabteilung dann nicht ausreichend wahrnehmen, wenn ihr nicht bekannt ist, welche Auswertung oder Übermittlung durch die zentrale Datenverarbeitung oder andere Stellen der Universität aus Studentendateien vorgenommen werden. Um zu vermeiden, daß organisatorische Unklarheiten im Ergebnis zu einer Verwischung von Zuständigkeiten und Verantwortlichkeiten führen, wie sie das Datenschutzgesetz vorsieht, empfiehlt sich folgende Konsequenz: Aufträge an die zentrale Datenverarbeitung für personenbezogene Daten dürfen nur von derjenigen Abteilung erteilt werden, die "speichernde Stelle" dieser Dateien ist. Datenverarbeitungsaufträge anderer Organisationseinheiten der Universität müssen über die zuständige Abteilung geleitet werden. Nur auf diese Weise können außerdem die verantwortliche Verwaltungsspitze bzw. der Datenschutzbeauftragte der Universität die notwendige Transparenz der Informationsströme innerhalb der Administration herstellen.

4.3.5 Datenschutz im Universitätsklinikum

Im Klinikbereich werden in erheblichem Umfang personenbezogene Daten verarbeitet. Schon im Hinblick auf die zur Verfügung stehende Zeit war eine Überprüfung nur in Form von Stichproben möglich. Auswahlkriterien waren dabei vor allem der Umfang der Datensammlung, die Sensitivität der gespeicherten Daten sowie der Einsatz elektronischer Datenverarbeitung.

Kontrollbesuche fanden statt in der Klinikums-Verwaltung sowie in den Zentren für Innere Medizin, Psychiatrie und medizinische Informatik. Mit Ausnahme des letzteren waren zahlreiche Mängel insbesondere im Hinblick auf die Datensicherung, die ausreichende Verpflichtung von Mitarbeitern auf das Datengeheimnis und die Vernichtung von Patientenunterlagen festzustellen. Folgende Punkte von übergreifendem Interesse will ich hervorheben:

- Die Klausel betr. die Einwilligung in die Datenverarbeitung im Formularaufnahmeantrag entspricht in ihrer derzeitigen Form nicht den gesetzlichen Anforderungen. Ich stehe mit der Hessischen Krankenhausgesellschaft in Kontakt, um zu einer korrekten Neuformulierung zu kommen.
- Kliniken, die Patientendaten nicht selbst, sondern im Hochschulrechenzentrum verarbeiten lassen, bleiben für die Einhaltung notwendiger Datenschutzvorkehrungen auch dort verantwortlich.
- Von besonderer Bedeutung sind effektive Datensicherungsmaßnahmen in den Archiven, die - wie etwa das des Zentrums für Psychiatrie - höchst sensitive Daten über Jahrzehnte hinweg aufbewahren.

4.3.6 Konsequenzen und Vorschläge

Trotz einer Stellungnahme der Universität, die mir vorliegt und einem anschließenden Gespräch mit der Universität und dem Kultusminister ist das Resultat im wesentlichen das gleiche geblieben. Zwar hat sich die Johann Wolfgang Goethe-Universität als erste Landesuniversität bemüht, den Datenschutz in ihrem Zuständigkeitsbereich zu realisieren. So hat der Präsident bereits 1977 zwei Datenschutzbeauftragte bestellt. In verschiedenen Hausverfügungen hat seither die Intention der Universitätsverwaltung ihren Niederschlag gefunden, alle Bediensteten und Angehörigen im Sinne des Datenschutzes zu orientieren. Keine andere Hochschule ist ihrer Meldepflicht zum Dateienregister des Hessischen Datenschutzbeauftragten im gleichen Umfang nachgekommen wie die Universität Frankfurt. Dennoch erlaubt die Prüfung Feststellungen, die ernsthafte Überlegungen und Maßnahmen zur Verbesserung des Datenschutzes in vielfacher Hinsicht erfordern.

Vor allem wird die Universität Initiativen ergreifen müssen, um die technischen und organisatorischen Maßnahmen der Datensicherung im Hochschulrechenzentrum nicht nur zu verbessern, sondern teilweise überhaupt erst zu realisieren. Obwohl die besonderen Bedingungen eines Forschungszentrums bei der Prüfung und deren Kriterien und dem anschließenden Gespräch ausdrücklich berücksichtigt worden sind, lassen jedoch die Ergebnisse keinen Zweifel zu: Die Datensicherungsmaßnahmen sind, soweit personenbezogene Daten verarbeitet werden, unzureichend. Die Organisation der Benutzerinformation über Probleme des Datenschutzes bedarf einer Veränderung, die tatsächlich jeden Benutzer und jedes Datenverarbeitungsprojekt an der Universität erfaßt. Zweifelsfrei ist allerdings ebenso, daß die baulichen Bedingungen eine optimale Datensicherung im Hochschulrechenzentrum nur begrenzt zulassen. Fortschritte sind aber auch ohne den von verschiedenen Seiten geforderten und angesprochenen Funktionsbau

für ein Hochschulrechenzentrum denkbar. Empfohlen wurde, die Datenverarbeitung für Forschungs- und Verwaltungszwecke funktionell zu trennen und sie im Hinblick auf einen closed-shop-Betrieb besser zu organisieren. Darüber hinaus sollte die Universität die Gebäudesicherung und den Feuerschutz im Hochschulrechenzentrum verbessern. Zu den Anforderungen, die durch das Hessische Hochschulgesetz und das Hessische Datenschutzgesetz an sie gestellt werden, gehören insbesondere das Aufstellen und Fortschreiben einer Ausstattungsliste der installierten Hardware, eine - soweit möglich - vollständige Gesamtübersicht über die Dateien mit personenbezogenen Daten sowie eine Bibliothek derjenigen Programme, mit denen personenbezogene Daten verarbeitet werden. Besondere Aufmerksamkeit verdienen, was die Rechtmäßigkeit der Datenverarbeitung im Sinne des Hessischen Datenschutzgesetzes angeht, die vielfältigen Probleme der Amtshilfe, bei der Zuständigkeiten bzw. Entscheidungsgang ungeregelt erschienen. Zu begrüßen wären weiterhin Richtlinien, die sich des Archivproblems annähmen. Wünschenswert bleibt auch nach wie vor eine allgemein verbesserte Information von Verwaltung, Fachbereichen und Kliniken über den Datenschutz. Abschließend bleibt noch darauf hinzuweisen, daß ein Referent für den Datenschutz im Sinne von § 27 des Hessischen Hochschulgesetzes bestellt werden muß, der für die Durchführung des Datenschutzes an der Universität dem Präsidenten unmittelbar verantwortlich berichtet. Ich strebe an, das Thema Datenschutz und Datensicherung im Hochschulrechnerverbund auf der AKHH zu thematisieren und den DASCH entsprechende Richtlinien für den Verbund der Hochschulrechenzentren anzuregen.

4.4 **Schutz von Wählerdaten - Beispiel: Die neue Hessische Kommunalwahlordnung (KWO)**

Bei der Vorbereitung und Durchführung von Wahlen zu den Parlamenten von Bund, Ländern und Gemeinden werden personenbezogene Daten aller volljährigen Bürger in großem Ausmaß verarbeitet. Wählerverzeichnisse stellen umfängliche Datensammlungen dar, in denen ein Großteil der Bevölkerung enthalten ist. Aus der Sicht des Datenschutzes gilt es abzuwägen zwischen der Notwendigkeit, Wählerdaten für die ordnungsgemäße Abwicklung der Wahlen offenzulegen und den berechtigten Belangen der Bürger, soweit der Schutz ihrer Privatsphäre betroffen ist. Die anstehende Kommunalwahl im März 1981 erscheint mir daher Grund genug, im folgenden auf die Problematik des Schutzes von Wählerdaten anhand der neuen Hessischen Kommunalwahlordnung vom 26. September 1980 (GVBl. I S. 351) einzugehen.

In meiner Stellungnahme gegenüber dem Hessischen Innenminister zu dem Entwurf dieser Kommunalwahlordnung hatte ich auf folgende verbesserungsbedürftige Punkte hingewiesen:

1. Nach § 12 Abs. 3 d.E. hatte der Wahlberechtigte das Recht zu verlangen, daß in dem Wählerverzeichnis während der Auslegungsfrist der Tag seiner Geburt unkenntlich gemacht wird. Ich wies darauf hin, daß dieses Recht ohne eine ausführliche Unterrichtung des Bürgers über seinen Anspruch leerlaufen würde. Damit verband sich der Vorschlag, auf der Wahlbenachrichtigung (§ 10) eine entsprechende Information des Bürgers aufzudrucken. Hilfsweise schlug ich vor, diese Information im Rahmen der öffentlichen Bekanntmachung über die Auslegung des Wählerverzeichnisses und die Erteilung von Wahlscheinen (§ 11) zu geben. Der Hessische Minister des Innern hat in § 11 Nr. 2 KWO die letztgenannte Alternative aufgenommen.
2. § 12 Abs. 4 KWO sieht vor, daß die Anfertigung von Auszügen oder Abschriften aus dem Wählerverzeichnis auf zwei Wegen erfolgen kann: Entweder nach Erlaubnis des Gemeindevorstands durch Wahlberechtigte oder Träger von Wahlvorschlägen selbst, wenn sie ein berechtigtes Interesse im Zusammenhang mit der Wahl darlegen oder durch den Gemeindevorstand gegen Erstattung der Auslagen. Die Auszüge bzw. Abschriften dürfen nur Namen und Anschriften, nicht aber die Geburtstage der Wahlberechtigten enthalten. Sie dürfen nur für Zwecke der Wahl verwandt und Dritten nicht zugänglich gemacht werden.

   In meiner Stellungnahme zum Entwurf hatte ich vorgeschlagen, nur die zweite Möglichkeit zuzulassen, da die Erstellung von Abschriften ausschließlich durch die zuständige Behörde die Einhaltung der genannten Datenschutzvorkehrungen besser sicherstellen würde. Der Hessische Minister des Innern ist diesem Vorschlag nicht gefolgt und hat dies damit begründet, daß die praktischen Auswirkungen in der zur Verfügung stehenden Zeit nicht ausreichend geprüft werden könnten. Zudem erfordere es die Einheitlichkeit der Wahlordnungen für die Bundestags-, Europa-, Landtags - und Kommunalwahlen, daß einheitliche Wählerverzeichnisse zu führen seien. Er sagte jedoch zu, im Hinblick auf verschiedene Lösungsmöglichkeiten des angesprochenen Problems eine bundeseinheitliche Klärung herbeizuführen.
3. Weiterhin hatte ich moniert, daß die Übermittlung der personenbezogenen Daten eines Wahlberechtigten an andere Wahlberechtigte oder Träger von Wahlvorschlägen nach § 12 Abs. 4 KWO von dem Betroffenen nicht gesperrt werden kann. Nach § 16 a Abs. 4 Hessisches Meldegesetz (HMG) kann nämlich unter bestimmten Umständen die Weitergabe der gleichen Angaben an Dritte aus dem

Melderegister gesperrt werden. Ohne eine entsprechende Norm auch in der Wahlordnung kann das Sperrecht im Meldegesetz umgangen werden. Zwar ist das Wählerverzeichnis - anders als das Melderegister - nur während eines kurzen Zeitraums zugänglich. Auch erlaubt es nur begrenzt, etwaige Wohnungswechsel eines Einwohners nachzuvollziehen. Nichtsdestoweniger sieht § 16 a Abs. 4 HMG aus gutem Grund vor, daß unter bestimmten Voraussetzungen eine Auskunft über Namen und Anschriften eines Einwohners in keinem Fall gegeben werden darf; dem entspricht nun auch § 21 Abs. 5 Melderechtsrahmengesetz. Eine absolute Sperre ist nach dieser Bestimmung dann zu gewähren, wenn "eine Gefahr für Leben, Gesundheit, persönliche Freiheit oder ähnliche schutzwürdige Belange" aus der Auskunft erwachsen kann. Auch die Wahlordnungen müssen dem Bürger die Möglichkeit geben, sich mit Hilfe einer Sperre der Übermittlung aus dem Wählerregister bei Vorliegen einer solchen Situation schützen zu können.

Der Hessische Minister des Innern hat meinen Vorschlag nicht übernommen und sich dabei wiederum auf die angeblich notwendige Einheitlichkeit aller Wahlordnungen gestützt. Aus der Sicht des Datenschutzes kann diese im wesentlichen formale Begründung nicht überzeugen. Ich halte vielmehr auch weiterhin eine konsequente und übereinstimmende Regelung der Übermittlungssperren für alle öffentlich zugänglichen Register und Verzeichnisse für unbedingt erforderlich.

4.5 Berichtigung - Konsequenzen für die Verwaltung

Effektiver Datenschutz verlangt, daß die Berichtigung falscher sowie die Streichung geheimzuhaltender Daten in Behördenbescheiden rasch und vollständig erfolgt.

Illustrativ für diese Problematik ist der folgende Sachverhalt einer bei mir eingegangenen Eingabe: Eine Bürgerin erhielt ihre Einkommensteuerbescheide von dem für sie zuständigen Finanzamt in Briefumschlägen mit Klarsichtfeld. In diesem Klarsichtfeld waren deutlich neben ihrem Namen die Worte "gesch. XY" erkennbar. Der Postbote und andere Dritte konnten so ohne weiteres Kenntnis von ihren Familienverhältnissen nehmen. Dies änderte sich auch trotz mehrmaliger Abmahnungen bei dem Finanzamt nicht.

Die Offenlegung der familären Situation durch den Zusatz im Adreßfeld verletzt das Datengeheimnis (§ 5 Abs. 1 BDSG, bzw. § 9 Abs. 1 HDSG). Darüber waren sich alle Beteiligten im klaren. Der Fall ist nicht deswegen bemerkenswert. Erstaunlich war vielmehr, daß die Behörde nach ihren eigenen Angaben nach der ersten Beschwerde das Adreßfeld korrigiert hatte, trotzdem aber weiterhin Bescheide mit dem alten Zusatz verschickt wurden.

Für die erfolglose Korrektur fand sich folgende Erklärung: Die Berichtigung war nur auf einem Band in der Hessischen Zentrale für Datenverarbeitung durchgeführt worden; auf andere Bänder, die zur Ausfertigung der Zahlungserinnerungen benutzt wurden, wirkte sie sich nicht aus. Diese wurden erst auf Grund meiner Intervention korrigiert. Mittlerweile wurde das Verfahren so geändert, daß derartige Pannen nicht mehr vorkommen können.

Zwei Schlüsse lassen sich aus diesem Fall ziehen: Die zentrale Verarbeitung von Verwaltungsdaten kann dazu führen, daß die den Datensatz kontrollierende Stelle, hier das Finanzamt, den Ablauf der technischen Verarbeitung nicht mehr überblickt und die Folgen bestimmter Fehler nicht mehr wirksam korrigieren kann. Die enge Zusammenarbeit von Behörde und datenverarbeitender Stelle und eine umfassende gegenseitige Information über mögliche Problemstellen bei der technischen Abwicklung sind jedoch Voraussetzung für eine korrekte Bearbeitung der Daten. Der Bürger hat zu Recht kein Verständnis dafür, daß organisatorische Probleme der Datenverarbeitung zu einer Verletzung des Datenschutzes führen.

Daraus folgt wiederum: Beschwert sich ein Betroffener über einen so offensichtlichen Verstoß gegen das Datenschutzgesetz, so ist jeweils in beiden Bereichen, d.h. nicht nur bei der Behörde sondern auch im Rechenzentrum das Verfahren unverzüglich zu überprüfen.

4.6 Datensicherung - Forderungen an Automationsvorhaben der Verwaltung

4.6.1 Vor- und Abschlußberichte

Die Arbeitsrichtlinien für die Automation von Aufgaben der Landesverwaltung und der Kommunalverwaltung (DV-Leitsätze -DVL-) legen das Verfahren fest, nach dem Tätigkeiten von Landes- und Kommunalbehörden automatisiert werden. Die DVL wurden inzwischen der durch das Hessische Datenschutzgesetz vom 31.1.1978 geänderten Rechtslage angepaßt. Vorberichte zur Verfahrensübernahme oder Abschlußberichte, die dem Landes- bzw. Kommunalen Automationsausschuß vorzulegen sind, müssen konkrete Aussagen zu Maßnahmen des Datenschutzes und der Datensicherung für das jeweilige Datenverarbeitungsprojekt enthalten.

Bei Überprüfung der 1980 vorgelegten oder beratenen Berichte habe ich festgestellt, daß diese Aussagen entweder fehlen oder in so unverbindlicher Form gehalten sind, daß den Anforderungen des Hessischen Datenschutzgesetzes und der DVL nicht genügt wird.

Ich habe mich deshalb an die Vorsitzenden der beiden Automationsausschüsse gewandt und folgende Mindestangaben in Automationsberichten gefordert:

- Wer ist speichernde Stelle gemäß § 2 Abs. 3 1 HDSG?
- Welche Aufbewahrungsfristen für Datenträger sind festgelegt?
- Wie wird das Benachrichtigungsverfahren realisiert, soweit dienst- oder arbeitsrechtliche Rechtsverhältnisse betroffen werden?
- Wie wird die Terminal-Identifizierung beim Einsatz von Datenfernverarbeitungstechniken durchgeführt?
- Wird zur Zugriffssicherung DS-software eingesetzt?
- Ist ein Password-Verfahren vorgesehen?
- Werden Benutzerprofile erstellt?
- Welche Auswertungen sind vorgesehen und wer ist auftrags- bzw. aufrufberechtigt?
- Wie ist ggf. der Transport von Datenträgern geregelt (Arbeitsdaten und Arbeitsergebnisse)?
- Welche Protokolle sind vorgesehen?
- Wie ist das Auskunftsverfahren realisiert?

Der Landesautomationsausschuß hat in seiner Sitzung vom 28.10.1980 dieses Problem beraten und beschlossen, daß Vertreter des Ministers des Innern, des Hessischen Ministers für Wirtschaft und Technik, der HZD und meiner Dienststelle eine Arbeitshilfe erstellen sollen, die Angaben über die von der HZD angebotenen Datensicherungsstandards enthält und die Realisierung weiterer verfahrensspezifischer Datenschutzmaßnahmen erleichtert.

4.6.2 Lösungsansätze im Hessischen DV-Verbund

- Terminalidentifikation

Das Problem der sog. "Terminalidentifikation", d.h. der Verhinderung von Datenübertragung ohne zweifelsfreie Identifizierung des berechtigten Empfängers, hat die HZD in gleichlautenden Schreiben an die beiden Automationsausschüsse dargelegt. Mit Beschluß vom 12.2.1980 (LAA Nr. 91-6) hat der Landesautomationsausschuß die Ressorts gebeten, die erforderlichen Maßnahmen zur Einführung von Terminal-Identifikationen in Abstimmung mit dem DV-Verbund vorzunehmen. Zwar hat die HZD mit den Ministerien entsprechende Gespräche zu diesem Punkt geführt, bisher konnte aber keine Einigung über die Kostenfrage und die technische Realisierung erzielt werden. Dieser Sachstand ist für mich Anlaß, nochmals und nachdrücklich darauf hinzuweisen, daß die Durchführung der notwendigen Vorkehrungen im Interesse einer wirksamen Datensicherung bei der Datenfernverarbeitung unverzichtbar ist.

- Datensicherungsprogramme

Datensicherungsprogramme sollten dort zum Einsatz kommen, wo herkömmliche Betriebssysteme keinen ausreichenden Datenschutz gewährleisten; dies gilt besonders für den Zugriff auf Dateien und Programme. Werden, wie im Hessischen DV-Verbund üblich, mehrere Betriebsarten gleichzeitig eingesetzt, muß das Betriebssystem spezielle Schutzfunktionen für Stapelbetrieb, Teilhaberbetrieb, Teilnehmerbetrieb oder Konsoloperating bereitstellen. Dazu gehören:

- Zugriffslimitierung für jeden - auch externen - Benutzer der DV-Anlage auf seine Daten und Programme.
- Protokollierungsmöglichkeiten für alle Zugriffe einschließlich der abgewiesenen Zugriffsversuche.

Bei der HZD werden Dialoganwendungen im Teilnehmerbetrieb durch ein spezielles Kontrollprogramm auf erlaubte Aktivitäten beschränkt und kontrolliert. Anders jedoch im sog. "background": Bei dieser Arbeitsweise werden Ergebnisse nicht sofort ausgegeben, sondern über den Drucker der HZD ausgedruckt bzw. über Leitung an einen Drucker des Anwenders übertragen. Während bei der Druckausgabe in den Räumen der HZD eine Kontrolle auf Empfangsberechtigung und Richtigkeit des Ergebnisses durchgeführt werden kann, ist dies bei einer dezentralen Ausgabe nicht möglich. Gemeinsam mit dem DV-Verbund muß hier nach realisierbaren technischen und organisatorischen Lösungen gesucht werden. Unverkennbar ist, daß selbst Betriebssysteme namhafter Hersteller im Hinblick auf die Datensicherung Lücken enthalten, so wenn etwa Bandkennungen mit Standardprogrammen des Herstellers zu umgehen sind, kein Schutz vor Veränderungen von Inhaltsverzeichnissen auf Magnetplatten besteht oder die Protokollierung abgewiesener Zugriffsversuche nicht möglich ist.

So lange aber Betriebssysteme den gestellten Anforderungen nicht voll entsprechen, setzt wirksame Abhilfe den Einsatz zusätzlicher Datensicherungsprogramme wie SECURE oder RACF voraus. SECURE ist zwar im Hessischen DV-Verbund vorhanden, wird jedoch zur Zeit nur in der HZD in größerem Maße benutzt, von den Kommunalen Gebietsrechenzentren (KGRZ) Frankfurt, Gießen und Wiesbaden, dagegen überhaupt nicht. Die KGRZ sind nach meinen Erkenntnissen nach wie vor nur in geringem Maße motiviert, zusätzliche Datensicherungsprogramme einzusetzen (siehe bereits meinen Achten Tätigkeitsbericht, unter 2.4.6).

5. Dateienregister

5.1 Stand des Verfahrens

Die Zahl der mir vorliegenden Meldungen zum Dateienregister hat sich gegenüber dem Berichtszeitraum 1978/79 nur geringfügig geändert und liegt derzeit bei etwa 8.500 Dateien. Das in meinem Achten Tätigkeitsbericht angekündigte DV-Verfahren "Führung und Auswertung des Dateienregisters beim Hessischen Datenschutzbeauftragten" konnte in der bereits beschriebenen Form technisch realisiert werden.

Gespeichert und damit über das Terminal in meiner Dienststelle auswertbar sind zur Zeit 4.000 Dateien von 270 speichernden Stellen. Große Schwierigkeiten bereitet nach wie vor die Aufbereitung der schriftlichen Meldungen zur Einspeicherung der Daten bei der Hessischen Zentrale für Datenverarbeitung (HZD). Dies ist zum einen in den fehlerhaft ausgefüllten Meldevordrucken begründet, zum anderen in der Tatsache, daß die mit dem Aufbau und der Führung des Dateienregisters beauftragte Mitarbeiterin sachbearbeitend alle formellen Fehler mit den speichernden Stellen und alle DV-Verfahrensfehler mit der HZD klären muß. Sie ist aber auch für die Dateieneingabe verantwortlich. Es kann jetzt schon gesagt werden, daß die Erfassungsarbeiten zum Dateienregister bei unveränderter personeller Situation noch mindestens ein Jahr dauern werden.

5.2 Auswertungen des Dateienregisters

Nach wie vor dient das Dateienregister - soweit es schon maschinell auswertbar ist - als Auskunftsmittel gegenüber ratsuchenden Bürgern.

Versuchsweise maschinelle Auswertungen haben bestätigt, daß das Register aber auch ein unentbehrliches Hilfsmittel zur Durchführung von Prüfungen durch meine Dienststelle ist. So habe ich beispielsweise festgestellt, daß

- Stellen mit gleicher Aufgabenzuweisung - z.B. kreisfreie Städte - von der Anzahl und vom Inhalt her unterschiedliche Dateien melden. In vier ausgewählten Vergleichfällen beträgt die Mindestzahl der Meldungen 41 und das Maximum 372 Dateien. Ähnliche Ergebnisse zeigt auch der Vergleich zwischen den Dateien verschiedener Kreisausschüsse. Hier meldete ein Kreis beispielsweise sieben, ein anderer dagegen 59 Dateien zum Dateienregister;
- Dateien, die gleichen Zwecken dienen, unterschiedliche Inhalte aufweisen. So enthält z.B. die Personalausweisdatei vieler Gemeinden lediglich Daten des Ausweisinhabers wie Name, Geburtsort und Geburtsdatum, Adresse und Staatsangehörigkeit. In anderen Gemeinden werden zusätzliche Angaben wie Familienstand, Augenfarbe, Größe, besondere Kennzeichen, Name der Eltern, Name des Ehegatten, Nummer der Geburts- oder Heiratsurkunde usw. aufgenommen. Bei Dateien über ausgestellte Fischereischeine fiel auf, daß es Gemeinden gibt, die zusätzlich zu den Grunddaten des Antragstellers auch z.B. den Namen der Eltern und Vorstrafen erheben;
- unterschiedliche Rechtsgrundlagen für gleiche Dateien angegeben wurden. Hier war auffällig, daß einige speichernde Stellen die entsprechenden bereichsspezifischen Gesetze wie z.B. Gewerbeordnung, Hessisches Meldegesetz, Wahlgesetze, Einkommensteuergesetz u.ä. nannten. Andere verwiesen generell auf die allgemeine Zulässigkeitsnorm des §11 HDSG.

Auf meinen Wunsch hin hat der Hessische Minister des Innern als Aufsichtsbehörde etwa 100 Gemeinden, die noch keine Meldung zum Dateienregister abgegeben hatten, auf ihre gesetzliche Pflicht hingewiesen. Im Ergebnis hat jedoch nur etwa ein Zehntel der angeschriebenen Stellen reagiert, so daß hier ein erneutes Nachgreifen notwendig ist. Ich möchte nochmals darauf hinweisen, daß die erwähnten Schwierigkeiten bei der maschinellen Erfassung der Dateien nicht, wie es die Hessische Landesregierung in ihrer Stellungnahme zu meinem Achten Tätigkeitsbericht angeboten hat, durch einen weiteren erläuternden Erlaß im Staatsanzeiger behoben werden können. Hier hilft nur die Einzelfallklärung.

6. Materialien

Erklärung
zum Datenschutz und zu der Verwendung personenbezogener Daten für Forschungszwecke

verabschiedet von der Generalversammlung der European Science Foundation am 12. November 1980

Präambel

Die Notwendigkeit, den einzelnen vor den Gefahren einer Verarbeitung der auf seine Person bezogenen Daten zu schützen, ist in den vergangenen Jahren sowohl auf nationaler als auch auf internationaler Ebene wiederholt betont worden. Dies gilt in ganz besonderem Maße für Staaten, deren Wissenschaftsorganisationen der European Science Foundation angehören. Österreich, Portugal und Spanien verweisen in ihren Verfassungen ausdrücklich auf den Datenschutz. In der Bundesrepublik Deutschland, Dänemark, Frankreich, Norwegen, Österreich und Schweden gibt es bereits besondere Datenschutzgesetze. In Belgien, den Niederlanden und der Schweiz werden gegenwärtig Gesetzesentwürfe beraten. Für Großbritannien liegt ein offizieller Bericht zu den mit dem Datenschutz verbundenen Fragen vor.

Der Datenschutz ist auch auf internationaler Ebene auf beachtliches Interesse gestoßen. So hat der Europarat erst kürzlich ein Übereinkommen zum Schutz des einzelnen unter besonderer Berücksichtigung der automatischen Verarbeitung personenbezogener Daten ausgearbeitet. Die Organisation für wirtschaftliche Zusammenarbeit und Entwicklung (OECD) hat ihrerseits Richtlinien für den Schutz der Privatsphäre und den grenzüberschreitenden Austausch personenbezogener Daten vorgelegt. Besondere Aufmerksamkeit verdienen auch die Diskussion im Rahmen der Europäischen Gemeinschaften über eine mögliche Richtlinie sowie die Untersuchung des Europäischen Parlaments, die zu einer Entschließung, in der unverzügliche Maßnahmen gefordert wurden, führte.

Die Anwendung der Datenschutzgesetze hat jedoch in einer wachsenden Zahl von Fällen ernsthafte Einschränkungen der Verwendung personenbezogener Daten für Forschungszwecke zur Folge gehabt. So geben etwa die Schwierigkeiten bei der Ermittlung und Auswertung von Informationen mit Hilfe von Fragebögen, die Komplikationen beim Zugang zu den Daten, die den Behörden und besonders den statistischen Ämtern zur Verfügung stehen und die Konsequenzen der Vernichtung personenbezogener Daten durch die öffentlichen Stellen, sobald die mit der Verarbeitung verfolgten Ziele erreicht sind, Anlaß zur Besorgnis. Diese Entwicklung hat zu der Verabschiedung der Bellagio-Grundsätze[1]) im August 1977 geführt. Sie ist auch der Grund für die im August 1978 von der IFDO (International Federation of Data Organisations) in Köln veranstaltete internationale Konferenz über die Auswirkungen der sich entwickelnden Datenschutzgesetzgebung auf den Zugang der Sozialwissenschaften zu personenbezogenen Daten. Das Verhältnis von Datenschutz und wissenschaftlicher Forschung ist schließlich im Rahmen des im September 1980 vom Europarat in Lüttich organisierten 10. Kolloquiums über Europäisches Recht erörtert worden.

Die ESF bejaht die Notwendigkeit des Datenschutzes uneingeschränkt. Sie ist jedoch der Meinung, daß die Aufmerksamkeit der Gesetzgeber und der internationalen Organisationen auf die im Interesse der wissenschaftlichen Forschung erforderlichen besonderen Bedingungen bei der Verarbeitung personenbezogener Daten gelenkt werden sollte. Mit Hilfe dieser Bedingungen soll der Zugang zu den für Forschungszwecke benötigten Daten unter Beachtung der jeweils angebrachten Kontrollvorkehrungen sichergestellt werden. Die ESF hat eine Expertengruppe unter dem Vorsitz des Hessischen Datenschutzbeauftragten und Professors an der Universität Frankfurt, Spiros Simitis, beauftragt, Vorschläge für eine solche Regelung zu erarbeiten.[2]) Die Generalversammlung der ESF hat in ihrer Sitzung im November 1980 auf die Grundlage dieser Vorschläge und nach einer eingehenden Diskussion und Überprüfung die nachfolgenden Grundsätze und Richtlinien verabschiedet. Sie werden der Öffentlichkeit in der Hoffnung vorgestellt, daß sie zu einer rechtlichen Regelung beitragen könnten, die sowohl den Datenschutz als auch den für die wissenschaftliche Forschung notwendigen Zugang zu personenbezogenen Daten gewährleistet.

Der Generalsekretär
J. Goormaghtigh

Straßburg, den 13. November 1980

---

1) Sie sind im Schlußbericht der "Bellagio Conference on Privacy, Confidentiality, and the Use of Government Microdata for Research and Statistical Purposes" enthalten. An dieser Konferenz nahmen Vertreter der statistischen Ämter der Bundesrepublik Deutschland, Großbritanniens, Kanadas, Schwedens und der Vereinigten Staaten teil. Sie fand im Bellagio Study and Conference Center der Rockefeller Foundation in Italien vom 16. bis 20. August 1977 statt.

2) Vgl. dazu den 8. Tätigkeitsbericht des Hessischen Datenschutzbeauftragten (1980) S. 123 ff.

Grundsätze

1.1
Als "personenbezogene Daten" werden im Rahmen dieses Dokuments in Übereinstimmung mit der Definition, die sowohl dem Übereinkommen des Europarats als auch den Richtlinien der OECD zugrundeliegt, alle Angaben angesehen, die sich auf eine bestimmte oder bestimmbare Person beziehen.

1.2
Die Datenschutzgesetzgebung muß, um die persönliche Integrität der Betroffenen zu gewährleisten, die Verarbeitung personenbezogener Daten umfassend regeln und deshalb auch die Verarbeitung für Forschungszwecke einbeziehen.

1.3
Das Standesrecht ergänzt die im Interesse des Datenschutzes erforderlichen legislativen Maßnahmen. Die wissenschaftlichen Organisationen sollten die Entwicklung von Standesnormen fördern, um den besonderen Erwartungen der verschiedenen Disziplinen im Rahmen der gesetzlich geregelten Verarbeitungsbedingungen besser Rechnung tragen zu können.

1.4
Die Freiheit der Forschung setzt den bestmöglichen Informationszugang voraus. Der Gesetzgeber sollte deshalb nicht nur die Bedingungen festlegen, unter denen personenbezogene Daten für wissenschaftliche Zwecke verarbeitet werden dürfen, sondern auch den Zugang zu den benötigten Informationen gewährleisten.

1.5
Die Forschungsaufgaben sollten, um des Datenschutzes willen, in Anlehnung an eine bereits geübte Praxis, soweit wie irgend möglich mit Hilfe anonymisierter Daten durchgeführt werden.

1.6
Die Wissenschaftsorganisationen und die Berufsvereinigungen sollten in Zusammenarbeit mit den öffentlichen Stellen die Weiterentwicklung der Techniken und Verfahren unterstützen, die eine Anonymisierung sicherstellen. Die Anonymität ist als gegeben anzusehen, wenn der Betroffene nur mit einem unverhältnismäßigen Aufwand an Zeit, Kosten und Personal identifiziert werden kann (sog. faktische Anonymisierung).

Richtlinien

2.1
Jede Verarbeitung personenbezogener Daten für Forschungsziele setzt, ohne Rücksicht auf den Zweck, für den die Angaben erhoben werden oder bereits erhoben worden sind, entweder eine ausdrückliche gesetzliche Ermächtigung oder die informierte Einwilligung des Betroffenen voraus. Etwas anderes gilt lediglich, wenn der Benutzer der Daten nicht in der Lage ist, den Betroffenen zu identifizieren (vgl. oben 1.6).

2.2
Eine informierte Einwilligung liegt vor, wenn die Betroffenen ausdrücklich und deutlich darüber aufgeklärt worden sind:

a) daß die Erhebung der Daten freiwillig ist und daß eine Weigerung, die Angaben zur Verfügung zu stellen, keinerlei Maßnahmen gegen den Betroffenen zur Folge haben wird;

b) welchen Zweck das Forschungsprojekt verfolgt und welches seine Besonderheiten sind;

c) durch wen und für wen die Daten erhoben werden;

d) daß die Daten ausschließlich für Forschungszwecke verwendet werden sollen.

2.3
Eine informierte Einwilligung ist, soweit sich die für den Datenschutz verantwortliche staatliche Kontrollinstanz oder eine ihr gleichgestellte Instanz damit einverstanden erklären sollte, nicht erforderlich, wenn mit Rücksicht auf den besonderen Charakter des Forschungsprojekts dadurch:

a) wichtige Forschungsziele in Frage gestellt würden;

b) der Betroffene psychisch oder physisch gefährdet werden könnte.

2.4
Soweit die Verarbeitung ausschließlich dazu dient, Stichproben für Forschungszwecke zu ziehen, sollte im Rahmen der gesetzlichen oder einer weiteren rechtlich anerkannten Regelung die Verwendung der von den Behörden zu anderen als wissenschaftlichen Zwecken erhobenen Angaben über den Namen, die Adresse, das Geburtsdatum, das Geschlecht und den Beruf des Betroffenen erlaubt werden.

2.5
Die für Forschungszwecke zur Verfügung gestellten personenbezogenen Daten sollten nicht für andere Zwecke verarbeitet werden.

2.6
Die für Forschungszwecke zur Verfügung gestellten personenbezogenen Daten sollten insbesondere nicht für Maßnahmen oder Entscheidungen genutzt werden, die sich unmittelbar auf den Betroffenen auswirken. Dies gilt nicht, wenn es sich um Maßnahmen oder Entscheidungen handelt, die im Rahmen des Forschungsprojektes getroffen werden oder wenn sich der Betroffene ausdrücklich damit einverstanden erklärt hat.

2.7
Personenbezogene Daten, die für Forschungszwecke verarbeitet worden sind, sollten nur mit Einwilligung des Betroffenen in personenbezogener Form veröffentlicht werden.

2.8
Das Recht des Betroffenen, Gewißheit darüber zu erlangen, ob Daten, die sich auf ihn beziehen, Verarbeitungsgegenstand sind, die Richtigkeit der ihn betreffenden Angaben zu bestreiten, sowie die Löschung, Berichtigung oder Ergänzung zu verlangen, sollte auf Forschungsprojekte beschränkt werden, bei denen eine Verarbeitung in personenbezogener Form beabsichtigt ist.

2.9
Die Leiter von Forschungsprojekten, die mit einer Verarbeitung personenbezogener Daten verbunden sind, sollten die Verantwortung dafür tragen, daß die für die Vertraulichkeit und die Sicherung der Angaben erforderlichen technischen und organisatorischen Maßnahmen getroffen und dem jeweils jüngsten Stand der wissenschaftlichen und technischen Entwicklung angepaßt werden.

2.10
Soweit der besondere Forschungszweck, für den personenbezogene Daten verarbeitet worden sind, erfüllt ist, sollten die Angaben anonymisiert und die für eine sichere Aufbewahrung erforderlichen Maßnahmen (etwa eine Speicherung von Identifikatoren bei einem zentralen Forschungsarchiv) getroffen werden.

2.11
Die Entscheidung, personenbezogene Daten zu vernichten, die sich bei öffentlichen Stellen befinden, sollte nur erfolgen, nachdem die Möglichkeit einer späteren Verwendung für Forschungszwecke geprüft und das zentrale Datenarchiv oder eine ähnliche Organisation konsultiert worden ist.

Professor Dr. Simitis