11. Wahlperiode

Drucksache **11/5232**

HESSISCHER LANDTAG

24. 01. 86

Vierzehnter Tätigkeitsbericht des Hessischen Datenschutzbeauftragten

Mit Schreiben vom 23. Januar 1986 legt der Datenschutzbeauftragte gemäß § 29 des Hessischen Datenschutzgesetzes vom 31. Januar 1978 dem Landtag folgenden Tätigkeitsbericht vor:

Eingegangen am 24. Januar 1986 · Ausgegeben am 20. März 1986

Druck und Auslieferung: Kanzlei des Hessischen Landtags · Postfach 32 40 · 6200 Wiesbaden 1

INHALTSVERZEICHNIS

KERNPUNKTE DES 14. TÄTIGKEITSBERICHTS

1. Die Gemeindeparlamente sind berechtigt, soweit dies für ihre Kontrolltätigkeit erforderlich ist, auch personenbezogene Unterlagen der Verwaltung einzusehen (Ziff. 2.1).

2. Eine personenbezogene Meldepflicht für AIDS-Fälle an das Gesundheitsamt ist verfassungsrechtlich unzulässig. Sie muß es so lange bleiben, wie unter seuchenmedizinischen Gesichtspunkten Information und Kooperation des Patienten den absoluten Vorrang verdienen (Ziff. 3.1.3).

3. Die undifferenzierte Unterrichtung der Bediensteten in Haftanstalten über AIDS-infizierte Gefangene verletzt die ärztliche Schweigepflicht (Ziff. 3.1.5).

4. Die Möglichkeiten des kassenübergreifenden Datenzugriffs im "Informations- und Datenverarbeitungssystem der Ortskrankenkassen (IDVS II)" sind auf die wenigen Fälle zu begrenzen, in denen für die sofortige Verfügbarkeit der Versichertendaten eine zwingende Notwendigkeit besteht (Ziff. 3.2).

5. Die Speicherung der Krankheitsdaten von Psychiatriepatienten zu statistischen und Planungszwecken darf nur in der Weise erfolgen, daß der einzelne Kranke nicht erkennbar ist. Ohne eine verbesserte Anonymisierung kann daher das Projekt "Basisdokumentation Psychiatrie (BADO)" nicht fortgeführt werden (Ziff. 3.3).

6. Die Übermittlung von Daten über Versammlungsteilnehmer insbesondere an Sicherheitsbehörden gefährdet nicht nur das informationelle Selbstbestimmungsrecht, sondern auch das Grundrecht auf Versammlungsfreiheit. Sie muß auf den unbedingt erforderlichen Umfang beschränkt werden und bedarf klarer Verfahrensvorschriften (Ziff. 4.1).

7. Die Protokollierung von Verarbeitungsvorgängen bei der automatisierten Datenverarbeitung ist für Kontroll- und Sicherungszwecke erforderlich. In Anbetracht einer zunehmenden zweckwidrigen Auswertung von Protokolldaten muß unbedingt sichergestellt werden, daß diese ausschließlich zu Kontroll- und Sicherungszwecken verwendet werden (Ziff. 4.2).

8. Mit der vom Hessischen Innenminister vorgeschlagenen Regelung der polizeilichen Datenverarbeitung und dem Musterentwurf der Innenministerkonferenz wird der längst fällige Weg einer bereichsspezifischen Regelung eingeschlagen. Die vom Hessischen Innenminister vorgeschlagene Regelung ist klarer und differenzierter als der Musterentwurf der Innenministerkonferenz. Gegen eine Reihe von Vorschriften bestehen jedoch erhebliche Bedenken (Ziff. 4.3).

9. Die Durchführung der Handels- und Gaststättenzählung im Mai 1985 entsprach nicht den verfassungs- und datenschutzrechtlichen Anforderungen an statistische Erhebungen (Ziff. 5.1).

10. Die von Wissenschaftsrat und Kultusministerkonferenz in der Diskussion um die Novellierung des Hochschulstatistikgesetzes geforderte Beibehaltung der Studienverlaufsstatistik ist aus verfassungsrechtlichen Gründen nicht möglich (Ziff. 5.2.1).

11. Die Prüfungskandidatenstatistik als Teil der Hochschulstatistik wird in Hessen auf Anregung des Hessischen Datenschutzbeauftragten nicht mehr personenbezogen durchgeführt (Ziff. 5.2.2).

12. Das am 15. November 1985 in Kraft getretene Volkszählungsgesetz 1987 erfüllt die Anforderungen des Bundesverfassungsgerichts; eine Volkszählung in der vorgesehenen Form kann allerdings nur durchgeführt werden, wenn zuvor ein Landesstatistikgesetz verabschiedet worden ist (Ziff. 5.3.1).

13. Das am 14. Juni 1985 in Kraft getretene Mikrozensusgesetz ist ein wichtiger Schritt hin zu einer auf Kooperation des Bürgers statt auf Zwang beruhenden amtlichen Statistik (Ziff. 5.3.2).

14. Die im Dezember 1985 vom Bundespostminister im Entwurf vorgelegte Telekommunikationsordnung erfüllt nicht die datenschutzrechtlichen Anforderungen an die gesetzliche Regelung der neuen Telekommunikationsdienste (Ziff. 7.1).

15. Der im Bereich der öffentlichen Verwaltung des Landes Hessen zur Datenfernverarbeitung innerhalb des öffentlichen Datennetzes genutzte Synchronknoten SK 12 bietet keine ausreichende Datensicherheit und darf daher nicht weiter zur Verarbeitung personenbezogener Daten verwendet werden (Ziff. 8.3).

16. Datenschutz und Informationsgleichgewicht sind nur zwei Aspekte einer konsequenten Datenverarbeitungsregelung. Ebenso wichtig ist das Recht auf Information. Seine gesetzliche Regelung sollte in Hessen im Zusammenhang mit der anstehenden Weiterentwicklung des Datenschutzes diskutiert werden (Ziff. 11.1).

17. Das Hessische Datenschutzgesetz verlangt mit seiner Forderung nach Informationsgleichgewicht auch eine bessere Information der Abgeordneten. Sie kann allerdings nur gewährleistet werden, wenn zuvor im einzelnen geprüft wird, wie in Kenntnis der besonderen Arbeitssituation der einzelnen Abgeordneten die von den neuen Informations- und Kommunikationstechniken gebotenen Möglichkeiten konsequent genutzt werden können (Ziff. 12).

1. Zur Situation

1.1
Drei Aspekte eines Problems

Was sich schon 1970, im ersten Hessischen Datenschutzgesetz, klar abzeichnete, hat sich seither immer wieder bestätigt: Die Auseinandersetzung mit den Auswirkungen einer ständig verbesserten Informationstechnologie beinhaltet drei, auf den ersten Blick ganz verschiedene, in Wirklichkeit aber eng miteinander verzahnte und deshalb nur in Kenntnis ihrer Verknüpfung lösbare Aufgaben:

- die Manipulation des einzelnen angesichts einer sich unentwegt ausweitenden Sammlung und einer immer konsequenteren Verarbeitung personenbezogener Daten zu verhindern;
- die Funktionsfähigkeit des Parlaments auch unter den Bedingungen einer Technologie sicherzustellen, die Regierung und Verwaltung einen wachsenden Informationsvorsprung gewährt und damit die parlamentarischen Kontroll- und Entscheidungsbefugnisse gefährdet;
- den Zugang des Bürgers zu jenem Mindestmaß an Information zu garantieren, das ihm die Chance einräumt, die politische und gesellschaftliche Entwicklung nicht passiv über sich ergehen zu lassen, sondern aktiv mitzugestalten.

Schaut man sich freilich die Tätigkeitsberichte an, dann fällt eines sofort auf: Im Vordergrund stand bisher ohne Zweifel der Datenschutz. Sicherlich, die Berichte enthalten immer wieder auch Bemerkungen und Vorschläge zur Sicherung des Informationsgleichgewichts, selbst wenn es dabei nicht durchweg um so zentrale Fragen geht wie 1976 im Zusammenhang mit der durch eine Große Anfrage der Opposition ausgelösten Debatte über den Zugang des Parlaments vor allem zu den von der HZD und den Kommunalen Gebietsrechenzentren verarbeiteten Daten. Nichts anderes gilt für das Recht auf Information. Zugegeben, weder die Überlegungen zur Verarbeitung personenbezogener Angaben im Rahmen der wissenschaftlichen Forschung noch die langen und mühevollen Diskussionen über die Notwendigkeit eines Archivgesetzes sind spektakuläre Beispiele für die Bedeutung sowie die Konsequenzen des Rechts auf Information. An beiden Fällen zeigt sich freilich, wie wenig eine überzeugende Regelung solange gefunden werden kann, wie nicht alle drei eingangs erwähnten Aspekte bedacht und sorgfältig aufeinander abgestimmt werden.

Trotzdem bleibt es dabei: Der Datenschutz war durchweg das beherrschende Thema. Verwunderlich ist es freilich nicht. Die Verarbeitung personenbezogener Angaben war und ist der entscheidende Ansatzpunkt für eine öffentliche Diskussion der politischen und sozialen Dimension einer durch die rechnergesteuerte Datenverarbeitung geprägten Informationstechnologie. Je deutlicher der Umfang und die möglichen Konsequenzen der Verarbeitung wurden, desto mehr wuchs auch die Bereitschaft, den Wandel der Informationstechnologie nicht nur als rein technische Frage anzusehen, sondern als zuvörderst politisches und rechtliches Problem. In dem Maße aber, in dem sich die Informations- und Kommunikationsbedingungen unter dem Eindruck einer sich rapide entwickelnden Technologie veränderten, schärfte sich auch das Bewußtsein für die Auswirkungen dieser Technologie auf die elementaren Funktionsvoraussetzungen einer demokratischen Gesellschaft. Konsequenterweise hat sich der Hessische Landtag in seinen Beschlüssen zum 12. Tätigkeitsbericht nicht darauf beschränkt, einzelne Datenschutzfragen aufzugreifen, sondern auch und gerade auf einer eingehenden Erörterung des Informationsgleichgewichts ebenso wie des Rechts auf Information bestanden (Beschlüsse Nr. 1 und 2 zum 12. Tätigkeitsbericht, Drucks. 11/1551 i.V.m. Protokoll der 12. Plenarsitzung vom 5. Juli 1984, S. 1378). Genauso folgerichtig war es, als in der Debatte über den letztjährigen Tätigkeitsbericht ausdrücklich an die Notwendigkeit erinnert wurde, die Arbeitsbedingungen der einzelnen Abgeordneten unter Berücksichtigung der veränderten Informations- und Kommunikationsmöglichkeiten zu überdenken. Der 14. Tätigkeitsbericht geht deshalb gezielt auf alle drei Problembereiche, Informationsgleichgewicht, Datenschutz und Recht auf Information ein.

1.2
Datenschutzgesetzgebung

Die Kontrolle der Verarbeitung personenbezogener Daten hat nur solange einen Sinn, wie die dabei gewonnenen Erfahrungen in verbindliche Verarbeitungsregeln umgesetzt werden. So gesehen ist die Kontrolle, jedenfalls zu weiten Teilen, Vorarbeit für den Gesetzgeber. Nur dann kann der Datenschutzbeauftragte die an ihn gerichtete, vom Bundesverfassungsgericht in seiner Entscheidung zum Volkszählungsgesetz ausdrücklich bestätigte Erwartung wirklich erfüllen, nicht nur Verstöße gegen die bestehenden Datenschutzvorschriften aufzudecken, sondern auch und vor allem neue und bessere Bestimmungen anzuregen, um auf diese Weise die Verarbeitung rechtzeitig in gefahrenfreie Bahnen zu lenken. Verständlicherweise beschäftigt sich deshalb der Tätigkeitsbericht einmal mehr mit der Datenschutzgesetzgebung. Die Palette ist breit. Sie reicht von der Novellierung des Hessischen Datenschutzgesetzes über den ersten Versuch einer datenschutzkonformen Regelung der polizeilichen Datenverarbeitung bis hin zu den verschiedenen Statistikgesetzen.

1.2.1
HDSG-Novellierung

Zum dritten Mal sieht sich der Hessische Landtag mit Vorschlägen zu einem Datenschutzgesetz konfrontiert. Zum dritten Mal geht es dabei um Regelungsvorstellungen, die weit über die bisher vorhandenen Vorschriften hinaus weisen. Gewiß, anders als 1970 kann der Gesetzgeber auf eine jetzt fünfzehnjährige Regelungstradition ebenso zurückgreifen wie auf umfangreiche Erfahrungen mit der Verarbeitungspraxis. Trotzdem, so verwunderlich es klingen mag, befindet sich der Gesetzgeber in einer Situation, die durchaus der Lage bei der Beratung des ersten Hessischen Datenschutzgesetzes ähnelt. Schon deshalb, weil es im Unterschied zu 1978 nicht darum geht, eine im Bundesbereich formulierte Vorlage aufzugreifen und sich kritisch damit auseinanderzusetzen. Im Gegenteil, der Entwurf ist der wirklich erste Versuch, ein Regelungskonzept zu entwickeln, das den Anforderungen des Bundesverfassungsgerichts konsequent Rechnung trägt.

Zudem haben sich seit der Verabschiedung der Datenschutzgesetze die Gewichte entscheidend verschoben. Spätestens seit der Entscheidung des Bundesverfassungsgerichts zum Volkszählungsgesetz steht fest: Ein ebenso verfassungskonformer wie wirksamer Datenschutz läßt sich nur über präzise bereichsspezifische Regelungen erzielen. Nur mit ihrer Hilfe können die Verarbeitungsvorschriften den Zugriff auf die personenbezogenen Daten an wirklich verbindliche, auch für den Betroffenen nachvollziehbare Voraussetzungen knüpfen. Je konsequenter freilich dieser Weg beschritten wird, desto mehr rückt das Datenschutzgesetz in den Hintergrund. Statt der eigentliche Regelungsansatz zu sein, greift es lediglich in den Fällen ein, in denen es an bereichsspezifischen Bestimmungen fehlt. Auch wenn es also keineswegs überflüssig wird, verliert es erheblich an Bedeutung. So klar aber auch die Auffangfunktion des Datenschutzgesetzes ist, so wenig berechtigt sie den Gesetzgeber, sich mit den bislang üblichen, überaus allgemein gehaltenen Formulierungen zufriedenzugeben. Im Gegenteil, der Rückzug in die Generalklauseln bleibt ihm hier ebenfalls weitgehend versperrt. Er muß also, will er den verfassungsrechtlichen Anforderungen an die Verarbeitungsregelung wirklich genügen, hier genauso versuchen, präzise Verarbeitungsbedingungen festzuschreiben. Die Schwierigkeiten sind gewiß im Hinblick auf den nach wie vor weiten Anwendungsbereich des Gesetzes nicht zu unterschätzen. Sie lassen sich aber, wie der bisherige Diskussionsverlauf zeigt, durchaus überwinden.

Kurzum, mit dem Entwurf hat der hessische Gesetzgeber die Chance, an die eigene Tradition anzuknüpfen und eine Pilotfunktion wahrzunehmen. Ähnlich wie in der Vergangenheit könnte Hessen damit die Maßstäbe für eine weit über die Grenzen des Landes hinausreichende Datenschutzregelung setzen. Soll dieses Ziel aber wirklich erreicht werden, dann bedürfen die Vorschriften des Entwurfs noch einer ganzen Reihe von Korrekturen. Der Tätigkeitsbericht enthält Vorschläge dazu (vgl. Ziff. 10). Sie unterstreichen einerseits, wie folgerichtig der Weg ist, den der Entwurf eingeschlagen hat, beispielsweise durch die Einbeziehung der Verarbeitung personenbezogener Daten in Akten und der Datenerhebung, zeigen aber auch andererseits, wie sehr er an einer Vielzahl von Punkten an einer längst korrekturbedürftigen Verarbeitungspraxis festhält.

Die Chance einer wirklich wegweisenden Regelung ist aber auch deshalb gegeben, weil die Diskussion über die Novellierung des Hessischen Datenschutzgesetzes parallel zu der Erörterung einer Reihe wichtiger bereichsspezifischer Regelungen verläuft. Besser denn jemals zuvor hat daher der Gesetzgeber die Möglichkeit, die einzelnen Vorschriften aufeinander abzustimmen, der Auffangfunktion des Datenschutzgesetzes also ebenso Rechnung zu tragen wie der Notwendigkeit, die Grundvorstellungen des Gesetzes auch im Rahmen der jeweiligen bereichsspezifischen Regelung aufzugreifen und weiter zu präzisieren.

1.2.2
Regelung der polizeilichen Datenverarbeitung

Mit einer der wichtigsten Anwendungsfälle eines bereichsspezifischen Datenschutzes sind nun ohne Zweifel die Vorschriften zur polizeilichen Datenverarbeitung. Genausowenig läßt sich freilich bestreiten, daß es kaum einen anderen Fall gibt, in dem der Versuch, die Anforderungen des Datenschutzes präzise festzulegen, auf so viel Schwierigkeiten stößt. Eines sollte zunächst klar sein: Der Gesetzgeber hat aus zwei Gründen keine Wahl, ganz gleich im übrigen wie der Inhalt der zu treffenden Regelung aussehen mag. Zunächst: Das Bundesverfassungsgericht hat gerade für Bereiche wie den der polizeilichen Datenverarbeitung nicht den geringsten Zweifel an der Notwendigkeit einer eigens darauf zugeschnittenen Regelung gelassen. Die Vorschriften des Datenschutzgesetzes geben, so gesehen, keine ausreichende Rechtsgrundlage ab.

Konsequenterweise hat die Rechtsprechung ihre Zweifel an der Rechtmäßigkeit der polizeilichen Datenverarbeitung bereits angemeldet. Man kann ihr beim besten Willen nicht den üblichen Hinweis auf den "Überraschungseffekt" der Entscheidung des Bundesverfassungsgerichts und den damit einhergehenden "Übergangsbonus" entgegenhalten. Die Diskussion über den möglichen Inhalt einer bereichsspezifischen Regelung hat nicht erst mit

den jetzt vorliegenden Entwürfen angefangen. Sie reicht, wie schon ein Blick in die Tätigkeitsberichte der vergangenen Jahre zeigt, lange zurück. Schon bei den ersten Überlegungen zu den Vorschriften über die Kriminalpolizeilichen Sammlungen stand beispielsweise fest, daß es eigentlich Aufgabe des Gesetzgebers sein müßte, die nötige Regelung zu treffen. Wenn jedoch davon abgesehen wurde, so auch und gerade mit dem Argument, daß es mit Hilfe von Verwaltungsvorschriften besser möglich sei, die erforderlichen Erfahrungen für die gesetzliche Regelung zu gewinnen. Anders ausgedrückt: Der "Übergang" war längst eingeleitet, als das Bundesverfassungsgericht seine Überlegungen formulierte. Kein Gesetzgeber kann es sich deshalb leisten, die Verabschiedung der notwendigen Vorschriften hinauszuzögern. Jeder Aufschub belastet den Bürger mit den Gefahren einer Verarbeitungspraxis, die in Widerspruch zu den Anforderungen der Verfassung gerät, gefährdet aber auch zugleich die polizeiliche Arbeit unmittelbar, indem er sie mit dem Makel versieht, sich in einem rechtlich nicht abgedeckten Raum zu vollziehen.

Manche Schwierigkeit könnte nun vermieden werden, wenn von Anfang an Klarheit über den Standort und die Aufgabe einer Regelung der polizeilichen Datenverarbeitung bestünde. Sie ist weder der rechte Ansatzpunkt, um die Existenz der Polizei in Frage zu stellen, noch ist sie der geeignete Anknüpfungspunkt, um sich eines längst als lästig empfundenen Datenschutzes weitgehend zu entledigen. Noch einmal: Zur Debatte stehen einzig und allein Vorschriften, die einen bestimmten, seiner ganzen Aufgabe nach klar eingegrenzten Verarbeitungsbereich zum Gegenstand haben. Im Unterschied also zu den ansonsten geführten abstrakten Datenschutzdiskussionen kann und darf hier nicht an den Besonderheiten der polizeilichen Arbeit vorbeiargumentiert werden. Sie geben erst die Grundlage für alle weiteren Überlegungen ab. Genauso kommt es aber darauf an, sich stets darüber im klaren zu sein, daß die polizeiliche Tätigkeit - wie auch jede andere staatliche Aktivität - streng an die Anforderungen der Verfassung gebunden ist. Sinn einer bereichsspezifischen Regelung ist es unter diesen Umständen, sich mit der bisherigen Verarbeitungspraxis und den von der Polizei formulierten Verarbeitungserwartungen präzise auseinanderzusetzen, um Verarbeitungsbedingungen festzuschreiben, die es ermöglichen, den von der Verfassung aufgestellten und vom Bundesverfassungsgericht bestätigten Verarbeitungsschranken auch unter den besonderen Voraussetzungen polizeilicher Tätigkeit Rechnung zu tragen. Anders ausgedrückt: Die Forderung nach einer bereichsspezifischen Regelung war und ist nicht Konkretisierung eines eigens und nur der Polizei gegenüber bestehenden Mißtrauens, sondern unmittelbare Konsequenz verbindlicher, jegliche Verarbeitung personenbezogener Daten gleichermaßen betreffender Grundsätze. Ebensowenig wie irgendein anderer Teil der staatlichen Verwaltung kann sich deshalb die Polizei der Notwendigkeit entziehen, ihre Verarbeitungsvorstellungen am Datenschutz messen zu lassen.

Einfach ist die Aufgabe freilich nicht. Allgemeine Datenschutzvorschriften lassen sich in aller Regel sehr viel leichter formulieren als bereichsspezifische Bestimmungen. Nicht nur, weil sie zu einer mühsamen Detailarbeit zwingen, sondern vor allem weil sich Konflikte nicht ohne weiteres mit Hilfe von Generalklauseln verhüllen lassen, die in der verschiedensten Weise interpretiert werden können. Wo nun die hauptsächlichen Konfliktzonen liegen, läßt sich dem Tätigkeitsbericht entnehmen (vgl. Ziff. 4.3). Die vorbeugende Bekämpfung von Straftaten, die Verarbeitung personenbezogener Daten im Zusammenhang mit Demonstrationen, die Datenerhebung in und aus Wohnungen sind mit die wichtigsten Beispiele.

Ganz gleich aber wie die Regelung der polizeilichen Datenverarbeitung letztlich ausfällt, sie bedarf in zweierlei Hinsicht der Ergänzung. Zum einen durch die nicht minder dringliche Novellierung der Strafprozeßordnung. Der enge Zusammenhang polizeilicher und staatsanwaltschaftlicher Tätigkeit im Rahmen der Strafverfolgung zwingt zu Regelungen, die vor allem sicherstellen, daß die für den polizeilichen Bereich aufgestellten Verarbeitungsschranken nicht etwa mit Hilfe strafprozessualer Bestimmungen umgangen werden können. Zudem muß für Vorkehrungen gesorgt werden, die eine Korrektur und Löschung der von der Polizei verarbeiteten Daten auch im Hinblick auf ihre prozessuale Verwendung sicherstellen. Zum anderen macht das in den Tätigkeitsberichten immer wieder erwähnte Beispiel des Staatsschutzes deutlich, daß Glaubwürdigkeit und Wirksamkeit einer Regelung der polizeilichen Datenverarbeitung in ganz besonderem Maße von den für den Informationsaustausch zwischen den einzelnen Sicherheitsbehörden geltenden Bestimmungen abhängen. Je pauschaler die Zusammenarbeitsvorschriften ausfallen, desto wertloser gerät die für den polizeilichen Bereich vorgesehene, den verfassungsrechtlichen Anforderungen entsprechende Zweckbindung. Zusammenarbeitsvorschriften, die letztlich nicht mehr tun, als die üblichen Generalklauseln zu wiederholen, die eine Übermittlung immer dann für zulässig erklären, wenn sie zur Aufgabenerfüllung der empfangenden Behörde erforderlich ist, sind deshalb nicht hinnehmbar. Der polizeiliche Datenbestand ist kein den Sicherheitsbehörden frei zugängliches Informationsmaterial. Nur soweit die Aufgaben der jeweiligen Sicherheitsbehörde präzise festgelegt sind und unter bestimmten gesetzlich genau festzulegenden Voraussetzungen kann ein Zugriff auf die für den konkreten, gesetzlich abgedeckten Zweck wirklich erforderlichen Angaben in Betracht kommen. Sicherlich, in beiden Fällen geht es um Regelungen, die außerhalb der Kompetenz des Landesgesetzgebers liegen. Es ist aber nur folgerichtig, wenn das Land die ihm gegebenen Möglichkeiten nutzt, um eine konsequente Anknüpfung an die für die polizeiliche Datenverarbeitung geltenden Grundsätze sowohl im strafprozessualen Bereich als auch bei der Zusammenarbeit zwischen den einzelnen Sicherheitsbehörden zu ermöglichen.

Noch eine letzte, scheinbar nur nebensächliche Bemerkung: Die besten Datenschutzvorschriften bleiben wirkungslose Leerformeln, solange nicht zugleich die für ihre konsequente Anwendung erforderlichen technischen und personellen Voraussetzungen geschaffen werden. Das Beispiel der im Zusammenhang mit früheren Tätigkeitsberichten immer wieder diskutierten Mängel bei der Verwirklichung der in den Richtlinien für die Kriminalpolizeilichen Sammlungen vorgesehenen Löschungsvorschriften ist lehrreich genug. Es darf sich nicht wiederholen, wenn die Polizei nicht Vorwürfen ausgesetzt werden soll, die sie selbst gar nicht treffen.

1.2.3
Statistikgesetzgebung

Ein zweiter wichtiger Anwendungsfall bereichsspezifischer Regelung ist die Statistik. Genau genommen war sie der eigentliche Adressat der vom Bundesverfassungericht formulierten Anforderungen an eine verfassungskonforme Verarbeitung personenbezogener Daten. Wohlgemerkt, das Gericht hat die Notwendigkeit statistischer Erhebungen keineswegs in Zweifel gezogen. Im Gegenteil, seine Überlegungen zielen darauf ab, Bedingungen herzustellen, die das Vertrauen der Bürger in die Arbeit der Statistischen Ämter erhöhen und ihre Bereitschaft zur Zusammenarbeit stärken. Deshalb legt das Bundesverfassungsgericht in seiner Entscheidung einen so großen Wert auf eine strikte, auch und gerade durch eine Reihe organisatorischer Vorkehrungen abgesicherte Abschottung der statistischen Daten. Aus dem gleichen Grund fordert es eine konsequente Überprüfung der statistischen Methoden, um den Auskunftszwang mehr und mehr durch eine freiwillige Beteiligung der Bürger zu ersetzen. Um so erstaunlicher ist freilich das oft hartnäckige Festhalten mancher Statistiker an den überkommenen, vom Bundesverfassungsgericht kritisierten Erhebungs- und Verarbeitungsprozeduren. Die im Tätigkeitsbericht geschilderten Erfahrungen mit der Handels- und Gaststättenzählung (Ziff. 5.1), aber auch mit den Vorbereitungen für den Mikrozensus (Ziff. 5.3.2) und die Volkszählung (Ziff. 5.3.1) sind bezeichnend dafür. Abstrakte Erörterungen über den Nutzen statistischer Erhebungen liegen ebensowenig wie eine zuweilen exzessive Berufung auf den "Übergangsbonus" im Interesse einer verläßlichen Statistik. Statt dessen kommt es entscheidend darauf an, offensiv im Sinne der Entscheidung des Bundesverfassungsgerichts vorzugehen, auf den Sachverstand der Statistischen Ämter ebenso wie auf die Erkenntnisse der sozialwissenschaftlichen Forschung zurückzugreifen, um kooperationsfreundliche Verfahren zu entwickeln.

Vordergründig ist gerade bei den am meisten beachteten Fällen, der Volkszählung und dem Mikrozensus, nur der Bund zu einer unmittelbaren Reaktion auf die Entscheidung des Bundesverfassungsgerichts verpflichtet. In Wirklichkeit argumentiert jede rein formale, lediglich auf Kompetenzgesichtspunkte gestützte Betrachtung an den Überlegungen des Bundesverfassungsgerichts vorbei. Noch einmal: Das Gericht hat die Durchführung der Volkszählung ausdrücklich in seine Anforderungen einbezogen. Ihre Übereinstimmung mit den verfassungsrechtlichen Grundsätzen läßt sich aber nur auf dem Hintergrund eines Landesstatistikgesetzes sicherstellen. Nach wie vor fehlt es aber an Vorschlägen dafür. Es ist nicht das erste Mal, daß an die Notwendigkeit einer solchen Regelung erinnert wird. Bereits frühere Tätigkeitsberichte hatten aus den verschiedensten Anlässen die Dringlichkeit eines Statistikgesetzes hervorgehoben. Eine Alternative zu einer gesetzlichen Regelung gibt es nach wie vor nicht.

1.2.4
Privater Bereich

Ein Mißverständnis gilt es allerdings zu vermeiden: Alle hier erwähnten Anwendungsfälle einer bereichsspezifischen Regelung betreffen den öffentlichen Bereich. Kaum verwunderlich, bedenkt man die Kompetenz des Landesgesetzgebers, aber auch die Kontrollzuständigkeit des Datenschutzbeauftragten. Allzu leicht könnte man aber versucht sein, aus der ausführlichen Erörterung dieser Fälle zu folgern, die Verpflichtung zu einer an konkreten Verarbeitungsvorgängen orientierten, klaren bereichsspezifischen Regelung wirke sich nur im Zusammenhang mit der staatlichen Tätigkeit aus. Ohnehin fehlt es, gerade im Hinblick auf die Novellierung des Bundesdatenschutzgesetzes, nicht an Bemerkungen, die offensichtlich darauf abzielen, eine Neuregelung so weit wie nur möglich auf den öffentlichen Bereich zu beschränken. Die Schuld an der verzerrten Perspektive trägt zu einem beträchtlichen Teil der Gesetzgeber selbst. Allein schon die unterschiedlichen Kontrollmodalitäten und die damit verbundene unterschiedliche Information der Öffentlichkeit haben die Aufmerksamkeit einseitig auf die staatliche Tätigkeit gelenkt. Um so bedenklicher sind die Bestrebungen, die Berichtsmöglichkeiten auch dort einzuschränken oder gar auszuschließen, wo der Datenschutzbeauftragte die vom Bundesdatenschutzgesetz vorgesehenen Aufsichtsaufgaben gegenüber privaten Unternehmen wahrnimmt. Für den privaten Bereich kann und darf aber nichts anderes gelten als für den staatlichen. Wer daran zweifelt, braucht sich nur die Rechtsprechung des Bundesgerichtshofes zu den Kreditinformationssystemen anzusehen oder auch die in den Tätigkeitsberichten immer wieder erwähnten Nutzungsmöglichkeiten des Bildschirmtextes und der intelligenten Chipkarten gerade für die Kreditinstitute. Wohlgemerkt, keineswegs ist es damit getan, das Bundesdatenschutzgesetz in zwei, jeweils dem öffentlichen und dem privaten Bereich gewidmete Teile zu spalten. Die Verdoppelung der Abstraktionen schafft noch keine bereichsspezifische Regelung. Sie läßt sich nur über eine bewußte Abkehr von den Generalklauseln der

Datenschutzgesetze, ganz gleich ob sie im Hinblick auf den öffentlichen oder im Zusammenhang mit dem privaten Bereich verwendet werden, und durch eine ebenso gezielte Hinwendung zu Verarbeitungsbedingungen, die auf bestimmte, genau erkennbare Verarbeitungsvorgänge zugemünzt sind, erreichen. Solange es aber an vergleichbaren Anstrengungen für den privaten Bereich fehlt, wird es schwer fallen, gerade die an den Datenschutzbeauftragten immer wieder gerichtete Frage der Angehörigen des öffentlichen Dienstes zu beantworten, warum nur die Tätigkeit der Meldebehörden, der Gesundheitsämter oder der Polizeidienststellen an strenge, bereichsspezifische Vorschriften gebunden sein soll und nicht etwa auch die Aktivität der Kreditinstitute, Auskunfteien oder Versicherungen.

1.3
Erfahrungsaustausch mit der Verwaltung

So wichtig präzise gesetzliche Regelungen auch sind, sie reichen für sich genommen nicht aus, schon deshalb weil es mit Rücksicht auf die wachsende Komplexität staatlicher Aufgaben und die sich verändernde Verarbeitungstechnik immer wieder offene Fragen geben wird. Für einen wirksamen Datenschutz kommt es deshalb ganz entscheidend auf die Bereitschaft der öffentlichen Verwaltung an, den Datenschutz als selbstverständliche Handlungsvoraussetzung anzusehen, die bisherige Verwaltungspraxis also von sich aus einer kritischen Überprüfung zu unterziehen, aber auch rechtzeitig auf entstehende Schwierigkeiten und Probleme hinzuweisen. Eines läßt sich mit Sicherheit sagen: Die Kooperationsbereitschaft hat sich in den letzten Jahren immer wieder bestätigt. Einen wesentlichen Teil seiner Erfahrungen verdankt der Datenschutzbeauftragte unmittelbar aus der Verwaltung kommenden Überlegungen und Anregungen. Nur so läßt sich in der Tat manche, zunächst abstrakte Vorstellung in Anforderungen umsetzen, die den konkret im Rahmen der Verwaltungstätigkeit gewonnenen Erfahrungen Rechnung tragen. Nur so kann es aber auch gelingen, Konflikte rechtzeitig offenzulegen und gezielt darauf zu reagieren.

Gerade diese über die Jahre entwickelte und gefestigte Kooperationsbereitschaft gerät dann aber unweigerlich in Gefahr, wenn das direkte Gespräch mit dem Datenschutzbeauftragten unterbunden wird. Das wohl einfachste Mittel dazu ist die Mahnung von Aufsichtsbehörden an nachgeordnete Dienststellen, Fragen und Vorstellungen zum Datenschutz, wenn überhaupt, nur über sie an den Datenschutzbeauftragten zu richten.

Vordergründig ist dies nur eine Erinnerung an ohnehin geltende administrative Grundsätze, in Wirklichkeit aber eine gezielte Einschränkung der Wirkungmöglichkeiten des Datenschutzbeauftragten. Wo ihm der direkte Kontakt zum Verwaltungsalltag bewußt abgeschnitten wird, verliert er auch einen großen Teil seiner Möglichkeiten, die Anwendung des Datenschutzes über die unmittelbare Problemkenntnis und das ungehinderte Gespräch mit den Beteiligten sicherzustellen. So ist auch der unmittelbare Kontakt meiner Dienststelle mit nachgeordneten Behörden gegenwärtig der Regelfall. Umso mehr bedauere ich es, daß der Hessische Innenminister in einem konkreten Fall hinsichtlich der Verfahrensweise eine andere Auffassung vertritt. Ich halte es für unabdingbar, daß einzelne Datenschutzprobleme auch in seinem Bereich im direkten Kontakt zwischen nachgeordneten Dienststellen und dem Datenschutzbeauftragten erörtert werden können. Strikt zurückweisen muß ich die Behauptung, nur der Bürger als Privatperson könne sich direkt an mich wenden, als öffentlicher Bediensteter sei ihm dieser Weg verschlossen.

Der Gesetzgeber hat gezielt davon abgesehen, den Datenschutzbeauftragten in die herkömmlichen Verwaltungsstrukturen einzubinden und es auch abgelehnt, ihn mit Eingriffsbefugnissen auszustatten. Beides allerdings in der Annahme, daß dem Datenschutzbeauftragten vor allem eine beratende Funktion zukommt. Genau diese Erwartung wird dort illusorisch, wo ihm die Chance des direkten Gesprächs genommen wird. Das gleichsam sorgfältig filtrierte Gespräch gefährdet aber auch die gesetzliche Aufgabe des Datenschutzbeauftragten, das Parlament genau und erschöpfend über Anwendungsschwierigkeiten des Datenschutzes zu unterrichten. Sicherlich, am gesetzlich garantierten Auskunftsanspruch des Datenschutzbeauftragten ändert sich nichts. Es macht aber einen großen Unterschied aus, ob mögliche Schwierigkeiten auf Initiative der unmittelbar betroffenen Verwaltungsangehörigen aufgegriffen und besprochen werden oder unter dem Zwang der gesetzlichen Auskunftspflicht. Wo darauf verwiesen wird, entfällt weitgehend auch die Chance des Datenschutzbeauftragten Instanz eines vorbeugenden Rechtsschutzes, in den Worten des Bundesverfassungsgerichts, zu sein.

1.4
Mangelhafter Datenschutz und unzureichende Datensicherung: Einzelfälle

1.4.1
Protokolldaten

Der Tätigkeitsbericht zeigt aber auch, daß es bei aller Kooperationsbereitschaft gravierende Konfliktfälle gibt, und zwar in den verschiedensten Verwaltungsbereichen. Mit am betrüblichsten ist die Erfahrung mit den Protokolldaten (vgl. Ziff. 4.2). Sie sind schon lange Gegenstand eingehender Unterhaltungen mit dem Hessischen Innenmini-

ster gewesen. Meinungsverschiedenheiten schien es gar nicht zu geben. Die Landesregierung hat in ihrer Stellungnahme zum 12. Tätigkeitsbericht ausdrücklich eine klare Zweckbindung akzeptiert, und zwar im Sinne einer gezielten Beschränkung der personenbezogenen Verwertung auf Zwecke der Datenschutzkontrolle. Ausgeschlossen war in jedem Fall eine Auswertung für kriminalpolizeiliche Aufgaben. Genau daran hat sich der Innenminister freilich nicht gehalten. Keines der vorgebrachten Argumente überzeugt. Weder kann es angehen, Arbeitserleichterungen als Begründung für eine rechtlich als unzulässig erkannte Verarbeitung anzuführen, noch erlaubt es der Hinweis auf die Strafprozeßordnung, sich über die zuvor ausdrücklich akzeptierten rechtlichen Bedenken gegen eine Zweckentfremdung der Protokolldaten hinwegzusetzen. Was bleibt, ist einmal mehr die Erfahrung, daß es eben doch keine Alternative zu einer die Zweckbindung unmißverständlich festlegenden gesetzlichen Regelung gibt.

1.4.2
Demonstrationen

Nicht minder bedenklich ist der im Tätigkeitsbericht eingehend geschilderte "Demonstrationsfall" (Ziff. 4.1). Zweimal hat das Bundesverfassungsgericht ausdrücklich auf die Notwendigkeit hingewiesen, auch und gerade bei der Verarbeitung personenbezogener Daten die besondere Bedeutung der Versammlungsfreiheit für einen demokratischen Staat zu beachten. So gesehen, ist der Umgang mit der Versammlungsfreiheit geradezu exemplarisch für die Bereitschaft, die Grundrechte zu respektieren, sich also stets der Folgen bewußt zu sein, die eine systematische behördliche Registrierung haben kann. Und doch setzt sich offentlichtlich immer wieder die Tendenz zu ebenso schematisierten wie routinisierten Datenerhebungen und - übermittlungen durch. Um noch einmal an das Bundesverfassungsgericht zu erinnern: Wer undifferenziert jeden Protest zum Anlaß nimmt, um ebenso undifferenziert Angaben über die Demonstrationsteilnehmer zu sammeln und an eine Vielzahl von Stellen weiterzugeben, unterbindet letztlich alle Proteste. Sicher, manches konnte inzwischen korrigiert werden. Nach wie vor gibt es aber offene Fragen. Solange sie nicht durch klare, datenschutzkonforme Verfahrensvorschriften beantwortet werden, ist der von der Verfassung geforderte Respekt vor dem Grundrecht auf Versammlungsfreiheit nicht gewährleistet.

1.4.3
Gesundheitsbereich

Ähnlich bezeichnend für die Schwierigkeiten einer konsequenten Anwendung des Datenschutzes sind die Erfahrungen im Gesundheitsbereich. Der Tätigkeitsbericht gibt die Ergebnisse zweier intensiver Prüfungen wieder (Ziff. 3.2 und 3.3). Beide lassen klar erkennen, welche Konsequenzen gerade eine gezielte Inanspruchnahme der von einer automatisierten Datenverarbeitung gebotenen Möglichkeiten haben kann. Unter reinen Verarbeitungsgesichtspunkten ist etwa das "Kassen-Verbundsystem" eine durchaus selbstverständliche Folge der Automatisierung. Man braucht nur an die langen Diskussionen über den Direktzugriff in anderen Verarbeitungsbereichen zu denken. Unter Datenschutzgesichtspunkten hingegen stellt jede solche Bestrebung zunächst einmal die im Interesse des Betroffenen erforderlichen verbindlichen Übermittlungsschranken in Frage. Während also die Automatisierung den Weg zu einem einheitlichen, jederzeit zugänglichen und für die verschiedensten Zwecke nutzbaren Datenbestand eröffnet, verlangt der Datenschutz eine funktionsorientierte, von vornherein auf einen bestimmten Ausschnitt der jeweils verarbeiteten Daten beschränkte Zugriffsmöglichkeit.

Auch bei der "Basisdokumentation Psychiatrie" wiederholen sich, genaugenommen, früher schon gemachte Erfahrungen. Einmal mehr geht es darum, die automatische Datenverarbeitung zu nutzen, um die gegenwärtige Kostenstruktur bei der medizinischen Versorgung zu überprüfen. Wiederum sind es also vor allem die steigenden Ausgaben, die dazu führen, gezielt und systematisch auf die über die einzelnen Patienten vorliegenden Daten zurückzugreifen. Ebensowenig aber, wie sich die Legitimität der Bestrebungen zur Korrektur der Kostenentwicklung bestreiten läßt, können und dürfen die Gefahren übersehen werden, die mit einer Verarbeitung der Patientendaten einhergehen. Erst wenn daher alle Voraussetzungen für einen wirksamen Schutz der Patienten gegen eine Identifizierung ihrer Daten gegeben sind, kommmt eine Verwirklichung der Dokumentationsabsichten in Betracht. Die Reflexion über die Kosten darf nicht von der Reflexion über die Wahrung des Patientengeheimnisses getrennt werden. Der Datenschutz wird, anders formuliert, nicht dort gegenstandslos, wo die Wirtschaftlichkeit der Krankenversorgung auf dem Spiel steht. Er bleibt vielmehr eine verbindliche, auch bei allen Anstrengungen zur Verbesserung der Wirtschaftlichkeit zu beachtende Vorgabe.

1.4.4
Datensicherheit

Bleibt ein letzter, noch besonders zu erwähnender Problembereich: die Datensicherheit. Der Tätigkeitsbericht enthält eine ganze Reihe von Beispielen für die festgestellten gravierenden Mängel (Ziff. 8). Nicht immer geht es dabei, wie bei der Sicherheit in Datennetzen, um Sicherheitsdefizite bei der automatischen Datenverarbeitung. Unter Sicherheitsgesichtspunkten spielt die traditionelle Verarbeitung personenbezogener Daten in Akten und

Dokumenten eine genauso wichtige Rolle. Manchen mag dies zunächst überraschen. Datensicherheit ist, so könnte man in der Tat meinen, eine Aufgabe, die unmittelbar mit der automatischen Datenverarbeitung zusammenhängt und die deshalb erst dort aktuell wird, wo die entsprechenden informationstechnischen Voraussetzungen vorliegen. Für die Zukunft mag dies weitgehend stimmen. Solange freilich ein erheblicher Teil der personenbezogenen Informationen in Akten festgehalten und bearbeitet wird, liegt einer der Schwerpunkte der Datensicherheit zwangsläufig bei den Vorkehrungen, die sich auf den Zugang zu den Akten beziehen. Über die Faszination einer sich ständig verändernden Verarbeitungstechnik dürfen nicht die mit einer konventionellen Verarbeitung personenbezogener Daten einhergehenden Gefahren vernachlässigt werden. Gerade weil es sich aber um längst bekannte, keineswegs erst im Rahmen der Datenschutzdiskussion bewußt gewordene Gefahren handelt, könnte, ja müßte man annehmen, daß die notwendigen Sicherheitsmaßnahmen schon zur Selbstverständlichkeit geworden sind. An Vorschriften fehlt es ohne Zweifel nicht. Wie aber vor allem bei einzelnen Finanzämtern durchgeführte Prüfungen gezeigt haben, bleiben sie weitgehend wirkungslos. Eines sollte jedoch nicht übersehen werden. Die Prüfung mag nur ganz bestimmte Verwaltungsbereiche zum Gegenstand gehabt haben, Finanzämter und das Statistische Landesamt. Die dort festgestellten Mängel sind aber keineswegs ausschließlich für diese Stellen typisch, sondern hängen in erster Linie mit den räumlichen, für eine Vielzahl anderer Behörden ebenso kennzeichnenden Bedingungen der Verwaltungstätigkeit zusammen. Insofern sollten die Ergebnisse der Prüfung für die Landesregierung Anlaß genug sein, um sich auch bei allen sonstigen Behörden zu vergewissern, ob entsprechende Mängel vorliegen, und für eine Korrektur sorgen.

1.5
Informationsgleichgewicht im Kommunalbereich

Der Tätigkeitsbericht greift bewußt einen bislang eher vernachlässigten Aspekt des Informationsgleichgewichts auf. Soweit es bisher diskutiert wurde, stand verständlicherweise das Parlament im Vordergrund. Doch das Hessische Datenschutzgesetz verweist ausdrücklich auf die Notwendigkeit, sich auch im kommunalen Bereich mit den Auswirkungen der Informationsverarbeitung auseinanderzusetzen. Ganz in diesem Sinn konzentriert sich der Tätigkeitsbericht auf die Kommunen (Ziff. 2.1). Dies um so mehr, als es gerade hier immer wieder zu Anfragen gekommen ist und sich wahrscheinlich am ehesten in diesem Bereich Konflikte zwischen dem vom Gesetzgeber geforderten konsequenten Datenschutz und der von ihm ebenfalls angestrebten Funktionsfähigkeit der parlamentarischen Vertretung aktualisieren. Sicher, einmal mehr zeigt sich, daß die Berufung auf den Datenschutz oft nur Vorwand ist, um sich einer Informationspflicht zu entziehen. Hier wie anderswo liegt die Versuchung nahe, sich genau und nachdrücklich an den Datenschutz zu erinnern, wenn man bestimmte Angaben gar nicht machen möchte, sei es um sich lästiger Arbeit zu entziehen, sei es, weil die geforderte Information - aus welchen Gründen auch immer - verweigert werden soll. Hier wie anderswo kommt es daher in erster Linie darauf an, Fehlinterpretationen der Datenschutzvorschriften zurechtzurücken, einer Zweckentfremdung des Datenschutzes also vorzubeugen. Dennoch gibt es unstreitig durchaus beachtliche Konfliktfälle. Der Tätigkeitsbericht beschäftigt sich deshalb intensiv mit den Informationserwartungen der kommunalen Vertretungen und versucht anhand der bislang vorliegenden Erfahrungen Wege aufzuzeigen, die es zugleich ermöglichen, den Schutz der betroffenen Bürger sicherzustellen.

1.6
Allgemeiner Zugang zu Informationen (Recht auf Information)

Der Tätigkeitsbericht nähert sich den mit der Forderung nach einem Recht auf Information verbundenen Fragen in einer zugegeben überaus vorsichtigen Weise (Ziff. 11.1). Der Grund liegt auf der Hand: Allzu pauschal sind in der Vergangenheit die entsprechenden Erwartungen formuliert worden. Was aber das Recht auf Information wirklich bedeutet, wie es sich genau zu den vom geltenden Recht gebotenen Informationsmöglichkeiten verhält und wie es im einzelnen realisiert werden könnte, läßt sich im Rahmen derart abstrakter, von der Realität der Verwaltung ebenso wie von den Möglichkeiten und Interessen des einzelnen Bürgers abgehobenen Erörterungen nicht angeben. Wer daran zweifelt, sollte sich einmal die Erfahrungen mit dem Recht auf Information in den Vereinigten Staaten genau ansehen. Aus einer zunächst und ausschließlich im Interesse der Bürger geschaffenen Regelung ist im Hinblick auf weite Teile der öffentlichen Verwaltung längst ein Mittel geworden, das letztlich der besseren Information der von der Verwaltungstätigkeit betroffenen Unternehmen dient.

Der Tätigkeitsbericht zieht es deshalb vor, sich auf zweierlei zu beschränken. Er gibt zunächst einen Überblick über die verschiedenen, im Ausland durchgeführten Versuche, das Recht auf Information durch gezielte gesetzliche Bestimmungen zu garantieren. Eines wird dabei sofort deutlich, und zwar am Beispiel Frankreichs und Kanadas: So dezidiert man auch für ein Recht auf Information eintreten mag, man muß sich von Anfang an der Notwendigkeit bewußt sein, alle in Betracht kommenden Vorschriften sorgfältig mit den Datenschutzbestimmungen abzustimmen. Zwar lassen sich Datenschutz und Informationsfreiheit nicht gegeneinander ausspielen, ebensowenig ist aber zu übersehen, daß eine getrennte, nicht koordinierte Regelung unweigerlich zu einer Anwendungspraxis führt, die einen konsequenten Datenschutz ebenso wie eine folgerichtige Informationsfreiheit in Frage stellt. Nicht nur

kommt es, um noch einmal das französische Beispiel anzuführen, zu unterschiedlichen, ja widersprüchlichen Interpretationen dessen, was unter "personenbezogenen Daten" zu verstehen ist, sondern die Möglichkeiten, die bestehenden Unklarheiten der jeweiligen Regelungen systematisch zu nutzen, um die Informationserteilung gezielt zu steuern, nehmen unverhältnismäßig zu.

Eben deshalb ist eine Diskussion vorzuziehen, die an einen bestimmten, von vornherein gezielt eingeschränkten Problembereich anknüpft. Nur dann kann es wirklich gelingen, mögliche Schwierigkeiten rechtzeitig offenzulegen und zugleich die Forderung nach einem Recht auf Information in konkrete, durchaus realisierbare Vorstellungen umzusetzen. Die Erfahrung mit der Verarbeitung personenbezogener Daten im Rahmen der wissenschaftlichen Forschung und mit den verschiedenen Regelungsvorschlägen zu den Archivgesetzen sollte ausreichen, um die Vorzüge eines solchen Verfahrens zu unterstreichen. So gesehen, spricht in der Tat viel dafür, alle weiteren Überlegungen zum Recht auf Information zunächst auf den Bereich des Umweltschutzes zu konzentrieren. So evident aber das Interesse der Bürger an den damit zusammenhängenden Problemen ist, so sehr kommt es darauf an, die konkret betroffenen Verwaltungsbereiche genau abzugrenzen, sich also erst auf weitere Überlegungen einzulassen, wenn das mögliche Anwendungsgebiet genau feststeht. Von der Präzision der Fragestellung hängt auch die Chance ab, den Bereich nichtssagender allgemeiner Diskussionen endlich zu verlassen und sich an konkreten, für den Bürger wirklich relevanten Aspekten der Informationsfreiheit zu orientieren.

2. Kommunen

2.1
Zugriff der Gemeindevertretung auf Daten der Gemeindeverwaltung

Ein Gemeindevorstand bat mich um rechtliche Bewertung folgenden Sachverhalts: Veranlaßt durch einen allgemeinen Bericht des Gemeindevorstands zu aktuellen Finanzproblemen der Gemeinde hatte die Gemeindevertretung beschlossen, einen Kontrollausschuß - bestehend aus Mitgliedern des Haupt- und Finanzausschusses - zu bilden. Der Gemeindevorstand befürchtete, die Einsicht in Steuerunterlagen durch diesen Ausschuß könne zu einer Verletzung des Steuergeheimnisses führen.

2.1.1
Informationsgleichgewicht

Normalerweise verbindet man mit dem Begriff Datenschutz Vorkehrungen zum Schutz des einzelnen Bürgers. Das Hessische Datenschutzgesetz hat jedoch von Anfang an ebenso das Informationsgleichgewicht der Verfassungsorgane des Landes und der Organe der kommunalen Selbstverwaltung untereinander sowie zueinander in den Vordergrund gestellt (§ 1 Abs. 1 Nr. 2 HDSG). Diesen Weg sind später auch Nordrhein-Westfalen und Rheinland-Pfalz gegangen. Die Parlamente dieser drei Bundesländer teilten die Befürchtung, daß die Landes- und Kommunalverwaltungen durch den Ausbau der automatisierten Datenverarbeitung gegenüber ihren Parlamenten einen entscheidenden Zugewinn an "Informationsmacht" erhalten könnten. Kein Zweifel, wer über eine breite Datenbasis und über umfassende Auswertungsinstrumente verfügt, kann auch Entscheidungssituationen Dritter so beeinflussen, daß ihm genehme Resultate wahrscheinlich werden. Konkreter: In den verschiedenen Bereichen der Landes- und kommunalen Entwicklungsplanung, der Sozialverwaltung oder auch der Ordnungsverwaltung gewährt die Automatisierung der Datenverarbeitung die unschätzbaren Vorteile eines schnellen Zugriffs und vielfältiger Auswertungsmöglichkeiten und liefert damit verbesserte Grundlagen für anstehende Entscheidungen.

Landes- oder Gemeindeparlamentariern steht dieses Instrument nicht ständig zur Verfügung. Die von der Verwaltung umfassend genutzten Vorteile können für sie daher in das Gegenteil umschlagen. Immer häufiger erhalten sie Vorlagen der Exekutive, die mit einem großen Aufwand an Zahlenmaterial eine bestimmte Entscheidung nahelegen. Die in die Auswahl der Daten einfließende Problemstellung muß jedoch nicht die richtige sein. Die Gefahr wächst, daß einmal auf dem Tisch liegendes Zahlenmaterial eine eigenständige Bedeutung gewinnt und den Weg zu einer Überprüfung der Ausgangslage verstellt. Bürgervertretungen, die diese Situation nicht immer wieder kritisch in Frage stellen, werden letztlich zum Instrument der Verwaltung.

Die Bürgervertretungen sind gegenwärtig weit davon entfernt, über eine eigene ausreichende Datenbasis zu verfügen. In zunehmendem Umfang ist die Erfüllung des parlamentarischen Auftrags, politische Entscheidungen zu treffen und die Arbeit der Verwaltung zu kontrollieren, nur noch in Abhängigkeit von den von der Verwaltung zur Verfügung gestellten Informationen möglich. Da die Bürgervertretungen gegenwärtig keine Möglichkeit haben, direkt auf Datenbestände der Verwaltung zuzugreifen, bleibt ihnen als Weg zur Erweiterung der eigenen Informationsbasis nur, gezielt Auskunftsansprüche geltend zu machen.

2.1.2
Auskunftsrechte nach dem HDSG

Der hessische wie der rheinland-pfälzische Gesetzgeber beließen es, im Unterschied zum nordrhein-westfälischen Gesetzgeber, nicht bei einem abstrakten Bekenntnis zum informationellen Gleichgewicht. § 13 HDSG räumt den Parlamenten ein Auskunftsrecht gegenüber ihren Verwaltungen bzw. auf kommunaler Ebene auch gegenüber dem zuständigen Kommunalen Gebietsrechenzentrum ein.

So klar der Gesetzgeber einen Auskunftsanspruch anerkannt hat, so schnell scheint dieser Anspruch in Vergessenheit geraten zu sein. Mir ist kaum ein Fall bekannt, in dem sich der Landtag oder eine seiner Fraktionen unter Berufung auf § 13 HDSG an die Rechenzentren des DV-Verbundes gewandt hätten. Gleiches gilt für Versuche kommunaler Vertretungsorgane, Daten von den Kommunalen Gebietsrechenzentren oder Kommunalbehörden, die Datenverarbeitungsanlagen betreiben, zu erhalten. Die Gründe für diese Zurückhaltung dürften vielfältig sein. Die Mehrheitsfraktionen in Landtag und Kommunalparlamenten werden sich oft mit den Vorlagen der Verwaltung zufriedengeben. Hinzu kommt, daß ein erheblicher personeller und zeitlicher Aufwand nötig ist, um die automatisierte Datenverarbeitung für die politische Argumentation zu nutzen. Schließlich dürften die Komplexität von Verwaltung und Datenverarbeitung dazu beitragen, daß weder beim Landtag noch den kommunalen Vertretungsorganen ein reges Interesse an Ergebnissen der automatisierten Datenverarbeitung zu verzeichnen ist.

Daraus den Schluß zu ziehen, das Auskunftsrecht sei praktisch bedeutungslos und könne genaugenommen mit der anstehenden Novellierung des Hessischen Datenschutzgesetzes entfallen, wäre freilich voreilig. Der Umfang der automatisierten Datenverarbeitung nimmt kontinuierlich zu. Auch eine Verdichtung der technischen Infrastruktur ist Jahr um Jahr zu verzeichnen. Wollen die Parlamente der Gefahr entgehen, in ihrer gesetzgeberischen Aktivität immer mehr auf notarielle Funktionen beschränkt zu werden und in ihrer Kontrolltätigkeit nur noch einen kleinen Ausschnitt des Verwaltungsgeschehens zu erfassen, müssen sie wirksame Maßnahmen ergreifen. Parlamentsinformationssysteme, die sich auf die Dokumentation des Parlamentsgeschehens und eine rasche Auswertung der parlamentarischen Aktivitäten beschränken, reichen nicht aus. Unabdingbar bleibt der Zugang zu den automatisierten Verwaltungsdaten.

Nach meinen Feststellungen sind sowohl auf Landesebene als auch in den größeren Kommunen Gegenstand und Ausmaß der automatisierten Datenverarbeitung nur selten intensiv diskutiert worden. Ohne die Bereitschaft, sich mit Stand und Ausbau der automatisierten Datenverarbeitung gründlich auseinanderzusetzen, wächst nicht nur die Gefahr einer fatalen Entfremdung zwischen Legislative und Exekutive. Ein nur noch von Experten verantworteter Ausbau der ADV kann kein Ersatz für datenverarbeitungspolitische Entscheidungen sein.

2.1.3
Akteneinsichtsrecht

2.1.3.1
Keine Beschränkung auf nicht personenbezogene Daten

Anzeichen für eine zunehmende Problematisierung der gegenwärtigen Informationsverteilung konnte ich gerade in diesem Jahr verzeichnen. Der Konflikt entzündete sich am Datenschutz: Kommunalverwaltungen haben den jeweiligen Vertretungsorganen die von diesen gewünschten Daten immer wieder unter Hinweis auf den Datenschutz vorenthalten. Vordergründig durchaus verständlich, denn die Daten, um die es sich dabei handelte, waren ohne Zweifel personenbezogen. § 13 HDSG beschränkt den Auskunftsanspruch ausdrücklich auf nicht personenbezogene Daten. Der Schluß, der Gemeindevertretung stünden nur anonymisierte Daten zu, auf personenbezogene Angaben müßte sie in jedem Fall verzichten, ist aber falsch. Gerade im Bereich von Subventionen, öffentlichen Aufträgen und anderen Aktivitäten fiskalischer Natur benötigen die Gemeindevertreter mitunter auch personenbezogene Informationen, um ihre Kontrollaufgabe wirksam erfüllen zu können. Da es sich hier um die originäre, von der Verfassung in den Vordergrund gestellte Aufgabe der Gemeindeparlamente handelt, müssen Lösungen gefunden werden, die jeden Versuch, die Kontrolltätigkeit zu unterlaufen, von vornherein ausschließen. Dabei ist selbstverständlich auch das legitime Geheimhaltungsinteresse der Verwaltung zu berücksichtigen. In diesem Sinne sind auch die Vorschriften der Hessischen Gemeindeordnung zu interpretieren.

Um auf den eingangs erwähnten Fall zurückzukommen: Die Gemeindevertretung stützte ihren Beschluß offensichtlich auf § 50 Abs. 2 HGO. Diese Vorschrift sieht vor, daß die Gemeindevertretung zum Zweck der Überwachung "in bestimmten Angelegenheiten vom Gemeindevorstand in dessen Amtsräumen Einsicht in die Akten durch einen von ihr gebildeten oder bestimmten Ausschuß fordern" kann. Dieses Akteneinsichtsrecht bildet das schärfste Kontrollinstrument der Gemeindevertretung. Sie bekommt auf diese Weise direkten Zugang zu den Unterlagen der Verwaltung - ohne die Filterwirkung eines besonders für sie angefertigten Berichts oder Protokolls.

2.1.3.2
Einschränkungen

Aus der Sicht eines betroffenen Bürgers könnte die Ausübung dieses Einsichtsrechts als Eingriff in seine "informationelle Selbstbestimmung" erscheinen. Persönliche Angaben, die er der Verwaltung unter dem Siegel der Vertraulichkeit etwa in Verbindung mit Vertragsverhandlungen zur Verfügung gestellt hat, können auf diese Weise in die kommunalpolitische Auseinandersetzung geraten. Die Schutzbedürftigkeit seiner Interessen muß deshalb berücksichtigt werden.

Dem trägt schon der Gesetzeswortlaut ein Stück weit Rechnung. Die Vertretung kann von der Verwaltung nur "in bestimmten Angelegenheiten" Akteneinsicht fordern. Das Akteneinsichtsrecht erstreckt sich somit nicht allgemein auf alle Verwaltungsmaßnahmen ohne zeitliche Begrenzung. Vielmehr muß die Vertretung einen Sachgegenstand bezeichnen und ihren Einblick auch zeitlich begrenzen.

Der Gesetzgeber hat sich mit dieser einen Einschränkung nicht zufriedengegeben. Da die Gemeindevertretung als Bindeglied zwischen Bürgern und Verwaltung in der Regel öffentlich verhandelt und ihr ein verhältnismäßig großer Personenkreis angehört - somit das öffentliche Tätigwerden und die uneingeschränkte Verbreitung der gewonnenen Informationen geradezu zum tragenden Merkmal ihrer Aktivitäten gehört - gesteht ihr der Gesetzgeber das Akteneinsichtsrecht nicht unmittelbar zu. Mit der Verpflichtung, das Einsichtsrecht auf einen Ausschuß zu delegieren, wird nicht nur dem praktischen Problem Rechnung getragen, daß ein gleichzeitig von allen Gemeindevertretern wahrgenommenes Akteneinsichtsrecht technische Schwierigkeiten mit sich brächte. Die in der Regel nicht-öffentliche Tätigkeit des Ausschusses erlaubt es zudem, die Einsicht ohne einen direkten öffentlichen Druck vorzunehmen und vor der Weitergabe der sich daraus ergebenden Resultate zu prüfen, welche Angaben ohne Verletzung berechtigter Interessen des Betroffenen - oder auch des legitimen Geheimhaltungsbedürfnisses der Verwaltung - offenbart werden können.

Aufgrund der Gesetzeslage wies ich deshalb den Gemeindevorstand darauf hin, daß die Gemeindevertretung das Thema ihrer Überprüfung einschränken und konkretisieren müsse. Aus den Umständen ergab sich schließlich, daß der mit der Akteneinsicht betraute Ausschuß sich damit beschäftigen sollte, die Festlegung von Erschließungsbeiträgen durch den Gemeindevorstand für einen bestimmten Zeitraum zu untersuchen. Insoweit stand seiner Tätigkeit nichts im Wege.

Hiervon zu trennen war die Frage, ob nicht aus besonderen Gründen - hier der Wahrung des Steuergeheimnisses - zusätzliche Schranken für die Einsichtnahme zu berücksichtigen sind. Der einschlägige § 4 Abs. 1 Nr. 16 lit. aa des Kommunalabgabengesetzes wendet das Steuergeheimnis jedoch nur bei der Festsetzung "kommunaler Steuern" an. Beiträge für die Erschließung von Grundstücken sind keine "Steuern" und unterfallen nicht dem Schutzbereich des Steuergeheimnisses. Auch allgemeine Grundsätze der Amtsverschwiegenheit und die Datenschutzgesetze stehen als Geheimnisschutzvorschriften einer Kontrolltätigkeit der Gemeindevertreter in einem Kontrollausschuß nicht entgegen. Da die Gemeindeverwaltung mit einer Vielzahl personenbezogener Angaben befaßt ist, wäre anderenfalls ein großer Bereich der Tätigkeit des Gemeindevorstands einer wirksamen Kontrolle durch die Gemeindevertretung entzogen. Dies gilt im übrigen auch für die Vorgänge, die den besonderen Schutz des Steuergeheimnisses nach § 30 der Abgabenordnung genießen.

2.1.3.3
Geheimhaltungspflicht der Ausschußmitglieder

Eine weitere Frage spielt oft in diesem Zusammenhang eine wichtige Rolle. Viele Gemeindeverwaltungen sind sich nicht sicher, ob die Gemeindevertreter vor ihrer Einsichtnahme in personenbezogene Unterlagen zur Einhaltung der Datenschutzvorschriften in einem besonderen Akt "verpflichtet" werden müssen. Um das Ergebnis vorwegzunehmen: Einer besonderen "Verpflichtung" der Gemeindevertreter, die in einem solchen Kontrollgremium arbeiten, bedarf es nicht. Das Verpflichtungsgesetz vom 2. März 1974 (BGBl. I, Seite 469) sieht lediglich für den Personenkreis eine förmliche Verpflichtung vor, der nicht bereits nach § 11 Abs. 1 Nr. 2 des Strafgesetzbuches kraft seiner Funktion oder Dienststellung "Amtsträger" im Sinne der Strafvorschriften ist. Ein solcher Amtsträger ist in besonderem Maße zur Geheimhaltung der ihm in seiner Funktion bekannt gewordenen Informationen verpflichtet. Das Strafgesetzbuch droht ihm bei Verletzung dieser Vorschriften beträchtliche Strafen an. Zwar sieht das Gesetz Gemeindevertreter, soweit sie im Rahmen ihrer mehr legislativ ausgerichteten Tätigkeit aktiv werden, nicht als "Amtsträger" an. Sofern sie jedoch in Kontrollausschüssen direkt eine verwaltende Funktion ausüben - nämlich die Kontrolle des Gemeindevorstands und der ihm nachgeordneten Dienststellen - üben sie bereits unmittelbar Tätigkeiten aus, die sie als "Amtsträger" qualifizieren. Sollten sie deshalb in diesem Zusammenhang unbefugt Geheimnisse offenbaren, so träfe sie auch ohne eine besondere Verpflichtung uneingeschränkt die entsprechende Sanktion der Strafgesetze.

2.1.3.4
Unterrichtung der gesamten Gemeindevertretung

Unabhängig von dem erwähnten Fall stellt sich die Frage, ob die von Ausschußmitgliedern eingesehenen Daten ungefiltert der Gemeindevertretung gegenüber offenbart werden dürfen. Wenn schon, wie bereits erwähnt, das Gesetz die Einsichtnahme der Gesamtvertretung an einen grundsätzlich nicht öffentlich tagenden Ausschuß delegiert, so hat dies auch Konsequenzen für die Weitergabe personenbezogener Daten durch diesen Ausschuß an seinen Auftraggeber. Ein völliges Verbot der Weitergabe personenbezogener Daten an die Gemeindevertretung würde dieser in vielen Fällen die Erfüllung ihrer Kontrollaufgabe unmöglich machen. Mit dem Datenschutz nicht zu vereinbaren wäre andererseits eine Offenbarung aller eingesehenen Informationen ohne jegliche Vorprüfung. Der Kontrollausschuß muß daher bei der Beantwortung der Frage, welche Inhalte er an seinen Auftraggeber weitergeben kann und soll, sowohl den Gegenstand der Untersuchung als auch das Ergebnis berücksichtigen. Eine wichtige Richtschnur bildet das von den Datenschutzvorschriften ausdrücklich vorgesehene "Erforderlichkeitsprinzip". Mit anderen Worten: Der Ausschuß darf gegenüber der Vertretung nur so viel personenbezogene Informationen offenbaren, wie diese zur Ausübung ihrer Kontrolle benötigt. Zudem sind die schutzwürdigen Belange Betroffener gegen die Bedeutung der Einzelangaben für das Kontrollergebnis abzuwägen. Je weniger ein Bürger an vorwerfbaren Handlungen beteiligt war, desto mehr ist von einer Verwendung seiner personenbezogenen Daten abzusehen. Umgekehrt: Hat sich der Bürger nach Ansicht des Ausschusses im Zusammenspiel mit der Verwaltung rechtswidrige Vergünstigungen verschafft, so können diese Aktivitäten auch Gegenstand einer öffentlichen Sitzung werden und zwar personenbezogen.

2.1.4
Fragerecht

Die Gemeindevertretung ist freilich nicht auf das Akteneinsichtsrecht beschränkt. Nach § 50 Abs. 2 Satz 4 i.V.m. § 59 der Hessischen Gemeindeordnung ist der Gemeindevorstand verpflichtet, im Rahmen der Tagesordnung der Gemeindevertretung während ihrer Sitzungen Fragen zu beantworten. Ohne eine Beschränkung auf die beschlossene Tagesordnung können eine Fraktion oder einzelne Gemeindevertreter auch schriftliche Anfragen an den Gemeindevorstand richten. Auch zu diesem Thema erreichten mich Fragen aus den Kommunen. In diesem Zusammenhang wurde ich beispielsweise um Stellungnahme zu dem Antrag einiger Fraktionen gebeten, mit dem diese die Gemeindeverwaltung aufgefordert hatten, die Praxis der Verpachtung gemeindeeigener Grundstücke darzulegen. Die Fraktionen verlangten eine schriftliche Antwort, die nicht nur die Bezeichnung der Grundstücke und der Flächeninhalte, sondern auch die Namen der Pächter und die Höhe des Pachtpreises enthalten sollte.

Das Fragerecht ist eine notwendige Ergänzung des bereits behandelten Akteneinsichtsrechts. Während das Akteneinsichtsrecht auf eine umfassendere und intensivere Kontrolle ausgerichtet ist, dient das Fragerecht der möglichst schnellen und direkten Beantwortung konkreter Fragen. Nun berührt eine direkte schriftliche oder eine mündliche, in der Öffentlichkeit der Gemeindevertretungssitzung gegebene Antwort datenschutzrechtliche Belange der Betroffenen mehr, als in nicht-öffentlicher Sitzung offenbarte Informationen.

Die Gemeindeordnung verlangt indes keine einheitliche Form der Beantwortung. So wird auch hier in jedem Fall zu prüfen sein, ob die Belange der Betroffenen eine einheitliche, auch personenbezogene, schriftliche oder mündliche Weitergabe von Daten zulassen, oder ob nicht eine Aufspaltung des Beantwortungsverfahrens vorzunehmen ist. So war es in dem geschilderten Fall sinnvoll und erforderlich, die nichtpersonenbezogenen Teile der Fragestellung (Bezeichnung der Grundstücke und der Flächeninhalte) öffentlich und schriftlich zu beantworten. Die personenbezogenen Fragen nach den Namen der Pächter und der Höhe des Pachtpreises waren aus Gründen des Datenschutzes jedoch in nicht-öffentlicher Sitzung des zuständigen Ausschusses den Fragestellern mitzuteilen. Auf diese Weise wurde im Ergebnis das Kontrollrecht der Gemeindevertretung ebenso gewahrt wie der Schutz der personenbezogenen Angaben der Pächter.

2.1.5
Sitzungsprotokolle des Gemeindevorstandes

Auch ein weiteres in der Gemeindeordnung vorgesehenes Kontrollinstrument war Gegenstand einer an mich gerichteten Anfrage. Nach § 50 Abs. 2 Satz 4 HGO kann die Gemeindevertretung beschließen, daß der Gemeindevorstand Niederschriften über das Ergebnis seiner Sitzungen an den Vorsitzenden der Gemeindevertretung und die Vorsitzenden der Fraktionen weiterzugeben hat. Ein Gemeindevorstand gab nun zu bedenken, daß mit dem vollen Wortlaut der in den Ergebnisniederschriften festgehaltenen Beschlüsse auch vertrauliche Personalangelegenheiten mitgeteilt würden. Nach seiner Ansicht habe bei Personalangelegenheiten der Datenschutz generell Vorrang gegenüber den Kontrollbefugnissen der Gemeindevertretung.

Nach Wortlaut und Sinn der Vorschrift sollen der Vorsitzende der Gemeindevertretung und die Vorsitzenden der Fraktionen durch die Übersendung der Sitzungsprotokolle in vollem Umfang über die Beschlüsse des Gemeindevorstands unterrichtet werden. Eine Einschränkung sieht die Gemeindeordnung nicht vor. Der von den Fragestellern behauptete allgemein gültige Grundsatz, Personalangelegenheiten, Steuerverhältnisse oder auch medizinische Daten - um nur einige vergleichbar sensible Datenarten anzusprechen - seien von der Übermittlungsverpflichtung nach § 50 Abs. 2 Satz 4 HGO auszunehmen, existiert nicht. Zwar kann es in bestimmten Fällen dazu kommen, daß der Gemeindevorstand sich in seinen Sitzungen mit sehr sensiblen Daten gerade von Gemeindebediensteten befaßt. Soweit es jedoch nicht zu umgehen ist, daß diese Daten in die Beschlüsse des Vorstandes mit einfließen und aus ihnen erkennbar werden, vermögen weitere Maßnahmen den Schutz der Belange der Betroffenen zu sichern: Die Vorschrift sieht ausdrücklich eine Übersendung der Protokolle nur an die Vorsitzenden von Gemeindevertretung oder Fraktionen vor. Sie schließt damit indirekt eine Offenbarung gegenüber allen Gemeindevertretern aus. In jedem Fall wird ein Vorsitzender deshalb prüfen müssen, ob er die ihm zugegangene Information ohne Verletzung des Datenschutzes an Dritte weitergeben kann. Um ihm diese Prüfung zu erleichtern, kann der Gemeindevorstand durch besondere Übersendungsformen - etwa einen zusätzlich gesicherten Umschlag mit einem Begleitschreiben - auf die Vertraulichkeit einzelner im Protokoll enthaltener Inhalte hinweisen. Ein Hinweis auf die in § 24 HGO niedergelegte Verschwiegenheitspflicht kann ebenfalls einer weiteren Verbreitung vertraulicher Informationen vorbeugen. Noch einmal: Nur eine differenzierte Lösung wird dem Problem gerecht. Da die Hessische Gemeindeordnung ausdrücklich die Informationsweitergabe zwischen Gemeindevorstand und Gemeindevertretung regelt und dabei erkennbar auch Datenschutzbelange berücksichtigt, kann nicht allgemein aus Gründen eines "besonderen Datenschutzes" jede Übermittlung personenbezogener Daten aus bestimmten sensiblen Bereichen verweigert werden.

2.2
Unzulässige Verwendung von Einwohnermeldedaten und Sozialdaten

Für den Datenschutzbeauftragten ist der ständige Meinungsaustausch mit den kommunalen Verwaltungen eine entscheidende Informationsquelle. Nur auf diesem Wege lassen sich Datenschutzprobleme frühzeitig erkennen und gemeinsam lösen. Der Aufbau einer Prüfgruppe in diesem Jahr hat es mir ermöglicht, über konkrete Anlässe und bestehende Kontakte hinaus in größerem Umfang und zum Teil flächendeckend Praktiken der Datenverarbeitung zu überprüfen. Über einen längeren Zeitraum hinweg wurden Inhalte und Zweck der von den Gemeinden bei ihren Kommunalen Gebietsrechenzentren bestellten Auswertungen von Einwohnermeldedaten untersucht. Dabei wurde eine Vielzahl von datenschutzrechtlichen Mängeln aufgedeckt. Offensichtlich hat eine Reihe von Gemeinden noch nicht die notwendigen Konsequenzen aus dem 1982 geänderten Hessischen Meldegesetz gezogen.

Im einzelnen:
1.
Immer noch ist die irrige Ansicht anzutreffen, daß Datenübermittlungen, die sich lediglich auf Namen und Anschriften von Personen beziehen, vom Datenschutz nicht erfaßt werden. "Freie Daten" gibt es jedoch weder nach dem Meldegesetz noch in anderen Vorschriften für den Datenschutz im öffentlichen Bereich. Auch bei diesen Angaben muß vor jeder Übermittlung genau geprüft werden, ob die gesetzlichen Voraussetzungen für eine Datenweitergabe erfüllt sind.

2.
Nach § 34 Abs. 3 des Hessischen Meldegesetzes kann an Privatpersonen und nicht-öffentliche Stellen eine Melderegisterauskunft über eine Vielzahl nicht namentlich bezeichneter Einwohner (Gruppenauskunft) erteilt werden, soweit dies im öffentlichen Interesse liegt. Der Gesetzgeber schränkt damit die Auskunftserteilung bewußt ein. Ein solches "Interesse" liegt nur dann vor, wenn es entweder von dem gesamten Gemeinwesen getragen wird oder in einem engen Zusammenhang mit dem Aufgabenbereich der Gemeinde oder der rechtmäßigen Tätigkeit anderer öffentlicher Stellen steht.

Das "öffentliche Interesse" deckt sich weder mit dem Begriff der "Gemeinnützigkeit", noch bezieht es sich auf allgemein billigenswerte kulturelle, sportliche oder vergleichbare Aktivitäten.

In einer Reihe von Fällen mußte ich deshalb darauf hinweisen, daß Übermittlungen zu Werbezwecken an Sport- oder Kulturvereine, Kreditinstitute oder auch an Veranstalter von sogenannten Jahrgangstreffen nicht zulässig sind. Will eine Gemeinde solche Aktivitäten fördern, kann sie dies allenfalls dadurch tun, daß sie die von dem Interessenten frankierten Schreiben an die Bürger entgegennimmt und durch eigene Mitarbeiter mit Adressen versieht. Auf diese Weise erhalten die Empfänger die Mitteilungen ohne eine Übermittlung ihrer Daten an den eigentlichen Absender.

In mehreren Fällen mußte ich zudem einen Bruch des Steuergeheimnisses rügen, weil Sparkassen gezielt Daten von Einwohnern erhalten hatten, für die Lohnsteuerkarten ausgestellt worden waren.

3.
Entgegen den detaillierten Vorschriften über die Datenübermittlungen an öffentlich-rechtliche Religionsgesellschaften (§ 32 HMG) wurden in einigen Fällen an Kirchengemeinden ohne Differenzierung ganze Einwohnerdatenbestände übermittelt. Die in dieser Vorschrift ausdrücklich vorgesehene Beschränkung auf die Daten der Angehörigen der jeweiligen Religionsgesellschaft - allenfalls dürfen bestimmte Grunddaten der jeweiligen Familienangehörigen hinzugefügt werden -, wurde nicht beachtet. Einwohner, die einer anderen oder keiner Religionsgemeinschaft angehören, müssen von der Datenübermittlung ausgenommen werden.

4.
Bei mehreren Städten und Gemeinden mußte ich feststellen, daß die Polizei von den Meldebehörden einen Ausschnitt aus dem Gesamtbestand aller Einwohnerdaten erhalten hatte. Begründet wurde dies mit dem Hinweis auf § 45 des Hessischen Meldegesetzes, eine Sonder- und Übergangsvorschrift, nach der die Polizei namentlich am Wochenende und während der Nachtzeit Einsicht in das Melderegister ohne Beteiligung der Meldebehörde nehmen kann, da in diesen Fällen trotz der Dringlichkeit kein Meldeamtsbediensteter als Ansprechpartner zur Verfügung steht. Diese zum 31. Dezember 1985 auslaufende Vorschrift gilt nicht für den Zeitraum der Dienstbereitschaft der Meldebehörde. Vielmehr regelt § 31 des Hessischen Meldegesetzes für den "Normalfall" im Detail, unter welchen Voraussetzungen die Polizei im Einzelfall von den Meldebehörden Daten erhalten kann. Eine Übermittlung des gesamten Meldedatenbestandes läßt das Gesetz hingegen nicht zu.

5.
Bei Auswertungsaufträgen, die Meldebehörden einzelner Gemeinden ihrem Kommunalen Gebietsrechenzentrum erteilten, um Daten zur Erfüllung eigener Zwecke zu erhalten, stellte ich eine große Unsicherheit über die Berücksichtigung von Auskunfts- oder Übermittlungssperren fest.
Grundsätzlich kann jeder Bürger eine Auswertung seiner Meldedaten nur sperren, soweit damit Privatpersonen oder nichtöffentlichen Stellen Auskünfte gewährt werden soll. Mit anderen Worten: Der Datenfluß zwischen den öffentlichen Stellen oder Auswertungen durch die Gemeinde selbst werden durch diese Sperren nicht berührt. Nicht selten stellte ich jedoch fest, daß bei Auswertungen, die für Zwecke der Gemeinden bestimmt waren, die vom Rechenzentrum im Anforderungsformular gestellte Frage, ob auch die Daten von Einwohnern mit ausgewertet werden sollen, die Auskunfts- und Übermittlungssperren eintragen ließen, mit "nein" beantwortet wurde. Konkret forderte eine Gemeinde die Zusammenstellung von Daten älterer Einwohner an, um eine Altenfeier zu veranstalten, und schloß ohne Grund die Verwertung der Daten von Einwohnern aus, die eine Übermittlungssperre für die Weitergabe ihrer Daten an Religionsgesellschaften beantragt hatten. Einwohner, die sich dagegen ausgesprochen hatten, daß ihre Daten Parteien oder Adreßbuchverlagen zur Verfügung gestellt werden, bezog man jedoch in den Adressatenkreis mit ein.

Dieses Ergebnis kennzeichnet die offensichtliche Unsicherheit über Sinn und Wirkung der jeweiligen Sperren. Die von den Kommunalen Gebietsrechenzentren zur Verfügung gestellten Programme gehen auf die gesetzlichen Vorschriften detailliert ein. Sie erlauben damit vielfältige und datenschutzgerechte Auswertungen und berücksichtigen den Willen und das Interesse jedes Bürgers, der bewußt seine Daten bestimmten Interessenten vorenthalten möchte. Sie setzen jedoch eine genaue Detailkenntnis der Meldevorschriften beim Sachbearbeiter in der Meldebehörde voraus. Offensichtlich besteht noch eine Gefälle zwischen dem Wissen um die Datenschutzvorschriften bei den Rechenzentren einerseits und den betroffenen Gemeinden andererseits. Dieser Eindruck wurde in vielen Gesprächen, die ich im Anschluß an die Auswertung der Protokolle durchgeführt habe, von den betroffenen Gemeinden bestätigt.

Immer wieder beklagten die Bediensteten der Kommunen, daß ihnen für die Anwendung des Hessischen Meldegesetzes noch keine Ausführungsbestimmungen und Verwaltungsvorschriften zur Verfügung stehen und sie sich deshalb oft wegen der Komplexität der Materie überfordert fühlen.

Um diesen Kenntnisstand zu verbessern, haben meine Mitarbeiter in diesem Jahr wieder eine Reihe von Schulungsveranstaltungen durchgeführt. Darüber hinaus habe ich mit den Kommunalen Gebietsrechenzentren vereinbart, daß diese vor der Ausführung der jeweiligen Auswertungsaufträge eine sorgfältige Kontrolle vornehmen, ob der gewünschte Auftrag mit den melderechtlichen Vorschriften im Einklang steht oder offensichtlich Fehler aufweist. Nach meinen Erfahrungen nehmen die Gemeinden diese Hilfe gern an. Damit wird im voraus ein Verfahren praktiziert, das nach § 4 Abs. 1 Satz 3 des Regierungsentwurfs für ein neues Hessisches Datenschutzgesetz allgemein und für alle Bereiche des Datenschutzes gelten soll: Die geplante Regelung verpflichtet jeden Auftragnehmer einer Datenverarbeitungsmaßnahme, seinen Auftraggeber unverzüglich zu unterrichten, wenn nach seiner Ansicht eine Weisung des Auftraggebers gegen Datenschutzvorschriften verstößt.

6.
Eine Kreisverwaltung leitete regelmäßig die Durchschriften von Sozialhilfebescheiden an die Wohnortgemeinde des Sozialhilfeempfängers weiter. Sie begründete diese Maßnahme damit, daß die Gemeindeverwaltung darüber informiert sein müsse, welcher Bürger Sozialhilfe erhält. Dadurch könne dem Kreissozialamt bei Änderung der Vermögensverhältnisse gegebenenfalls rasch eine Benachrichtigung zukommen. Eine solche Übermittlung ist jedoch nach dem Sozialgesetzbuch X nicht vorgesehen. Nachdem ich die Kreisverwaltung auf die Rechtslage hingewiesen habe, wurde das Verfahren sofort eingestellt. Soweit ich die einzelnen Gemeinden darauf angesprochen habe, daß bestimmte Datenverarbeitungsmaßnahmen mit den Gesetzen nicht im Einklang stehen, führte der Kontakt beinahe ausnahmslos dazu, daß die Praktiken sofort abgestellt wurden. Fast durchweg reagierten die betroffenen Gemeinden kooperativ und zeigten sich auch an einer weiteren intensiven Zusammenarbeit interessiert.

3. Gesundheit

3.1
AIDS

AIDS war 1985 eines der zentralen Themen der gesundheitspolitischen Diskussion in der Öffentlichkeit und wird es allem Anschein nach in den nächsten Jahren bleiben. Nicht nur die Medien, sondern auch die Gesundheitsbehörden haben sich intensiv mit den medizinischen und sozialen Problemen von AIDS beschäftigt. Auch von den gesetzgebenden Körperschaften in Bund und Ländern sind diese Fragen ausführlich diskutiert worden.

Die neue, zur Zeit noch unheilbare Krankheit wirft aber nicht nur gesundheits- und gesellschaftspolitische Probleme auf, sondern berührt ebenfalls das informationelle Selbstbestimmungsrecht des von der Krankheit Betroffenen, das Recht des einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu entscheiden.

Dieser Aspekt ist allerdings bislang in der öffentlichen Diskussion - wenn überhaupt - nur am Rande behandelt worden. Er verdient jedoch nicht weniger Aufmerksamkeit, denn sowohl bei der Einführung einer personenbezogenen Meldepflicht für AIDS-Fälle, wie bei der Erstellung einer AIDS-Krankenstatistik durch das Bundesgesundheitsamt stellen sich gewichtige Datenschutzfragen.

Besonders klar erkennbar wird die Bedeutung gerade dieses Gesichtspunktes an dem Problem AIDS in Justizvollzugsanstalten. Die Frage, ob und wie Anstaltsärzte die Bediensteten der Haftanstalten über AIDS-Virusträger unter den Gefangenen unterrichten dürfen oder müssen, ist sicherlich bedeutsam für die Funktionsfähigkeit der Anstalten. Unterbleibt die Unterrichtung, sind Leistungsverweigerungen der Bediensteten nicht ausgeschlossen. Das Hauptproblem, das sich hier stellt, liegt jedoch in der Abwägung zwischen dem informationellen Selbstbestimmungsrecht der AIDS-infizierten Gefangenen und den Interessen Dritter.

3.1.1
Verbreitung der Krankheit

Aus Hessen sind bis zum 16. August 1985 dem Bundesgesundheitsamt 45 AIDS-Fälle gemeldet worden, davon 23 Todesfälle. Bundesweit sind bis zum 2. September 1985 vom Bundesgesundheitsamt 262 AIDS-Fälle, darunter 109 Todesfälle, registriert worden. Verglichen mit den in den USA bis August 1985 registrierten 12.000 AIDS-Erkrankungen, davon 6.000 mit tödlichem Verlauf, ist dies absolut und verhältnismäßig noch eine geringe Zahl. Ein dramatischer Anstieg der AIDS-bedingten Krankheits- und Todesfälle in der Bundesrepublik wird jedoch von den Gesundheitsexperten für die nächsten Jahre vorausgesagt. Hauptsächlich betroffen sind gegenwärtig zwar noch bestimmte gesellschaftliche Gruppen: Homosexuelle, Prostituierte, Drogenabhängige und Bluter. Von ca. 360 Drogenabhängigen, die sich in hessischen Rehabilitationseinrichtungen befinden, waren im September 1985 nach vorläufigen Tests 16,7% AIDS-infiziert. Unter den 75% der Gefangenen hessischer Strafanstalten, die sich an den seit August 1985 auf freiwilliger Basis angebotenen Tests beteiligt haben, waren 94 oder 2,5% AIDS-Infizierte. Nach Expertenprognosen steht allerdings die zunehmende Ausbreitung der Krankheit auch unter der Allgemeinbevölkerung bevor.

3.1.2 Konsens der politischen Entscheidungsträger

Die Gefahr der Stigmatisierung AIDS-Kranker oder lediglich AIDS- Infizierter wird, das hat die Aussprache am 12. November 1985 im Hessischen Landtag gezeigt, sowohl von der Landesregierung als auch von sämtlichen Parteien erkannt. Tatsächliche Anhaltspunkte für diese Gefahr gibt es in der Tat bereits genügend; so stößt laut Presseberichten eine AIDS-Selbsthilfegruppe in Frankfurt seit Monaten bei dem Versuch, ein Büro anzumieten, auf die mit Hinweis auf die Gefährlichkeit von AIDS begründete Weigerung der Vermieter. Einvernehmen besteht, daß Aufklärung vorrangig ist, Panik und Hysterie zu vermeiden sind und es nicht zur gesellschaftlichen Ausgrenzung und Isolierung der Betroffenen kommen darf. Ob dieser Konsens auch dann noch Bestand haben wird, wenn es darum geht, unter dem Druck der sich ausbreitenden Krankheit konkrete Abwehrmaßnahmen zu treffen, muß sich erst noch erweisen - Zweifel sind zumindest angebracht.

3.1.3
Personenbezogene Meldepflicht

Zwar hat es im Hessischen Landtag bisher nur Stimmen gegen eine personenbezogene Meldepflicht für AIDS-Infizierte an das Gesundheitsamt und damit eine staatliche Registrierung gegeben. Die Gesundheitsministerkonferenz hat sich einhellig in ihrem Beschluß vom 8./9. Oktober 1985 gleichfalls gegen die Einführung einer Meldepflicht ausgesprochen. Auch die Justizminister haben von ihrer Forderung nach einer Meldepflicht Abstand genommen. Die Bundesregierung hat erst kürzlich wieder öffentlich erklärt, eine Meldepflicht sei nicht vorgesehen (Bundestags-Drucks. 10/4239). Der Verzicht ist jedoch nur ein vorläufiger. Sowohl die Gesundheitsminister als auch die Justizminister halten die Einführung einer Meldepflicht allein zum jetzigen Zeitpunkt nicht für erforderlich. Der Hessische Minister für Arbeit, Umwelt und Soziales hat mehrfach betont, daß die Einführung einer Meldepflicht noch weiterer Prüfung bedarf und gegebenenfalls neu zur Diskussion gestellt werden muß.

Andere sind weniger zurückhaltend. Für eine Meldepflicht tritt beispielsweise der Bundesverband der Ortskrankenkassen ein. In Frankfurt hat sich eine Ärztegruppe gebildet, deren erklärtes Ziel die Einführung der Meldepflicht ist.

Wie jede gesetzliche Regelung, die eine von der Einwilligung der Betroffenen unabhängige Übermittlung und Registrierung personenbezogener Daten vorsieht, muß auch die gesetzliche Meldepflicht für AIDS-Fälle und eine damit verbundene Registrierung von AIDS-Infizierten als Eingriff in das informationelle Selbstbestimmungsrecht dem verfassungsrechtlichen Verhältnismäßigkeitsgrundsatz entsprechen. Das bedeutet, die Maßnahme muß zur Erreichung des angestrebten Zweckes geeignet sein und der mit ihr verbundene Eingriff darf seiner Intensität nach nicht außer Verhältnis zur Bedeutung der Sache und den vom Bürger hinzunehmenden Einbußen stehen (BVerfGE 65, 1, 54).

Beide Erfordernisse sind nach meiner Ansicht für die Meldepflicht nicht erfüllt. Bei Aufnahme einer Meldepflicht für AIDS-Fälle in das Bundesseuchengesetz wären u.a. der behandelnde Arzt, die hinzugezogene Hebamme oder die Leiter von Pflegeanstalten, Justizvollzugsanstalten und Heimen verpflichtet, dem Gesundheitsamt die AIDS-Infizierten oder -Erkrankten namentlich zu melden (§§ 4 und 5 BSeuchenG). Aufgabe des Gesundheitsamtes wäre dann, die erforderlichen, gesetzlich vorgesehenen seuchenpolizeilichen Maßnahmen zu treffen. Gerade deren Wirksamkeit wird jedoch für AIDS bestritten. So hält der Hessische Sozialminister die klassischen Methoden der Seuchenbekämpfung (Absonderung, Isolierung oder z.B. Tätigkeitsverbote für Prostituierte) bei sogenannten Intimkontaktkrankheiten wie AIDS für untauglich. Die Meldepflicht leiste über die statistische Erfassung hinaus keinen Beitrag zur Verhütung der Ausbreitung von AIDS (Hessischer Landtag, Plenarprotokoll 11/61). Sollte diese Einschätzung zutreffen, und ich sehe keinen Grund an ihrer Richtigkeit zu zweifeln, wäre die Aufnahme einer personenbezogenen Meldepflicht für AIDS unter im übrigen unveränderten gesetzlichen Bedingungen in das Bundesseuchengesetz verfassungsrechtlich unzulässig, da die mit einer Meldung von AIDS-Infizierten an das Gesundheitsamt auszulösenden Maßnahmen nicht geeignet sind, das angestrebte Ziel, die Verhütung und Bekämpfung von AIDS, zu erreichen.

Im Gegenteil: Befürchtungen gehen dahin, daß nach Einführung einer Meldepflicht die bestehenden Beratungs- und Untersuchungsangebote von den Betroffenen aus Furcht vor staatlicher Registrierung nicht mehr angenommen werden und damit eine wesentliche Grundlage für die Verhütung entfiele. Die Einführung einer Meldepflicht unter den derzeitigen seuchenpolizeilichen Bedingungen würde sich demnach gesundheitspolitisch eher kontraproduktiv auswirken.

Auch die Aufnahme von AIDS in das Geschlechtskrankheitengesetz, das nur in eingeschränktem Umfang eine namentliche Meldepflicht des Arztes an das Gesundheitsamt vorsieht (§§ 12 und 13 GeschlechtskrankheitenG), würde an dieser rechtlichen Bewertung der Einführung einer Meldepflicht nichts ändern.

Als Fazit läßt sich somit festhalten: Lautet das seuchenmedizinisch gebotene Handlungskonzept Information statt Isolation, ist eine personenbezogene Meldepflicht verfassungsrechtlich unzulässig.

3.1.4
Meldungen an das AIDS Register des Bundesgesundheitsamtes

Es darf nun freilich nicht der Schluß gezogen werden, jegliche Meldepflicht sei schlechthin unzulässig. Eine gesetzliche Regelung, die zum Zwecke einer sozialmedizinischen Statistik eine ausreichend anonymisierte Meldung von AIDS-Fällen vorschreibt, wäre datenschutzrechtlich natürlich anders zu bewerten.

In der Diskussion um die Meldepflicht sollte im übrigen nicht übersehen werden, daß bereits gegenwärtig Ärzte freiwillig ihnen bekannt gewordene AIDS-Krankheits- und Todesfälle an das vom Bundesgesundheitsamt geführte AIDS-Register melden. Mir ist in diesem Zusammenhang kürzlich vom Hessischen Sozialminister ein vom Bundesgesundheitsamt ausgearbeiteter Entwurf eines Fallberichtsbogens zur datenschutzrechtlichen Überprüfung zugesandt worden. Mit dem Berichtsbogen sollen die AIDS-Krankheitsfälle und AIDS-Todesfälle erfaßt werden. Der Bogen sieht eine Verschlüsselung des Vor- und Familiennamens vor. Er enthält Angaben zur Person (Geburtsdaten, Geschlecht, Obduktion, Wohnsitz etc.), Labor- und Klinikbefunde und Angaben zur Anamnese wie die Frage, ob der Patient nach 1979 gefixt hat und welche Art von Sexualkontakten er nach 1979 hatte. Die Berichte sollen mit zwei Kopien erstellt werden, von denen eine beim berichtenden Arzt verbleibt und die andere nach Abschluß der Registrierung im AIDS-Register des Bundesgesundheitsamtes an den Seuchenreferenten des betroffenen Landes weitergeleitet wird. Offen bleibt in dem Entwurf der Umfang des Datensatzes der an den Seuchenreferenten weiterzuleitenden Kopie. Der Hessische Sozialminister hat bereits Bedenken gegen die Erfassung des Namens und der Angaben zur Person geltend gemacht und vertritt die Ansicht, daß der Fallbericht in der Entwurfsform in Hessen nicht verwendet werden dürfe. Die Arbeiten an meiner Stellungnahme sind noch nicht abgeschlossen.

3.1.5
AIDS in Justizvollzugsanstalten

Hier hat ein Erlaß des Hessischen Ministers der Justiz vom 8. August 1985 (AZ.: 4550 - IV/5 - 1533/84) an die Justizvollzugsanstalten eine scharfe Kontroverse ausgelöst, die ihren Höhepunkt wohl noch nicht erreicht hat. Der Erlaß war inzwischen Anlaß von Anfragen im Hessischen Landtag wie im Bundestag. Er war außerdem Gegenstand einer Eingabe von Gefangenen aus der Justizvollzugsanstalt Kassel an mich.

In dem erwähnten Erlaß legt der Justizminister seine Rechtsauffassung zu der Frage dar, unter welchen Voraussetzungen die Anstaltsärzte verpflichtet oder berechtigt sind, die Bediensteten der Anstalt über festgestellte AIDS- (HTLV III-) Infektionen zu unterrichten. Nach Ansicht des Justizministers ist es "zulässig und erforderlich, daß alle mit der Versorgung und Betreuung der Gefangenen befaßten Vollzugsbediensteten über das Vorliegen von HTLV III-Infektionen informiert werden".

3.1.5.1
Durchbrechung der ärztlichen Schweigepflicht

Ich habe sowohl in einem gemeinsamen Gespräch mit dem Hessischen Justizminister, Anstaltsleitern und Anstaltsärzten als auch in einem nachfolgenden Schreiben an den Minister deutlich gemacht, daß ich eine derart undifferenzierte Unterrichtung der Bediensteten für rechtlich unzulässig halte. Beamtete oder angestellte Anstaltsärzte unterliegen wie ihre übrigen Kollegen der strafrechtlich gesicherten beruflichen Schweigepflicht (§ 203 Abs. 1 Nr. 1 Strafgesetzbuch). Die ärztliche Schweigepflicht erstreckt sich auf alles, was dem Arzt im Zusammenhang mit der Ausübung seines Berufs sei es mündlich, schriftlich oder sonst wie mitgeteilt wird, oder was ihm auf sonstige Weise bekannt geworden ist. Dazu gehören zweifellos auch die Ergebnisse der seit September 1985 den Gefangenen auf freiwilliger Basis angebotenen AIDS-Tests.

Die Schweigepflicht ist allerdings dann kein Hindernis für die Datenweitergabe durch den Arzt, wenn der Betroffene darin eingewilligt hat, eine Rechtsvorschrift den Arzt zur Offenbarung verpflichtet oder der Schutz eines höherwertigen Rechtsgutes die Weitergabe der Daten erfordert (sogenannter rechtfertigender Notstand - § 34 Strafgesetzbuch). Da unstreitig keine gesetzliche Vorschrift den Arzt zur Bekanntgabe von AIDS-Fällen verpflichtet, kommt neben der Einwilligung des Betroffenen mithin nur der rechtfertigende Notstand für die Durchbrechung der ärztlichen Schweigepflicht in Betracht.

3.1.5.2
Persönlichkeitsschutz der Betroffenen und Sicherheitsinteressen

Es ist anerkannt, daß ein solcher Notstand dann gegeben ist, wenn die Mitteilung zur Abwehr einer Lebens- oder schweren Gesundheitsgefahr Dritter erforderlich ist. Da die unheilbare und in der Regel tödlich verlaufende Krankheit AIDS bekanntermaßen durch Blutkontakt übertragen wird, ist nicht von der Hand zu weisen, daß das Ansteckungsrisiko für Bedienstete in den Haftanstalten aufgrund der dort herrschenden spezifischen Bedingungen besonders hoch sein kann.

Nur gilt dies meines Erachtens nicht ausnahmslos für alle (zum Teil mehrere hundert) Bediensteten einer Justizvollzugsanstalt, d.h. vom Anstaltsleiter bis zum Pförtner. Das Infektionsrisiko ist sicherlich unterschiedlich, je nachdem ob ein Bediensteter zum Krankenversorgungspersonal, Werksdienst, Stationsdienst, zu den besonderen Fachdiensten (Sozialarbeiter, Psychologen, Seelsorger), zum Transportpersonal oder zur Verwaltung gehört. Die Gründe, die mir bislang für die Notwendigkeit einer Unterrichtung genannt worden sind, lassen gerade eine nach Risikogruppen unter den Beschäftigten differenzierte Unterrichtung geboten erscheinen. Mit Erste-Hilfe-Leistungen bei Unfällen und Notfällen wie Suizidversuchen wird eben nicht jeder Bedienstete einer Haftanstalt konfrontiert. Auch die erhöhte Gefahr, in Schlägereien mit Gefangenen verwickelt zu werden, besteht nicht für alle Bediensteten. Um zu vermeiden, daß bei Belegungen von Zellen oder kurzfristig notwendig werdenden Verlegungen innerhalb der Haftanstalt Virusträger mit nichtinfizierten Gefangenen zusammengelegt werden (in diesem Falle also zur Verhinderung einer Lebensgefahr für die Mitgefangenen, die unter den spezifischen Anstaltsbedingungen entstehen könnte), braucht gleichfalls nicht jeder Bedienstete die HTLV-III-Infizierten zu kennen.

Keine ausreichende Eingrenzung ist allerdings die auf mein Schreiben gegebene Erläuterung des Justizministers, mit der Formulierung im Erlaß seien nur die unmittelbar im Kontakt mit den Gefangenen stehenden Bediensteten gemeint.

Ganz und gar nicht teilen kann ich die im Erlaß vertretene Ansicht, ein die Durchbrechung der ärztlichen Schweigepflicht rechtfertigender Notstand sei auch dann gegeben, wenn das dem Anstaltsarzt Bekanntgewordene ein behördliches Handeln unerläßlich mache, um die Sicherheit aufrechtzuerhalten oder eine schwerwiegende Störung der Ordnung der Anstalt abzuwehren. Das verfassungsrechtlich und durch die ärztliche Schweigepflicht gesicherte Persönlichkeitsrecht der AIDS-infizierten Gefangenen darf nicht um der Verwirklichung einer unbestimmten Anstaltssicherheit oder der Aufrechterhaltung der ebenfalls nicht näher beschriebenen Anstaltsordnung willen zur Disposition des Arztes gestellt werden.

Regelungsbedürftig ist jedoch nicht nur, wer von den Bediensteten zu unterrichten ist, sondern auch wie dies zu geschehen hat. Zum Verfahren der Unterrichtung enthält der Erlaß des Justizministers aber keinerlei Hinweise. Angesichts der hohen Sensibilität der Daten ist außerdem deren strenge zweckgebundene Verwendung durch die Bediensteten sicherzustellen. Auch dazu ist dem Erlaß nichts zu entnehmen.

Schließlich sollte nicht unbeachtet bleiben, daß mit der Unterrichtung von Bediensteten eine Schleuse teilweise geöffnet wird, die unter Kontrolle zu halten noch große Schwierigkeiten bereiten dürfte. Das Interesse, über AIDS-infizierte Gefangene unterrichtet zu werden, besteht nämlich keineswegs nur bei Bediensteten der Haftanstalten. Ein solches Informationsinteresse haben beispielsweise auch die in den Anstalten ehrenamtlich Tätigen, die Beschäftigten von Firmen, die Arbeiten in den Anstalten ausführen, Arbeitgeber von Freigängern, Richter, Staatsanwälte und Strafverteidiger. In jedem der genannten Fälle wird genauestens festzustellen sein, ob für die Mitglieder dieser Personengruppen aufgrund ihrer Arbeitssituation eine von AIDS-infizierten Gefangenen ausgehende Lebens- oder schwere Gesundheitsgefahr besteht, zu deren Abwehr es der Unterrichtung über AIDS-Virusträger bedarf.

3.1.6
Weitere Problembereiche

Fragen des Datenschutzes stellen sich jedoch nicht nur im Zusammenhang mit Meldepflicht, AIDS-Register und AIDS im Strafvollzug. Weitere Problemfelder sind etwa die Ausgestaltung und Durchführung von AIDS-Tests und AIDS-Beratung, die Frage, inwieweit die Polizei verpflichtet oder befugt ist, die ihr bekannten Kontaktpersonen eines AIDS-Infizierten - z.B. in der Drogenszene - über dessen Infektion zu informieren oder beispielsweise die bislang wohl nur in den USA aufgetretene Frage der schulischen Behandlung von AIDS-kranken oder -infizierten Schülern. In allen Fällen gilt es sorgfältig abzuwägen zwischen dem Recht auf informationelle Selbstbestimmung der AIDS-Infizierten und den rechtlich geschützten Interessen Dritter.

3.2
Prüfung des Rechenzentrums des AOK Landesverbands

3.2.1
Zielsetzung der Prüfung

Meine Kontrollen der Einhaltung des Datenschutzes und der Datensicherung bei den öffentlichen Stellen in Hessen beschränken sich nicht auf Überprüfungen aus konkretem Anlaß, etwa aufgrund eines Hinweises aus der Bevölkerung oder der konkreten Beschwerde eines betroffenen Bürgers. Ich sehe es als meine Aufgabe an, nach und nach bei allen großen Rechenzentren und Datenverarbeitungseinrichtungen in Hessen umfassende Kontrollen im Hinblick auf die Rechtmäßigkeit der Datenspeicherung und Datenverwendung sowie auf die Vorkehrungen der Datensicherung vorzunehmen.

Nur auf diese Weise lassen sich möglichst frühzeitig Schwachstellen aufdecken, die wegen des großen Umfangs der von diesen Stellen betriebenen Datenverarbeitung für eine Vielzahl von Bürgern negative Konsequenzen haben könnten. Nur mit eingehenden Prüfungen von Großsystemen und umfangreichen Programmpaketen lassen sich fundierte Erkenntnisse über Stand und Weiterentwicklung der datenverarbeitungs-technischen Infrastruktur in Hessen gewinnen. Schließlich bilden Kontrollergebnisse immer auch eine wertvolle Grundlage für meine präventive Beratungstätigkeit bei Behörden, die ihre Verarbeitungseinrichtungen zu größeren Rechenzentren erweitern oder sich vorhandenen Großrechenzentren anschließen wollen.

3.2.2
Umfang der Datenverarbeitung

Zweifellos gehört das Rechenzentrum des AOK Landesverbands in Ziegenhain zu den größten Einrichtungen dieser Art in Hessen. 18 der 23 Allgemeinen Ortskrankenkassen in Hessen lassen ihre Versichertendaten dort verarbeiten. Gespeichert sind Datensätze von ca. 900.000 Hauptversicherten und ca. 600.000 mitversicherten Familienangehörigen, und zwar in für Süd- und Nord-Hessen getrennten Beständen. Etwa 750 Datenendgeräte werden in den angeschlossenen Kassen eingesetzt und können direkt ("on-line") auf den Datenbestand beim Rechenzentrum zugreifen. Die zahlreichen Verarbeitungsprogramme sind Bestandteil des bundesweit entwickelten und benutzten "Informations- und Datenverarbeitungssystems der Ortskrankenkassen" (IDVS II). Meine Prüfung erstreckte sich vorrangig auf dieses System sowie die bauliche und organisatorische Datensicherung im Rechenzentrum selbst.

3.2.3
Die wichtigsten Prüfergebnisse

3.2.3.1
Datensicherung

Bei den technischen und organisatorischen Maßnahmen der Datensicherung geht es in erster Linie darum, zu verhindern, daß Unbefugte gespeicherte Daten abrufen oder in sonstiger Weise zur Kenntnis nehmen können, daß sie unberechtigt auf Daten zugreifen oder Datenträger entfernen können. § 10 HDSG sowie der gleichlautende § 6 BDSG und die zugehörigen Anlagen verlangen daher von den speichernden Stellen wirksame Vorkehrungen u.a. zur Zugangs-, Abgangs-, Organisations- und Transportkontrolle.

In diesen Punkten konnte das AOK-Rechenzentrum insgesamt einen guten Standard vorweisen. Einzelne verbesserungswürdige Schwachstellen waren den Verantwortlichen bekannt und entsprechende Korrekturen waren in Aussicht genommen. Mängel ergaben sich allerdings - wenn auch systembedingt durch den Einsatz des IDVS II - bei der Zugriffs- bzw. Benutzerkontrolle. Hier mußte ich ergänzende Maßnahmen wie z.B. regelmäßigen Wechsel der von den Mitarbeitern der Kassen verwendeten Paß-Worte verlangen. Positiv hervorzuheben ist, daß bereits während der Bauplanung des Rechenzentrums ein Gutachten zur Bausicherung beim Landeskriminalamt eingeholt wurde, um rechtzeitig fällige Schutzvorkehrungen treffen zu können.

3.2.3.2
Unzulässigkeit pauschaler Datenzugriffe

Kritisieren mußte ich dagegen die weitreichenden Möglichkeiten, die das System IDVS II für den kassenübergreifenden Datenzugriff bietet, d.h. die Möglichkeit jeder angeschlossenen Kasse, auf die Mitglieds- und Leistungsdaten jeder anderen AOK im gleichen Verbund (also Nord- bzw. Südhessen) in großem Umfang zuzugreifen bzw. diese abzurufen. Ein solcher sog. "Kassenübergriff" stellt rechtlich eine Datenübermittlung zwischen zwei Leistungsträgern dar, die nach § 69 Abs. 1 Nr. 1 SGB X nur zulässig ist, wenn die abgerufenen Daten für die Leistungserbringung der abrufenden Mitgliedskasse im Einzelfall erforderlich ist. Zwar sind solche Situationen denkbar, etwa beim Wechsel eines Versicherten von einer zur anderen Kasse. Jedoch gibt es keine juristische Rechtfertigung für ein umfassendes Datenverbund-System von Sozialversicherungsträgern, bei dem Datenflüsse mit teilweise sehr sensitiven Informationen - wie z.B. Diagnosen - ohne Kontrolle durch die zuständige, als speichernde Stelle verantwortliche AOK möglich sind.

Ich habe daher den AOK Landesverband aufgefordert, im einzelnen nachzuweisen, zu welchen Zwecken jeweils welche Datensätze aus den verfügbaren Verarbeitungsprogrammen bestimmten anderen Kassen im direkten Zugriff zur Verfügung stehen müssen und wie getätigte Abrufe von der speichernden Kasse kontrolliert werden können. Außerdem habe ich darauf hingewiesen, daß für die Übertragung von Aufgaben von einer AOK an eine andere nach § 88 SGB X bestimmte einschränkende Voraussetzungen gelten und ein förmlicher Auftrag erteilt werden muß. Soweit hinsichtlich Anlaß und Umfang solcher "Kassenübergriffe" die Notwendigkeit nicht belegt werden kann, müssen die Datenbestände der einzelnen Kassen durch entsprechende Programmänderungen (wieder) abgeschottet werden.

Daß bei der Entwicklung des IDVS II die Bequemlichkeit der technischen Möglichkeiten der automatisierten, dezentral ausgestalteten Datenverarbeitung Vorrang hatte vor einer eingehenden Bedarfsanalyse für die dadurch eröffneten Datenflüsse, wie sie die datenschutzrechtlichen Bestimmungen verlangen, ist offensichtlich. Auch die Datenschutzbeauftragten anderer Länder haben die zu weitgehenden Abrufmöglichkeiten zwischen den Kassen beanstandet; gleiches gilt für den Hessischen Sozialminister. Daß erhebliche Begrenzungen des kassenübergreifenden Datenzugriffs geboten sind, wird auch aus Kreisen der Ortskrankenkassen eingeräumt; zuständige Gremien der Landesverbände bzw. des AOK-Bundesverbands sind mit der Prüfung von Restriktionsmöglichkeiten beauftragt.

Ich habe allerdings vorsorglich darauf aufmerksam gemacht, daß die gesetzliche Aufgabe der Bundesverbände, ADV-Programme sowie Datenschutzmaßnahmen bundesweit zu entwickeln und abzustimmen (§ 414 f Satz 2 Buchst. h RVO), an der Verantwortlichkeit der einzelnen Kassen bzw. deren Landesverbänden für die Rechtmäßigkeit der eingesetzen Verfahren nichts ändert. Ich werde m.a.W. darauf dringen, daß von mir zur Einhaltung der sozialdatenschutzrechtlichen Vorgaben für erforderlich gehaltene Programmänderungen zügig realisiert werden, und zwar gegebenenfalls auch allein auf Landesebene, wenn die Korrekturen nicht rechtzeitig über den Bundesverband umgesetzt werden können.

3.2.3.3
Sperrung und Löschung

Die Datenschutzgesetze verlangen von den datenspeichernden Stellen, daß sie personenbezogene Daten zumindest sperren, wenn sie für die Aufgabenerfüllung nicht mehr benötigt werden (vgl. § 14 Abs. 2 Satz 2 BDSG, § 19 Abs. 2 Satz 2 HDSG). Gesperrte Daten stehen für den laufenden Verwaltungsvollzug nicht mehr zur Verfügung; sie können nur noch unter bestimmten engen Voraussetzungen - z.B. zur Behebung einer bestehenden Beweisnot - reaktiviert werden. § 84 SGB X verschärft diese Sperrungspflicht für die Sozialleistungsträger zu einer Löschungspflicht.

Damit soll verhindert werden, daß gerade die vielfach sensitiven Datenbestände der Sozialverwaltung auf Dauer und auf Vorrat vorgehalten werden. Allerdings hat der Gesetzgeber für die Löschungspflicht die zusätzliche Voraussetzung aufgestellt, daß durch die Datenlöschung schutzwürdige Belange des Versicherten, Sozialhilfeempfängers usw. nicht beeinträchtigt werden dürfen. Dies wäre z.B. dann der Fall, wenn der Betroffene umfangreiche Antragsunterlagen nach längerer Zeit wieder beibringen müßte.

Nach meinen Feststellungen tun sich nahezu alle Sozialleistungsträger mit der Einhaltung des gesetzlichen Sperrungs- bzw. Löschungsgebots sehr schwer. Dies liegt nicht zuletzt daran, daß insbesondere in der Sozialversicherung, etwa der Rentenversicherung, häufig auf vor langer Zeit erhobene bzw. ermittelte Informationen zurückgegriffen werden muß. Pauschale Lösungen kommen mithin sicherlich nicht in Betracht.

Beim Prüfbesuch im AOK-Rechenzentrum mußte ich jedoch feststellen, daß seit dem erstmaligen Einsatz des IDVS II in dieser Einrichtung, also seit 1975, kein einziges Versichertendatum gesperrt oder gelöscht worden war, ja daß dieses System gar keine Sperrungs- oder Löschungsprogramme oder jedenfalls Prüffristverfahren anbietet. Ich muß jedoch verlangen, daß die Krankenkassen bzw. ihre Verbände sich für die einzelnen gespeicherten Datenkategorien über die Notwendigkeit der Bereithaltung im laufenden Bestand klar werden und solche personenbezogenen Informationen, die für die Aufgabenerfüllung nicht mehr benötigt werden, löschen bzw. sperren. Auch bei anderen Sozialversicherungsträgern werde ich künftig verstärkt auf die Einhaltung des § 84 SGB X achten.

3.2.3.4
Weiteres Verfahren

Ich habe den AOK Landesverband um Stellungnahme zu meinen Kritikpunkten gebeten und weitere Gespräche angeboten, um meine Bereitschaft zu unterstreichen, bei der Lösung der angesprochenen Datenschutz- und Datensicherungsprobleme beratend mitzuwirken. Den Hessischen Sozialminister als oberste Aufsichtsbehörde für die Sozialversicherungsträger in Hessen habe ich von meinen Prüfergebnissen unterrichtet.

3.3
Basisdokumentation Psychiatrie (BADO) des LWV Hessen

3.3.1
Zielsetzung und Durchführung

"Die psychiatrische Basisdokumentation hat zum Ziel, über die Nutzung verschiedener Einrichtungen durch Patienten zu informieren. Die Daten sollen darüber Auskunft geben, welche Patienten in welche stationäre Behandlung gelangen, wie sie dort hinkommen, und wohin sie entlassen werden. Die Basisdokumentation schafft Voraussetzungen für eine erste Annäherung an die Fragestellung: 'Welche Leistungen (Versorgung von wievielen Kranken mit welchen Erkrankungen sowie mit welchen personenbezogenen und sozialen Merkmalen) werden von welchen Krankenhäusern für welche Regionen zu welchen Kosten erbracht?' Die Dokumentation beschränkt sich z.Z. auf die klinisch-stationäre Behandlung. Mittel- und langfristiges Ziel muß es sein, die Dokumentation auf ambulante und teilstationäre sowie komplementäre und rehabilitative Formen der am regionalen Bedarf orientierten Versorgung auszudehnen."

So formuliert die "Bundesarbeitsgemeinschaft der Träger psychiatrischer Krankenhäuser" Auftrag und Zielsetzung dieses bundesweit durchgeführten Projekts. In Hessen werden zur Durchführung dieses Vorhabens von allen Patienten, die ein psychiatrisches Krankenhaus (PKH) des Landeswohlfahrtsverbands (LWV) aufsuchen, im Zusammenhang mit der ärztlichen Anamnese Angaben zu folgenden Fragen erhoben: Welche Art von Krankenhaus bzw. ein Arzt welcher Fachrichtung hat den Patienten eingewiesen? Durch welche Institution wurde der Zugang des Patienten veranlaßt (z.B. Suchtberatungsstelle, Heim)? Wie ist die Wohnsituation des Patienten (z.B. Privatwohnung, Altenheim, ohne festen Wohnsitz)? Mit wem lebt der Patient zusammen (z.B. Eltern, alleinlebend)? Wie ist seine jetzige berufliche Situation? Und schließlich: War der Betroffene bereits früher - und wenn ja, wie häufig - in stationärer psychiatrischer Behandlung?

Diese auch und gerade für die spezielle psychiatrische Behandlung wichtigen Daten werden in den Krankenhäusern erfaßt und gespeichert; der Originalerhebungsbogen kommt in die Krankenakte. An die Hauptverwaltung des Landeswohlfahrtverbands werden diese Informationen, kombiniert mit weiteren Daten über die Aufenthaltsdauer, die gestellten Diagnosen usw. weitergegeben. Dies geschieht ohne Nennung der Personalien des Patienten, die individuelle Aufnahmenummer wird verschlüsselt, statt des vollen Geburtstags wird nur das Geburtsjahr übermittelt. Damit soll sichergestellt werden, daß der LWV als Krankenhausträger nur aggregierte Daten zur Verbesserung der Analyse und Planung der stationären psychiatrischen Versorgung erhält, das Patienten- bzw. Arztgeheimnis jedoch im Interesse des einzelnen Kranken gewahrt bleibt (zur Unzulänglichkeit dieser Anonymisierung vgl. unten 3.3.3.2).

Die Datenerfassung für die BADO im Bereich des LWV wird seit Januar 1984 vorgenommen. Auswertungen sind bis heute nicht durchgeführt worden; die Auswertungsprogramme sollen erst dann freigegeben werden, wenn der Hessische Datenschutzbeauftragte keine datenschutzrechtlichen Einwände mehr erhebt. Daß und warum dieser datenschutzgerechte Zustand des BADO-Projekts nach wie vor nicht erreicht ist, ich vielmehr eine förmliche Beanstandung aussprechen mußte, wird in den folgenden Abschnitten erläutert.

3.3.2
Erste Datenschutzkontrolle
Anfragen und Reaktionen

Anfang Juni 1984 fand mein erster Prüfbesuch, verbunden mit einem ausführlichen Informationsgespräch, bei der Hauptverwaltung des LWV in Kassel statt. Dabei zeigte sich, daß eine abschließende Prüfung des BADO-Projekts noch nicht möglich war: Einmal konnten wegen des im Umbau befindlichen Rechenzentrums des LWV die Datensicherungsmaßnahmen - wesentlicher Bestandteil der Datenschutzvoraussetzungen für das BADO-Projekt - nur vorläufig geprüft werden. Zum anderen lag die notwendige exakte Verfahrensbeschreibung noch nicht vor. Ich konnte daher dem Verwaltungsausschuß des LWV Hessen in meiner Stellungnahme vom 5. Juli 1984 lediglich mitteilen, daß ein DV-Verfahren, das der Verbesserung der Planung und stationären Patientenversorgung im psychiatrischen Bereich des LWV Hessen dient, nur dann als datenschutzrechtlich zulässig betrachtet werden könne, wenn es gewährleistet, daß eine Verletzung des Patientengeheimnisses ausgeschlossen ist. Dies bedeute, daß lediglich statistische Daten verarbeitet werden dürften, und daß die Hauptverwaltung des LWV Hessen, die die BADO-Daten erhält, nicht in der Lage sein dürfe, diese statistischen Daten mit den bereits vorhandenen Patientendaten für die Kostenabrechnung zu verknüpfen. Für die Erfüllung dieser Forderung habe ich dem Verwaltungsausschuß des LWV eine Anzahl von Voraussetzungen genannt, insbesondere habe ich Vorschläge und Anregungen für die datenschutzkonforme Ausgestaltung des DV-Verfahrens gegeben.

Im Laufe des zweiten Halbjahres 1984 erhielt ich dann verschiedene Eingaben von Personen und Stellen innerhalb und außerhalb des LWV, die Bedenken gegen die Einführung des BADO- Projekts äußerten. Ich habe diesen in einer Zwischennachricht die wesentlichen Ergebnisse meines Prüfbesuches vom Juni 1984 mitgeteilt und darauf hingewiesen, daß ich grundsätzlich die Einführung einer Basisdokumentation Psychiatrie unter Beachtung des Patientengeheimnisses und des Datenschutzes für möglich halte, jedoch gegen das BADO-Projekt des LWV Hessen zum damaligen Stand noch erhebliche datenschutzrechtliche Vorbehalte machen müsse.

Mit Datum vom 12. Juli 1984 stellte die Abgeordnete Blaul (Grüne) eine Kleine Anfrage im Hessischen Landtag "betreffend Einführung der medizinischen Basisdokumentation (BADO) in den psychiatrischen Krankenhäusern des LWV" (Drucks. 11/1615). Diese Anfrage wurde mit Landtagsdrucksache vom 27. August 1984 (Nr. 11/1789) beantwortet. Der Hessische Minister für Arbeit, Umwelt und Soziales teilte in seiner Antwort mit, der Hessische Datenschutzbeauftragte habe "keine datenschutzrechtlichen Bedenken gegen die Basisdokumentation", eine in dieser Verkürzung und Pauschalität irreführende Information.

Trotz verschiedener Erinnerungen äußerte sich der Verwaltungsausschuß des LWV Hessen erst mehr als ein halbes Jahr später zu meinen Kritikpunkten, Anregungen und Vorschlägen. Dabei fehlte immer noch ein Teil der von mir erbetenen Unterlagen. Außerdem stellte sich heraus, daß auch die baulichen Datensicherungsmaßnahmen noch nicht abgeschlossen waren. Unter diesen Umständen mußte ich meinen vorgesehenen zweiten Prüfungsbesuch immmer wieder verschieben, da eine endgültige datenschutzrechtliche Beurteilung des BADO-Projekts nicht möglich gewesen wäre.

Aus den mir Anfang Juli 1985 nach erneuter Anmahnung übersandten Unterlagen konnte ich entnehmen, daß eine Reihe meiner Kritikpunkte noch immer nicht ausgeräumt war. Dies galt insbesondere hinsichtlich der Maßnahmen der Datensicherung, einer ausreichenden Anonymisierung, der Zugangsregelung zu den Terminals in den einzelnen Kliniken und für die vom LWV an seine psychiatrischen Kliniken versandten "Informationen über die Erfassung, Speicherung und Weiterleitung von Daten" vom 30. April 1985.

3.3.3
Zweite Datenschutzkontrolle

3.3.3.1
Maßstäbe

Daraufhin habe ich am 24. und 25. Oktober 1985 den zweiten Kontrollbesuch durchgeführt, der sich im wesentlichen auf das Rechenzentrum der LWV-Hauptverwaltung und - exemplarisch für die datenerfassenden Krankenhäuser - auf die Räumlichkeiten im PKH Merxhausen erstreckte, in denen die BADO-Daten erfaßt und in die Terminals eingegeben werden. Ausgangspunkt dieser zweiten Datenschutzprüfung waren die Kriterien, die ich in meiner ausführlichen Stellungnahme vom 5. Juli 1984 für eine datenschutzgerechte Durchführung des BADO-Projekts aufgestellt hatte. Maßstab für meine Bewertung war auch die seither verstrichene Frist, mithin die Tatsache, daß zum Zeitpunkt dieses Prüfbesuchs fast 16 Monate (!) vergangen waren, in denen die von mir genannten datenschutzrechtlichen Vorgaben realisiert werden konnten. Schließlich erscheint es mir auch geboten, noch einmal zu unterstreichen, daß es sich angesichts der schrecklichen Vorkommnisse während der Nazi-Zeit bei jedweder Registrierung oder Speicherung von Psychatriepatienten nicht um ein "normales" Verarbeitungsprojekt handelt, sondern höchste Sensibilität für die Wahrung des Patientengeheimnisses gerade in diesem Bereich angezeigt ist. Dies bewiesen nicht zuletzt die Interventionen von Mitgliedern der Verbandsversammlung des LWV, von betroffenen Gruppen wie der Hessischen Gesellschaft für Soziale Psychiatrie und von Ärzten in den Krankenanstalten des LWV.

Sicher, einiges war in der Zwischenzeit geschehen: Bestimmte Mängel der Bausicherung bei der DV-Stelle, etwa bei den Türen und Fenstern, wurden abgestellt. Eine Arbeitsanweisung regelt Einzelheiten des Umgangs mit den BADO-Daten im Rechenzentrum. Doch mußte ich feststellen, daß nach wie vor erhebliche Defizite vor allem bei der Anonymisierung der Patientendaten (vgl. 3.3.3.2) sowie bei den Vorkehrungen der Datensicherung (vgl. 3.3.3.3) bestehen. Auch liegt mir nach wie vor für die Datenverarbeitung zur Durchführung der BADO keine exakte Verfahrensbeschreibung vor, wie sie bei ADV-Anwendern üblich ist und die für mich eine unabdingbare Voraussetzung ordnungsgemäßer Datenverarbeitung darstellt. Darunter verstehe ich ein Dokument, das zusammenfassend Ist- und Sollzustand darstellt, den zu verarbeitenden Datenkatalog festlegt, Schnittstellen zu anderen Verfahren aufzeigt, die Auswertungen vorgibt, die Datenschutzmaßnahmen aufführt usw. - kurz eine Unterlage, die den für den Landes- und Kommunalen Automationsausschuß obligatorischen Untersuchungsberichten entspricht. Für den Datenschutzbeauftragten ist es ein inakzeptabler Zustand, daß er sich das Gesamtbild über die Erhebung, Speicherung und Verknüpfung der BADO-Daten aus einer Vielzahl verstreuter - teilweise veralteter - Unterlagen und mündlicher Zusatzauskünfte, teilweise sogar aus Unterlagen dritter Stellen zusammensuchen muß.

3.3.3.2
Anonymisierung

Kernpunkt der Zulässigkeit des BADO-Projekts - das hatte ich in meinem Schreiben vom 5. Juli 1984 unterstrichen und eingehend begründet - ist die ausreichende Anonymisierung der von den psychiatrischen Krankenhäusern an den LWV übermittelten Patientendaten. Es muß gewährleistet sein, daß der LWV zum einen nur anonymisierte Angaben erhält und daß beim LWV der Rückbezug auf den einzelnen Kranken nicht oder nur mit unverhältnismäßigem Aufwand wiederhergestellt werden kann.

Nur so kann die Zielsetzung der BADO, dem LWV als Krankenhausträger die Planung der psychiatrischen Versorgung mit aggregiertem Zahlenmaterial zu erleichtern, mit der gebotenen strikten Wahrung des Patientengeheimnisses in Einklang gebracht werden.

Betrachtet man zum einen die Art der Verschlüsselung der Aufnahmenummer, zum anderen den erheblichen Umfang personenbezogener Datenverarbeitung zu Abrechnungszwecken in der DV-Stelle des LWV, stellt sich heraus, daß jedenfalls für den Teil der Patienten in den psychiatrischen Krankenhäusern, für die der LWV auch als Kostenträger fungiert, die Gefahr einer vergleichsweise einfachen Reidentifizierung besteht. Die Aufgabe, die Verknüpfbarkeit von BADO-Daten und Abrechnungsdaten beim LWV zu verhindern, ist mithin nicht ausreichend gelöst.

Zwar wird die Aufnahmenummer im BADO-Datensatz verschlüsselt. Der für diese Verschlüsselung gewählte Algorithmus ist jedoch so einfach aufgebaut, daß er unschwer erraten werden kann, wenn man nur wenige verschlüsselte Fallnummern mit den zugehörigen ursprünglichen Aufnahmenummern vergleicht.

Die entschlüsselte Aufnahmenummer wiederum kann als Verknüpfungsmerkmal der BADO-Datensätze mit der Schnittstellendatei verwendet werden, die aus dem FALK-Verfahren erzeugt und als Datenträger von den Kommunalen Gebietsrechenzentren geliefert wird (sog. DATAUS); diese Schnittstellensätze aber enthalten den Patientennamen im Klartext.

Auch ohne Entschlüsselung der Fallnummer lassen sich BADO-Daten mit dieser Schnittstellendatei abgleichen, weil mehrere Merkmale, wie etwa die Hausnummer, das Aufnahme- und Entlassungsdatum sowie der Kostenträger, in beiden Datensätzen korrespondieren; auch auf diese Weise könnte also in vielen Fällen der Patientenbezug wiederhergestellt werden.

Nun ist zwar das von mir geforderte Verbot der Erstellung und Verwendung von Merkmalsvergleichsprogrammen zur Deanonymisierung der BADO-Daten durch die "Arbeitsanweisung" vom 25. Juni 1985 erlassen worden - nebenbei gesagt ein volles Jahr (!) nach meinem Schreiben vom 5. Juli 1984, in dem ich diesen Punkt als dringlich angesprochen hatte. Doch kann diese Maßnahme die aufgezeigte DV- technisch oder mittels Listenvergleich mögliche Wiederherstellung des Patientenbezugs nicht kompensieren.

Zur Klarstellung: Niemand unterstellt den Mitarbeitern des LWV, die sensitiven, teilweise sogar intimen (vgl. 3.3.1) BADO-Daten unzulässigerweise entschlüsseln und einzelnen Psychiatriepatienten zuordnen zu wollen. Auf solche individuellen Motive kommt es jedoch für die Beurteilung der Frage, ob die Anonymisierung ausreicht, nicht an. Entscheidend für die Personenbeziehbarkeit ist allein das bei der speichernden Stelle oder dem Datenempfänger - hier dem LWV - vorhandene Zusatzwissen, das eine Reidentifizierung möglich machen könnte.

3.3.3.3
Datensicherung

Vor diesem Hintergrund erhalten auch die weiteren anläßlich meines Kontrollbesuchs festgestellten Mängel der Datensicherung sowohl im Rechenzentrum des LWV als auch beim PKH Merxhausen besonderes Gewicht. Dazu nur wenige Beispiele:

Die "Arbeitsanweisung" an die DV-Stelle des LWV vom 25. Juni 1985 enthält zwar eine Reihe konkreter Gebote der Datensicherung an die mit der Verarbeitung von BADO-Daten Beschäftigten, doch stellte sich heraus, daß ein Teil der angeordneten Maßnahmen nicht realisiert worden war. Oder die Zugriffskontrolle mittels Paßwort: Beim LWV arbeiten Rechenzentrum, Datenerfassung und Kasse jeweils nur mit einem Paßwort, das zudem bisher noch nie geändert worden ist. Damit verliert das Paßwort jegliche Funktion für den Schutz vor unbefugtem Zugriff und für die Sicherung des auf die Arbeitsaufgabe des einzelnen Mitarbeiters beschränkten Datenzugangs. Eine individuelle Paßwortzuteilung fehlte auch im PKH Merxhausen, wobei dort die Funktion der Eingabe- und Speicherkontrolle im Vordergrund steht.

Und schließlich: Trotz allen Verständnisses für die organisatorischen und finanziellen Probleme, die der Ausbau einer kleineren DV-Stelle zu einem Rechenzentrum mit umfangreichen personenbezogenen DV-Aufgaben für den LWV mit sich bringt, gehört für mich der Closed-Shop-Betrieb im Rechenzentrum ebenso zu den Bedingungen ordnungsgemäßer Datenverarbeitung wie die ebenfalls noch nicht realisierte Funktionstrennung zwischen Systemanalyse und Programmierung sowie zwischen Test und Produktion.

3.3.3.4
Interner Datenschutzbeauftragter

Zu den vom LWV nicht erfüllten Leitungsaufgaben im Bereich des Datenschutzes gehört auch, daß bisher nicht förmlich ein Datenschutzbeauftragter bestellt worden ist. Die gesetzliche Pflicht für alle Sozialleistungsträger, einen Datenschutzbeauftragten zu bestellen, gilt bereits seit fünf Jahren, seit dem Inkrafttreten des 2. Kapitels des SGB X und damit des § 79 Abs. 1, 2. Halbs. in Verbindung mit Abs. 3. Für die persönlichen Voraussetzungen ebenso wie für die Aufgaben und Befugnisse dieses Beauftragten gelten die Vorschriften der §§ 28, 29 BDSG entsprechend.

Zwar ist in der Geschäftsverteilung der Datenschutz einem Mitarbeiter übertragen worden. Unter einer ordnungsgemäßen Bestellung im Sinne des § 28 Abs. 1 BDSG verstehe ich jedoch, daß sie förmlich durch die Leitung der Hauptverwaltung des LWV erfolgt, daß in einer entsprechenden Verfügung das Verhältnis des Beauftragten zur Behördenleitung ebenso wie seine Befugnisse gegenüber den Fachabteilungen (vgl. § 28 Abs. 3 und § 29 Sätze 1 und 3 BDSG) festgelegt werden und daß die Mitarbeiter über Aufgaben und Kompetenzen des bestellten Beauftragten informiert werden. Dabei ist darauf zu achten, daß der betroffene Mitarbeiter nicht durch die hausinterne Datenschutzkontrollfunktion in einen Interessenkonflikt zu seinen anderen Dienstaufgaben, etwa die gleichzeitige Verantwortlichkeit für die Datenverarbeitung und den Betrieb des Rechenzentrums, gebracht wird.

3.3.3.5
Unterrichtung der Patienten

Bleibt das Problem der Information der Patienten über die Verarbeitung ihrer Daten in den psychiatrischen Krankenhäusern. Dazu hat der LWV ein Informationsblatt betr. "die Erfassung, Speicherung und Weiterleitung von Daten" erarbeitet und an die Krankenhäuser versandt. Zumal im Zusammenhang mit der BADO ist es jedoch geeignet, zu erheblichen Mißverständnissen zu führen. Es suggeriert, mit der Weiterleitung von medizinischen Angaben für die BADO komme der LWV einer "gesetzlich auferlegten Dokumentationspflicht" nach und der Patient müsse daran mitwirken, was nicht zutrifft. Außerdem geht die Begründung der Zulässigkeit der Datenspeicherung mit §§ 13, 14 Hessisches Krankenhausgesetz fehl.

Richtig ist, daß für die psychiatrischen Krankenhäuser, die vom LWV in seiner Funktion als Leistungsträger (§ 35 SGB I) betrieben werden, wegen der Verweisung in § 79 Abs. 2 SGB X die Vorschrift des § 9 BDSG anzuwenden ist. § 9 Abs. 2 BDSG verlangt, daß der Betroffene auf die Rechtsgrundlage der Datenspeicherung und bei deren Fehlen auf die Freiwilligkeit der Angabe seiner Daten hinzuweisen ist. Für die zur Abrechnung wie zur medizinischen Behandlung erforderlichen Daten, die beim Patienten erhoben werden - sei es durch eigene Eintragung in das Aufnahmeformular oder sei es bei Ausfüllung durch einen Krankenhausmitarbeiter nach Angaben des Patienten -, ist der Kranke über die jeweilige Rechtsgrundlage zu informieren; in Betracht kommen z.B. das Hessische Freiheitsentziehungsgesetz (HFEG), das Strafgesetzbuch (StGB), die Reichsversicherungsordnung (RVO), der Behandlungsvertrag usw.

3.3.3.6
Beanstandung nach § 26 HDSG; notwendige Maßnahmen

Das Ergebnis dieses zweiten Kontrollbesuchs läßt sich mithin wie folgt zusammenfassen: Die Anonymisierung der BADO-Daten ist unzureichend; durch den Abgleich mit anderen personenbezogenen Datenbeständen läßt sich ohne unverhältnismäßigen Aufwand ein Rückbezug auf den einzelnen Patienten herstellen. Die notwendigen technischen und organisatorischen Vorkehrungen der Datensicherung sind nicht in ausreichendem Maß vorhanden. Es gibt keinen ordnungsgemäß bestellten internen Datenschutzbeauftragten. Die Patienten werden irreführend informiert. Zwar sind die größten Mängel der baulichen Zugangssicherung behoben, im übrigen aber stellt sich die Datenschutzsituation im Hinblick auf die Verarbeitung der BADO-Daten - wie übrigens auch der sonstigen verarbeiteten Abrechnungs- und Hilfeempfänger-Daten - kaum besser dar als zum Zeitpunkt meines ersten Prüfbesuchs im Juni 1984.

Die aufgezeigten Verstöße und Mängel mußte ich daher nach § 26 HDSG beanstanden, über diese Beanstandung den Hessischen Sozialminister unterrichten und den LWV unter Fristsetzung zur Stellungnahme auffordern.

Daraus folgt, daß bis auf weiteres eine Freigabe der Auswertungsprogramme für die BADO nicht in Betracht kommt. Vielmehr gilt es zunächst, die folgenden vordringlichen Maßnahmen durchzuführen:

1. Es wird eine aktuelle BADO-Verfahrensbeschreibung vorgelegt.
2. Die Anonymisierung der BADO-Datensätze wird verbessert. Dies kann z.B. durch eine Komplizierung der Verschlüsselungsmethode, verbunden mit der Herausnahme einiger Angaben aus dem übermittelten Datensatz, geschehen.
3. Die Verknüpfungs- bzw. Abgleichsmöglichkeit mit anderen personenbezogenen Dateien muß so erschwert werden, daß sie auch technisch nur mit unverhältnismäßigem Aufwand zu einer Reidentifizierung der Patienten führen kann.
4. Es wird dafür Sorge getragen und im einzelnen nachgewiesen, daß die "Arbeitsanweisung" vom 25. Juni 1985 strikt eingehalten wird.
5. Die Funktionen "Test" und "Produktion" werden - zumindest projektweise - getrennt.
6. Es wird sichergestellt, daß entsprechend der DV-Befugnis des einzelnen Mitarbeiters, also personen- und funktionsbezogen, Paßworte vergeben und in regelmäßigen Abständen geändert werden, und zwar sowohl im LWV als auch bei den psychiatrischen Krankenhäusern.
7. Die Protokollierung der Dateizugriffe wird eingeführt und deren regelmäßige Überprüfung sichergestellt.
8. Im Vorgriff auf die noch im Entwurf stehende LWV-weite "Dienstanweisung Datenschutz/Datensicherung" wird für die psychiatrischen Krankenhäuser einer der o.a. "Arbeitsanweisung" entsprechende Verfügung für den datenschutzgerechten Umgang mit BADO-Daten erlassen.
9. Es wird entsprechend §§ 28, 29 BDSG ein Datenschutzbeauftragter bestellt.
10. Die irreführende Patienteninformation wird aus den Krankenhäusern zurückgerufen und durch die zutreffende Unterrichtung der Betroffenen ersetzt.

Die Realisierung dieser Maßnahmen soll ermöglichen, daß die BADO- Datenverarbeitung weitergeführt werden kann; davon werde ich mich bei einem weiteren Prüfbesuch überzeugen.

Die Anregung des Hessischen Ministers für Arbeit und Soziales für ein gemeinsames Gespräch aller Beteiligten halte ich im Interesse einer Klärung der Fragen, wie und in welchem Zeitraum die Voraussetzungen für eine Fortsetzung des BADO-Projekts geschaffen werden können, für nützlich. Ich würde es bedauern, wenn organisatorische und technische Unzulänglichkeiten beim Umgang mit den Patientendaten das von nahezu allen Beteiligten für dringlich gehaltene Vorhaben, die Informationsgrundlage für die stationäre psychiatrische Versorgung zu verbessern, scheitern ließen.

4. Polizei

4.1
Datenverarbeitung und Versammlungsfreiheit

4.1.1
Demonstrationsanmeldung - Datenübermittlung

Im Februar 1985 fand in Marburg eine Demonstration gegen die 1984 erfolgte Novellierung des Deutschen Richtergesetzes statt. Der Protest richtete sich gegen die Einführung von sogenannten studienbegleitenden Leistungskontrollen für das juristische Studium, die an zahlreichen rechtswissenschaftlichen Fachbereichen in der Bunderepublik auf Kritik gestoßen sind. An der ohne Zwischenfälle verlaufenen Demonstration nahmen weniger als hundert Personen teil. Nach der Demonstration schickte die Marburger Polizei an eine Reihe von Behörden Fernschreiben, in denen mitgeteilt wurde, daß die Demonstration stattgefunden hatte und ohne besondere Vorkommnisse verlaufen war. Die Fernschreiben enthielten außerdem die genauen Personalien der Anmelderin und den Hinweis, daß über sie bei der Marburger Polizei keine Erkenntnisse vorlägen. Empfänger waren der Hessische Innenminister, der Justizminister, der Kultusminister, das Landeskriminalamt, das Landesamt für Verfassungsschutz, der Regierungspräsident in Gießen sowie die Staatsschutzabteilung des Bundeskriminalamtes.

Der Fall ist ein anschauliches Beispiel dafür, wie Daten routinemäßig weitergegeben werden, ohne zu fragen, ob ein hinreichender Anlaß dafür besteht und ob die Angaben für die Aufgabenerfüllung der jeweiligen Dienststellen erforderlich sind. Weder konnte von einem hinreichenden Anlaß die Rede sein, noch läßt sich die Erforderlichkeit bejahen.

4.1.1.1
Verstoß gegen das Grundrecht auf Versammlungsfreiheit

Besonders ins Gewicht fällt hierbei, daß es sich um die Anmeldung einer Demonstration handelte. Hier ist nicht nur das informationelle Selbstbestimmungsrecht des Bürgers, sondern auch sein Grundrecht auf Versammlungsfreiheit tangiert. Auf diesen Zusammenhang zwischen der Verarbeitung personenbezogener Daten über Demonstrationen einerseits und dem Grundrecht auf Versammlungsfreiheit andererseits hat auch das Bundesverfassungsgericht in zwei grundlegenden Entscheidungen hingewiesen.

Im Urteil über das Volkszählungsgesetz sagt das Gericht ausdrücklich: "Mit dem Recht auf informationelle Selbstbestimmung wäre eine Gesellschaftsordnung und eine diese ermöglichende Rechtsordnung nicht vereinbar, in der Bürger nicht mehr wissen können, wer was wann und bei welcher Gelegenheit über sie weiß ... Wer damit rechnet, daß etwa die Teilnahme an einer Versammlung oder Bürgerinitiative behördlich registriert wird und daß ihm dadurch Risiken entstehen können, wird möglicherweise auf eine Ausübung seiner entsprechenden Grundrechte verzichten. Dies würde nicht nur die individuellen Entfaltungschancen des einzelnen beeinträchtigen, sondern auch das Gemeinwohl, weil Selbstbestimmung eine elementare Funktionsbedingung eines auf Handlungs- und Mitwirkungsfähigkeit seiner Bürger begründeten freiheitlichen demokratischen Gemeinwesens ist" (BVerfG-65, 1, 43). Zwei Jahre später ging das Gericht noch einmal auf die besondere Bedeutung des Grundrechts der Versammlungsfreiheit für den demokratischen Staat ein und betonte in diesem Zusammenhang, daß Eingriffe in dieses Recht nur unter engen Voraussetzungen zulässig sind: "Mit diesen Anforderungen wären ... behördliche Maßnahmen unvereinbar, die über die Anwendung grundrechtsbeschränkender Maßnahmen hinausgehen und etwa den Zugang zu einer Demonstration durch Behinderung von Anfahrten oder schleppende vorbeugende Kontrollen unzumutbar erschweren oder ihren staatsfreien unreglementierten Charakter durch exzessive Observationen und Registrierungen verändern" (BVerfG 69, 315, 349).

4.1.1.2
Reaktion des Innenministers

Mit diesen Grundsätzen läßt sich die erfolgte Datenübermittlung nicht vereinbaren. In seiner Antwort auf mein entsprechendes Schreiben verwies der Innenminister zunächst darauf, daß der Bericht auf seinem Erlaß von 1975 zur Berichterstattung über wichtige Ereignisse in vollzugspolizeilichen Angelegenheiten (WE-Erlaß) beruhe. Auch seiner Auffassung nach habe jedoch im konkreten Fall kein hinreichender Grund bestanden, die Personalien der Anmelderin in den Bericht aufzunehmen. Die Empfängerbehörden würden daher um Löschung der erhaltenen Daten ersucht.

Leider blieben eine Reihe wesentlicher Punkte unklar. Dies gilt zum einen für den Adressatenkreis. Der Erlaß verpflichtet die Polizeidienststellen zur Berichterstattung über wichtige Ereignisse (sog. WE-Meldungen) und erwähnt als solche ausdrücklich öffentliche Versammlungen. Die Berichte sind dem Innenminister, dem Landeskriminalamt und dem Regierungspräsidenten zu übersenden. Die Fernschreiben gingen jedoch - wie bereits erwähnt - an einen wesentlich größeren Empfängerkreis. Offen blieb auch ob und gegebenenfalls in welchem Umfang solche WE-Meldungen in Zukunft überhaupt personenbezogene Daten enthalten sollen.

Auf meine erneute Anfrage teilte mir der Innenminister nunmehr mit, im konkreten Fall sei eine WE-Meldung über die Demonstration zum Zweck der Verwaltungsvereinfachung verbunden worden mit einer sogenannten "kriminalpolizeilichen Erkenntnisanfrage" bezüglich der Anmelderin, d.h. die Empfängerbehörden wurden zugleich nach Erkenntnissen über die Anmelderin gefragt. Aus diesem Grund seien auch personenbezogene Daten übermittelt und der Empfängerkreis über den im Erlaß vorgesehenen ausgedehnt worden. Das Verfahren werde jedoch künftig nicht mehr praktiziert. In Zukunft sollten WE-Meldungen keine personenbezogenen Daten mehr enthalten und von Erkenntnisanfragen strikt getrennt werden.

Diese Absicht kommt ohne Zweifel den Grundsätzen des Datenschutzes entgegen. Der Inhalt der jeweiligen Mitteilung und ihr Empfängerkreis können auf diese Weise strikt auf den für den konkreten Zweck der Meldung erforderlichen Umfang begrenzt werden. Allerdings ist zu bedenken, daß Erkenntnisanfragen zugleich auch immer eine Übermittlung der personenbezogenen Daten über den Betroffenen enthalten. Mit einer strengen Trennung der WE-Meldungen von der Erkenntnisanfrage ist daher das hier angesprochene Problem der breiten Streuung der Daten noch nicht gelöst. Es geht nicht an, daß nunmehr in anderer Form, aber im Ergebnis in demselben Umfang personenbezogene Daten verbreitet werden. Der Innenminister bemerkt dazu folgendes: Die Versammlungsbehörde habe nach Eingang der Anmeldung zu einer Demonstration zu prüfen, ob Auflagen notwendig sind oder Gründe für ein Verbot der Demonstration vorliegen. Neben den Auswirkungen auf den Verkehr habe die Versammlungsbehörde zu überlegen, ob andere Umstände bei Durchführung der Demonstration die öffentliche Sicherheit und Ordnung unmittelbar gefährden können. Dabei seien alle Erkenntnisquellen zu berücksichtigen, insbesondere die örtlich zuständigen Polizeidienststellen, unter Umständen auch das Landesamt für Verfassungsschutz zu unterrichten, wenn Anhaltspunkte dafür vorliegen, daß extreme Gruppierungen hinter der Anmeldung stehen bzw. sich an ihr beteiligen wollen.

Auch dieses zweite Schreiben des Innenminister stellt keine völlig überzeugende Antwort dar. Zum einen liegen mir bis heute keine Informationen über tatsächliche Anhaltspunkte dafür vor, daß im konkreten Fall eine Erkenntnisanfrage insbesondere an das Landesamt für Verfassungsschutz erforderlich war. Zum anderen geht der Innenminister nach wie vor nicht auf die Frage der Übermittlung der Daten an die Staatsschutzabteilung des Bundeskriminalamtes ein. Vor allem aber erging die Mitteilung erst nach Abschluß der Demonstration. Sie konnte daher den von dem Innenminister angegebenen Zweck, eine Gefährdung der öffentlichen Sicherheit und Ordnung durch die Demonstration zu verhindern, nicht erfüllen. Im übrigen wurde in den Fernschreiben auch nicht explizit nach Erkenntnissen über die Anmelderin der Demonstration gefragt.

Es erscheint mir deshalb wichtig noch einmal zu betonen, daß die Übermittlung personenbezogener Daten über Versammlungsteilnehmer auf den unbedingt erforderlichen Umfang beschränkt werden muß. Es bedarf klarer Verfahrensvorschriften.

4.1.2
PIOS-Datei "Innere Sicherheit" (APIS)

Die Ausführungen des Bundesverfassungsgerichts zur Bedeutung der Versammlungsfreiheit veranlassen mich, noch ein weiteres derzeit aktuelles Problem zu erwähnen: Die mehrfach diskutierte Konzeption der vom Bundeskriminalamt geführten "Arbeitsdatei PIOS - Innere Sicherheit" - APIS -(Zum gegenwärtigen Diskussionsstand s. die zusammenfassende Darstellung unter Ziff. 13.1.7). Die Verarbeitung von Daten über Demonstrationen ist insofern betroffen, als damit zu rechnen ist, daß künftig regelmäßig die Daten über Bürger, die im Zusammenhang mit Demonstrationen in den Verdacht geraten sind, eine Straftat begangen zu haben, nicht nur in HEPOLIS, dem zentralen Hessischen Polizeiinformationssystem, sondern darüber hinaus auch in APIS gespeichert werden. Diese Daten sind dann mit den Daten aus dem Bereich Terrorismus zusammen in einer Datei gespeichert und stehen bundesweit im Direktabrufverfahren zur Verfügung.

Ich halte dies nicht für akzeptabel: Hier werden höchst unterschiedliche Datenbestände in einer Datei zusammengefügt. Geringfügige Straftaten werden zusammen mit schwerwiegenden, gegen den Bestand des Staates gerichteten Straftaten gespeichert.

Dadurch ist der Zweck der Datei nicht mehr klar bestimmt. Es besteht im übrigen die Gefahr, daß Personen, deren Daten in dieser Datei gespeichert sind, vorschnell und pauschal das Etikett "staatsgefährdend" erhalten.

Die zentrale Speicherung beim Bundeskriminalamt und die bundesweite Möglichkeit des Direktabrufs halte ich auch nicht für verhältnismäßig. Sie unterläuft die bei der Einführung des bundesweiten Kriminalaktennachweises (KAN) getroffene Grundsatzentscheidung, nur besonders schwerwiegende Straftaten für den bundesweiten Direktabruf aller Polizeidienststellen bereitzuhalten.

4.2
Zweckwidrige Auswertung von Protokolldaten

In meinem 12. und 13. Tätigkeitsbericht (Ziff. 3.1.4 bzw. Ziff. 4.1.5) habe ich dargelegt, daß Protokolldaten nicht für die Erfüllung der polizeilichen Aufgaben der Gefahrenabwehr und Strafverfolgung verwendet werden dürfen. Darüber bestand bislang Konsens mit dem Innenminister. Die Erfahrungen des vergangenen Jahres haben gezeigt, daß diese Übereinstimmung offensichtlich nicht mehr besteht. Die zweckwidrige Auswertung von Protokolldaten hat zugenommen. Ich halte eine eingehende Diskussion dieses Problems auch deshalb für besonders wichtig, weil die Frage der Verwertung von Protokolldaten für alle Verwaltungsbereiche von grundsätzlicher Bedeutung ist.

4.2.1
Nochmals: Zur Notwendigkeit einer strikten Zweckbindung von Protokolldaten

Durchgeführt werden Protokollierungen zur Sicherung einer fehlerfreien Datenverarbeitung und als Nachweismöglichkeit für die Datenschutzkontrolle (vgl. § 10 HDSG). Der Umfang der Protokollierungen ist sehr unterschiedlich. Grundsätzlich können Protokollbänder folgende Arten von Informationen enthalten:

- Daten technischer Natur über den Betrieb des Rechners
- Daten über die Identität des Benutzers des Rechners sowie Zeitpunkt und Art der vom Benutzer veranlaßten Aktivitäten (z.B. Änderungen oder Abfragen von Datenbeständen im Dialogbetrieb am Bildschirm)
- Daten über die Inhalte der Aktivitäten des Rechners, d.h. die zwischen dem Rechner und Benutzer ausgetauschten Nachrichten.

Das Problem der Verwertung der Protokolldaten ist bei den Protokollbändern des zentralen Hessischen Polizeiinformationssystems (HEPOLIS) aktuell geworden. Beim Betrieb dieses Informationssystems wird derzeit in erheblichem Umfang protokolliert. So kann z.B. aus den Protokollbändern ersehen werden, welche in HEPOLIS gespeicherten personenbezogenen Daten zu welchem Zeitpunkt geändert oder gelöscht wurden. Auch sämtliche Anfragen werden protokolliert. Gerät etwa ein Bürger in eine Polizeikontrolle und überprüft die Polizei, ob seine Daten in HEPOLIS enthalten sind, so wird dieser Vorgang einschließlich der personenbezogenen Daten des Betroffenen auf dem Protokollband festgehalten, und zwar auch dann, wenn die polizeiliche Überprüfung zu dem Ergebnis geführt hat, daß der Betroffene nicht gespeichert ist (sogenannte Negativanfrage) und auch kein Anlaß für ein weiteres polizeiliches Tätigwerden besteht.

So können die Protokollbänder u.U. Auskunft darüber geben, wo sich ein Bürger zu einem bestimmten Zeitpunkt aufgehalten hat. Selbst die personenbezogenen Daten, die in HEPOLIS nach den Richtlinien für die Führung kriminalpolizeilicher Sammlungen (Kps-Richtlinien) bereits gelöscht wurden, sind noch auf den Protokollbändern enthalten. Insgesamt sind damit auf den Protokollbändern in erheblichem Umfang personenbezogene Daten vorhanden, die nach § 11 HDSG i.V.m. HSOG bzw. StPO bei der Polizei nicht gespeichert werden dürften, da sie für die Erfüllung ihrer Aufgaben der Gefahrenabwehr (HSOG) bzw. der Strafverfolgung (StPO) nicht erforderlich sind.

Diese umfassenden Protokollierungen stellen allerdings eine zusätzliche Möglichkeit der Datenschutzkontrolle dar und sind insoweit grundsätzlich - auch aus der Sicht des Datenschutzes (§ 10 HDSG) - sinnvoll. Dies gilt jedoch nur dann, wenn die Verwendung der Protokollbänder ausschließlich zu Kontroll- und Sicherungszwecken erfolgt. Wird dagegen eine solche Zweckbindung der Daten nicht sichergestellt, ergeben sich Probleme, die eine Durchführung derartiger Protokollierungen generell in Frage stellen: Protokolldaten, die über Kontroll- und Sicherungszwecke hinaus generell für kriminalpolizeiliche Zwecke verwendet werden, sind zum "normalen" Datenbestand der Polizei zu rechnen. Die Zulässigkeit ihrer Speicherung muß demzufolge an den Vorschriften des HDSG gemessen werden. Das Ergebnis ist eindeutig: Die Speicherungen sind rechtswidrig.

Sollen diese Konsequenzen vermieden und Protokollierungen für Kontroll- und Datensicherungszwecke weiterhin durchgeführt werden, so sind die Protokolldaten einer strikten Zweckbindung zu unterwerfen: Sie dürfen von der Polizei nicht für ihre Aufgaben der Gefahrenabwehr und Strafverfolgung genutzt und ebensowenig zur Auskunftserteilung an andere Behörden verwendet werden.

4.2.2
Die vorausgegangenen Diskussionen

Die Landesregierung hat in ihrer Stellungnahme zu meinem 12. Tätigkeitsbericht (Drucks. 11/1258, S. 24) meine Auffassung akzeptiert, daß die Protokolldaten ausschließlich zu Zwecken der Datenschutzkontrolle personenbezogen ausgewertet werden dürfen. In einem Gespräch mit dem Hessischen Minister des Innern wurde dann übereinstimmend festgestellt:

- Die Protokolldaten werden nicht mehr für kriminalpolizeiliche Zwecke verwandt.
- Andere personenbezogene Auswertungen dürfen von der Polizei nur noch mit Zustimmung des Innenministers vorgenommen werden.

Inzwischen ist jedoch der Innenminister von dieser Auffassung abgerückt. Wie sich aus seinem Schreiben vom 28. März 1985 ergibt, teilt er zwar grundsätzlich weiterhin meine Ansicht, weist im übrigen aber darauf hin, daß die Staatsanwaltschaft im Rahmen eines konkreten Ermittlungsverfahrens gegenüber der Polizei wie gegenüber jeder anderen Behörde ein Recht auf Auskunft habe (§ 161 Strafprozeßordnung). Dieser Auskunftsanspruch erstrecke sich auch auf die Protokolldaten. Ferner müsse die Polizei u.U. die Protokolle selbst auswerten, um einer Verdunklungsgefahr zu begegnen (§ 163 StPO).

Keines dieser Argumente überzeugt mich:

- Wenn der Innenminister der Auffassung ist, daß aus Rechtsgründen keine Auswertung der Protokolldaten für kriminalpolizeiliche Zwecke erfolgen darf, weil es sich hierbei um einen besonderen Datenbestand handelt, so kann nichts anderes gelten, wenn die Polizei als Hilfsbeamte der Staatsanwaltschaft tätig wird.
- Wenn die Protokolldaten aus Rechtsgründen von der Kriminalpolizei weder zur Gefahrenabwehr noch zur Strafverfolgung verwendet werden dürfen, so kann für die Verwendung der Daten durch die Staatsanwaltschaft nichts anderes gelten.

- Die Tatsache, daß § 161 StPO der Staatsanwaltschaft einen allgemeinen Auskunftsanspruch gegenüber anderen Behörden gewährt, kann zu keinem anderen Ergebnis führen. Ein derartiger Auskunftsanspruch kann sich nur auf solche Datenbestände beziehen, die den angefragten Behörden für ihre eigene Aufgabenerfüllung zur Verfügung stehen. Es wäre völlig widersinnig, der Polizei selbst eine umfassende Verwertung ihrer Protokolldaten zu untersagen und die Daten dann anderen Behörden zur Verfügung zu stellen. § 161 StPO - wie auch vergleichbare andere Auskunftsansprüche - muß daher einschränkend dahingehend interpretiert werden, daß er zu Kontroll- und Sicherungszwecken angefertigte Protokollbänder nicht umfaßt.

4.2.3
Erfahrungen:

Drei konkrete Fälle zweckwidriger Auswertungen der HEPOLIS-Protokollbänder sind mir in diesem Jahr bekannt geworden. Im ersten Fall wertete das Polizeipräsidium Frankfurt mit Einverständnis des Innenministers das Protokollband von HEPOLIS im Rahmen der Ermittlungen zum Sprengstoffanschlag auf den Flughafen Frankfurt aus. Auf meinen Einwand, daß hier entgegen der getroffenen Festlegung Protokolldaten für kriminalpolizeiliche Zwecke verwendet wurden, erwiderte der Innenminister:

Die durch die Auswertung der Protokollbänder gewonnenen Daten hätten der Polizei bereits in anderer Form vorgelegen. Die Bänder seien von der Polizei lediglich ausgewertet worden, um die Daten mit einem möglichst geringen Aufwand auf einem bestimmten Datenträger zu speichern. Es habe sich daher nicht um eine "Auswertung" der Protokollbänder gehandelt, sondern lediglich um eine "erhebliche Unterstützung der Polizei bei ihren schwierigen Ermittlungen". Den getroffenen Festlegungen sei insoweit nicht zuwidergehandelt worden.

Demgegenüber ist folgendes festzustellen:
In der Vereinbarung zwischen dem Innenminister und mir wird jede Verwendung der Protokolldaten für kriminalpolizeiliche Zwecke untersagt. Damit waren selbstverständlich auch Auswertungen jeder Art gemeint. Diese Vereinbarung ist nicht eingehalten worden. Es geht nicht an, diese Tatsache durch Erörterungen zu vernebeln, ob die Daten bereits irgendwo vorhanden waren oder hätten vorhanden sein dürfen oder was unter dem Begriff der "Auswertung" zu verstehen ist, auch wenn die Absicht, der Polizei die Arbeit zu erleichtern, grundsätzlich verständlich ist. Damit wird eindeutig der Festlegung des Benutzungsumfangs der Protokolldaten zuwidergehandelt und das Ziel dieser Festlegung, klare rechtliche Grenzen für die Verwertung dieser Daten vorzusehen, generell in Frage gestellt.

Anlaß des zweiten Falls war ein Diebstahl in einer Fabrik in Bingen. Der Täter benutzte für den Abtransport der Beute einen gestohlenen LKW. Im Rahmen der strafrechtlichen Ermittlungen wollte die Staatsanwaltschaft Mainz die Protokollbänder von HEPOLIS daraufhin überprüfen, ob dieser LKW in der Zeit nach dem Diebstahl innerhalb Hessens zufällig in eine Polizeikontrolle geraten war. Gegebenenfalls hätte das Protokollband möglicherweise Auskunft darüber gegeben, wo sich der LKW zu einem bestimmten Zeitpunkt befand. Auf Antrag der Staatsanwaltschaft Mainz ordnete das Amtsgericht Mainz an, daß die in Frage kommenden Protokollbänder als Beweismittel zur Auswertung an die Staatsanwaltschaft Mainz herausgegeben werden müßten. Es berief sich hierbei auf § 94 StPO. Zur Vermeidung der Durchführung dieses Beschlagnahmebeschlusses stellte der Innenminister seine Bedenken, die wegen der vereinbarten Zweckbindung der Protokolldaten bestanden, zurück und gab die Bänder an die Staatsanwaltschaft heraus. Einige Zeit später erfolgte ein ähnlicher Beschluß durch das Amtsgericht Frankfurt im Zusammenhang mit Ermittlungen wegen einer Brandstiftung.

Ich möchte noch einmal besonders betonen, daß die Anwendung der Beschlagnahmevorschriften der StPO auf die Protokolldaten der Polizei mit dem Grundsatz der Zweckbindung unvereinbar ist. Bei der Formulierung der StPO-Vorschriften sind sicherlich solche Fallkonstellationen nicht bedacht worden. Spätestens seit der Entscheidung des Bundesverfassungsgerichts zum Volkszählungsgesetz sollte aber feststehen, daß auch die Interpretation der StPO-Bestimmungen den Grundsatz der Zweckbindung beachten muß.

4.2.4
Konsequenzen

Jenseits aller Überlegungen zur StPO ist festzuhalten: Ob und in welchem Umfang das Recht auf informationelle Selbstbestimmung beschränkt werden darf, hängt von einer klaren Aussage darüber ab, zu welchem Zweck Angaben erhoben werden und welche Verknüpfungs- und Verwendungsmöglichkeiten bestehen, (BVerfGE 65, 1, 45). An dieser Klarheit fehlt es jedenfalls seit der veränderten Haltung des Innenministers.

Zunächst kommt es aber darauf an, die sich im Zusammenhang mit HEPOLIS stellenden Fragen zu klären. Polizeiintern heißt dies: Die vom Innenminister aus Rechtsgründen getroffene Festlegung, daß Protokolldaten nicht für kriminalpolizeiliche Zwecke verwendet werden dürfen, ist strikt einzuhalten und nicht durch fragwürdige Rechtsauslegungen im Einzelfall wieder in Frage zu stellen. Die Zweckbindung der Protokolldaten muß auch bei der nunmehr anstehenden Novellierung des HSOG gesetzlich abgesichert werden. Die derzeit in § 44a Abs. 5 des Entwurfs vorgesehene Formulierung, daß die Berichtigung, Sperrung und Löschung für Datensicherungszwecke zu protokollieren ist und die Protokolle gesondert aufzubewahren sind, ist insoweit nicht ausreichend. Sie regelt nur den Zweck der Herstellung der Protokolle sowie die Art und Weise ihrer Aufbewahrung, nicht jedoch den Zweck ihrer Verwendung. Was die Verwertung der auf den Protokollbändern gespeicherten personenbezogenen Daten durch polizeiexterne Stellen anbelangt, so darf sie über die Kontroll- und Sicherungszwecke nicht hinausgehen. Die Interpretation der einschlägigen Auskunftsbestimmungen, wie z.B. § 161 StPO, bedarf insoweit im Hinblick auf das verfassungsrechtlich gewährleistete informationelle Selbstbestimmungsrecht einer einschränkenden Interpretation.

Eine Alternative zur Zweckbindung gibt es unter Datenschutzgesichtspunkten nicht. Dies umso mehr, als die derzeitig eingesetzten Datenverarbeitunssysteme ein Mindestmaß an Protokollierung zum einwandfreien technischen Betrieb voraussetzen.

4.3
Novellierung des HSOG

4.3.1
Konkrete Regelungsvorschläge zur polizeilichen Datenverarbeitung

In meinem letzten Tätigkeitsbericht bin ich auf die Entwicklung der Diskussion über eine Regelung der polizeilichen Datenverarbeitung ausführlich eingegangen und habe noch einmal dargelegt, daß eine solche Regelung dringend erforderlich ist (13. Tätigkeitsbericht, Ziff. 3.5). Auch die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat sich damit erneut befaßt und Grundsätze für eine bereichsspezifische Regelung formuliert (vgl. Ziff. 14.1 dieses Berichts). Nachdem die Erforderlichkeit präziser Vorschriften für die Polizei jahrelang gegenüber den Datenschutzbeauftragten immer wieder bestritten worden ist, liegen nunmehr erstmalig konkrete Regelungsvorschläge vor:

- Der im Auftrag der Innenministerkonferenz erarbeitete Vorentwurf zur Änderung des Musterentwurfs eines einheitlichen Polizeigesetzes des Bundes und der Länder (Stand: 08. Februar 1985).
- Der Gesetzentwurf der CDU-Fraktion im Hessischen Landtag über ein Gesetz zur Änderung des Hessischen Gesetzes über die öffentliche Sicherheit und Ordnung (HSOG), (Drucks. 11/4438).
- Der Entwurf des Hessischen Ministers des Innern eines Gesetzes zur Änderung des Hessischen Gesetzes über die öffentliche Sicherheit und Ordnung (Stand: 30. September 1985).

Sowohl die Vorschläge der hessischen CDU als auch der Entwurf des Innenministers berücksichtigen den Musterentwurf. Eine parlamentarische Beratung der CDU-Vorschläge hat bislang nicht stattgefunden. Die Frist für Stellungnahmen zum Entwurf des Hessischen Innenministers läuft am 31. Januar 1986 ab. Im Hinblick darauf stellen die nachfolgenden Überlegungen den Entwurf des Innenministers in den Mittelpunkt.

Der Entwurf erfaßt - entsprechend meiner Forderung - jede Art und Form der Verarbeitung personenbezogener Daten und bezieht sowohl die Erhebung als auch jede Nutzung der Daten ein. Die vorgeschlagenen Regelungen sind im Vergleich zum Musterentwurf klarer und differenzierter. Den potentiellen Gefahren für das informationelle Selbstbestimmungsrecht der Bürger wird zudem durch ein abgestuftes Verfahren entgegengewirkt. Gegen eine Reihe der im Entwurf enthaltenen Vorschriften habe ich jedoch erhebliche Bedenken.

4.3.2
Vorbeugende Bekämpfung von Straftaten

Ein zentraler Punkt des Entwurfs ist die Normierung der vollzugspolizeilichen Zuständigkeit für die vorbeugende Bekämpfung von Straftaten (§ 44 Abs. 1 Nr. 2) und die Zuweisung von Befugnissen zur Erfüllung dieser Aufgabe (insbesondere § 44b Abs. 1 Nr. 2). In der Begründung zum Entwurf wird ausgeführt, daß diese Aufgabe der Sache nach schon seit langem von der Vollzugspolizei wahrgenommen werde. Die polizeilichen Maßnahmen zur Erfüllung dieser Aufgabe seien bisher der schlichten Hoheitsverwaltung zugerechnet worden. In der neueren Diskussion werde den Maßnahmen nunmehr Eingriffsqualität zugesprochen. Aus diesem Grund müßten die Aufgaben der vorbeugenden Bekämpfung von Straftaten und die hierzu erforderlichen Befugnisse gesetzlich geregelt werden. Konkret bedeutet dies, daß sich nach Ansicht des Innenministers in der Praxis nichts ändert. Was bisher schon erfolgt sei, werde auch in Zukunft geschehen. Die Regelung habe also nur den Sinn, der rechtsdogmatischen Diskussion Rechnung zu tragen.

Diese Darstellung kann nicht unwidersprochen bleiben. Ganz unabhängig von der Diskussion um die Eingriffsqualität der polizeilichen Maßnahmen muß vielmehr folgendes festgestellt werden: Die Besonderheit von Maßnahmen der vorbeugenden Bekämpfung von Straftaten liegt darin, daß sie Bürger treffen, die weder Straftatverdächtige i.S.d. Strafprozeßordnung noch Störer i.S.d. Polizeigesetze sind. Es mag sein, daß die Polizei in der Vergangenheit in Einzelfällen auch die Daten von solchen Personen in ihren Akten erfaßt hat. Die neuen Techniken der Datenverarbeitung eröffnen jedoch weitreichende Möglichkeiten, derartige Angaben in Dateien zu speichern, zu verknüpfen und auszuwerten.Dadurch wird eine systematische vorbeugende Bekämpfung von Straftaten in größerem Umfang erstmals möglich.

Die vorhandene Technik ist zudem erfahrungsgemäß ein Anreiz, den Umfang der vorbeugenden Bekämpfung von Straftaten ständig auszuweiten. Die Entwicklung des PIOS-Verfahrens gibt hierfür ein anschauliches Beispiel. Das PIOS-Verfahren wurde in den siebziger Jahren zur Unterstützung der Bekämpfung der terroristischen Gewaltkriminalität entwickelt und für den Aufbau der Datei PIOS- Terrorismus verwendet. Diese Datei zeichnet sich dadurch aus, daß in erheblichem Umfang Personen, die weder Straftatverdächtige i.S.d. Strafprozeßordnung noch Störer i.S.d. Polizeigesetze sind, - sog. "andere Personen" - systematisch erfaßt werden und für Recherchezwecke zur Verfügung stehen. Die Brisanz dieser Datei wurde durchaus von Anfang an gesehen. Zweifelsohne werden in ihr die Daten einer Vielzahl unbeteiligter Bürger gespeichert. Gerechtfertigt wurde dies mit der besonderen Gefährlichkeit des Terrorismus und seiner verdeckten und organisierten Arbeitsweise. Inzwischen wurde der Einsatz des PIOS-Verfahrens auf eine Reihe anderer Kriminalitätsbereiche ausgedehnt. Neuestes Beispiel ist die Datei PIOS - Innere Sicherheit, auf deren Problematik ich bereits mehrfach hingewiesen habe (s. hierzu Ziff. 13.1.7)

Vor diesem Hintergrund wird deutlich, daß die Zuweisung der Aufgabe der vorbeugenden Bekämpfung von Straftaten der Polizei weitreichende neue Handlungsmöglichkeiten eröffnet. Die Technik darf hier keine ungesteuerte und unstrukturierte Eigendynamik entfalten.

4.3.3
Grundsätze vollzugspolizeilicher Datenverarbeitung

In § 44a des Entwurfs sind wichtige Grundsätze vollzugspolizeilicher Datenverarbeitung festgelegt. Zum einen ist in Abs. 1 der Grundsatz der Zweckbindung der personenbezogenen Daten aufgeführt: Die Polizei darf personenbezogene Daten nur zu den in diesem Gesetz genannten Zwecken verarbeiten. Die Datenverarbeitung zu unbestimmten oder nicht bestimmbaren Zwecken ist unzulässig. Allerdings bedarf dieser Grundsatz der Zweckbindung noch weiterer Konkretisierung. Dies ist in den darauffolgenden Einzelvorschriften nicht in hinreichendem Maße erfolgt. Zwar sind im Entwurf eine Reihe konkreter Regelungen zur Zweckbindung enthalten, andererseits ist jedoch z.B. in der Speicherungsvorschrift pauschal festgelegt, daß die Polizei die von ihr gespeicherten Daten zur Wahrnehmung ihrer Aufgaben auswerten darf.

Zum anderen wird in Abs. 2 der verfassungsrechtliche Grundsatz der Verhältnismäßigkeit noch einmal ausdrücklich aufgeführt. Dies ist von besonderer Bedeutung, weil im Gesetz notwendigerweise in gewissem Umfang eine generalisierende Regelung getroffen werden muß und es entscheidend auf die konkrete Handhabung der Befugnisse im Einzelfall ankommt.

Abs. 3 schließlich enthält eine Verfahrensregelung für den Fall der Verarbeitung von Daten aufgrund einer Einwilligung des Betroffenen. Insbesondere soll die Einwilligung des Betroffenen schriftlich eingeholt werden. Mit dieser Verfahrensregelung wird allerdings zugleich implizit ausgesagt, daß eine Verarbeitung personenbezogener Daten durch die Polizei über den konkret festgelegten Umfang hinaus mit Einwilligung jederzeit zulässig sein soll. Gerade im Bereich der Polizei sind jedoch Situationen denkbar, in denen sich der Betroffene faktisch gezwungen sieht, seine Einwilligung zu geben. Konkrete Rechtsvorschrift und Einwilligung dürfen im Sicherheitsbereich keine gleichwertigen Rechtsgrundlagen für die Datenverarbeitung sein. Dies würde auch das Ziel der Novellierung, die Datenverarbeitung durch die Polizei präzise zu regeln, erheblich relativieren.

4.3.4
Datenerhebung

4.3.4.1
Umfang der Datenerhebung zur vorbeugenden Bekämpfung von Straftaten

Für die Überlegungen zur Datenverarbeitung zu Zwecken der vorbeugenden Straftatenbekämpfung spielt die Frage eine entscheidende Rolle, in welchem Umfang der Polizei die Befugnis der Datenerhebung zur vorbeugenden Bekämpfung von Straftaten eingeräumt werden soll. Ich habe von Anfang an die Auffassung vertreten, daß eindeutige Beschränkungen der Erhebungsbefugnisse unerläßlich sind, und zwar zunächst mit Hilfe einer konkreten, sowie abschließenden gesetzlichen Aufzählung derjenigen Straftatbestände, zu deren vorbeugender Bekämpfung die Erhebung personenbezogener Daten zulässig ist. Es kann hierbei grundsätzlich nur um besonders schwerwiegende Straftatbestände gehen.

§ 44b Abs. 1 Nr. 2 des hessischen Entwurfs enthält keine ausreichende qualitative Unterscheidung. Ausgehend von konkreten Straftatbeständen werden zwei Fallgruppen unterschieden. Personenbezogene Daten dürfen von der Polizei erhoben werden zur vorbeugenden Bekämpfung

a) der in § 100a der Strafprozeßordnung genannten Straftaten sowie der Straftaten nach §§ 147, 176 bis 181a, 243 und 244, 259 und 260, 262 bis 265, 265b bis 266, 324 bis 330a des Strafgesetzbuchs, § 29 des Betäubungsmittelgesetzes und § 47a des Ausländergesetzes, wenn dies auf Grund tatsächlicher Anhaltspunkte erforderlich ist,

b) der Straftaten nach §§ 86a, 127, 131, 174, 182 bis 184b, 223 bis 226, 227 und 242 des Strafgesetzbuches, wenn aufgrund tatsächlicher Anhaltspunkte zu erwarten ist, daß diese Straftaten in erheblichem Umfang begangen werden.

Eine Datenerhebung nach der zweiten Fallgruppe darf nur der Innenminister nach Unterrichtung des Datenschutzbeauftragten anordnen. Sie ist räumlich einzuschränken und regelmäßig auf sechs Monate zu begrenzen.

Der Musterentwurf der Innenministerkonferenz sieht demgegenüber eine wesentlich pauschalere Regelung vor. Lediglich für bestimmte Formen der Datenerhebung wie z.B. langfristige Observationen sind einige konkrete Einschränkungen vorgesehen. Im übrigen ist die Polizei generell befugt, personenbezogene Daten zu erheben, wenn dies aufgrund tatsächlicher Anhaltspunkte zur vorbeugenden Bekämpfung von Straftaten erforderlich ist (§ 8a). Diese Formulierung findet sich auch im CDU-Entwurf (§ 44b).

Eine solche generalklauselartige Befugnisregelung halte ich nicht für akzeptabel. Aber auch gegen die Regelung des hessischen Entwurfs habe ich erhebliche Bedenken: Die erste Fallgruppe ist zu weit gefaßt. Es handelt sich nicht ausschließlich um besonders schwerwiegende Straftaten. So sind z.B. auch alle Fälle von Betrug (§ 263 StGB) aufgenommen worden. Im übrigen sollte auch die besondere Intensität der Erfüllung der Straftatbestände berücksichtigt werden. Vor allem aber werden mit der zweiten Fallgruppe sehr weitreichende zusätzliche Möglichkeiten zur Datenerhebung zum Zwecke der vorbeugenden Straftatenbekämpfung eröffnet, und zwar weit über den Bereich der schweren Straftaten hinausgehend. Der Katalog umfaßt sogar die Erregung öffentlichen Ärgernisses (§ 183a StGB) und die einfache Körperverletzung (§ 223 StGB). Ich sehe nicht, wie eine solche Ausdehnung mit dem Grundsatz der Verhältnismäßigkeit vereinbart werden kann. Hinzu kommt, daß auch hier nicht konkretisiert ist, bei welchen besonderen Begehungsformen eine Datenerhebung möglich sein soll.

Ich verkenne nicht, daß versucht wurde, den hierdurch entstehenden Gefahren für das informationelle Selbstbestimmungsrecht der Bürger durch besondere Verfahrensregelungen zu begegnen. Die Einzelentscheidung soll dem Minister des Innern obliegen. Ich habe jedoch Zweifel daran, daß das informationelle Selbstbestimmungsrecht hinreichend gewährleistet werden kann, wenn eine Einzelentscheidung des Ministers unter dem Druck einer aktuellen Situation gefällt werden muß und bin daher nach wie vor der Auffassung, der grundsätzliche Rahmen der Datenerhebung zur vorbeugenden Straftatenbekämpfung sollte im Gesetz enger eingegrenzt werden. In jedem Fall sollte eine Datenerhebung nach der 2. Fallgruppe auch nur dann zulässig sein, wenn bereits Straftaten in erheblichem Umfang begangen worden sind.

Die vorgesehene Verpflichtung des Innenministers zur vorherigen Unterrichtung des Datenschutzbeauftragten halte ich nicht für angemessen. Selbstverständlich ist der Datenschutzbeauftragte jederzeit bereit, den Innenminister zu beraten und zu geplanten Projekten Stellung zu nehmen. Dies zählt zu seinen Aufgaben. Hierzu bedarf es keiner Regelung im Gesetz. Die vorgesehene Regelung erscheint mir hingegen im Hinblick auf die Kontrollfunktion des Datenschutzbeauftragten bedenklich.

4.3.4.2
Art und Weise der Datenerhebung

In § 44b des Entwurfs wird auch die Art und Weise der Datenerhebung geregelt. Festgelegt wird, daß die Daten grundsätzlich bei dem Betroffenen selbst (Abs. 2) und offen (Abs. 3) zu erheben sind. Demgegenüber wird in § 8a Abs. 1 des Musterentwurfs eine wesentlich allgemeinere Regelung getroffen und die Frage der Offenheit polizeilicher Maßnahmen überhaupt nicht behandelt. Dies gilt auch für den CDU-Entwurf (§44b). Ich halte die im Entwurf des Innenministers aufgestellten Grundsätze für sehr wesentlich. Auch und gerade im Bereich der Polizei ist es von besonderer Bedeutung, daß diese Grundsätze klar festgelegt sind und die notwendige Transparenz der Datenverarbeitung für den Bürger und die Öffentlichkeit sichergestellt wird, auf die auch bei der Polizei nicht generell, sondern nur in begründeten Ausnahmefällen verzichtet werden darf. Die im Entwurf getroffenen Regelungen reichen jedoch insbesondere in folgender Hinsicht nicht aus:

Die Frage, unter welchen Voraussetzungen die Polizei mit Hilfe von Kfz-Halteranfragen beim Kraftfahrt-Bundesamt bzw. bei den örtlichen Zulassungsstellen Bürger identifizieren darf, ist im Entwurf nicht konkret geregelt. Ich bin nach wie vor der Meinung, daß diese Voraussetzungen restriktiv festgelegt werden müssen. Die Identifizierung von Bürgern mit Hilfe von Kfz-Daten ist in der Praxis von erheblicher Bedeutung. Aus Reihen der Polizei wird immer wieder vorgetragen, es müsse im Belieben der Polizei stehen, ob sie mit dem Bürger direkt Kontakt aufnimmt, seinen Ausweis verlangt oder ob sie mit Hilfe der Kfz-Halterdaten feststellt, um wen es sich jeweils (mutmaßlich, da der Halter und nicht der Fahrer erfragt wird) handelt.

Dieser Auffassung kann ich nicht zustimmen. Sie steht auch im Widerspruch zu dem mit den Absätzen 2 und 3 des § 44 b angestrebten Ziel einer grundsätzlichen Transparenz polizeilicher Arbeit. Die Problematik gewinnt im Zuge des derzeitigen Ausbaus der technischen Infrastruktur der Kfz-Zulassungsstellen, des Kraftfahrt-Bundesamts und der Polizei immer mehr an Tragweite. Die Kfz-Halterdaten werden schneller und leichter zugänglich sein. Wenn der Zugriff auf diese Daten in zunehmendem Maße faktisch die Identifizierung von Bürgern durch das Verlangen des Personalausweises ersetzt, so stellt dies eine bedenkliche strukturelle Veränderung der Arbeitsweise der Polizei dar. Es ist auch die Gefahr nicht von der Hand zu weisen, daß diese Veränderung sich auf den Umfang polizeilicher Maßnahmen auswirken könnte. Das Bewußtsein, daß die getroffenen Maßnahmen nicht öffentlich erkennbar sind und daher im Regelfall keine Diskussionen über sie zu erwarten sind, kann die Hemmschwelle für eine Überprüfung von Bürgern senken. Die Voraussetzungen für eine Abfrage der Kfz-Halterdaten sollten daher im Gesetz präzise eingeschränkt werden. Nach der derzeit vorgesehenen Regelung ist es der Polizei im wesentlichen freigestellt, ob sie den Bürger für ihn selbst erkennbar oder mit Hilfe seines Kfz-Kennzeichens identifiziert. Das Ziel der in § 44 b Abs. 2 und 3 enthaltenen Vorschriften wird damit grundsätzlich in Frage gestellt. Transparenz der polizeilichen Vorgehensweise wird nicht in dem notwendigen und möglichen Umfang sichergestellt.

4.3.4.3
Spezialregelung für Versammlungen

Datenerhebungen und -speicherungen im Zusammenhang mit Demonstrationen tangieren das Grundrecht der Versammlungsfreiheit (s. hierzu auch Ziff. 4.1). Ich begrüße daher, daß im Entwurf eine besondere Regelung für den Umfang der Datenerhebung in Versammlungen vorgesehen ist. Gem. § 44b Abs. 6 dürfen in öffentlichen Versammlungen personenbezogene Daten nur erhoben werden, wenn Anhaltspunkte dafür vorliegen, daß aus oder wegen der Versammlung Straftaten begangen werden. Die Anfertigung von Bild- und Tonaufzeichnungen ist nur zulässig, wenn Anhaltspunkte dafür vorliegen, daß die Begehung einer Straftat unmittelbar bevorsteht.

Im letzten Tätigkeitsbericht hatte ich kritisiert, daß die Frankfurter Polizei bei einem Ökumenischen Bußgang Videoaufnahmen angefertigt hatte (s. hierzu 13. Tätigkeitsbericht, Ziff. 3.5.2.3). Dieser Fall hat zu kontroversen Diskussionen zwischen dem Innenminister und mir geführt. Derartige Aufnahmen schließt die vorgesehene Vorschrift eindeutig aus.

Der Musterentwurf (§ 8b) und der CDU-Entwurf (§ 44c) sehen demgegenüber eine sehr pauschale Regelung vor: Die Polizei kann "personenbezogene Daten, auch durch Bild- und Tonaufnahmen, bei oder im Zusammenhang mit öffentlichen Versammlungen erheben, wenn tatsächliche Anhaltspunkte die Annahme rechtfertigen, daß Gefahren für die öffentliche Sicherheit und Ordnung entstehen". Eine solche Regelung trägt der durch praktische Erfahrungen erwiesenen Notwendigkeit detaillierter Vorschriften nicht Rechnung.

Darüber hinaus müßte hier wie auch im Entwurf des Hessischen Innenministers klargestellt werden, ob die Regelung auch Fotografien erfaßt. In jedem Fall - auch dies gilt für alle drei Regelungsvorschläge - sollte ergänzend festgelegt werden, daß erhobene Daten unverzüglich zu vernichten sind, wenn eine Straftat nicht begangen wurde.

4.3.4.4
Spezialregelung für Datenerhebung in oder aus Wohnungen

Auch für die verdeckte Datenerhebung in oder aus Wohnungen mit Hilfe "optischer oder akustischer Hilfsmittel" ist eine Sonderregelung vorgesehen (§ 44 b Abs. 7). Die Polizei darf personenbezogene Daten erheben

- zur Abwehr einer gegenwärtigen erheblichen Gefahr für Leib oder Leben einer Person und
- zur Abwehr einer erheblichen Gefahr für Leib oder Leben der bei einem polizeilichen Einsatz in der Wohnung tätigen Personen, wenn diese das Hilfsmittel mitführen.

Außer bei Gefahr im Verzug soll die Entscheidung dem zuständigen Amtsrichter obliegen.

Die verdeckte Datenerhebung in oder aus Wohnungen mit Hilfe des Einsatzes optischer und akustischer Hilfsmittel ist ein Eingriff in Art. 13 GG. Hierauf weist auch das BVerfG im Volkszählungsurteil hin. Es geht davon aus, daß Art. 13 für die öffentliche Gewalt ein grundsätzliches Verbot des Eindringens in die Wohnung oder des Verweilens darin gegen den Willen des Wohnungsinhabers normiere. Dazu gehöre etwa der Einbau von Abhörgeräten und ihre Benutzung in der Wohnung (BVerfG 65, 1, 40). In Art. 13 Abs. 2 GG ist festgelegt, daß Durchsuchungen außer bei Gefahr im Verzuge nur durch den Richter angeordnet werden können. So ist es folgerichtig, wenn § 44 b Abs. 7 - ähnlich auch § 8c II des Musterentwurfs sowie § 44d Abs. 2 des CDU-Entwurfs - die Entscheidung über verdeckte Datenerhebungen in oder aus Wohnungen durch den Einsatz optischer und akustischer Hilfsmittel außer bei Gefahr im Verzuge ebenfalls dem Richter zuweist. Sie stellen eine mindestens ebenso schwere Beeinträchtigung des Betroffenen dar. Zudem ist die Transparenz und Kontrollierbarkeit derartiger Maßnahmen im Vergleich zu Wohnungsdurchsuchungen wesentlich eingeschränkt. Aus diesem Grund bin ich der Auffassung, daß die Voraussetzungen noch enger gefaßt werden sollten. Dem Innenminister habe ich einen entsprechenden Vorschlag gemacht. Wegen der besonderen Tragweite der Maßnahmen sollte die Entscheidung ferner ausschließlich dem Richter vorbehalten bleiben.

Bedenken habe ich gegen die Vorschrift schließlich deshalb, weil sie als Blankoermächtigung für den Einsatz jedweder optischen und akustischen Hilfsmittel ausgelegt werden könnte. Um so wichtiger erscheint es mir, daß der Gesetzentwurf eine frühzeitige Unterrichtung des Datenschutzbeauftragten über die Entwicklung und Erprobung neuer optischer und akustischer Erhebungstechniken vorsieht (§ 44b Abs. 7).

4.3.4.5
Polizeiliche Beobachtung

Auf die Notwendigkeit einer präzisen Regelung der polizeilichen Beobachtung habe ich im letzten Tätigkeitsbericht besonders hingewiesen (Ziff. 3.5.2.3). Der Entwurf des Innenministers sieht in § 44b Abs. 9 eine Regelung vor, die im Vergleich zum Musterentwurf (§ 8d) und auch zum CDU-Entwurf (§ 44e) die Voraussetzungen einer Ausschreibung zur polizeilichen Beobachtung konkreter festlegt und klare Verfahrensvorschriften enthält. Die Entscheidung soll dem Richter obliegen. Die Ausschreibung soll in der Regel nur für die Dauer von sechs Monaten angeordnet werden. Dies entspricht der Bedeutung der polizeilichen Beobachtung. Damit für den Bürger die notwendige Transparenz hergestellt wird, halte ich es allerdings für wünschenswert, daß der Begriff der polizeilichen Beobachtung im Gesetz klar definiert wird.

4.3.5
Speicherung und Auswertung von Daten

Gem. § 44 d Abs. 1 darf die Polizei die nach dem HSOG und anderen Rechtsvorschriften erhobenen Daten speichern, wenn dies zur Wahrnehmung ihrer Aufgaben erforderlich ist. Dies soll insbesondere für personenbezogene Daten gelten, die sie aus Strafermittlungsverfahren gewonnen hat. Damit ist zunächst einmal festgelegt, daß die Datenspeicherung sich - wie bisher auch in entsprechender Anwendung des HDSG - am sog. "Erforderlichkeitsgrundsatz" messen lassen muß. Dies entspricht auch der Formulierung im Musterentwurf (§ 10a Abs. 1) und im CDU-Entwurf (§ 44g Abs. 1).

Bedenken habe ich dagegen, daß hinsichtlich des Umfangs der polizeilichen Kriminalaktensammlungen keine detaillierte Regelung getroffen wird. Ich bin der Auffassung, daß dieser Umfang eingeschränkt werden muß. Die derzeitige Praxis, zu jedem Strafermittlungsverfahren - unabhängig von der Art und Ausführung der Straftat, der Täterpersönlichkeit und dem Ermittlungsergebnis - eine parallele polizeiliche Akte anzulegen, die nach der Abgabe des Ermittlungsverfahrens an die Staatsanwaltschaft bei der Polizei verbleibt und zum Zwecke der vorbeugenden Bekämpfung von Straftaten weiter aufbewahrt wird, kann nicht länger akzeptiert werden (s. hierzu auch Nr. 2.1.2 des Forderungskatalogs der Datenschutzbeauftragten - Ziff. 14.1 dieses Berichts). Sie ist unverhältnismäßig und auch keinesfalls für die polizeiliche Aufgabenerfüllung geboten. In Strafermittlungsverfahren erhobene Daten sollten für die Zwecke der vorbeugenden Straftatenbekämpfung bei der Polizei nur dann gespeichert werden, wenn nach Art und Ausführung der Tat und nach der Persönlichkeit des Täters die Gefahr der Begehung weiterer erheblicher Straftaten besteht.

Im Entwurf des Innenministers ist darüber hinaus festgelegt, daß sich auch die Automatisierung der Datenverarbeitung als solche am "Erforderlichkeitsgrundsatz" messen lassen muß. Gem. § 44d darf die Polizei personenbezogene Daten in automatisierten Dateien nur speichern, soweit und solange die ständige Verfügbarkeit der Daten für die Wahrnehmung ihrer Aufgaben erforderlich ist. Dies halte ich für sehr wichtig. Von den verschiedenen Arten der Datenverarbeitung (z.B. Akten, manuelle Karteien, automatisierte Karteien, Aktennachweissysteme, Freitextspeicherungen) gehen unterschiedliche Gefährdungen aus. Der Datenschutz hat daher nicht nur die Frage des "ob" der Speicherung, sondern auch des "wie" der Speicherung notwendig zum Gegenstand. Die vorgesehene Vorschrift ist ein richtiger Schritt in die Richtung, auch für die Form der Datenverarbeitung klare Kriterien vorzugeben.

4.3.6
Datenübermittlung

In § 44e ist eine detaillierte Regelung der Voraussetzungen einer Übermittlung personenbezogener Daten erfolgt. Eine weitere Einschränkung der Übermittlungsvoraussetzungen halte ich jedoch für notwendig, und zwar vor allem im Hinblick auf folgende Punkte:

- Es bedarf einer besonderen Regelung für diejenigen Daten, die im Rahmen der vorbeugenden Bekämpfung von Straftaten erhoben worden sind. Derartige Daten dürfen grundsätzlich nur polizeiintern verwendet werden.
- Für die Datenübermittlung von der Polizei an den Verfassungsschutz, MAD und BND ist eine gesonderte Vorschrift notwendig, nicht zuletzt mit Rücksicht auf die Probleme, die es in diesem Bereich gerade in den letzten Jahren gegeben hat. Eine Datenübermittlung an Nachrichtendienste darf wegen der verfassungsrechtlich gebotenen Trennung von polizeilicher und nachrichtendienstlicher Tätigkeit entgegen der derzeitigen Praxis nur in engen Grenzen zugelassen werden. Dies sollte im Gesetz präzise festgelegt werden. Ein geeigneter Maßstab hierfür sind die Übermittlungsregelungen nach dem Gesetz zu Art. 10 GG.

4.3.7
Auskunftsanspruch des Bürgers

Ich begrüße es, daß in § 44i des Entwurfs des Innenministers ein Auskunftsanspruch des Bürgers gegenüber der Polizei nunmehr eindeutig festgelegt wird. Dieser Anspruch soll sich grundsätzlich auch auf Akten erstrecken, die nicht personenbezogen geführt werden. Allerdings bin ich der Auffassung, daß die im Entwurf aufgeführten Voraussetzungen, unter denen eine Auskunft ausnahmsweise versagt werden kann, zu weit gefaßt sind. Eine Auskunftserteilung soll u.a. dann unterbleiben, wenn "die Wahrnehmung vollzugspolizeilicher Aufgaben ... gefährdet würde". Diese Formulierung ist auch in den entsprechenden Vorschriften des Musterentwurfs (§ 10e) und des CDU-Entwurfs (§ 44k) enthalten. Sie ist zu pauschal und es ist zu befürchten, daß in der Praxis das im Gesetz festgelegte Regel- Ausnahme-Verhältnis umgekehrt wird und das gesetzlich eingeräumte Recht auf Auskunft damit weitgehend leerläuft.

5. Statistik

5.1
Handels- und Gaststättenzählung

Die Handels- und Gaststättenzählung 1985 war die erste "Totalerhebung" nach dem Volkszählungsurteil des Bundesverfassungsgerichts vom 15. Dezember 1983. Sie war insoweit Prüfstein dafür, wie weit die in dieser Entscheidung formulierten Anforderungen wirklich in die Praxis umgesetzt worden sind. In einer Reihe von Punkten ist diese Frage negativ zu beantworten:

5.1.1
Beteiligung des Hessischen Datenschutzbeauftragten

Die Beteiligung des Hessischen Datenschutzbeauftragten bei der Vorbereitung der Handels- und Gaststättenzählung entsprach nicht den verfassungsrechtlichen Vorgaben. Erst am 13. März 1985 anläßlich einer Sitzung des Hessischen Statistischen Koordinierungsausschusses - mithin nur 14 Tage vor dem ersten Zählungsstichtag am 28. März - erhielt ich einen ersten, allerdings noch unvollständigen Satz der Erhebungsvordrucke für den Handels- und Gaststättenzensus 1985 zur Kenntnis. Vorherige Anfragen beim Hessischen Statistischen Landesamt waren erfolglos.

Zwar gab es Kontakte zwischen dem Statistischen Bundesamt und dem Bundesbeauftragten für den Datenschutz: Diese kann und will ich mir jedoch nicht entgegenhalten lassen: Keineswegs durfte deshalb von meiner Beteiligung abgesehen werden, weil - wie die Landesregierung meint - die Interessen der Landesdatenschutzbeauftragten "kanalisiert" über den Bundesbeauftragten in die Vorbereitungsarbeiten des Statistischen Bundesamtes eingebracht werden können.

Eine solche Auffassung ist verfassungsrechtlich nicht haltbar. Ebensowenig wie von einer "Kanalisierung" der Interessen der Landesregierung durch die Bundesregierung die Rede sein kann, läßt sich ernsthaft behaupten, die Argumente des Hessischen Datenschutzbeauftragten seien ausschließlich auf dem Umweg über den Bundesbeauftragten in die Diskussion über die Ausführung einer bundesgesetzlichen Regelung einzubringen. Die Ausführung von Bundesstatistiken ist grundsätzlich Ländersache. Die Koordinierungsaufgabe des Statistischen Bundesamtes für Bundesstatistiken - § 3 Bundesstatistikgesetz - ändert nichts an der originären Verantwortlichkeit des Landes für die Rechtmäßigkeit des jeweiligen Verwaltungshandelns. Der Hessische Datenschutzbeauftragte überwacht auch präventiv die Rechtmäßigkeit der Verarbeitung personenbezogener Daten bei der Landesverwaltung. Die frühzeitige Beteiligung des Datenschutzbeauftragten im Sinne eines vorverlagerten Rechtsschutzes ist lange bevor das Bundesverfassungsgericht darauf hingewiesen hat von der Landesregierung in ihrem Kabinettsbeschluß vom 15. November 1979 ausdrücklich anerkannt und seither praktiziert worden. Auch in diesem konkreten Fall hätte der Hessische Datenschutzbeauftragte daher rechtzeitig eingeschaltet werden müssen.

Die Ansicht der Landesregierung läßt sich auch nicht mit § 19 Abs. 5 Bundesdatenschutzgesetz begründen. Danach ist der Bundesbeauftragte zwar gehalten, auf eine Zusammenarbeit der Kontrollinstanzen des Datenschutzes hinzuarbeiten, aber keineswegs verpflichtet, sich nach einer mehrheitlich akzeptierten Ansicht der Landesbeauftragten zu richten.

Schließlich ist es auch kein Geheimnis, daß gerade im Statistikbereich - wie sich an der Handels- und Gaststättenzählung zeigt - die Ansichten der Datenschutzbeauftragten nicht immer deckungsgleich sind.

5.1.2
Einzelne Mängel

Das Handelsstatistikgesetz von 1978 wird, wie es das Statistische Bundesamt selbst in einem Schreiben an den Bundesbeauftragten für den Datenschutz formuliert hat, "nicht allen Anforderungen, die das Bundesverfassungsgericht in seinem Urteil zum Volkszählungsgesetz aufgestellt hat, gerecht". So fehlt es bei der Bezeichnung der Hilfsmerkmale in § 7 des Handelsstatistikgesetzes an der notwendigen Normenklarheit und an grundrechtssichernden Maßnahmen. Die Trennung und Löschung der Hilfsmerkmale ist bisher im Gesetz überhaupt nicht vorgesehen. Hinzu kommt, daß der Inhalt der Fragebögen nicht mit dem gesetzlich angeordneten Erhebungsprogramm übereinstimmt. Zudem ist für verschiedene Fragen, wie etwa die über den gewerblichen Umsatz oder die unternehmensinternen Dienstleistungen, die gesetzliche Absicherung zumindest zweifelhaft. Es geht mithin nicht lediglich um eine Frage des "Übergangsbonus" nach dem Volkszählungsurteil, sondern um die Realisierung des Grundsatzes der Gesetzmäßigkeit der Verwaltung, der im Legalisierungsgebot des § 6 Bundesstatistikgesetz seit jeher verankert ist.

Besonders gravierend ist die im Handelsstatistikgesetz nicht vorgesehene Übermittlung und Speicherung der Steuernummern der betroffenen Unternehmen und der bundeseinheitlichen Finanzamtsnummer, die von dem Statistischen Landesamt als Sortierkriterium für die Adreßleitdatei verwendet werden. Die Steuernummer erleichtert die Verknüpfbarkeit steuerlicher und statistischer Angaben und erhöht mithin die Gefahr einer Vermischung statistischer und administrativer Datenbestände.

Eine Rechtsgrundlage für diese Übermittlung ist nicht zu ersehen. Ein Fall zulässiger Durchbrechung des Steuergeheimnisses nach der Abgabenordnung liegt jedenfalls nicht vor. Zuweilen ist seitens der amtlichen Statistik der Eindruck vermittelt worden, als sei diese Übermittlung den Statistischen Ämtern gleichsam aufgedrängt worden. Das Gegenteil ist richtig: Der Programmierverbund der Statistischen Landesämter hat in seinem eigens für die Durchführung der Handels- und Gaststättenzählung entwickelten Programmpaket eine Satzbeschreibung für die Adreßdatei der Statistischen Ämter festgelegt, in der gerade die beiden umstrittenen Merkmale Steuer- und Finanzamtsnummer enthalten sind. Aufgrund dieser seitens der amtlichen Statistik vorgegebenen Satzstruktur der Adreßdatei sind die Übermittlungen von den Finanzbehörden an die Statistischen Ämter vorgenommen worden.

Die Hessische Staatskanzlei verweist auf die Kompetenz des Bundes mit der Begründung, der Datensatz gehöre zu den technischen Vorbereitungen der Bundesstatistik. Das Statistische Landesamt habe keinen Einfluß auf den Inhalt des Datensatzes. Dazu ist zu bemerken: Jedes Land trägt im Rahmen seiner Verwaltungskompetenz die Verantwortung für die Gesetzmäßigkeit der Verwaltung. Soweit das Land für die Durchführung von Bundesstatistiken zuständig ist, hat es deren Gesetzmäßigkeit zu verantworten. Käme es zu einem Verwaltungsprozeß, würde dies auch durch Sachlegitimation und Stellung im Prozeß deutlich: Beklagter wäre das Land Hessen als durchführende, nicht aber der Bund als lediglich koordinierende Stelle.

Den Hessischen Finanzminister habe ich auf die rechtswidrige Übermittlung von Steuernummer und Finanzamtsnummer hingewiesen. Er hat sich dazu eine Stellungnahme vorbehalten.

Jenseits aller Meinungsdivergenzen über die Kompetenzfragen ist aber noch einmal festzuhalten: Die Durchführung der Handels- und Gaststättenzählung widerspricht den auch vom Bundesverfassungsgericht nachdrücklich bestätigten Anforderungen an eine verfassungskonforme und dem Datenschutzrecht entsprechende statistische Erhebung.

5.2
Hochschulstatistik

5.2.1
Studienverlaufsstatistik

Die Diskussion um die Novellierung des Hochschulstatistikgesetzes (HStatG) hat im Laufe des Jahres 1985 eine für manche überraschende Wendung genommen.

Anlaß dafür ist die Studienverlaufsstatistik. Gemeint ist eine statistische Aufbereitungsmethode, bei der Individualangaben der Studenten mit Hilfe konstanter Identifikationsmerkmale semesterweise zusammengeführt werden, um auf diese Weise "Stromgrößen" über den Studienverlauf, d.h. beispielsweise Aussagen über Verweilzeiten, Fachrichtungs- und Hochschulwechsel, zu erhalten. Unter anderem soll die Studienverlaufsstatistik auch Erkenntnisse über etwaige Korrelationen des Sozialstatus des einzelnen Studenten mit Studiendauer, -wechsel, -erfolg oder -abbruch ermöglichen.

5.2.1.1
Vorgeschichte

Nachdem die Referentenentwürfe des Bundesministeriums für Bildung und Wissenschaft auf eine Studienverlaufsstatistik verzichtet hatten, kam es - angeregt durch den Bayerischen Staatsminister für Unterricht und Kultus - zu einer Initiative des Wissenschaftsrates, mit der die bisherige Studienverlaufsstatistik als Teil der Hochschulstatistik auch in Zukunft für unverzichtbar erklärt wird. ("Empfehlungen zum Wettbewerb im deutschen Hochschulsystem", erschienen im Juli 1985). Zuvor schon hatte die Konferenz der Kultusminister der Länder in der Bundesrepublik Deutschland (KMK) auf ihrer Sitzung am 8. Februar 1985 mehrheitlich die Auffassung vertreten, daß "die Länder bei der Novellierung des Hochschulstatistikgesetzes von sich aus nicht auf die Studienverlaufsstatistik verzichten können, da mit dieser Statistik die insbesondere auch im parlamentarischen Bereich immer wieder verlangten planungsrelevanten Daten über den tatsächlichen Studienverlauf erst verfügbar werden".

Überraschend ist nun daran, daß alle Länder zu Beginn der Diskussion über die Novellierung des Hochschulstatistikgesetzes der Meinung waren, das Volkszählungsurteil des Bundesverfassungsgerichts lasse eine Fortführung der Studienverlaufsstatistik in der bisherigen Form nicht zu; eine Auffassung, die zudem in Ressortbesprechungen und schriftlichen Stellungnahmen einvernehmlich vom Bundesminister für Bildung und Wissenschaft, Bundesjustizminister, Bundesinnenminister, und zunächst auch vom Statistischen Bundesamt vertreten wurde. Gestützt wird diese Ansicht durch Zweifel an der fachlichen Geeignetheit und Erforderlichkeit der Studienverlaufsstatistik im Hinblick auf die Ziele, die sie nach Angaben ihrer Befürworter erreichen soll.

Bis 1971 beruhte die Hochschulstatistik auf Verwaltungsanordnungen der Länder. Das Statistische Bundesamt wirkte koordinierend mit und stellte unter anderem die Bundesergebnisse der sogenannten "Großen Hochschulstatistik" über die Studenten zusammen, deren fast fünfjährige Verzögerung im Vergleich zum Berichtszeitraum in der amtlichen Begründung zum Hochschulstatistikgesetz 1971 beklagt wurde. Das Hochschulstatistikgesetz von 1971 sollte eine Statistik institutionalisieren, die für Zwecke der Hochschulplanung neben aktuellen Angaben über Bestand und Struktur der Studenten auch Informationen über Studienverläufe aus einer Studienverlaufsstatistik vermitteln sollte. Mit der Umstellung der "Großen Hochschulstatistik" auf dieses neue Verfahren der Verlaufsstatistik war, ohne dies zuvor gesetzlich zu verankern, bereits im Wintersemester 1966/67 begonnen worden. Bei der Verabschiedung des Hochschulstatistikgesetzes 1971 ging der Gesetzgeber noch davon aus, daß die für eine Verlaufsstatistik notwendige Identifikation des einzelnen Studenten nur mit Hilfe des bundeseinheitlichen Personenkennzeichens garantiert werden könnte.

Neun Jahre später stellte der Gesetzgeber fest, daß sich die an die Studienverlaufsstatistik geknüpften Erwartungen nicht erfüllt hatten. In der Begründung zu Art. 2 (HStatG) zum 1. Statistikbereinigungsgesetz vom 14. März 1980 (Bundestags-Drucks. 8/2518) heißt es unter Nr. 3: "Die geplante Verlaufsstatistik soll nur mit wenigen wichtigen Merkmalen durchgeführt werden". Mit anderen Worten: Bis dato war es nach neun Jahren "Studienverlaufsstatistik" noch nicht zu einer bundesweiten Auswertung gekommen. Gleichwohl hielt der Gesetzgeber 1980 noch an der Studienverlaufsstatistik - wenn auch bereits in eingeschränkter Form - fest. Seine Rechtfertigung dafür war schon damals wenig überzeugend: "Die entsprechenden methodischen und programmtechnischen Voraussetzungen für die individualisierte Erfassung und Verarbeitung der Studentenstatistik sind nach mehrjähriger Anlaufzeit zwi-

schenzeitlich bei den Hochschulen, Statistischen Landesämtern und dem Statistischen Bundesamt geschaffen worden". Auch diese Feststellung entspricht nicht der Realität: Bis heute - 14 Jahre nach Verabschiedung des ersten Hochschulstatistikgesetzes, 19 Jahre nach der ersten Erhebung von Angaben für eine Verlaufsstatistik - ist noch keines der anvisierten Ziele durch die Statistischen Ämter von Bund und Ländern realisiert worden.

Dafür gibt es mehrere Gründe: Die Zusammenführung der ca. 1,3 Mio. Bestandsdatensätze pro Semester und ihre Speicherung in der Verlaufsdatei des Statistischen Bundesamtes geschieht nicht zeitnah genug, ist zu arbeits- und kostenaufwendig und wird außerdem durch das Fehlen von eindeutigen Identifikationsmerkmalen beeinträchtigt. Die Datei eignet sich genaugenommen allein für Aussagen über Hochschul- und Studiengangwechsel. Wegen der faktisch sehr eingeschränkten Exmatrikuliertenstatistik sind Aussagen über die Studiendauer nur bedingt möglich, kaum zu erfassen sind Unterbrecher und Beurlaubte. Schließlich konnte eine Studienerfolgsstatistik deshalb nicht entstehen, weil die notwendige Verknüpfung von Individualprüfungsstatistik und Studienverlaufsstatistik wegen unzureichender Identifikatoren nicht funktioniert.

5.2.1.2
Verfassungsrechtliche Risiken

Eine unter Umständen funktionierende Studienverlaufsstatistik wäre andererseits mit erheblichen verfassungsrechtlichen Risiken belastet. Die Forderungen von Statistikern nach einem Personenkennzeichen oder zumindest dem auf Dauer gespeicherten Namen des Studenten als Ordnungsmerkmal sind in diesem Zusammenhang ebenso kritisch zu betrachten wie das Verlangen nach weiterer Verknüpfung oder nach einer gesteigerten Intensität personenbezogener Rückfragen der Statistischen Ämter bei den Hochschulen. Zur Illustration dieser Forderung ein Zahlenbeispiel: In Bayern sind nach Angaben des Bayerischen Landesamtes für Statistik und Datenverarbeitung pro Semester bei derzeit rund 203.000 Studierenden ca. 7.000 Rückfragen mit Hilfe von Namen ggfs. Geburtsdatum und Geburtsort bei den Hochschulen erforderlich. Bundesweit hochgerechnet bedeutet dies etwa 45.300 namensbezogene Rückfragen je Semester allein für die Studienverlaufsstatistik. Die von Wissenschaftsrat und Kultusministerkonferenz geforderte Verknüpfung mit der Prüfungsindividualstatistik würde die Komplexität weiter erhöhen und damit die Quote der erforderlich werdenden Rückfragen noch weiter steigen lassen.

In Anbetracht funktional äquivalenter Methoden aus der empirischen Sozialforschung zur Evaluierung von Studienverläufen gewinnen die dargelegten statistikfachlichen Bedenken eine erhebliche Bedeutung für die verfassungsrechtliche Beurteilung der Studienverlaufsstatistik und ihrer Fortführung. Dies umso mehr, als der Gesetzgeber verpflichtet ist zu prüfen, ob und in welchem Umfang herkömmliche Methoden der Informationserhebung und -verarbeitung beibehalten werden können (vgl. BVerfGE 65, 1, 55).

Auch wenn zuweilen das Gegenteil behauptet wird: Die methodischen Probleme lassen sich nicht in kurzer Zeit und noch dazu leichthin aus dem Wege räumen. Da ist zunächst das in der verfassungsrechtlichen Diskussion gescheiterte Personenkennzeichen. Erst dieses Ordnungskennzeichen, von dessen Einführung der Gesetzgeber 1971 noch ausgegangen war, würde eine eindeutige bis zu 10 Jahren erforderliche Verknüpfung der Studienverläufe erlauben. Die an seine Stelle getretene statistische Ordnungsnummer ist kein vollwertiger Ersatz. Die Alternative, eine über 10 Jahre namensbezogene zwangsweise Erhebung und Verknüpfung, die zugleich Totalerhebung wäre, verstieße angesichts ihrer Ungeeignetheit so offensichtlich gegen die Verfassung, daß sich jede weitere Äußerung dazu erübrigt. Schließlich würde jede über ein Pesonenkennzeichen oder dessen Substrat durchgeführte Verlaufsstatistik es ermöglichen, eine Studentenkarriere nachzuzeichnen, die nur aus der Verknüpfung verschiedener Erhebungskontexte konstruierbar wäre. Der Auskunftszwang für eine solche Statistik wäre daher anders und grundsätzlicher als bei einer Bestandserhebung zu beurteilen. Die Statistik würde zu einem mit Hilfe des gesamten Bildungsverlaufs erstellten Teilabbild der Persönlichkeit führen. Derartige Teilabbilder, durch Zusammenführung verschiedener Bereiche erzeugt, sind auch in der Anonymität statistischer Erhebungen unzulässig (vgl. BVerfGE 27, 1, 6). War also die Verlaufsstatistik als solche schon nach der Mikrozensusentscheidung des Bundesverfassungsgerichts von 1969 mit verfassungsrechtlichen Risiken behaftet, muß dies erst recht nach dem Volkszählungsurteil von 1983 gelten.

Die Hessische Landesregierung hat daher allen Grund, ihre ablehnende Haltung zur Studienverlaufsstatistik aufrechtzuerhalten. In diesem Sinne habe ich mich gegenüber der Ministerin für Wissenschaft und Kunst geäußert.

5.2.2
Prüfungskandidatenstatistik

Auch die gegenwärtige Praxis der Hochschulstatistik wird in Hessen bereits durch das Volkszählungsurteil unmittelbar beeinflußt. Als Ergebnis gemeinsamer Besprechungen mit der Ministerin für Wissenschaft und Kunst und dem Hessischen Statistischen Landesamt wurde ein gemeinsamer Verfahrensvorschlag entwickelt, der bis zur Novellierung des Hochschulstatistikgesetzes eine verfassungskonforme Durchführung der Prüfungskandidatenstatistik garantieren soll:

"1. Das Hessische Statistische Landesamt verzichtet - trotz weiterhin gültiger Rechtsgrundlage - bei der Erhebung der Prüfungskandidaten künftig auf die Übermittlung von

- Matrikelnummer
- Familienname
- Geburtsname
- Vorname
- Geburtsort
- Land des Geburtsortes

durch die Prüfungsämter.

Dadurch wird der Forderung des Hessischen Datenschutzbeauftragten nach Übermittlung anonymisierter Daten Rechnung getragen.

2. Diese Regelung ist als Übergangslösung anzusehen und greift einer evtl. anderen Regelung durch eine Novellierung des Hochschulstatistikgesetzes nicht vor.

3. Der Vorschlag erfordert die Umgestaltung des Erhebungsbogens für Prüfungskandidaten: Das abtrennbare Deckblatt mit den Angaben zur Person verbleibt beim Prüfungsamt der Hochschule und hat lediglich Hilfsfunktion zur Prüfung der Vollständigkeit für Rückfragen. Es kann nach Abschluß der Aufbereitung vernichtet werden. Nähere Einzelheiten sind noch mit den Prüfungsämtern zu klären.

4. Bis zum Neudruck der Erhebungsbogen kann der bisher verwendete Beleg noch benutzt werden. Sofern hierbei die unter Ziff. 1 genannten Merkmale nicht mehr an das Hessische Statistische Landesamt geliefert werden, ist für eventuelle Rückfragen sicherzustellen, daß im jeweiligen Prüfungsamt der Personenbezug hergestellt werden kann. Hierzu ist es erforderlich, auf dem Erhebungsbogen hinter der Paginiernummer eine vierstellige fortlaufende Nummer einzutragen und diese neben dem Namen des Prüfungskandidaten in eine beim Prüfungsamt verbleibende Liste zu übertragen. Diese Hilfsliste hat analog dem künftigen Deckblatt Hilfsfunktion und kann ebenfalls nach Abschluß der Aufbereitung vernichtet werden."

Das Statistische Landesamt erhält somit keine formalen Identifikatoren mehr von Prüfungskandidaten. Die Prüfungskandidatenstatistik erfolgt in Hessen nunmehr mit Hilfe eines Verfahrens, das ohne wesentlichen Aussageverlust für die Statistik zugleich den Datenschutz respektiert.

5.3
Volkszählung und Mikrozensus

Die Entscheidung des Bundesverfassungsgerichts zum Volkszählungsgesetz 1983 hat die Mängel der gegenwärtigen Statistikgesetzgebung offengelegt und die Notwendigkeit einer Neuregelung bestätigt. Die Bemühungen um eine Novellierung sind allerdings immer wieder durch den Hinweis auf den "Übergangsbonus" verzögert worden. Statt sich sofort auf die erforderlichen neuen Bestimmungen zu konzentrieren, hielt man sich mit langwierigen Überlegungen darüber auf, wie eine verfassungswidrige Praxis wenigstens noch teilweise beibehalten werden könnte. Trotzdem ist festzustellen, daß die Anstrengungen, die überholten Gesetze durch verfassungskonforme Bestimmungen zu ersetzen, zugenommen und auch zu konkreten Ergebnissen geführt haben.

5.3.1
Volkszählungsgesetz 1987

Am 15. November 1985 ist das Volkszählungsgesetz 1987 in Kraft getreten (BGBl. I, S. 2078). Die Bundesregierung hatte im November 1984 den Entwurf eines Gesetzes über eine Volks-, Berufs-, Gebäude-, Wohnungs- und Arbeitsstättenzählung 1986 im Bundestag eingebracht (Bundestags-Drucks. 10/2814). Der Entwurf verzichtete darauf, ein neues Methoden- und Verfahrenskonzept vorzulegen. Abgesehen von der Frage nach den Anstaltsinsassen enthielt er das gleiche Erhebungsprogramm wie das gescheiterte Volkszählungsgesetz 1983. Ziel war also offensichtlich eine Anpassung des seit 1960 im Grunde unveränderten Volkszählungskonzepts der amtlichen Statistik an die Vorgaben des Bundesverfassungsgerichts. In meiner Stellungnahme gegenüber der Hessischen Landesregierung wie vor dem Innenausschuß des Deutschen Bundestags zu dem Regierungsentwurf habe ich besonders auf die Notwendigkeit hingewiesen, das Erhebungsprogramm konsequent einzuschränken, die zeitliche Parallelität der vier Befragungsteile (Volks-, Berufs-, Gebäude- und Wohnungs- sowie Arbeitsstättenzählung) aufzulösen und die Durchführung der Volkszählung mit dem beabsichtigten Weltzensus abzustimmen.

Wie ein Vergleich des Regierungsentwurfs für ein Volkszählungsgesetz 1986 vom November 1984 mit dem in Kraft getretenen Volkszählungsgesetz 1987 zeigt, haben Bundesrat und vor allem der Innenausschuß des Deutschen Bundestages die Entwurfsfassung erheblich verändert und wesentlich verbessert. In der Diskussion haben die Informationsinteressen der Städte und Gemeinden eine entscheidende Rolle gespielt. Während alle anderen vom Bundesverfassungsgericht geforderten verfahrenstechnischen Maßnahmen der Grundrechtssicherung mehr oder weniger vorgegeben waren, war das Ausmaß derjenigen statistischen Einzelangaben, die an die Kommunen übermittelt werden sollten, erneut umstritten. Die Bundesregierung hatte in ihrem Entwurf überhaupt keine Übermittlung von Einzelangaben vorgesehen; erst die Bundesvereinigung der Kommunalen Spitzenverbände hat dieses Thema in die Beratungen eingebracht, obwohl gerade die in den verschiedenen Tatbeständen des § 9 des Volkszählungsgesetzes 1983 vorgesehene Übermittlung von Einzelangaben an die Gemeinden die Volkszählung im wesentlichen hat scheitern lassen. Die nunmehr gefundene Regelung (§ 14) stellt einen akzeptablen, zugleich aber restriktiven Kompromiß zwischen Statistikgeheimnis und legitimen Informationsinteresse dar. Bedingung für eine Übermittlung von Einzelangaben an Gemeinden ist danach neben der organisatorischen und personellen Abschottung in der Gemeindeverwaltung eine landesrechtliche Norm, die Aufgabe und Befugnis sowie die grundrechtssichernden Verfahren der Kommunalstatistik abschließend umschreibt.

Für Hessen bedeutet diese Regelung: Ohne ein Landesstatistikgesetz kommt eine Übermittlung statistischer Einzelangaben an die Kommunen nicht in Betracht. Daran erweist sich einmal mehr, wie sehr eine verfassungskonforme Volkszählung von einer vorherigen engen Abstimmung zwischen Bundes- und Landesgesetzgebung abhängt. Die notwendigen landesrechtlichen Regelungen können nicht beliebig aufgeschoben werden, sie müssen vor der Volkszählung in Kraft getreten sein. Eine Verwendung statistischer Angaben, die der Betroffene nicht vorhersehen konnte, wäre mit dem Bestimmtheitsgebot wie auch dem Vertrauensgrundsatz des Rechtsstaatsprinzips nicht zu vereinbaren. Die Hessische Landesregierung hat - soweit ich sehe - diese Auffassung geteilt. Andererseits ist festzustellen, daß bis zum Ende des Berichtzeitraums weder der Entwurf einer Verordnung nach § 9 Abs. 2 VZG '87 noch - obwohl der Hessische Landtag wiederholt darum gebeten hat (vgl. Ziff. 13.1.4 dieses Berichts) - der Entwurf eines Landesstatistikgesetzes von der Landesregierung vorgelegt worden ist.

Selbst wenn jedoch ein Landesstatistikgesetz rechtzeitig zustande kommen sollte, könnten von einer Übermittlung statistischer Einzelangaben aus der Volkszählung nur solche Kommunen profitieren, die in der Lage sind, die strikte Abschottung der Kommunalstatistik und -planung von der übrigen Verwaltung sicherzustellen. Dies sind nach meiner Kennntnis lediglich einige Großstädte des Landes, die für die Erfüllung ihrer Planungsaufgabe auf eine funktionierende Kommunalstatistik angewiesen sind.

5.3.2
Mikrozensus

Neben der Volkszählung ist der Mikrozensus der zweite zentrale Ansatzpunkt der öffentlichen Diskussion über Voraussetzungen und Grenzen statistischer Erhebungen gewesen. Das neue Gesetz zur Durchführung einer Repräsentativstatistik über die Bevölkerung und den Arbeitsmarkt (Mikrozensusgesetz) ist am 14. Juni 1985 in Kraft getreten (BGBl. I, 955).

Im Rahmen des Gesetzgebungsverfahrens führte der Innenausschuß des Deutschen Bundestages zu dem Gesetzentwurf (Bundestags-Drucks. 10/2600) eine Anhörung durch, an der ich als Sachverständiger beteiligt war (Sitzung des Innenausschusses vom 25. Februar 1985, Protokoll 10/49). In meiner Stellungnahme habe ich vor allem auf die auch vom Bundesverfassungsgericht angestellte Überlegung hingewiesen, daß der Erfolg statistischer Erhebungen keineswegs allein von einer überzeugenden gesetzlichen Regelung abhängt. Den Ausschlag gibt vielmehr letztlich die Kooperationsbereitschaft der angesprochenen Bürger. Dem Staat fällt beim Mikrozensus genauso wie bei der Volkszählung deshalb vor allem anderen die Aufgabe zu, die Bürger von der Notwendigkeit der Erhebung zu überzeugen und in ihnen zugleich das Vertrauen in eine einwandfreie, auf die statistischen Zwecke bezogene und sich in ihr erschöpfende Verarbeitung der jeweils erhobenen Daten zu wecken. Die statistische Erhebung muß, anders ausgedrückt, von den Bürgern mitgetragen und nicht nur als sanktionsbewehrte Maßnahme wahrgenommen werden.

5.3.2.1
Freiwilligkeit

Schaffung von Kooperationsbereitschaft, darin liegt der Sinn der Forderung nach einer freiwilligen Erhebung. Wie wenig davon die Rede sein kann, daß es sich dabei um eine wirklichkeitsfremde Spekulation handelt, zeigen die ausländischen Erfahrungen.

In der Bundesrepublik hat man dagegen gemeint, die Möglichkeit freiwilliger Erhebungen abstreiten zu müssen. Sie fügten sich nicht in die Tradition statistischer Erhebungen. Zudem seien es die Bürger nicht gewohnt, von sich aus, also auch ohne jeden Zwang, an den Erhebungen teilzunehmen. Noch einmal ist freilich an die Aussagen des Bundesverfassungsgerichts zu erinnern. Der Staat darf sich nicht auf den Zwang verlassen, er muß die Kooperation des Bürgers suchen. Sie verdient den unbedingten Vorrang und ist letztlich der einzig verfassungskonforme Weg. Eben deshalb hat es das Bundesverfassungsgericht nicht bei Anforderungen an die Organisation und den Ablauf der Erhebung belassen, sondern bewußt auch die Frage der statistischen Methode angesprochen. Die Revision der Methode ist der deutlichste Ausdruck der Abkehr von einer Einstellung, die den Bürger nur als Informationsvermittler sieht, und damit Kennzeichen der Bereitschaft, den Bürger wirklich in die Erhebung einzubeziehen, sich auf Zusammenarbeit und nicht auf Zwang zu stützen. Sicher mag es, gerade weil die Freiwilligkeit als Grundsatz der statistischen Erhebung bislang kaum, und wenn nur kritisch, zur Kenntnis genommen worden ist, nicht ganz einfach sein, sich völlig auf die Bereitschaft der Bürger zu verlassen, Auskunft zu geben. Keine wie immer geartete Schwierigkeit rechtfertigt es jedoch, sich weiterhin über die Bürger hinwegzusetzen. Entsprechend hatte auch der Deutsche Bundestag in seiner Entschließung vom 15.12.1982 (Bundestags-Drucks. 9/2261) eine Auseinandersetzung mit der Erhebungsmethode, und zwar mit dem Ziel ihrer Überprüfung, gefordert.

5.3.2.2
Testerhebungen

Der Gesetzgeber ist mit der Verabschiedung des neuen Mikrozensusgesetzes nicht den Weg einer konsequenten Anerkennung der Freiwilligkeit gegangen, sondern hat sich für eine Zwischenlösung entschieden. § 13 sieht Testerhebungen mit freiwilliger Auskunftserteilung vor. Die Testerhebungen, denen alternative Verfahren zugrundezulegen sind, sollen Erkenntnisse für die künftige Ausgestaltung des Mikrozensus liefern. Diese Erhebungen dürfen aber keineswegs als bloße Konzession an zeitbedingte Widrigkeiten verstanden und gehandhabt werden. Seine Funktion kann § 13 lediglich erfüllen, wenn die Testerhebung von Anfang an als Grundlage für die Ablösung der bisherigen Methoden gesehen wird. Tests haben nur den Sinn, den Modus zu klären, nicht aber, die Veränderung selbst in Frage zu stellen.

Ganz in diesem Sinne hat der Deutsche Bundestag am 14. Mai 1985 in einer mit großer Mehrheit angenommenen Entschließung zu dem von ihm verabschiedeten Mikrozensusgesetz festgestellt:

"2.1 Die im vorliegenden Mikrozensusgesetz enthaltenen freiwilligen Befragungssteile (Angaben zum Eheschließungsjahr, zu Urlaubs- und Erholungsreisen sowie zur Gesundheit) sind ein wichtiger Schritt für die methodische Weiterentwicklung der Bundesstatistik.

Der eingeschlagene Weg, Bevölkerungsbefragungen als Bundesstatistiken auf freiwilliger Grundlage durchzuführen, sollte konsequent mit dem Ziel fortgesetzt werden, die Freiwilligkeit der Beantwortung möglichst auf alle Sachverhalte zu erstrecken." (Bundestags-Drucks. 10/3328 und Bundestags-Plenarprotokoll 10/137)

5.3.2.3
Sanktionen

Mit § 13 allein ist es jedoch nicht getan. Wenn der Gesetzgeber Kooperation wirklich ernst nehmen will, muß er darüber hinaus, bereits gegenwärtig, auf jede Sanktion bei der Auskunftsverweigerung verzichten. Bedauerlicherweise ist dies in dem neuen Mikrozensusgesetz trotz der in den vorausgegangenen Diskussionen geäußerten Zweifel an Erforderlichkeit und Geeignetheit einer sanktionsbewehrten Auskunftspflicht nicht geschehen. Wiederum ist auf die ausländischen Erfahrungen zu verweisen, die vergleichbare Sanktionsmechanismen nicht kennen und gar nicht erst in Betracht ziehen. Ganz abgesehen davon kann eine auf das Vertrauen und die Kooperation des Bürgers abzielende Gesetzgebung nicht auf Sanktionen bauen. Sie muß vielmehr alles daran setzen, dem Bürger die Ziele der Erhebung zu verdeutlichen, ihm also rechtzeitig die Möglichkeit geben, die Bedeutung der statistischen Untersuchung nachzuvollziehen und sich selbst damit auseinanderzusetzen. Vor einem Mißverständnis gilt es sich allerdings zu hüten. Das Vertrauen des Bürgers läßt sich nicht einfach damit gewinnen, daß die Vermittlung der Bedeutung einer statistischen Erhebung mit einer Marketingstrategie verwechselt wird. Statistische Erhebungen sind nicht wie Konsumgüter zu verkaufen. Ihr Erfolg ist keine Frage einer noch so aufwendig betriebenen Überredung, sondern allein des ebenso kontinuierlichen wie unentbehrlichen Dialogs mit dem Bürger. Sanktionen öffnen nicht den Weg dazu. Sie versperren ihn.

5.3.2.4
Fortschritte

Positiv ist demgegenüber die im Gesetz geregelte funktionelle Trennung von Hilfs-und Erhebungsmerkmalen (§ 3) mit jeweils unterschiedlichen Rechtsfolgen und Konsequenzen für den Verarbeitungsprozeß hervorzuheben.

Im Gegensatz zur Volkszählung ist der Mikrozensus bei externen Informationsinteressen von vornherein auf den statistischen Aussagegehalt beschränkt. Übermittlungs- bzw. Weitergabevorschriften für statistische Einzelangaben enthält daher das Gesetz selbst nicht. Es verweist insoweit auf die Bestimmungen des Bundesstatistikgesetzes.

Das Reidentifikationsrisiko ist ohne Kenntnis, ob ein Bürger in der Grundgesamtheit enthalten ist, sehr niedrig, selbst wenn ein Mikrodatensatz ohne Namen und Adresse bekannt wird.

Auch die Organisation der Erhebung ist einfacher als bei der Volkszählung. Beim Mikrozensus sind die statistischen Ämter der Länder die zuständigen Erhebungsstellen, die sich auf eigens für den Mikrozensus rekrutierte Interviewer stützen (§§ 7 u. 8).

Dem Gebot der Normenklarheit folgend, hat der Gesetzgeber das Erhebungsprogramm gegenüber der alten Regelung präziser bestimmt. Um zu gewährleisten, daß der Fragebogen auch tatsächlich dem gesetzlich festgelegten Erhebungsprogramm entspricht, gibt das Mikrozensusgesetz der Bundesregierung auf, den Inhalt des Fragebogens durch Rechtsverordnung mit Zustimmung des Bundesrats festzulegen (§ 10), was inzwischen mit der Mikrozensusverordnung vom 14. Juni 1985 (BGBl. I, 967) geschehen ist.

Das Mikrozensusgesetz stellt einen wichtigen Schritt in Richtung auf eine Gesetzgebung dar, die versucht, der Kooperation mit dem Bürger Rechnung zu tragen und den vom Bundesverfassungsgericht formulierten Anforderungen gerecht zu werden. Wie schwer sich aber der Gesetzgeber tut, diesen Weg zu gehen, zeigt das nach dem Mikrozensusgesetz verabschiedete Volkszählungsgesetz, in das beispielsweise eine Verfahrensregelung für die Festlegung des Fragebogeninhaltes nicht aufgenommen worden ist.

5.4
Bundesstatistikgesetz

Ein weiterer entscheidender Teil der Statistikreform ist die Novellierung des Bundesstatistikgesetzes. Mit seinen Verfahrens-, Institutionalisierungs- und Geheimhaltungsbestimmungen bildet es die rechtliche Infrastruktur der Bundesstatistik. Dem Bundesstatistikgesetz kommt insofern die Funktion eines "allgemeinen Teils" für die rechtlichen Regelungen der einzelnen Bundesstatistiken zu.

Der Bundesinnenminister hat am 28. November 1985 den Entwurf eines Gesetzes über die Statistik für Bundeszwecke vorgelegt. Zu diesem Entwurf ist folgendes zu bemerken: Jede Bundesstatistik, ganz gleich ob sie auf einer freiwilligen Erhebung beruht oder nicht, muß grundsätzlich umfassend durch ein Gesetz geregelt werden. Dieser auch bislang anerkannte und vom Bundesverfassungsgericht bestätigte Grundsatz wird durch den Entwurf weitgehend durchbrochen: So können im Gegensatz zum früheren Rechtszustand ohne gesetzliche Grundlage Fragebogen und Erhebungsverfahren auf ihre Zweckmäßigkeit mit Auskunftspflicht für die Betroffenen erprobt werden (§ 6 Abs. 1 Ziff. 2 Satz 2). Für einen kurzfristig auftretenden Datenbedarf dürfen Bundesstatistiken ohne einzelstatistische Rechtsgrundlagen durchgeführt werden (§ 7 Abs. 1), wobei unter "kurzfristig" auch Wiederholungsbefragungen für eine Verlaufsdarstellung bis zu zehn Jahren nach der ersten Befragung verstanden werden (vgl. § 7 Abs. 5 BStatGE). Soweit schließlich prozeßproduzierte Daten aus den Datenbanken der öffentlichen Verwaltung statistisch ausgewertet werden - eine unter dem Aspekt der funktionalen Trennung von Statistik und Verwaltung besonders problematische Vorschrift - wird das einzelstatistische Gesetz völlig in den Hintergrund gedrängt (§ 8 BStatGE).

Der Entwurf schreibt außerdem die Priorität der Auskunftspflicht fest (§ 15). Damit setzt er sich über die im Zusammenhang mit dem Volks- und Mikrozensusgesetz geführten langen wie intensiven Diskussionen hinweg, aber auch über den gleichzeitig mit der Verabschiedung des Mikrozensusgesetzes gefaßten Beschluß des Bundestages (vgl. Ziff. 5.3.2.2). In der Diskussion um beide Gesetze ist die Notwendigkeit klar geworden, sich um der Kooperation des Bürgers willen mehr und mehr an der Freiwilligkeit zu orientieren. Diesem Ziel würde es entsprechen, von festen Prioritäten abzusehen und statt dessen Mechanismen vorzusehen, die einen langfristigen Übergang zur Freiwilligkeit ermöglichen. Gerade deshalb hat das Bundesverfassunsgericht die Verpflichtung des Gesetzgebers betont, festzustellen "ob und in welchem Umfang die herkömmlichen Methoden der Informationserhebung und -verarbeitung beibehalten werden können" (BVerfGE 65, 55).

Worauf es also ankommt, ist nicht eine abstrakte Festschreibung der Auskunftspflicht, sondern umgekehrt eine Anerkennung des Grundsatzes, daß die Ziele der jeweiligen Einzelstatistik im Vordergrund zu stehen haben und von dort her die Geeignetheit und Erforderlichkeit der Auskunftspflicht zu prüfen sind. Anders ausgedrückt: Die Auskunftspflicht ist der weitestgehende Eingriff in das informationelle Selbstbestimmungsrecht, sie muß deshalb so lange unterbleiben, wie es weniger belastende Möglichkeiten gibt.

Im Sinne der Anforderungen des Bundesverfassungsgerichts müssen schließlich auch die Regelungen über Erhebungs-und Hilfsmerkmale genau überprüft werden. Erst eindeutige Vorschriften über die Trennung und Löschung können die verfassungsrechtlichen Risiken der geplanten Regelungen ausschließen.

6. Melderecht: Meldedatenübermittlungsverordnung

Die in den Melderegistern der Gemeinden gespeicherten Angaben über jeden einzelnen Einwohner werden von vielen öffentlichen und nichtöffentlichen Stellen zur Kontrolle der eigenen Datenbestände genutzt. Soweit im Einzelfall Anfragen an die Meldestellen ergehen, enthält das Landesmeldegesetz Kriterien, nach denen sich - differenziert nach Empfänger, Datenarten und Zweck der Übermittlung - jeweils feststellen läßt, ob dem Übermittlungsersuchen entsprochen werden kann.

Eine Reihe öffentlicher Stellen möchte sich mit dem umständlichen Verfahren (Anfrage - Prüfung der datenschutzrechtlichen Zulässigkeit der Übermittlung - Übermittlung oder Verweigerung der Übermittlung) jedoch nicht zufriedengeben. Sie verweisen darauf, daß sie von einer Vielzahl von Personen in nahezu identischen Situationen insbesondere Nachweise über den aktuellen Wohnort benötigen und fordern deshalb ein standardisiertes und vereinfachtes Auskunftsverfahren.
Sowohl das Melderechtsrahmengesetz des Bundes als auch das Hessische Meldegesetz sehen daher vor, daß durch Bundes- oder Landesrecht, insbesondere aber durch den Erlaß von Rechtsverordnungen, regelmäßige Datenübermittlungen an öffentliche Stellen vorgesehen werden können, soweit die entsprechenden Vorschriften den Anlaß und Zweck der Übermittlungen sowie den Datenempfänger und die zu übermittelnden Daten festlegen.

Im September dieses Jahres hat der Hessische Minister des Innern den Entwurf einer Verordnung über regelmäßige Datenübermittlungen der Meldebehörden (Meldedaten-Übermittlungsverordnung - MeldDÜVO -) vorgelegt. Nachdem die Bundesregierung mit zwei Meldedatenübermittlungsverordnungen bereits die regelmäßige Weitergabe von Daten der örtlichen Meldestellen an Bundesbehörden geregelt hat, sollen mit der geplanten Rechtsverordnung Übermittlungen an hessische Stellen festgelegt werden.

Von Detailfragen einmal abgesehen, in denen der Innenminister meinen Anregungen zum Teil gefolgt ist, wirft die geplante Regelung vier unter dem Gesichtspunkt des Datenschutzgesetzes besonders gewichtige Fragen auf.

6.1
Datenübermittlung an Ausländerbehörden

§ 11 des Entwurfs der Verordnung sieht vor, daß die Meldebehörde der zuständigen Ausländerbehörde aus Anlaß eines Wohnungswechsels, einer familienrechtlichen Statusänderung, einer Änderung staatsangehörigkeitsrechtlicher Verhältnisse oder wegen des Todes des Betroffenen einen Katalog der Daten des betroffenen Ausländers übermitteln darf.

Ursprünglich sollten nach dem Entwurf auch die Daten von Deutschen übermittelt werden, die zugleich eine fremde Staatsangehörigkeit besitzen. Zwar bestimmt § 27 des Ausländergesetzes derzeit noch, daß Deutsche, die zugleich eine fremde Staatsangehörigkeit haben, einer von der Landesregierung bestimmten Behörde ihre zusätzliche Staatsangehörigkeit anzeigen müssen. Auf diese Vorschrift bezog sich die geplante regelmäßige Datenübermittlung. Andererseits sind ausländerrechtliche Verfügungen wie die Erteilung einer Aufenthaltserlaubnis oder -berechtigung, die Ausweisung oder Abschiebung oder auch die Zurückweisung an der Grenze gegenüber Deutschen, die gleichzeitig eine ausländische Staatsangehörigkeit besitzen, nicht zulässig. Die Datenübermittlung liefe deshalb auf eine bloße Speicherung ohne denkbare Folgen für die Betroffenen hinaus und wäre insoweit nicht erforderlich. Der Innenminister hat daher meinen Vorschlag, Deutsche mit mehrfacher Staatsangehörigkeit von der Regelung auszunehmen, aufgegriffen und sich bereit erklärt, die Vorschrift abzuändern.

6.2
Datenübermittlung an Sozialbehörden

Wesentlich problematischer sind die Übermittlungstatbestände, die es Sozialbehörden ermöglichen sollen, den Kreis der berechtigten Empfänger zu kontrollieren, um insbesondere Überzahlungen nach dem Tode des Betroffenen zu vermeiden. Datenübermittlungen, die zu Kontrollzwecken erfolgen, bedingen regelmäßig die Übermittlung des Gesamtbestands der Daten eines bestimmten Personenkreises. Aus diesem Gesamtbestand werden dann durch Vergleich mit den bei der empfangenden Dienststelle bereits vorliegenden Angaben jene Personen ermittelt, die sich vorschriftswidrig verhalten haben. Es werden also wesentlich mehr Daten der empfangenden Stelle gegenüber offenbart, als diese im Ergebnis für konkrete Maßnahmen benötigt. Der Gesetzgeber hat deshalb den Verordnungsgeber verpflichtet, genau zu prüfen, ob die Übermittlung des Gesamtbestandes der Daten bestimmter, durch ein Merkmal ausgezeichneter Personen angesichts des Kontrollproblems verhältnismäßig ist.

Ich habe jedenfalls soweit keine Zweifel an der grundsätzlichen Berechtigung der Übermittlungsbegehren, als es um die regelmäßige Weitergabe von Meldedaten an die Versorgungsämter zum Zweck der Durchführung bestimmter Versorgungsgesetze geht. Ziel dieser Übermittlungen ist es, möglichst zeitnah die Zahlung von Versorgungsbezügen auszusetzen und gegebenenfalls neu festzusetzen, wenn aufgrund eines Wohnungswechsels des Leistungsempfängers oder wegen seines Todes die Gefahr von Überzahlungen besteht.

Nach dem in der Verordnung vorgesehenen Verfahren stellen die Versorgungsämter der Meldebehörde auf Datenträgern Namen, Geburtstage und Anschriften der Leistungsempfänger zur Verfügung, so daß ein Abgleich mit den Meldedatenbeständen vorgenommen werden kann, der wiederum zur Rückmeldung von Leistungsempfängern führt. Mit dieser Rückmeldung wird bestätigt, daß der Leistungsempfänger entweder gemeldet, nicht gemeldet, weggezogen oder umgezogen ist bzw. nicht eindeutig identifizierbar ist. Das Verfahren des automatisierten Abgleichs führt dazu, daß nur die Daten derjenigen Personen an die Versorgungsämter weitergegeben werden, die tatsächlich Leistungsempfänger sind. Die große Zahl des betroffenen Personenkreises und die Höhe der erbrachten Sozialleistungen rechtfertigen das Verfahren.

Diese Überlegung trifft aber nicht auf die Überprüfung von Zahlungen nach dem Landesblindengesetz zu. Hier ist nur ein sehr kleiner Personenkreis betroffen. Nach meinen Erkenntnissen dürfte es in ganz Hessen weniger als hundert Fälle im Jahr geben, in denen die Gefahr der Überzahlung besteht. Angesichts dieser Zahl halte ich einen Datenabgleich für unverhältnismäßig.

Der Verordnungsentwurf sieht auch vor, daß aus Anlaß des Wegzugs oder des Todes jedes Einwohners dessen Namen und Anschriften sowie gegebenenfalls der Sterbetag an die zuständige Wohngeldstelle zum Zweck der Durchführung des Wohngeldgesetzes übermittelt werden soll. Dies bedeutet, daß in jedem Fall, ganz gleich ob der Betroffene Wohngeld bezogen hat oder nicht, die Wohngeldstelle die veränderten Daten erhält. Da nur ein relativ kleiner Kreis von Einwohnern Wohngeld tatsächlich bekommt, erhält diese Stelle eine Unmenge von Daten, die sie gar nicht benötigt. Ich bezweifle zudem, daß sie in der Lage ist, aus der Flut der ihr zugehenden Unterlagen diejenigen Personen herauszufinden, die nach ihrem Wegzug entgegen den gesetzlichen Vorschriften nicht rechtzeitig der Behörde die veränderten Daten mitgeteilt haben.

6.3
Datenübermittlung an das Statistische Landesamt

Einen weiteren wichtigen Problembereich stellt die vorgesehene Übermittlung von personenbezogenen Meldedaten an das Hessische Statistische Landesamt zum Zweck der Durchführung der Wanderungsstatistik nach dem Gesetz über die Statistik der Bevölkerungsbewegung und die Fortschreibung des Bevölkerungsstandes dar.

Nach § 4 dieses Statistikgesetzes sollen ohne Personenbezug bei der An- und Abmeldung jedes Einwohners lediglich Tag des Bezugs der neuen oder des Auszugs aus der alten Wohnung, alte und neue Wohngemeinde, Haupt- und Nebenwohnsitz, Geschlecht, Alter und Familienstand, Erwerbstätigkeit und Zugehörigkeit oder Nichtzugehörigkeit zu einer Religionsgemeinschaft sowie die Staatsangehörigkeit jedes Einwohners erfaßt werden. In der Statistik sollen die genannten Daten somit anonym gespeichert und weiterverarbeitet werden.

Da jede Speicherung personenbezogener Daten in einer Statistik einer gesetzlichen Grundlage bedarf, ist die Übermittlung von Namen und Anschriften an das Statistische Landesamt nicht zulässig. In keinem Fall kann die geplante Meldedatenübermittlungsverordnung als selbständige und ausreichende Rechtsgrundlage für die Speicherung dieser personenbezogenen Daten angesehen werden, wenn das Statistikgesetz selbst die Verarbeitung dieser Angaben nicht vorsieht. Sie bildet vielmehr nur das Bindeglied zwischen der Verarbeitung im Melderegister und der Verarbeitung zu statistischen Zwecken. Für beide Bereiche - das Meldewesen und die Statistik - sind selbständige Rechtsgrundlagen nötig, die den Gegenstand und die Art der Datenverarbeitung regeln.

Auch der Hinweis auf die bisherige Praxis kann eine Aufnahme in die Verordnung nicht rechtfertigen. Als im Jahre 1983 aufgrund des neuen Hessischen Meldegesetzes aus dem Jahr 1982 landeseinheitlich neue Meldescheine eingeführt wurden, hat meine datenschutzrechtliche Prüfung des für das Statistische Landesamt vorgesehenen Durchschlagmeldescheins bereits ergeben, daß der für diese Behörden vorgesehene Datensatz nicht mit dem nach dem Gesetz über die Statistik der Bevölkerungsbewegung und die Fortschreibung des Bevölkerungsstandes zu speichernden Katalog von Daten übereinstimmt. Das Problem war damals wie heute das gleiche. Ich habe seinerzeit von einer Beanstandung der vorgesehenen Datenübermittlung abgesehen, da - wie mir damals versichert wurde - eine Anpassung der Rechtsgrundlage erfolgen sollte. Auch und gerade nach dem Urteil des Bundesverfassungsgerichts zur Volkszählung 1983 und angesichts des in der Zwischenzeit verstrichenen Zeitraums kann ich die bisherige Praxis ohne eine eindeutige Anpassung von Verfahren und Rechtsgrundlage nicht mehr hinnehmen. Ich habe deshalb die zuständigen Ressorts darauf aufmerksam gemacht, daß ich eine personenbezogene Datenübermittlung an das Statistische Landesamt zu den erwähnten Zwecken beanstanden müßte.

6.4
Datenübermittlung an die Polizei

Den Schwerpunkt der Verordnung bilden die vorgesehenen Datenübermittlungen zu polizeilichen Zwecken.

6.4.1
Zugriff der Polizei auf Meldedaten

Nach § 45 des Hessischen Meldegesetzes haben Polizeidienststellen die Möglichkeit, wenn die Meldestellen nicht besetzt sind, die Meldeunterlagen einzusehen. Zweck dieser Vorschrift ist es, die notwendige Information für die Polizei auch während dieser Zeit zu sichern. Der Gesetzgeber hat diese Möglichkeit nur bis zum 31. Dezember 1985 befristet zugelassen, da bei einer Einsichtnahme immer der gesamte Datenbestand offenbart wird. Der Gesetzgeber ging davon aus, daß es nach diesem Zeitpunkt technisch möglich sein würde, einen Zugriff der Polizei auf einen beschränkten Meldedatensatz einzurichten. In der Meldedatenübermittlungsverordnung soll deshalb der Polizei entweder über die Einrichtung von Direktzugriffsverfahren oder über andere technische Instrumente die Möglichkeit eingeräumt werden, außerhalb der Dienstzeiten der Meldebehörden auf einen bestimmten Meldedatensatz zugreifen zu können.

§ 13 des Verordnungsentwurfs sieht vor, daß zentral gelegenen Polizeidienststellen ein automatisiertes Abrufverfahren für die bei den Kommunalen Gebietsrechenzentren gespeicherten Einwohnerdaten zur Verfügung gestellt wird. Der Datensatz enthält über die - nahezu mit dem in § 31 Abs. 1 des Hessischen Meldegesetzes genannten Datenkatalog identischen - Grunddaten jedes Einwohners hinaus eine Reihe von Angaben zu seinem Personenstand sowie zu möglicherweise eingeräumten Übermittlungssperren. Damit würde ein Teilausschnitt der Meldedaten von etwa 92 v.H. aller Hessen der Polizei zur Verfügung gestellt.

Soweit einzelne Meldebehörden ihre Daten nicht bei den Rechenzentren verarbeiten, sieht eine Ergänzungsvorschrift vor, daß diese Behörde einer für sie unmittelbar zuständigen Polizeidienststelle denselben Datensatz im automatisierten Verfahren oder durch Überlassen von Mikrofiches zur Verfügung stellt. Der Entwurf regelt nicht klar, daß beide Möglichkeiten alternativ gesehen werden müssen und mit dieser Regelung die Daten eines Teils der übrigen 8 v.H. aller hessischen Bürger erfaßt werden sollen. Diese Einschränkung müßte ausdrücklich in die Verordnung aufgenommen werden. Ein kumulativer Zugriff auf die Daten jedes Einwohners - zentral und dezentral - wäre datenschutzrechtlich nicht hinnehmbar.

Viel bedeutsamer ist jedoch das Grundkonzept der lückenlosen Anbindung der Polizeidienststellen an die Meldebehörden. Wenn der Entwurf auch eine für ganz Hessen zentral eingerichtete Abrufstelle der Polizei nicht zuläßt und von der ursprünglichen Vorstellung eines Rechner-Rechner-Verbundes von Polizei und Kommunalen Gebietsrechenzentren aufgrund meiner ablehnenden Stellungnahme Abstand nimmt, so werden doch durch die Konzentration des Zugriffs in den Bereichen der fünf regionalen Rechenzentren Daten so zusammengeführt, daß von einer Vorstufe zu einem Landesadreßregister für den Bereich der Polizei gesprochen werden kann. Die dezentrale Struktur der Melderegister, die das Melderechtsrahmengesetz und das Hessische Meldegesetz auch aus datenschutzrechtlichen Gründen vorschreibt, wird insoweit in Frage gestellt.

Hinzu kommt: Verlangt die Polizei im Einzelfall während der Dienstzeiten der Meldebehörde Daten eines bestimmten Einwohners, so ist die Polizeidienststelle nach dem Gesetz verpflichtet, die Erforderlichkeit der Datenübermittlung darzulegen. Die sich an diese Darlegung anschließende Prüfung durch die Meldebehörde entfällt bei einem Direktzugriff. Die Meldebehörde registriert nicht einmal die Tatsache des Zugriffs durch den Dritten. Die "präventive" Datenschutzkontrolle entfällt demnach. Sie wird allenfalls ersetzt durch eine spätere Nachkontrolle der Zugriffsprotokolle des Abrufverfahrens. Zu diesem Zeitpunkt ist die Datenübermittlung jedoch immer schon erfolgt. Daraus ergeben sich folgende Konsequenzen:

- Ein Direktzugriff darf nur insoweit eingerichtet werden, als dies aus polizeilichen Gründen und unter Berücksichtigung des Rechts auf informationelle Selbstbestimmung der Betroffenen unabdingbar ist.
- Andere Formen der Datenübermittlung, die die datenschutzrechtlichen Nachteile des Direktzugriffsverfahrens nicht aufweisen, müssen in die Überlegung einbezogen werden.
- Die datenschutzrechtlichen Vor- und Nachteile eines zentralen bzw. dezentralen Zugriffs auf die Meldedaten sind zu berücksichtigen.

Dem Argument der Polizei, der Direktzugriff als schnellstes Verfahren der Datenübermittlung sei gerade an Wochenenden notwendig, um zu verhindern, daß ein aufgegriffener Bürger, der seinen festen Wohnsitz nicht nachweisen könne, gegebenenfalls bis zum Montag festgehalten werden müsse, bis die von ihm angegebene Meldeanschrift überprüft werden könne, habe ich verständlicherweise besondere Aufmerksamkeit geschenkt. Der Datenschutz als Rechtfertigung einer - wenn auch zeitlich beschränkten - Freiheitsentziehung ist in der Tat eine befremdliche Vorstellung. Meine stichprobenhafte Überprüfung bei etwa zehn Klein- und Mittelstädten auch aus dem südhessischen Bereich ergab jedoch ein erstaunliches Ergebnis: Obwohl nach § 45 des Hessischen Meldegesetzes die für diese Meldebehörden zuständigen Polizeidienststellen bis zum 31. Dezember 1985 berechtigt waren, die Meldeunterlagen einzusehen, nahmen sie dieses Recht praktisch nicht wahr. Die von mir angesprochenen Leiter der Einwohnermeldeämter und Polizeibediensteten gaben an, daß ihnen trotz langjähriger Praxis eine Einsichtnahme der Polizei am Wochenende oder während der Nachtzeit nicht bekannt sei. Mehr noch: In allen diesen Fällen hatte die Polizei noch nicht einmal die Meldebehörden darum gebeten, ihr einen Schlüssel zur Verfügung zu stellen.

Im Gegensatz hierzu stellte ich fest, daß in den südhessischen Großstädten im Jahre 1985 in hunderten bzw. bis nahezu 2.000 Fällen auch während dieser Zeiten auf Meldedaten zugegriffen wurde. Meine These, daß der permanente Zugriff auf Meldedaten nur in den Ballungsgebieten als den Schwerpunkten des kriminellen Handelns erforderlich erscheint, wurde durch diese Umfrage in überraschender Eindeutigkeit bestätigt.

Nach diesem Ergebnis wäre es durchaus ausreichend, wenn das Direktzugriffsverfahren sich lediglich auf die Anbindung der Polizeipräsidenten in den Großstädten an die örtlichen Meldeämter beschränken würde. Außerhalb dieses Bereiches müßte es deshalb genügen, wenn die örtlichen Polizeidienststellen über Ausschnitte der Melderegister aus ihrem Zuständigkeitsbereich verfügten.

Andererseits hätte ein zentraler Zugriff der Polizei aus der Sicht des Datenschutzes auch Vorteile. So könnten die einzelnen Abrufe genau protokolliert werden und anschließend stichprobenhaft auch durch den Datenschutzbeauftragten überprüft werden. Ein individueller Mißbrauch der Ausschnitte der Melderegister auf örtlicher Ebene wäre dann nicht möglich.

Meine Gespräche mit dem Hessischen Minister des Innern zu diesem Themenbereich sind noch nicht vollständig abgeschlossen. Eines ist jedenfalls unabdingbar: Die Lösung muß sich vor allem an den durch das Melderecht vorgegebenen und dem Datenschutz verpflichteten Wertungen orientieren. Die Wünsche der Polizei nach einem schnelleren Zugriff auf Meldedaten sind insbesondere auch daran zu messen, was sich bisher für ihre Tätigkeit als notwendig erwiesen hat.

6.4.2
Datenübermittlung zu Fahndungszwecken

Eine weitere Vorschrift des Entwurfs sieht vor, daß die Meldebehörde der zuständigen Polizeidienststelle zu Fahndungszwecken und zur Berichtigung kriminalpolizeilicher Unterlagen und Dateien aus Anlaß der Anmeldung eine Reihe von Daten übermitteln kann.

Diese Vorschrift halte ich für verfassungsrechtlich unzulässig. Wie bereits in der Diskussion um das Berliner Meldegesetz im Zusammenhang sowohl mit der sogenannten Krankenhaus- als auch der Hotelmeldepflicht dargelegt worden ist, verstößt die Annahme, der Aufenthalt einer Person im Krankenhaus oder Hotel sei von "polizeilicher Bedeutung", gegen das informationelle Selbstbestimmungsrecht. Gleiches muß auch für die vorgeschlagene Regelung gelten. Der Zuzug eines Bürgers in eine Gemeinde kann keinesfalls als Handlung gewertet werden, die wegen ihrer Nähe zu einer Straftat oder aus Gründen der Gefahrenabwehr der Polizei mitgeteilt werden muß.

7. Telekommunikationsrecht

7.1
Telekomunikationsordnung

Bereits in meinem letzten Tätigkeitsbericht habe ich für die neuen Telekommunikationsdienstleistungen klare, den Anforderungen des Datenschutzes entsprechende gesetzliche Regelungen gefordert (vgl. 13. Tätigkeitsbericht, Ziff. 3.1).

Die vom Bundespostminister Anfang Dezember 1985 im Entwurf vorgestellte Telekommunikationsordnung (TKO) erfüllt diese Forderung nicht. Ihr Ziel ist, die benutzungsrechtlichen Voraussetzungen für die Einführung von ISDN und die damit zusammenhängende Integration der einzelnen Telekommunikationsdienste zu schaffen, wenn man einmal von den Fragen der Gebührengestaltung absieht. Die Abkürzung ISDN steht für Integrated Services Digital Network. Gemeint ist damit das von der Bundespost geplante digitale Fernmeldenetz, das eine vollständig integrierte Übertragung von Sprache, Text, Daten und Bild ermöglichen soll. Die TKO soll nach dem Entwurf die bisher 5 Fernmeldebenutzungsverordnungen (Fernmeldeordnung, Telegrammordnung, Verordnung über den Fernschreib- und Datexdienst, Verordnung über das öffentliche Direktrufnetz für die Übertragung digitaler Nachrichten, Verordnung über den Post- und Fernmeldeverkehr mit der deutschen Post der DDR) zusammenfassen.

Zu dem Entwurf ist festzustellen: Die medienpolitische Kompetenz der Länder wird damit weiter zurückgedrängt. Darüber hinaus erscheint fraglich, ob die Verordnungsermächtigung in § 14 Postverwaltungsgesetz (PVerwG) die vorgelegten Vorschläge abdeckt.

§ 14 PVerwG ermächtigt den Bundespostminister, die Rechtsverordnungen über die Bedingungen und Gebühren für die Benutzung der Einrichtungen des Post- und Fernmeldewesens zu erlassen. Zwar sind als Grundlage für die Benutzungsverordnungen nicht allein § 14, sondern auch die §§ 2 Abs. 3, 15 Abs. 1, 20 und 21 PVerwG herangezogen worden. Entscheidend ist jedoch, daß es sich um die Regelung des Post- und Fernmeldewesens handeln muß. "Was unter Post- und Fernmeldewesen... zu verstehen ist", so das Bundesverfassungsgericht, "ergibt sich hinreichend deutlich aus der historischen Entwicklung und dem allgemeinen Sprachgebrauch." (BVerfGE 28, 25). Die neuen Telekommunikationsdienste können kaum als Entwicklung aus dem Post- und Fernmeldewesen angesehen werden. Ebensowenig deckt "Post- und Fernmeldewesen" im allgemeinen Sprachgebrauch die durch Integration von Datenverarbeitung und -übertragung gekennzeichneten neuen Telekommunikationsmöglichkeiten ab.

Selbst wenn man berücksichtigt, daß das Bundesverfassungsgericht in einer späteren Entscheidung den Begriff der Fernmeldeanlage für zukünftige Entwicklungen geöffnet hat, "für neue, seinerzeit noch nicht bekannte Techniken der Nachrichtenübertragung" (BVerfGE 46, 120, 143), beseitigt dies nicht die Zweifel an der ausreichenden Rechtsgrundlage für die TKO.

Wenn es zutrifft, daß über das geplante integrierte breitbandige Glasfasernetz alle Massen- und Individualkommunikation abgewickelt werden wird, dann erfordert dies auch gerade im Hinblick auf den Datenschutz in integrierten Netzen landespolitische Überlegungen zur Gestaltung der Kommunikation. Der Landesgesetzgeber wird auf Dauer nicht umhin können, einen eigenen landesrechtlichen Ordnungsrahmen für Telekommunikationsdienste zu schaffen. Die zunehmende internationale Vernetzung sowie der damit verbundene, immer intensiver werdende, grenzüberschreitende Datenaustausch lassen schließlich darauf abgestellte internationale Vereinbarungen über den Datenschutz bei supranationalen bzw. grenzüberschreitenden Telekommunikationssystemen als erforderlich erscheinen. Der Anschluß Frankreichs und der Niederlande an das Btx-System der Deutschen Bundespost, dem weitere Staaten folgen werden, verdeutlichen mehr denn je die internationale Rechtsetzungsaufgabe.

7.2
Das Elektronische Telefonbuch

7.2.1
Entwicklungsstand

Die Deutsche Postreklame, ein privatrechtliches Unternehmen der Deutschen Bundespost, hat auf der Internationalen Funkausstellung 85 in Berlin das "Elektronische Telefonbuch" (ETB) als neuen Bildschirmtext-Service vorgestellt. Seit September können die Teilnehmer der Ortsnetze Berlin, Hamburg und München abgerufen werden. Erste positive Erfahrungen waren zuvor in Düsseldorf gemacht worden. Bereits im Frühjahr 1983 konnten dort die Teilnehmer eines Feldversuchs rund 500.000 Telefonnummern aus dem Versuchsgebiet abfragen. Interessant sind dabei die Zahlen: In Anbetracht von lediglich 2.000 Btx-Versuchsteilnehmern wurden zu Beginn täglich etwa 200 Auskünfte über die Teleauskunft erteilt, nach Darstellung der Zeitschrift "Btx Praxis" (6/85) haben sich die Abfragen je Tag zwischen 50 und 100 eingependelt. Dieser im Vergleich zu anderen Btx-Angeboten große Erfolg sowie das überraschend gut angenommene elektronische Telefonbuch in Frankreich haben den entscheidenden Impuls für die Deutsche Postreklame und rund 100 Verleger der örtlichen Fernsprechbücher gegeben, das ETB bundesweit zu realisieren. Von 1986 an sollen alle 25 Millionen Telefonkunden im Bereich der Deutschen Bundespost gespeichert und über Btx abfragbar sein.

Der Regierungspräsident in Darmstadt als zuständige Btx- Aufsichtsbehörde hat dies zum Anlaß genommen, sich über das Projekt ETB umfassend zu informieren. Er hat mich auf meinen Wunsch hin gemäß § 6 Abs. 2 des Hessischen Gesetzes zum Staatsvertrag über Bildschirmtext vom 24. Juni 1983 (GVBl I, 91) an der Überprüfung beteiligt. Teilgenommen hat außerdem der Bundesbeauftragte für den Datenschutz, da es auch um die Deutsche Bundespost unmittelbar angehende Datenschutzfragen ging. Dieses gemeinsame Informationsgespräch hat noch zu keiner abschließenden Beurteilung geführt, vielmehr haben sich verschiedene Probleme rechtlicher und technischer Art abgezeichnet, die noch vor der endgültigen Inbetriebnahme des Systems gelöst werden sollten.

7.2.2
Funktionsweise

Zur technischen Situation und einzelnen Leistungsmerkmalen des ETB:

Das Informationssystem wird getragen durch drei Rechenzentren in Essen, Frankfurt und Nürnberg, die miteinander verbunden sind. Jeder Fernsprechteilnehmer, der das ETB abfragt, wird automatisch auf das für seine Abfrage zuständige Zentrum geschaltet, wobei generell nur der Ortstarif berechnet wird.

Der Einstieg in das System erfolgt ausschließlich über die Ortsangabe, von denen etwa 200.000 im Ortsbestand gespeichert sind. Ist der Ort identifiziert, führt dies zu einem der 6.000 Buchabschnitte, die aus dem herkömmlichen Amtlichen Fernsprechbuch bekannt sind.

Die Suche des Teilnehmers erfordert dann die Eingabe des Namens mit evtl. notwendig werdenden Zusatzangaben, wenn die Zahl der gefundenen Teilnehmer 60 - oder wie später vorgesehen 30 - überschreitet.

Führen beide vorgenannten Suchformen nicht zum Ziel, findet der Benutzer noch zwei Sondersuchformen in dem System vor: Die Nahbereichsuche und die phonetische Namenssuche. Die Nahbereichsuche gestattet es dem Telefonteilnehmer auch in den Buchabschnitten eines Nahbereiches (ca. 20 km Radius, 8 Minuten-Takt der Deutschen Bundespost) zu suchen. So kann eine Familie Fuckner in Kiedrich aufgefunden werden, auch wenn die Suche vom Ortsnetz Wiesbaden ausgegangen ist. Die andere Variante der Sondersuche ist die phonetische Suche. Sie hilft dem Anwender z.B.bei der Namenseingabe Rydzy. Das System erreicht auch die Namen Ritzi, Ritzy, Ricci oder Rüdzy bei einer Eingabe von Rydzy.

7.2.3
Gefahren

Diese gegenüber dem herkömmlichen Telefonbuch neuartige Telefonkundendatenbank bringt allerdings auch Gefahren mit sich: Die Möglichkeit, die Datei selbst zu duplizieren sowie das ETB zu benutzen, um schnell und gezielt bestimmte Personengruppen zusammenzustellen. Ließen sich diese Ziele mit Hilfe eines Rechners ohne erheblichen Kostenaufwand erreichen, dann würde sich das ETB als Substrat des unter Datenschutzgesichtspunkten immer wieder abgelehnten automatisierten Bundesadreßregisters erweisen. Wirksame Vorkehrungen gegen beide Möglichkeiten sind daher der Prüfstein für die Zulässigkeit des ETB. Die Interessen der Postreklame sowie der Verleger der örtlichen Fernsprechbücher lassen sich allerdings nicht ohne weiteres mit solchen Einschränkungen in Einklang bringen. Die Postreklame hat jedoch zugesagt, mögliche technische Sicherungen zu prüfen und, soweit die Benutzbarkeit des Systems nicht zu weit eingeschränkt wird, auch einzusetzen.

Darüber hinaus bietet das ETB die Möglichkeit, weitaus leichter als bisher einen Fernsprechteilnehmer ausfindig zu machen. So könnte man z.B. über die Nahbereichsuche Frankfurt, Darmstadt und Wiesbaden prinzipiell jeden Fernsprechteilnehmer ausfindig machen, von dem bekannt ist, daß er nach Südhessen umgezogen ist. Dies kann durchaus vorteilhaft, im Einzelfall allerdings auch mit großen Nachteilen für den Betroffenen verbunden sein. Für Inkassobüros, Detekteien, Auskunfteien bis hin zu den Sicherheits- und Finanzbehörden bietet das ETB eine erleichterte Möglichkeit der Feststellung der Wohnung.

Dieser Aspekt muß umso mehr bedacht werden, als das ETB - jedenfalls in seiner gegenwärtigen Form - die Chance bietet, die vom Gesetzgeber für die Melderegister ausdrücklich vorgesehenen Informationsschranken zu überwinden. Es ist nach wie vor wesentlich einfacher, eine Auskunftsperre im Meldebereich durchzusetzen als einen Eintrag im Telefonbuch zu vermeiden.

7.2.4
Konsequenzen

Ohne einer noch ausstehenden, gemeinsamen datenschutzrechtlichen Bewertung durch den Regierungspräsidenten in Darmstadt und den Hessischen Datenschutzbeauftragten vorgreifen zu wollen, läßt sich soviel schon anmerken: Diese qualitative Veränderung der Fernsprechauskunft findet in den §§ 12 Abs. 2, 39 Fernmeldeordnung keine Grundlage mehr. Die qualitative Veränderung vom gedruckten Fernsprechbuch hin zur automatisierten Teleauskunft wird von diesen Bestimmungen nicht erfaßt.

In Anbetracht der möglichen Konsequenzen der Automatisierung muß erneut und weitaus nachdrücklicher geprüft werden, ob die Übermittlung personenbezogener Daten von der Deutschen Bundespost an die Deutsche Postreklame hingenommen werden darf. Konkret: Eine Weitergabe kann erst akzeptiert werden, wenn zuvor die Verarbeitungskonsequenzen bei der Postreklame offengelegt, an den Anforderungen des Datenschutzes gemessen und - wo notwendig - entsprechend eingeschränkt worden sind.

8. Datensicherheit

8.1
Datensicherheit in Finanzämtern

Um mir einen Eindruck über die Aufbewahrung von Steuerakten zu verschaffen, habe ich zwei Finanzämter überprüft.

Vorweg ist soviel festzustellen: Die unzureichenden räumlichen Verhältnisse führen immer wieder dazu, die unter Datenschutzgesichtspunkten unverzichtbaren Sicherheitsvorkehrungen zu vernachlässigen. So verständlich die sich aus der räumlichen Situation ergebenden Schwierigkeiten sind, so wenig darf daraus eine Vernachlässigung der Datensicherung folgen.

Bei einem Finanzamt stellte ich folgende Mängel fest: Wegen der beengten Verhältnisse in den Büroräumen stapeln die Mitarbeiter die Akten von Steuerpflichtigen in offenen Regalen auf den Fluren. Besucher können unter diesen Umständen ohne Schwierigkeiten die Akten einsehen. Vorkehrungen dagegen waren nicht zu erkennen. Eine Kontrolle läßt sich bei verständlicherweise geschlossenen Bürotüren nicht durchführen.

Auf den Fluren befanden sich ferner Rollschränke mit herausgebrochenen oder nicht mehr funktionsfähigen Schlössern. Sofern die Schränke überhaupt abschließbar waren, mußte ich mehrfach feststellen, daß - entgegen vorliegender Anweisungen - die Schlüssel nicht abgezogen waren.

Solche Mängel wirken um so gravierender, als auch die Zugangskontrolle für das Gesamtgebäude zu Wünschen übrig ließ. In dem Gebäude waren noch andere Ämter untergebracht. Der Pförtner erfüllte letztlich nur eine Auskunfts- nicht aber eine Überprüfungsfunktion.

Der Hessische Minister der Finanzen hat auf meine Beanstandung hin eine Reihe von Maßnahmen getroffen: Die Oberfinanzdirektion wurde unter anderem angewiesen, Vorschläge zur Beseitigung der festgestellten Sicherungsmängel vorzulegen. Darüber hinaus wurden die Vorsteher der hessischen Finanzämter nochmals nachdrücklich auf die Einhaltung der bereits vorliegenden Anweisungen zur Datensicherung hingewiesen.

8.2
Datensicherheit im Hessischen Statistischen Landesamt

Bei einer Prüfung des Statistischen Landesamts mußte ich feststellen, daß die Datensicherung erhebliche Mängel aufweist.

Die Erhebungsbögen waren zum Teil offen in Regalen gelagert, die archivierten Unterlagen früherer statistischer Erhebungen nicht ausreichend gesichert und die Zugangssicherungen zu dem Dienstgebäude, in dem die gesamte Datenerfassung für die Landesstatistik untergebracht ist, unzureichend.

Ähnlich wie im Fall des Finanzamts spielen auch hier der bauliche Zustand des Gebäudes aus dem Jahre 1836 und die räumliche Situation eine wichtige Rolle. Insofern handelt es sich keineswegs um Mängel, die ausschließlich beim Statistischen Landesamt bestehen, sondern im Gegenteil in weiten Bereichen bei der Landesverwaltung immer wieder anzutreffen sind. Die Landesregierung müßte deshalb die im Zusammenhang mit dem Finanzamt und dem Statistischen Landesamt getroffenen Feststellungen zum Anlaß nehmen, generell die mit räumlich problematischen Verhältnissen zusammenhängenden Datensicherungsmängel zu beseitigen.

Die verschiedenen Mängel beim Statistischen Landesamt habe ich dem Hessischen Ministerpräsidenten als Aufsichtsbehörde mitgeteilt. Seiner Antwort entnehme ich, daß noch vor dem Volkszählungsurteil des Bundesverfassungsgerichts bei den zuständigen Stellen ein Gutachten über Sicherungsmaßnahmen im Hessischen Statistischen Landesamt in Auftrag gegeben worden ist. Auf der Grundlage dieses Gutachtens wurden in dem Haushaltsvoranschlag 1984 für Sicherungsmaßnahmen Mittel eingestellt. Die zur Ausführung notwendigen Aufträge sollen bis zum Ende des Berichtszeitraums abgeschlossen sein. Ich habe daher zunächst davon abgesehen, die Datensicherung im Hessischen Statistischen Landesamt zu beanstanden, behalte mir allerdings eine Überprüfung vor.

8.3
Datensicherheit in Datennetzen

Im Bereich der öffentlichen Verwaltung des Landes Hessen, insbesondere im Bereich der fünf Kommunalen Gebietsrechenzentren, wird zur Datenfernverarbeitung innerhalb des öffentlichen Datennetzes in großem Umfang der Synchronkonten SK 12 genutzt.

8.3.1
Grund für den Einsatz

Knoten wie der SK 12 werden im Bereich öffentlicher Netze eingesetzt, um Leitungskosten zu sparen. Die Leitungskosten steigen entsprechend der Länge der verwendeten Leitung. Verbindet man jede Datenendeinrichtung (DEE; beispielsweise Datensichtgerät, Kleinrechner) einzeln mit dem Rechner, können hohe Leitungskosten entstehen. Man kann statt dessen aber auch mehrere Datenendeinrichtungen, die räumlich nahe beieinander, aber vom Rechner weit entfernt liegen, jeweils mit einem in der Nähe gelegenen Knoten (z.B. einem SK 12) verbinden und vom Knoten zum Rechner eine einzige Leitung schalten, die von den Datenendeinrichtungen gemeinsam benutzt wird. Für die gemeinsame Leitung fallen dann nur einmal Leitungskosten an, die sich die am Knoten angeschlossenen Anwender teilen können. Dieses Verfahren, bei dem eine Leitung vom Rechner abgeht, die sich dann an einem Knoten in mehrere Leitungen aufteilt, die zu den verschiedenen Anwendern führen, wird "Mehrpunktbetrieb" genannt.

8.3.2
Konfiguration

Der Synchronknoten SK 12 wird zusammen mit Übertragungseinheiten und Datenanschlußgeräten für Mehrpunktbetrieb verwendet.

Die Konfiguration sieht folgendermaßen aus:

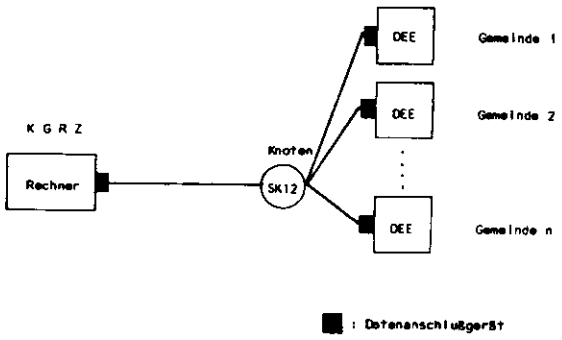

Abb.: Mehrpunktbetrieb unter Verwendung des SK 12

Das Datenanschlußgerät an dem zentralen Rechner ist über eine Postleitung (HfD) mit dem SK 12 verbunden. Bis zu acht Datenendeinrichtungen können mit Hilfe von Datenanschlußgeräten - ebenfalls über jeweils eine Post-Standleitung - an den SK 12 angeschlossen werden. Der SK 12 selbst kann entweder im Bereich der Deutschen Bundespost oder bei einem Anwender aufgestellt sein.

8.3.3
Funktionsbeschreibung

Die Kommunikation zwischen dem Rechner und den Datenendeinrichtungen wird über ein Datenübertragungssteuerungsverfahren, auch Leitungsprozedur genannt, geregelt. Diese Leitungsprozedur ist weder genormt noch sonst eindeutig festgelegt. Die verschiedenen (herstellerspezifischen) Leitungsprozeduren arbeiten aber alle so, daß den Datenendeinrichtungen jeweils eine eindeutige Adresse zugeordnet wird und daß eine Datenendeinrichtung nur dann Daten senden kann, wenn sie durch Nennung ihrer Adresse ausdrücklich vom Rechner dazu aufgefordert worden ist. Die Daten der aufgerufenen Teilnehmerstationen werden vom SK 12 an die Zentrale durchgeschaltet. Umgekehrt versieht der Rechner die zu sendenden Ausgabedaten mit der Adresse der Datenendeinrichtung, für die diese Ausgabe bestimmt ist (wo und wie in dem zu übertragenden Datenblock diese Adresse angegeben ist, wird durch die verwendete Leitungsprozedur festgelegt). Der Synchronknoten SK 12 wertet nun aber diese Adreßinformation nicht aus, sondern gibt den gesamten Datenblock an alle Datenanschlußgeräte weiter, die an diesem Knoten angeschlossen sind. Erst vom Datenanschlußgerät oder der Datenendeinrichtung wird bei der Abwicklung der Leitungsprozedur diese Adresse normalerweise so ausgewertet, daß an jeder Datenendeinrichtung nur die Daten angezeigt werden, die für die eigene Adresse bestimmt sind.

8.3.4
Risiken

Es gibt verschiedene Möglichkeiten (durch Manipulation am Datenanschlußgerät oder der zugehörigen Datenendeinrichtung oder unter Einsatz von Zusatzgeräten), wie ein Teilnehmer die richtige Adreßauswertung umgehen und damit nicht nur die für ihn bestimmten Daten empfangen kann, sondern auch alle Daten, die vom Rechner kommen und für irgendwelche anderen Teilnehmer bestimmt sind, die hinter dem SK 12 angeschlossen sind. Mir ist bekannt geworden, daß sich ein Mitarbeiter einer Gemeinde Daten einer anderen Gemeinde ausgedruckt hat, die über denselben SK 12 an einem Kommunalen Gebietsrechenzentrum angeschlossen ist. Meine Recherchen haben darüber hinaus ergeben, daß es "Lausch- Verfahren" gibt, bei denen weder die übrigen Anwender noch das Rechenzentrum feststellen können, ob und gegebenenfalls wem die für einen der Anwender bestimmten Daten auf einem solchen Weg zur Kenntnis gelangen. Dies entspricht nicht den Anforderungen des Datenschutzes, zumal keine hard- und softwaretechnischen Maßnahmen bekannt sind, mit denen bei Verwendung des SK 12 solcher Mißbrauch verhindert oder festgestellt werden kann.

8.3.5
Konsequenzen

1.
Zunächst habe ich den Bundesminister für das Post- und Fernmeldewesen als den Betreiber der öffentlichen Netze auf die mir bekannt gewordenen Gefahren hingewiesen. Ich habe dabei betont, daß die Benutzer, für die die Risiken nicht ohne weiteres ersichtlich sind, unbedingt in den entsprechenden Beschreibungen (z.B. im DATEL-Handbuch) und in Beratungsgesprächen von der Post darauf aufmerksam gemacht werden müssen, daß der Datenschutz in öffentlichen Netzen bei Verwendung des SK 12 nicht gewährleistet ist. Darüber hinaus müsse es im Interesse des Betreibers umfangreicher öffentlicher Netze liegen, eine Alternative anzubieten, die den Anforderungen des Datenschutzes in vollem Umfang gerecht wird und die gleichzeitig eine besonders wirtschaftliche Nutzung - vergleichbar der des SK 12 - von Datenfernverarbeitungssystemen erlaubt.

Die Post hat in ihrer Antwort die von mir gegebene Funktionsbeschreibung bestätigt und zugesagt, daß sie den Beschreibungsmängeln in ihren speziellen Unterlagen durch Ergänzungen abhelfen wird.

2.
Den Arbeitsausschuß für die Automation von Verwaltungsaufgaben des Landes (LAA) und den Arbeitsausschuß für die Automation von Aufgaben der Gemeinden und Landkreise (KAA) habe ich auf dieses Problem ebenfalls aufmerksam gemacht.

Der LAA hat in seiner Sitzung am 1. Oktober 1985 festgestellt, daß für den Landesbereich kein Handlungsbedarf besteht. Um diese Frage auch für den Landesbereich außerhalb des DV-Verbundes zu klären, habe ich den Minister für Wissenschaft und Kunst angeschrieben mit der Bitte, zu klären, ob im Bereich der Fachhochschulen, Hochschulen und Universitätskliniken der SK 12 zur Verarbeitung personenbezogener Daten genutzt wird, und ihn gegebenenfalls zu ersetzen.

Eine Anfrage bei den Kommunalen Gebietsrechenzentren und der Hessischen Zentrale für Datenverarbeitung hat ergeben, daß die KGRZ den SK 12 in großem Umfang (ca. 10-17 SK 12 je KGRZ) nutzen. Damit sind gerade die an die KGRZ angeschlossenen öffentlichen Stellen betroffen, zumal auch die o.g. mißbräuchliche Nutzung von einer dieser Stellen durchgeführt wurde. Der KAA hat dieses Thema auf seiner Sitzung am 12. Dezember 1985 beraten und mit Rücksicht auf die technischen Aspekte den Koordinierungsausschuß (KOA), der aus dem Vorstand der Hessischen Zentrale für Datenverarbeitung und den Direktoren der Kommunalen Gebietzsrechenzentren besteht, eingeschaltet.

Ich bin nach wie vor der Meinung, daß der SK 12 nicht weiter zur Verarbeitung personenbezogener Daten verwendet werden darf. Statt dessen halte ich es für geboten, daß die betroffenen Rechenzentren den SK 12 durch technisch sichere Alternativen ablösen, die den Anforderungen des Datenschutzes entsprechen. Dies habe ich auch in einem Schreiben an den KOA zum Ausdruck gebracht.

Meine Bedenken habe ich auch den anderen Datenschutzbeauftragten mitgeteilt. Im Anschluß daran streben vor allem die Länder Nordrhein-Westfalen und Baden-Württemberg Korrekturen an. klären, habe ich den Minister für Wissenschaft und Kunst angeschrieben mit der Bitte, zu klären, ob im Bereich der Fachhochschulen, Hochschulen und Universitätskliniken der SK 12 zur Verarbeitung personenbezogener Daten genutzt wird, und ihn gegebenenfalls zu ersetzen.

Eine Anfrage bei den Kommunalen Gebietsrechenzentren und der Hessischen Zentrale für Datenverarbeitung hat ergeben, daß die KGRZ den SK 12 in großem Umfang (ca. 10-17 SK 12 je KGRZ) nutzen. Damit sind gerade die an die KGRZ angeschlossenen öffentlichen Stellen betroffen, zumal auch die o.g. mißbräuchliche Nutzung von einer dieser Stellen durchgeführt wurde. Der KAA hat dieses Thema auf seiner Sitzung am 12. Dezember 1985 beraten und mit Rücksicht auf die technischen Aspekte den Koordinierungsausschuß (KOA), der aus dem Vorstand der Hessischen Zentrale für Datenverarbeitung und den Direktoren der Kommunalen Gebietzsrechenzentren besteht, eingeschaltet.

Ich bin nach wie vor der Meinung, daß der SK 12 nicht weiter zur Verarbeitung personenbezogener Daten verwendet werden darf. Statt dessen halte ich es für geboten, daß die betroffenen Rechenzentren den SK 12 durch technisch sichere Alternativen ablösen, die den Anforderungen des Datenschutzes entsprechen. Dies habe ich auch in einem Schreiben an den KOA zum Ausdruck gebracht.

Meine Bedenken habe ich auch den anderen Datenschutzbeauftragten mitgeteilt. Im Anschluß daran streben vor allem die Länder Nordrhein-Westfalen und Baden-Württemberg Korrekturen an.

9. Dateienregister - Defizite bei Registermeldungen

In früheren Tätigkeitsberichten ist bereits mehrfach auf die Mängel bei Form, Inhalt und Anzahl der Meldungen der meldepflichtigen Behörden zu dem nach § 25 HDSG von mir zu führenden Dateienregister hingewiesen worden (vgl. 9. Tätigkeitsbericht, Ziff. 5.2; 11. Tätigkeitsbericht, Ziff. 4.6).
Daran hat sich bis heute wenig geändert:

- Der amtliche Meldevordruck wird z.B. nicht verwendet oder nur unvollständig ausgefüllt.
- Die von der Behörde vorzunehmende Veröffentlichung über die gespeicherten Daten (§ 17 HDSG) wird zugleich als Meldung zum Dateienregister angesehen.
- Für gleiche Dateien werden unterschiedliche Rechtsgrundlagen angegeben, oder es erfolgt ein genereller Verweis auf die allgemeine Zulässigkeitsnorm des § 11 HDSG, obwohl bereichsspezifische Regelungen existieren.
- Meldepflichtige manuelle Karteien werden mitunter nicht gemeldet.
- Änderungsmeldungen unterbleiben, beispielsweise bei Änderung der Verarbeitungsart, der Art der gespeicherten Daten oder der Stellen an die regelmäßig übermittelt wird.
- Der überwiegende Teil der Meldungen wurde in den ersten 12 Monaten nach Inkrafttreten der Hessischen Verordnung über die von dem Hessischen Datenschutzbeauftragten zu führenden Dateienregister (Hessische Datenschutzregisterordnung - HDSRegO), d.h. 1979/80, erstattet. Nicht von mir angeforderte Nachmeldungen erfolgten lediglich dann, wenn es sich um automatisierte Verfahren handelte, bei denen von den zuständigen Rechenzentren den Anwendern wesentliche Teile der Meldung vorgegeben wurden (z.B. kommunales Finanzwesen, Einwohner- und Personalwesen).

Die Aufzählung der Mängel ließe sich fortsetzen. Diese Defizite habe ich in allen Bereichen der öffentlichen Verwaltung festgestellt, in besonderem Maße sind allerdings die Gemeinden betroffen.

Bei einem Gesamtbestand von 10.093 Dateien beträgt der Anteil der Dateimeldungen aus dem Kommunalbereich nunmehr 5.409 Dateien. Das dürften schätzungsweise 50% der tatsächlich bei den Kommunen vorhandenen Dateien sein, wenn man davon ausgeht, daß bei einer mittelgroßen Verwaltung in der Regel ca. 20 Dateien vorhanden sein müßten - so jedenfalls der Erfahrungswert aus Prüfungen. Eine Auswertung des Dateienregisters ergab außerdem, daß fünf Gemeinden trotz mehrfacher Erinnerungen bis heute noch keine Meldung abgegeben und 158 der 426 Gemeinden Hessens nur die automatisierten Dateien gemeldet haben. Ich habe mit dem Hessischen Minister des Innern daher vereinbart, daß er im Rahmen seiner Kommunal- und Fachaufsicht die Städte und Gemeinden nochmals auf ihre Meldepflicht zum Dateienregister hinweist.

Nach wie vor besteht bei den Gemeinden große Unklarheit über die Meldepflicht von manuellen Dateien. Es sei deshalb nochmals ausdrücklich darauf hingewiesen. Jede manuelle Kartei, bei der nicht ausgeschlossen ist, daß aus ihr personenbezogene Daten - und sei es auch nur gelegentlich, z.B. im Rahmen der Amtshilfe - übermittelt werden, ist zu melden.

Die folgende Übersicht enthält einige Beispiele typischer Dateien im kommunalen Bereich. Wie die korrekte Meldung einer Datei zum Dateienregister aussieht, demonstriert das anschließend abgedruckte Muster am Beispiel einer automatisiert geführten Datei.

Dateien im kommunalen Bereich (manuell oder automatisiert)

Bauamt	Bauantragskartei Grundstückskartei Wohnungsbindungskartei Erschließungsbeitragskartei
Bücherei	Leserkartei
Einwohnermeldeamt	Einwohnerdatenbank
Finanzabteilung	Dateien des kommunalen Finanzwesens
Gemeindekasse	Personenkonten Buchungsnachweise und Belegsammlungen
Hauptverwaltung	Mandatsträgerverzeichnis
Kindergarten	Kindergartenkartei
Ordnungsamt	Fischereischeinkartei Gewerberegister Personalausweiskartei Reisepaßkartei
Personalamt	HESPA-ANG HESPA-ARB Personalwesen - Beamte
Standesamt	Gräberkartei Personenstandsbücher Testamentskartei

MUSTER FÜR DIE MELDUNG EINER AUTOMATISIERTEN DATEI (AUTONOME LÖSUNG) ZUM DATEIENREGISTE

Formblatt zur Erfassung der vom Hessischen Datenschutzgesetz betroffenen Dateien (§ 1 Abs. 2 HDSG)

Stand vom: 1.1.1985 [x] Ersterfassung [ ] Änderung

1. **Speichernde Stelle**

1.1 Bezeichnung: Gemeindevorstand Musterstadt - Ordnungsamt -

1.2 Anschrift: Rathausstraße
6299 Musterstadt

als Behörde oder sonstige öffentliche Stelle

1.3 [ ] des Landes

1.3.1 Dienststellen-Nr.: [ ][ ][ ][ ]

1.3.2 Dienstst. Schl. Nr.: [ ]

1.4 [x] der Gemeinde / ~~des Kreises~~

1.4.1 Name: Musterstadt

1.4.2 Kennziffer: (Gemeindekennziffer)

1.5 [ ] einer sonst. jur. Person

1.5.1 Name:

1.5.2 Anschrift:

2. **Datei**

2.1 Bezeichnung: Gewerbedatei

2.2 Lfd. Nr.

2.3 [x] Verarbeitung erfolgt automatisiert [ ] nicht automatisiert

2.3.1 [ ] Landeseinheitliches Verfahren [x] regionales Verfahren

2.3.2 Name des federführenden Rechenzentrums

2.3.3 KAT Nr.:

2.3.4 KAP Nr.:

1.210
LBSt, 10. 78

3. **Betroffener Personenkreis**

Gewerbetreibende

4. **Arten der gespeicherten personenbezogenen Daten**

lfd. Nr.	Datenart	verschlüsselt ja	verschlüsselt nein
1	Firmenbezeichnung		x
2	Name, Vorname		x
3	Geburtsdatum, Geburtsort		x
4	Staatsangehörigkeit		x
5	Adresse		x
6	Sitz der Geschäftsleitung		x
7	Sitz der Betriebsstätte		x
8	Gewerbegegenstand		x
9	Datum des Beginns bzw. der Niederlegung des Betriebes		x
10	Gewerberechtliche Erlaubnisse, Handelsregistereintragung		x

5. **Aufgaben, zu deren Erfüllung die Kenntnis der Daten erforderlich ist und Rechtsgrundlage der Speicherung**

5.1 lfd. Nr. aus 4.	Aufgaben
1 - 10	Entgegennahme der Gewerbean-, Gewerbeum- und Gewerbeabmeldungen

5.2 Rechtsgrundlage der Speicherung

[x] spezielle Rechtsvorschrift §§ 14, 15 und 55 c Gewerbeordnung in der Fassung der

(Gesetz. Fundstelle) Bekanntmachung vom 1. Januar 1978, BGBl. I, Seite 97

betr. lfd. Nr. (aus 4.): 1 - 10

[ ] HDSG / betr. lfd. Nr.:

[ ] Einwilligung d. Betroffenen / betr. lfd. Nr.:

6 **Stellen, an die personenbezogene Daten regelmäßig übermittelt werden**

lfd. Nr.	Stelle
1	Hessisches Statistisches Landesamt
2	Landesverband Hessen-Mittelrhein der gewerblichen Berufsgenossenschafter
3	Finanzamt
4	Staatliches Gewerbeaufsichtsamt
5	Industrie- und Handelskammer
6	Handwerkskammer
7	Eichamt
8	Landesarbeitsamt
9	Landratsamt

7. **Arten der zu übermittelnden Daten**

lfd. Nr.	Datenart	Empfänger (lfd. Nr. aus 6.)
1	siehe 4.)	1-9
2		1-9
3		1-3,5,6,8,9
4		1,3,5,6,8,9
5		1-3,5-9
6		1-7,9
7		1-9
8		1-9
9		1-7,9
10		5,6,9

8. **Aufgaben, zu deren Erfüllung die Übermittlung erforderlich ist und Rechtsgrundlage der Übermittlung**

8.1

lfd. Nr. aus 7.	Aufgabe
1-10	Zur Erfüllung der in der Zuständigkeit dieser Behörden liegenden Aufgabe

8.2 Rechtsgrundlage der Übermittlung

[x] spezielle Rechtsvorschrift §§ 150 und 150a Gewerbeordnung in der Fassung der

(Gesetz, Fundstelle) Bekanntmachung vom 1. Januar 1978, BGBl. I, Seite 97

betr. lfd. Nr. (aus 7.): 1 - 10

[ ] HDSG / betr. lfd. Nr.: _____

[ ] Einwilligung d. Betroffenen / betr. lfd. Nr.: _____

9. Mit der automatischen Datenverarbeitung (einschließlich Erfassung) beauftragte Stelle

Werden Daten durch andere Personen oder Stellen verarbeitet?

9.1 ☐ nein ☒ Verarbeitung erfolgt mit eigener Anlage

(Erfassung siehe Ziff. 9.2.3)

9.2 ☒ ja Verarbeitungsart:

☐ Stapelverarbeitung

☐ Stapelfernverarbeitung (remote job entry)

☐ Datenfernverarbeitung im Dialogverkehr

☐ Datenfernübertragung

☒ sonstige Arten Textautomat Modell Bitsy 200

Verarbeitung erfolgt durch

9.2.1 ☐ HZD

9.2.2 ☐ KGRZ ☐ Frankfurt ☐ Gießen ☐ Kassel ☐ Starkenburg ☐ Wiesbaden

9.2.3 Service-Unternehmen (Firma, Anschrift)

Erfassung durch Fa. XY

---

10 Veröffentlichung gemäß § 17 HDSG

10.1 Fundstelle: Musterstädter Anzeiger

10.2 Datum: 1.1.1985

Erläuterungen zu diesem Formblatt s. Erl. d. HMdI v. 2. 10. 1978 (StAnz. S. 2015)

10. Novellierung des Hessischen Datenschutzgesetzes

Spätestens seit der Entscheidung des Bundesverfassungsgerichts zum Volkszählungsgesetz steht die Notwendigkeit einer Novellierung des Hessischen Datenschutzgesetzes fest. Ganz in diesem Sinne hat der Hessische Landtag in seinem Beschluß zu meinem 12. Tätigkeitsbericht die Landesregierung aufgefordert, einen Entwurf vorzulegen (Drucks. 11/1551 Nr. 7 i.V.m. Protokoll der 22. Plenarsitzung vom 5. Juli 1984, S. 1378). Die Landesregierung ist dem mit dem Entwurf vom 26. November 1985 nachgekommen (Drucks. 11/4749).

Ohne Zweifel hat sich seit der Verabschiedung des zweiten HDSG im Jahr 1978 der Akzent mehr und mehr auf bereichsspezifische Regelungen verschoben. Nur mit Hilfe solcher, an konkreten Verarbeitungsbereichen orientierten Regelungen kann in der Tat der Forderung des Bundesverfassungsgerichts nach präzisen, die Verarbeitungsvoraussetzungen genau und für den Bürger nachvollziehbar definierenden rechtlichen Regelungen entsprochen werden. Dennoch kommt dem Datenschutzgesetz nach wie vor eine zentrale Bedeutung zu. Es legt die generellen Verarbeitungsbedingungen fest und bestimmt insofern Inhalt und Tragweite des Datenschutzes.

Mit dem Entwurf greift die Landesregierung die Tradition des Landes Hessen auf. Der Hessische Landtag hatte mit dem Datenschutzgesetz von 1970 den allerersten Versuch unternommen, die Gefahren der Datenverarbeitung für den Bürger aufzufangen und damit die Akzente für die weitere in- und ausländische Diskussion gesetzt. Acht Jahre später gab sich der Landtag keineswegs damit zufrieden, das Bundesdatenschutzgesetz zu übernehmen, sondern verabschiedete ein Datenschutzgesetz, das unabhängig von der bundesgesetzlichen Regelung neue und wichtige Regelungen für zentrale Datenschutzprobleme brachte.

Ganz in dieser Tradition versucht der Entwurf die Erfahrungen der letzten Jahre zu verarbeiten und zugleich den Anforderungen des Bundesverfassungsgerichts zu entsprechen. Man kann und wird sicherlich über Einzelheiten streiten, es läßt sich aber nicht leugnen, daß es einen vergleichbaren Regelungsansatz bisher nicht gibt.

Der Entwurf enthält vor allem folgende Neuerungen:

1.
Er erweitert den Anwendungsbereich des Datenschutzgesetzes. Von der Speicherung bis zur Löschung definierte das bisherige Datenschutzgesetz eine Reihe von Phasen der Datenverarbeitung, die eine Anwendung der Datenschutzvorschriften darüber hinaus ausschlossen. Nach dem Entwurf fällt jede Verwendung gespeicherter oder zur Speicherung vorgesehener personenbezogener Daten unter den Datenschutz. Damit wird klar, daß jede Form der innerbehördlichen Verwendung personenbezogener Angaben, insbesondere aber auch die Erhebung nach den Grundsätzen des Datenschutzes vorzunehmen ist. Mit anderen Worten: Auch das Beschaffen von Daten über den Betroffenen ist nur zulässig, soweit es zur rechtmäßigen Erfüllung der in der Zuständigkeit der datenverarbeitenden Stelle liegenden Aufgaben erforderlich ist. Diese Erweiterung bildet die richtige Antwort auf das Problem, daß neue Formen der automatisierten Datenverarbeitung mit dem bisherigen Phasenmodell nicht mehr erfaßt werden können. Dies gilt namentlich für den Bildschirmtext.

Außerdem sollen in Zukunft nicht mehr nur die in Dateien gespeicherten personenbezogenen Daten, sondern generell auch die in Akten enthaltenen Angaben dem Datenschutzgesetz unterliegen. Sicher, nicht alle Regeln, die bisher für den dateiorientierten Datenschutz galten, können unverändert auch auf Akten übertragen werden. Der Entwurf sieht eine Reihe von Sondervorschriften vor. Gerade diese einschränkenden Vorschriften bedürfen der kritischen Durchsicht des Gesetzgebers. In jedem Fall nicht annehmbar ist jedoch eine geplante Sondervorschrift, die die Strafverfolgungs- und Strafvollstreckungsakten der Staatsanwaltschaften sowie die Akten der Steuerbehörden generell von den inhaltlichen Vorschriften des Datenschutzgesetzes ausnimmt.

2.
Sieht man einmal von der Einführung des verschuldensunabhängigen Schadensersatzanspruchs jedes durch einen Akt der Datenverarbeitung geschädigten Betroffenen ab, so bildet die Ausdehnung der Zweckbindung den weiteren Schwerpunkt der Novelle. Der Entwurf sieht vor, daß personenbezogene Angaben grundsätzlich nur für den Zweck verarbeitet werden dürfen, für den sie erhoben oder gespeichert worden sind. Dieser Grundsatz wird allerdings durch eine Vielzahl von Ausnahmen in Frage gestellt. Auch sie bedürfen einer besonders kritischen Überprüfung.

3.
Der automatisierte Abruf personenbezogener Daten einer Stelle durch Dritte bedarf nach einhelliger Meinung einer Neuregelung. Die Landesregierung will dem Rang dieses Problems dadurch Rechnung tragen, daß sie in jedem Fall eine besondere Rechtsvorschrift für die Einrichtung eines solchen Verfahrens vorschreibt.

4.
Es entspricht der infolge des qualitativen wie quantitativen Wachstums der automatisierten Datenverarbeitung zunehmenden Bedeutung der Datensicherung, daß die einzelnen Maßnahmen der Datensicherung aus der bisherigen Anlage zum Gesetz in das Gesetz selbst übernommen und erweitert werden.

5.
Nicht nur mittelbar über eine Verschärfung und Erweiterung der Datenschutzvorschriften, sondern auch direkt über die Erweiterung des Auskunftsrechts auch auf in Akten gespeicherte Daten und die Einführung einer Reihe von Benachrichtigungspflichten erhält der Bürger begrüßenswerte zusätzliche Rechte. Die Landesregierung hofft, auf diese Weise die Transparenz der Datenverarbeitung zu verstärken und die Stellung des Bürgers in der Datenverarbeitung zu verbessern.

6.
Sondervorschriften für die Datenverarbeitung zu Planungszwecken, wissenschaftlichen Zwecken, bei Dienst- und Arbeitsverhältnissen sowie im Zusammenhang mit automatisiertem Fernmessen und Fernwirken sind für das Datenschutzgesetz neu. Sie streben die Lösung bestimmter Zielkonflikte an, die sich in der Praxis der Datenverarbeitung als lösungsbedürftig erwiesen haben und für die besondere bereichsspezifische Regelungen nach dem derzeitigen Stand der Entwicklung nicht erwartet werden können.

7.
Die Stellung des Hessischen Datenschutzbeauftragten wird durch die Novelle nicht wesentlich verändert. In einer Reihe von Punkten kann er jedoch nach dem Entwurf mit einer Stärkung seiner Befugnisse rechnen. So soll er in Zukunft die Datenverarbeitung öffentlich-rechtlicher Unternehmen, die am Wettbewerb teilnehmen, kontrollieren können. Damit wird ihm zum ersten Mal die Gelegenheit gegeben, für den Bürger in den überaus automatisierungsfreudigen Bereichen vor allem der öffentlich-rechtlichen Kreditinstitute auf die Einhaltung des Datenschutzes hinzuwirken. Darüber hinaus verpflichtet der Entwurf alle öffentlichen Stellen, den Datenschutzbeauftragten über Verfahrensentwicklungen und Gesetzesvorhaben im Zusammenhang mit der automatisierten Verarbeitung personenbezogener Daten zu unterrichten. Diese Verpflichtung galt bislang nur aufgrund eines Erlasses der Landesregierung und beschränkt auf ihren Bereich.

8.
Außer den erwähnten Punkten gibt es noch eine Reihe von Detailfragen, die gleichfalls bei der weiteren Diskussion bedacht werden müssen. Um das Verfahren zu erleichtern, sind nachfolgend meine Korrektur-, Ergänzungs- und Gegenvorschläge, die ich dem Innenminister in meiner Stellungnahme vom 4. Juni 1985 zu dem von ihm erarbeiteten Vorentwurf vom 5. Februar 1985 gemacht habe, dem Gesetzentwurf der Landesregierung vom 26. November 1985 synoptisch gegenübergestellt. Der Gesetzentwurf der Landesregierung hat einige meiner Anregungen übernommen; die Abweichungen meiner Vorschläge vom Gesetzentwurf sind durch Unterstreichungen gekennzeichnet.

Gesetzentwurf der Landesregierung für ein
Hessisches Datenschutzgesetz (HDSG)
vom 26. November 1985
(Drucks. 11/4749)

Inhaltsübersicht

Änderungsvorschläge des
Hessischen Datenschutzbeauftragten
zum Referentenentwurf
vom 05. Februar 1985

§ 1
Aufgabe

Aufgabe des Gesetzes ist es,

1. das Recht des einzelnen zu schützen, selbst über die Preisgabe und Verwendung seiner Daten zu bestimmen, soweit keine Ausnahmen in diesem Gesetz oder in anderen Rechtsvorschriften zugelassen sind.

2. das auf dem Grundsatz der Gewaltenteilung beruhende verfassungsmäßige Gefüge des Staates, insbesondere der Verfassungsorgane des Landes und der Organe der kommunalen Selbstverwaltung untereinander und zueinander, vor einer Gefährdung infolge der automatisierten Datenverarbeitung zu bewahren.

§ 2
Begriffsbestimmungen

(1) Personenbezogene Daten sind Einzelangaben über persönliche und sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener).

(2) Datenverarbeitung ist jede Verwendung gespeicherter oder zur Speicherung vorgesehener personenbezogener Daten, insbesondere das Erheben, Speichern, Übermitteln, Sperren und Löschen. Im einzelnen ist

1. Erheben das Beschaffen von Daten über den Betroffenen,

2. Speichern das Erfassen, Aufnehmen oder Aufbewahren von Daten auf einem Datenträger zum Zwecke ihrer weiteren Verarbeitung,

3. Übermitteln das Bekanntgeben gespeicherter oder durch Datenverarbeitung gewonnener Daten an einen Dritten in der Weise, daß die Daten durch die datenverarbeitende Stelle an den Dritten weitergegeben werden oder daß der Dritte zum Abruf bereitgehaltene Daten abruft,

4. Sperren das Verhindern weiterer Verarbeitung gespeicherter Daten,

5. Löschen das Unkenntlichmachen gespeicherter Daten

ungeachtet der dabei angewendeten Verfahren.

(3) Datenverarbeitende Stelle ist jede der in § 3 Abs. 1 genannten Stellen, die Daten für sich selbst verarbeitet oder durch andere verarbeiten läßt.

(4) Dritter ist jede Person oder Stelle außerhalb der datenverarbeitenden Stelle, ausgenommen der Betroffene oder diejenigen Personen und Stellen, die in den Fällen des Abs. 3 im Geltungsbereich des Grundgesetzes im Auftrag tätig werden.

§ 1
Aufgabe

Aufgabe des Gesetzes ist es, die Verarbeitung personenbezogener Daten durch öffentliche Stellen zu regeln, um

- das Recht des einzelnen auf informationelle Selbstbestimmung zu schützen,

- das auf dem Grundsatz der Gewaltenteilung beruhende verfassungsmäßige Gefüge des Staates, insbesondere der Verfassungsorgane des Landes und der Organe der kommunalen Selbstverwaltung untereinander und zueinander, vor einer Gefährdung durch die automatisierte Datenverarbeitung zu bewahren.

§ 2
Begriffsbestimmungen

(1) Personenbezogene Daten sind Einzelangaben über persönliche und sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener).

(2) Datenverarbeitung ist jeder Gebrauch personenbezogener Daten, insbesondere das Erheben, Speichern, Übermitteln, Sperren und Löschen. Im einzelnen ist

1. Erheben das Beschaffen von Daten über den Betroffenen,

2. Speichern das Erfassen, Aufnehmen oder Aufbewahren von Daten auf einem Datenträger zum Zwecke ihrer weiteren Verwendung,

3. Übermitteln das Bekanntgeben gespeicherter oder durch Datenverarbeitung gewonnener Daten an einen Dritten in der Weise, daß die Daten durch die datenverarbeitende Stelle an den Dritten weitergegeben werden oder daß der Dritte zum Abruf bereitgehaltene Daten abruft,

4. Sperren das Verhindern weiterer Verarbeitung gespeicherter Daten,

5. Löschen das Unkenntlichmachen gespeicherter Daten

ungeachtet der dabei angewendeten Verfahren.

(3) Datenverarbeitende Stelle ist jede der in § 3 Abs. 1 genannten Stellen, die Daten für sich selbst verarbeitet oder durch andere verarbeiten läßt.

(4) Dritter ist jede Person oder Stelle außerhalb der datenverarbeitenden Stelle, ausgenommen der Betroffene oder diejenigen Personen und Stellen, die in den Fällen des Absatz 3 im Geltungsbereich des Grundgesetzes im Auftrag tätig werden.

(5) Eine Datei ist

1. eine Sammlung von Daten, die durch automatisierte Verfahren ausgewertet werden kann (automatisierte Datei), oder

2. eine gleichartig aufgebaute Sammlung von Daten, die nach bestimmten Merkmalen geordnet und ausgewertet werden kann, (nicht automatisierte Datei).

(6) Eine Akte ist jede amtlichen Zwecken dienende Unterlage.

§ 3
Anwendungsbereich

(1) Dieses Gesetz gilt für Behörden und sonstige öffentliche Stellen des Landes, der Gemeinden und Landkreise sowie der sonstigen der Aufsicht des Landes unterstehenden juristischen Personen des öffentlichen Rechts und für deren Vereinigungen.

(2) Die Vorschriften dieses Gesetzes gehen denen des Hessischen Verwaltungsverfahrensgesetzes vor, soweit bei der Ermittlung des Sachverhalts personenbezogene Daten verarbeitet werden.

(3) Soweit besondere Rechtsvorschriften für die Verarbeitung personenbezogener Daten vorhanden sind, gehen sie den Vorschriften dieses Gesetzes vor.

(4) Die Vorschriften des Ersten Teils finden insbesondere auf Akten der Gerichte im Rahmen gerichtlicher Verfahren, auf Akten der Staatsanwaltschaften im Rahmen der Strafverfolgung und der Strafvollstreckung sowie auf Akten der Steuerbehörden nach der Abgabenordnung keine Anwendung.

(5) Dieses Gesetz gilt nicht für Gnadenverfahren.

(6) Dieses Gesetz gilt nicht für personenbezogene Daten, solange sie in allgemein zugänglichen Quellen gespeichert sind sowie für Daten des Betroffenen, die von ihm zur Veröffentlichung bestimmt sind.

(7) Soweit der Hessische Rundfunk personenbezogene Daten ausschließlich zu eigenen publizistischen Zwecken verarbeitet, gelten von den Vorschriften dieses Gesetzes nur die §§ 10 und 37. Im übrigen gilt anstelle des Zweiten Teils § 37 dieses Gesetzes.

(8) Soweit öffentlich-rechtliche Unternehmen am Wettbewerb teilnehmen, gelten für sie nur der Zweite Teil sowie die §§ 34 und 36 dieses Gesetzes. Mit Ausnahme der Vorschriften über die Aufsichtsbehörde sind im übrigen die für nicht-öffentliche Stellen geltenden Vorschriften des Bundesdatenschutzgesetzes einschließlich der Straf- und Bußgeldvorschriften anwendbar.

(5) Eine Datei ist

a) eine Sammlung von Daten, die durch automatisierte Verfahren ausgewertet werden kann, oder

b) eine gleichartig aufgebaute Sammlung von Daten, die nach bestimmten Merkmalen geordnet und ausgewertet werden kann, ungeachtet der dabei angewendeten Verfahren.

§ 3
Anwendungsbereich

(1) Dieses Gesetz gilt für Behörden und sonstige öffentliche Stellen des Landes, der Gemeinden und Gemeindeverbände und der sonstigen Aufsicht des Landes unterstehenden juristischen Personen des öffentlichen Rechts und für deren Vereinigungen.

(2) Soweit der Datenschutz in besonderen Rechtsvorschriften geregelt ist, gehen sie den Vorschriften dieses Gesetzes vor. Die Kontrollbefugnisse des Hessischen Datenschutzbeauftragten bleiben unberührt.

(3) Soweit der Hessische Rundfunk personenbezogene Daten ausschließlich zu eigenen publizistischen Zwecken verarbeitet, gilt von den Vorschriften dieses Gesetzes nur § 10 Abs. 1 und 2.

§ 4
Verarbeitung personenbezogener Daten im Auftrag

(1) Die datenverarbeitende Stelle bleibt für die Einhaltung der Vorschriften dieses Gesetzes und anderer Vorschriften über den Datenschutz verantwortlich, auch wenn personenbezogene Daten in ihrem Auftrag durch andere Personen oder Stellen verarbeitet werden. Der Auftragnehmer darf personenbezogene Daten nur im Rahmen der Weisungen des Auftraggebers verarbeiten. Ist der Auftragnehmer der Ansicht, daß eine Weisung des Auftraggebers gegen dieses Gesetz oder andere Vorschriften über den Datenschutz verstößt, hat er den Auftraggeber unverzüglich darauf hinzuweisen. Der Auftraggeber hat darauf zu achten, daß beim Auftragnehmer die nach § 10 erforderlichen Maßnahmen getroffen sind.

(2) Sofern die Vorschriften dieses Gesetzes auf den Auftragnehmer keine Anwendung finden, ist der Auftraggeber verpflichtet, vertraglich sicherzustellen, daß der Auftragnehmer die Bestimmungen dieses Gesetzes befolgt und sich der Kontrolle des Hessischen Datenschutzbeauftragten unterwirft. Der Auftraggeber hat den Hessischen Datenschutzbeauftragten über die Beauftragung zu unterrichten.

(3) Juristische Personen, Gesellschaften und andere Personenvereinigungen des privaten Rechts, bei denen dem Land oder einer der Aufsicht des Landes unterstehenden Körperschaft, Anstalt oder Stiftung des öffentlichen Rechts die Mehrheit der Anteile gehört oder die Mehrheit der Stimmen zusteht, unterstehen der Kontrolle des Hessischen Datenschutzbeauftragten, soweit diese Personen oder Personenvereinigungen für die in § 3 Abs. 1 genannten Stellen im Auftrag tätig werden.

§ 4
Verarbeitung personenbezogener Daten im Auftrag

(1) Die in § 3 Abs. 1 genannten Stellen bleiben als datenverarbeitende Stellen im Sinne von § 2 Abs. 3 Nr. 1 für die Einhaltung der Vorschriften dieses Gesetzes und anderer Vorschriften über den Datenschutz verantwortlich, wenn personenbezogene Daten in ihrem Auftrag durch andere Personen oder Stellen bearbeitet werden. Der Auftragnehmer darf personenbezogene Daten nur im Rahmen der Weisungen des Auftraggebers verarbeiten. Ist der Auftragnehmer der Ansicht, daß eine Weisung des Auftraggebers gegen dieses Gesetz oder andere Vorschriften über den Datenschutz verstößt, hat er den Auftraggeber unverzüglich darauf hinzuweisen. Der Auftraggeber hat bei der Auswahl des Auftragnehmers darauf zu achten und später zu überprüfen, ob die nach § 10 Abs. 1 erforderlichen Maßnahmen getroffen sind.

(2) Sofern die Vorschriften dieses Gesetzes auf den Auftragnehmer keine Anwendung finden, ist der Auftraggeber verpflichtet, vertraglich sicherzustellen, daß der Auftragnehmer die Bestimmungen dieses Gesetzes und anderer Rechtsvorschriften über den Datenschutz beachtet und sich der Kontrolle des Hessischen Datenschutzbeauftragten unterwirft.

(3) Juristische Personen, Gesellschaften und andere Personenvereinigungen des privaten Rechts, bei denen dem Land oder einer der Aufsicht des Landes unterstehenden Körperschaft, Anstalt oder Stiftung des öffentlichen Rechts die Mehrheit der Anteile gehört oder die Mehrheit der Stimmen zusteht, unterstehen der Kontrolle des Hessischen Datenschutzbeauftragten, soweit diese Personen oder Personenvereinigungen für die in § 3 Abs. 1 genannten Stellen im Auftrag tätig werden.

§ 5
Durchführung des Datenschutzes

(1) Die obersten Landesbehörden, Gemeinden und Landkreise sowie die sonstigen der Aufsicht des Landes unterstehenden juristischen Personen des öffentlichen Rechts haben jeweils für ihren Bereich die Ausführung dieses Gesetzes sowie anderer Vorschriften über den Datenschutz sicherzustellen.

(2) Die datenverarbeitende Stelle hat einen behördlichen Beauftragten für den Datenschutz zu bestellen, der nicht gleichzeitig für die Entscheidung über die Einführung, Anwendung, Änderung oder Erweiterung der automatisierten Verarbeitung personenbezogener Daten zuständig sein darf. Dieser hat insbesondere bei der Erfüllung der sich aus §§ 6, 26 Abs. 1 und 29 ergebenden Aufgaben sowie bei der Überwachung der nach § 10 erforderlichen Datensicherungsmaßnahmen mitzuwirken.

§ 6
Dateibeschreibung

(1) Die speichernde Stelle ist verpflichtet, in einer Beschreibung jeder Datei festzulegen:

1. die Zweckbestimmung der Datei,
2. die Art der gespeicherten Daten sowie die Rechtsgrundlage ihrer Verarbeitung,
3. den Kreis der Betroffenen,
4. die Art regelmäßig übermittelter Daten, deren Empfänger sowie die Herkunft regelmäßig empfangener Daten,
5. Fristen für die Sperrung und Löschung der Daten,
6. die technischen und organisatorischen Maßnahmen nach § 10,
7. bei automatisierten Verfahren die Betriebsart des Verfahrens, die Art der Geräte sowie das Verfahren zur Übermittlung, Sperrung, Löschung und Auskunftserteilung.

(2) Abs. 1 findet keine Anwendung auf nicht automatisierte Dateien, aus denen keine Daten an Dritte übermittelt werden.

§ 5
Durchführung des Datenschutzes

(1) Die obersten Landesbehörden, Gemeinden und Gemeindeverbände sowie die sonstigen der Aufsicht des Landes unterstehenden juristischen Personen des öffentlichen Rechts haben jeweils für ihren Bereich die Ausführung dieses Gesetzes sowie anderer Rechtsvorschriften über den Datenschutz sicherzustellen.

(2) Um die Einhaltung dieses Gesetzes sowie anderer Vorschriften über den Datenschutz sicherzustellen, hat die datenverarbeitende Stelle einen Beauftragten für den Datenschutz zu bestellen. Zum Beauftragten für den Datenschutz darf nur bestellt werden, wer dadurch keinem Interessenkonflikt mit sonstigen dienstlichen Aufgaben ausgesetzt wird und die zur Erfüllung seiner Aufgabe erforderliche Fachkunde und Zuverlässigkeit besitzt.

§ 6
Dateibeschreibung

Die speichernde Stelle ist verpflichtet, jede Datei zu beschreiben. Sie hat dabei insbesondere festzulegen:

1. die Zweckbestimmung der Datei
2. die Art der gespeicherten Daten sowie die Rechtsgrundlage ihrer Verarbeitung,
3. den Kreis der Betroffenen
4. die Art regelmäßig übermittelter Daten, deren Empfänger sowie die Herkunft regelmäßig empfangener Daten,
5. Fristen für die Sperrung und Löschung der Daten,
6. die technischen und organisatorischen Maßnahmen nach § 10,
7. bei automatisierten Verfahren die Betriebsform des Verfahrens, die Art der Geräte sowie das Verfahren zur Übermittlung, Sperrung, Löschung und Auskunfterteilung.

§ 7
Zulässigkeit der Datenverarbeitung

Die Verarbeitung personenbezogener Daten ist nur zulässig, wenn

1. dieses Gesetz oder eine andere Rechtsvorschrift sie erlaubt oder zwingend voraussetzt oder

2. der Betroffene eingewilligt hat.
   Die Einwilligung bedarf der Schriftform, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist; wird die Einwilligung zusammen mit anderen Erklärungen schriftlich erteilt, ist der Betroffene hierauf schriftlich besonders hinzuweisen.

   Der Betroffene ist in geeigneter Weise über die Bedeutung der Einwilligung, insbesondere über den Verwendungszweck der Daten aufzuklären. Die Aufklärungspflicht umfaßt bei beabsichtigten Übermittlungen auch den Empfänger der Daten.

   Der Betroffene ist unter Darlegung der Rechtsfolgen darauf hinzuweisen, daß er die Einwilligung verweigern kann.

§ 8
Rechte des Betroffenen

(1) Jeder hat nach Maßgabe dieses Gesetzes ein Recht auf

1. Auskunft und Benachrichtigung über die zu seiner Person gespeicherten Daten (§ 18),

2. Berichtigung, Sperrung oder Löschung der zu seiner Person gespeicherten Daten (§ 19),

3. Schadensersatz (§ 20),

4. Anrufung des Datenschutzbeauftragten (§ 28 und § 37 Abs. 5),

5. Einsicht in das beim Hessischen Datenschutzbeauftragten geführte Register (§ 26 Abs. 1).

§ 7
Zulässigkeit der Datenverarbeitung

(1) Die Verarbeitung personenbezogener Daten ist zulässig, wenn dieses Gesetz oder eine andere Rechtsvorschrift sie erlaubt.

(2) Die Verarbeitung personenbezogener Daten ist auch zulässig, wenn der Betroffene einwilligt und dadurch abschließend durch Rechtsnorm zugewiesene Aufgaben und Befugnisse zur Verarbeitung personenbezogener Daten nicht erweitert werden.

(3) Die Einwilligung bedarf der Schriftform, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist. Wird die Einwilligung zusammen mit anderen Erklärungen schriftlich erteilt, ist der Betroffene hierauf schriftlich besonders hinzuweisen. Der Betroffene ist in geeigneter Weise über die Bedeutung der Einwilligung, insbesondere über den Verwendungszweck der Daten, bei beabsichtigten Übermittlungen auch über die Empfänger der Daten aufzuklären; er ist unter Darlegung der Rechtsfolgen darauf hinzuweisen, daß er die Einwilligung verweigern kann.

§ 8
Rechte des Betroffenen

Jeder hat nach Maßgabe dieses Gesetzes ein Recht auf

1. Benachrichtigung und Auskunft über die zu seiner Person gespeicherten Daten (§ 17),

2. Berichtigung, Sperrung oder Löschung der zu seiner Person gespeicherten Daten (§ 18),

3. Folgenbeseitigung und Schadensersatz (§ 19),

4. Anrufung des Hessischen Datenschutzbeauftragten (§ 27),

5. Einsicht in das nach § 25 Abs. 1 geführte Register.

§ 9
Datengeheimnis

Den bei der datenverarbeitenden Stelle oder in deren Auftrag beschäftigten Personen, die Zugang zu personenbezogenen Daten haben, ist eine Verarbeitung dieser Daten zu einem anderen als dem zur jeweiligen rechtmäßigen Aufgabenerfüllung gehörenden Zweck während und nach Beendigung ihrer Tätigkeit untersagt.

§ 10
Technische und organisatorische Maßnahmen

(1) Die datenverarbeitende oder in ihrem Auftrag tätige Stelle hat die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften dieses Gesetzes zu gewährleisten. Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.

(2) Werden personenbezogene Daten in nicht automatisierten Dateien oder Akten verarbeitet, dann sind insbesondere Maßnahmen zu treffen, um den Zugriff Unbefugter bei der Bearbeitung, der Aufbewahrung, dem Transport und der Vernichtung zu verhindern.

(3) Werden personenbezogene Daten automatisiert verarbeitet, sind Maßnahmen zu treffen, die je nach der Art der zu schützenden personenbezogenen Daten geeignet sind,

1. Unbefugten den Zugang zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet werden, zu verwehren (Zugangskontrolle),

2. zu verhindern, daß Datenträger unbefugt gelesen, kopiert, verändert oder entfernt werden können (Datenträgerkontrolle),

3. die unbefugte Eingabe in den Speicher sowie die unbefugte Kenntnisnahme, Veränderung oder Löschung gespeicherter personenbezogener Daten zu verhindern (Speicherkontrolle),

4. die Benutzung von Datenverarbeitungssystemen mit Hilfe von Einrichtungen zur Datenübertragung durch Unbefugte zu verhindern (Benutzerkontrolle),

§ 9
Datengeheimnis

(1) Den bei öffentlichen Stellen oder in deren Auftrag tätigen Personen, die Zugang zu personenbezogenen Daten haben, ist eine Verarbeitung der Daten zu einem anderen als dem zur jeweiligen rechtmäßigen Aufgabenerfüllung gehörenden Zweck untersagt.

(2) Diese Personen sind bei der Aufnahme ihrer Tätigkeit über ihre Pflicht nach Abs. 1 sowie die sonstigen bei ihrer Tätigkeit zu beachtenden Vorschriften des Datenschutzes zu unterrichten und auf deren Einhaltung zu verpflichten. Ihre Pflichten bestehen auch nach Beendigung ihrer Tätigkeit fort.

§ 10
Technische und organisatorische Maßnahmen

(1) Wer im Rahmen des § 3 Abs. 1 oder im Auftrag der dort genannten Stellen personenbezogene Daten verarbeitet, hat die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften dieses Gesetzes zu gewährleisten.

(2) Je nach Art der zu schützenden personenbezogenen Daten und des verwendeten Verfahrens sind insbesondere Maßnahmen zu treffen, die geeignet sind,

1. Unbefugten den Zugang zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet werden, zu verwehren (Zugangskontrolle),

2. zu verhindern, daß Datenträger unbefugt gelesen, kopiert, verändert oder entfernt werden können (Datenträgerkontrolle),

3. die unbefugte Eingabe in den Speicher sowie die unbefugte Kenntnisnahme, Veränderung oder Löschung gespeicherter personenbezogener Daten zu verhindern (Speicherkontrolle),

4. zu verhindern, daß Datenverarbeitungssysteme mit Hilfe von Einrichtungen zur Datenübertragung von Unbefugten benutzt werden können (Benutzerkontrolle),

5. zu gewährleisten, daß die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden personenbezogenen Daten zugreifen können (Zugriffskontrolle),

6. zu gewährleisten, daß nachträglich überprüft und festgestellt werden kann, an welche Stellen personenbezogene Daten durch Einrichtungen zur Datenübertragung übermittelt werden können (Übermittlungskontrolle),

7. zu gewährleisten, daß nachträglich überprüft und festgestellt werden kann, welche personenbezogenen Daten zu welcher Zeit von wem in Datenverarbeitungssysteme eingegeben worden sind (Eingabekontrolle),

8. zu gewährleisten, daß personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (Auftragskontrolle),

9. zu gewährleisten, daß bei der Übermittlung personenbezogener Daten sowie beim Transport von Datenträgern diese nicht unbefugt gelesen, kopiert, verändert oder gelöscht werden können (Transportkontrolle),

10. die innerbehördliche oder innerbetriebliche Organisation so zu gestalten, daß sie den besonderen Anforderungen des Datenschutzes gerecht wird (Organisationskontrolle).

5. zu gewährleisten, daß die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden personenbezogenen Daten zugreifen können (Zugriffskontrolle),

6. zu gewährleisten, daß nachträglich überprüft und festgestellt werden kann, an wen wann welche personenbezogenen Daten durch Einrichtungen zur Datenübertragung übermittelt worden sind (Übermittlungskontrolle),

7. zu gewährleisten, daß nachträglich überprüft und festgestellt werden kann, welche personenbezogenen Daten zu welcher Zeit von wem in Datenverarbeitungssysteme eingegeben worden sind (Eingabekontrolle).

8. zu gewährleisten, daß personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (Auftragskontrolle),

9. zu verhindern, daß bei der Übertragung personenbezogener Daten sowie beim Transport von Datenträgern diese unbefugt gelesen, kopiert, verändert oder gelöscht werden können (Transportkontrolle),

10. die innerbehördliche oder innerbetriebliche Organisation so zu gestalten, daß sie den besonderen Anforderungen des Datenschutzes gerecht wird (Organisationskontrolle).

(3) Die Landesregierung wird ermächtigt, durch Rechtsverordnung die in Abs. 1 Satz 2 genannten Anforderungen nach dem jeweiligen Stand der Technik und Organisation fortzuschreiben.

Zweiter Abschnitt
Rechtsgrundlage der Datenverarbeitung

§ 11
Erforderlichkeit

(1) Die Verarbeitung personenbezogener Daten ist nach Maßgabe der nachfolgenden Vorschriften zulässig, wenn sie zur rechtmäßigen Erfüllung der in der Zuständigkeit der datenverarbeitenden Stelle liegenden Aufgaben erforderlich ist.

(2) Sind personenbezogene Daten in Akten derart verbunden, daß ihre Trennung nach erforderlichen und nicht erforderlichen Daten nicht oder nur mit unverhältmäßig großem Aufwand möglich ist, dann sind die Kenntnisnahme, die Weitergabe innerhalb der datenverarbeitenden Stelle und die Übermittlung der Daten, die nicht zur Erfüllung der jeweiligen Aufgabe erforderlich sind, über Abs. 1 hinaus zulässig. Diese Daten unterliegen insoweit einem Verwertungsverbot.

§ 11
Allgemeine Zulässigkeit

Die Verarbeitung personenbezogener Daten ist zulässig, wenn sie zur rechtmäßigen Erfüllung der durch Rechtsnorm der datenverarbeitenden Stelle zugewiesenen Aufgaben und für den jeweils damit verbundenen Zweck erforderlich ist.

§ 12
Erheben

(1) Personenbezogene Daten sind grundsätzlich bei dem Betroffenen mit seiner Kenntnis zu erheben. Dies gilt nicht, wenn

1. eine Rechtsvorschrift es erlaubt oder zwingend voraussetzt oder der Betroffene eingewilligt hat,

2. die Bearbeitung eines vom Betroffenen gestellten Antrags ohne Kenntnis der Daten nicht möglich ist oder Angaben des Betroffenen überprüft werden müssen. Der Betroffene ist darauf hinzuweisen, bei welchen Personen oder Stellen seine Daten erhoben werden können,

3. die Abwehr erheblicher Nachteile für das Allgemeinwohl oder Gefahren für Leben, Gesundheit, persönliche Freiheit oder ähnlich schutzwürdige Belange einzelner dies gebietet,

4. Die Verfolgung von Straftaten oder Ordnungswidrigkeiten, die Strafvollstreckung, der Vollzug einer gerichtlich angeordneten Freiheitsentziehung sowie die Bewährungsaufsicht oder die Erledigung eines gerichtlichen Auskunftsersuchens es erfordert,

5. die Erhebung beim Betroffenen einen unverhältnismäßigen Aufwand erfordern würde und keine Anhaltspunkte dafür bestehen, daß schutzwürdige Belange des Betroffenen beeinträchtigt werden können.

(2) Werden die Daten beim Betroffenen erhoben, dann ist er in geeigneter Weise über den Zweck der Datenerhebung aufzuklären. Die Aufklärungspflicht umfaßt bei beabsichtigten Übermittlungen auch den Empfänger der Daten.
Werden die Daten bei dem Betroffenen aufgrund einer durch Rechtsvorschrift festgelegten Auskunftspflicht erhoben, dann ist er auf die Rechtsgrundlage hinzuweisen. Bei freiwilligen Angaben ist er unter Darlegung der Rechtsfolgen darauf hinzuweisen, daß er die Angaben verweigern kann.

§ 12
Erheben

(1) Personenbezogene Daten sind grundsätzlich beim Betroffenen zu erheben. Ohne seine Mitwirkung dürfen sie nur erhoben werden, wenn

1. eine Rechtsvorschrift dies vorsieht,

2. die Erhebung beim Betroffenen einen unverhältnismäßigen Aufwand erfordern würde und keine Anhaltspunkte dafür bestehen, daß schutzwürdige Belange des Betroffenen beeinträchtigt werden können.

(2) Werden Daten beim Betroffenen auf Grund einer durch Rechtsvorschrift festgelegten Auskunftspflicht erhoben, dann ist er unter Hinweis auf die Rechtsgrundlage über den Verwendungszweck aufzuklären. Werden vom Betroffenen freiwillige Angaben erbeten, so ist er unter Darlegung des Verwendungszwecks auf die Freiwilligkeit seiner Angaben hinzuweisen. Die Aufklärungspflicht umfaßt auch die regelmäßigen Datenempfänger. Dem Betroffenen dürfen aus einer Verweigerung seiner Einwilligung keine Rechtsnachteile entstehen.

(3) Werden beim Betroffenen Angaben erhoben, die für die Gewährung einer Leistung erforderlich sind, so ist er über die möglichen Folgen einer Nichtbeantwortung aufzuklären.

§ 13
Zweckbindung

(1) Personenbezogene Daten dürfen grundsätzlich nur für den Zweck weiterverarbeitet werden, für den sie erhoben oder gespeichert worden sind.

(2) Sollen personenbezogene Daten zu Zwecken verarbeitet werden, für die sie nicht erhoben oder gespeichert worden sind, dann ist dies nur aus den in § 12 Abs. 1 Satz 2 genannten Gründen zulässig. Besondere Amts- oder Berufsgeheimnisse bleiben unberührt.

(3) Sind personenbezogene Daten in Akten derart verbunden, daß ihre Trennung nach verschiedenen Zwecken nicht oder nur mit unvertretbar großem Aufwand möglich ist, so tritt an die Stelle der Trennung ein Verwertungsverbot nach Maßgabe von Abs. 2 für die Daten, die nicht mit Zweck der jeweiligen Verarbeitung dienen.

(4) Personenbezogene Daten, die für andere Zwecke erhoben worden sind, dürfen auch zur Ausübung von Aufsichts- und Kontrollbefugnissen sowie zu Ausbildungs- und Prüfungszwecken in dem dafür erforderlichen Umfang verwendet werden.

§ 14
Übermittlung innerhalb des öffentlichen Bereichs
(vgl. § 13 Entwurf des Hessischen Datenschutzbeauftragten)

(1) Die Übermittlung ist über § 11 hinaus zulässig, wenn sie zur rechtmäßigen Erfüllung von Aufgaben des Empfängers erforderlich ist.

(2) Die Verantwortung für die Zulässigkeit der Übermittlung trägt die übermittelnde Stelle. Ist die Übermittlung zur Erfüllung von Aufgaben des Empfängers erforderlich, so trägt dieser hierfür die Verantwortung und hat sicherzustellen, daß die Erforderlichkeit nachträglich überprüft werden kann. Die übermittelnde Stelle hat in diesem Fall lediglich die Zuständigkeit des Empfängers und im übrigen die Erforderlichkeit der Übermittlung nur dann zu prüfen, wenn im Einzelfall hierzu Anlaß besteht. Der Empfänger hat der übermittelnden Stelle die für ihre Prüfung erforderlichen Angaben zu machen.

§ 13
Weitere Verarbeitung

(1) Personenbezogene Daten dürfen grundsätzlich nur für den Zweck genutzt, übermittelt oder sonst gebraucht werden, für den sie erhoben oder gespeichert worden sind.

(2) Sollen personenbezogene Daten zu Zwecken verarbeitet werden, für die sie nicht erhoben oder gespeichert worden sind, ist dies nur aufgrund einer gesetzlichen Regelung zulässig.

(3) Sind personenbezogene Daten in Akten derart verbunden, daß ihre Trennung nach verschiedenen Zwecken nicht oder nur mit unvertretbar großem Aufwand möglich ist, so tritt an die Stelle der Trennung ein Verwertungsverbot für die Daten, die nicht dem Zweck der jeweiligen Verarbeitung dienen.

(4) Personenbezogene Daten, die für andere Zwecke erhoben worden sind, dürfen auch zur Ausübung von Aufsichts- und Prüfungsbefugnissen in dem dafür erforderlichen Umfang verwendet werden.

§ 14
Automatisiertes Abrufverfahren
(vgl. § 15 Regierungsentwurf)

(1) Ein automatisiertes Verfahren zum Abruf personenbezogener Daten durch Dritte darf nur eingerichtet werden, wenn das Recht der Betroffenen auf informationelle Selbstbestimmung gewahrt und das Bereithalten der Daten zum sofortigen Abruf durch den Empfänger angemessen ist. Die Einrichtung setzt eine Rechtsvorschrift unter Festlegung des Datenempfängers, der Datenart und des Zwecks des Abrufs voraus. Sie hat zu gewährleisten, daß die Erforderlichkeit des einzelnen Abrufs überprüft werden kann. Außerdem hat sie verhältnismäßige Maßnahmen zur Datensicherung und zur Kontrolle vorzusehen.

(2) Die Landesregierung wird ermächtigt, die Einrichtung automatisierter Abrufverfahren durch Rechtsverordnung zu regeln. Der Hessische Datenschutzbeauftragte ist vor der Entscheidung anzuhören.

(3) Die Einrichtung automatisierter Verfahren zum Abruf personenbezogener Daten, die einem Berufs- oder besonderen Amtsgeheimnis unterliegen, bedarf eines Gesetzes.

§ 15
Automatisiertes Abrufverfahren
(vgl. § 14 Entwurf des Hessischen Datenschutzbeauftragten)

(1) Ein automatisiertes Verfahren zum Abruf personenbezogener Daten durch Dritte darf nur eingerichtet werden, wenn eine Rechtsvorschrift dies zuläßt.

(2) Die Landesregierung wird ermächtigt, die Einrichtung automatisierter Abrufverfahren durch Rechtsverordnung einzuführen, wenn dies unter Berücksichtigung der schutzwürdigen Belange der Betroffenen und der Aufgabe der beteiligten Stellen angemessen ist. Der Hessische Datenschutzbeauftragte ist vorher zu hören. Die Verordnung hat den Datenempfänger, die Datenart und den Zweck des Abrufs festzulegen. Sie hat Maßnahmen zur Datensicherung und zur Kontrolle vorzusehen, die in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck stehen.

§ 16
Datenübermittlung an Personen oder Stellen außerhalb des öffentlichen Bereichs
(vgl. § 15 Entwurf des Hessischen Datenschutzbeauftragten)

(1) Die Übermittlung personenbezogener Daten an Personen und Stellen außerhalb des öffentlichen Bereichs ist über §§ 11 und 13 hinaus zulässig, wenn der Empfänger ein berechtigtes Interesse an der Kenntnis der zu übermittelnden Daten glaubhaft macht und keine Anhaltspunkte dafür bestehen, daß schutzwürdige Belange des Betroffenen beeinträchtigt werden können.

(2) Der Empfänger darf die übermittelten Daten nur zu dem Zweck verwenden, zu dessen Erfüllung sie ihm übermittelt wurden.

§ 15
Datenübermittlung an Stellen außerhalb des öffentlichen Bereichs sowie an öffentlich-rechtliche Religionsgesellschaften
(vgl. §§ 16, 35 Regierungsentwurf)

(1) Die Übermittlung personenbezogener Daten an Personen und Stellen außerhalb des öffentlichen Bereichs sowie an öffentlich-rechtliche Religionsgesellschaften ist über § 11 und § 13 hinaus zulässig, wenn der Empfänger ein rechtliches Interesse an der Kenntnis der zu übermittelnden Daten glaubhaft macht und keine Anhaltspunkte dafür bestehen, daß schutzwürdige Belange des Betroffenen beeinträchtigt werden. Jede weitere Übermittlung bedarf der Einwilligung des Betroffenen.

(2) Der Empfänger darf die übermittelten Daten nur zu dem Zweck verwenden, zu dessen Erfüllung sie ihm übermittelt wurden.

§ 16
Datenübermittlung an öffentliche Stellen außerhalb des Geltungsbereiches des Grundgesetzes
(vgl. § 17 Regierungsentwurf)

(1) Eine Übermittlung personenbezogener Daten an Behörden oder sonstige öffentliche Stellen außerhalb des Geltungsbereichs des Grundgesetzes sowie an über- und zwischenstaatliche Stellen ist zulässig, soweit die Übermittlung in einem Gesetz oder einer internationalen Vereinbarung ausdrücklich geregelt ist.

(2) Eine Übermittlung darf auch erfolgen, wenn im Empfängerland gleichwertige Datenschutzregelungen vorhanden und die Voraussetzungen der § 11 und § 13 erfüllt sind.

(3) Die Übermittlung unterbleibt, soweit Grund zu der Annahme besteht, daß dadurch gegen den Zweck eines deutschen Gesetzes verstoßen oder das Recht auf informationelle Selbstbestimmung des Betroffenen verletzt würde.

§ 17

Datenübermittlung an öffentliche Stellen außerhalb des Geltungsbereichs des Grundgesetzes
(vgl. § 16 Entwurf des Hessischen Datenschutzbeauftragten)

(1) Eine Übermittlung personenbezogener Daten an Behörden oder sonstige öffentliche Stellen außerhalb des Geltungsbereichs des Grundgesetzes sowie an über- und zwischenstaatliche Stellen ist zulässig, soweit die Übermittlung in einem Gesetz oder einer internationalen Vereinbarung ausdrücklich geregelt ist.

(2) Eine Übermittlung darf auch erfolgen, wenn für den Empfänger gleichwertige Datenschutzregelungen gelten und die Voraussetzungen der §§ 11 und 13 erfüllt sind. Die Übermittlung unterbleibt, soweit Grund zu der Annahme besteht, daß dadurch gegen den Zweck eines deutschen Gesetzes verstoßen und insbesondere das Recht des Betroffenen aus § 1 Nr. 1 verletzt würde.

Dritter Abschnitt
Rechte des Betroffenen

§ 18
Auskunft und Benachrichtigung

(1) Werden personenbezogene Daten in einer Datei gespeichert, dann ist dem Betroffenen von der speichernden Stelle auf Antrag gebührenfrei Auskunft zu erteilen über

1. die zu seiner Person gespeicherten Daten,

2. den Zweck und die Rechtsgrundlage der Verarbeitung sowie

3. die Herkunft der Daten und die Empfänger regelmäßiger Übermittlungen, soweit dies gespeichert ist.

In dem Antrag soll die Art der Daten, über die Auskunft erteilt werden soll, näher bezeichnet werden.

(2) Werden personenbezogene Daten in einer automatisierten Datei gespeichert, dann ist der Betroffene von dieser Tatsache zu benachrichtigen. Die Benachrichtigung umfaßt die nach § 6 Abs. 1 Nr. 1 bis 5 festzulegenden Angaben. Spätere Änderungen dieser Angaben sind ihm ebenfalls mitzuteilen.

(3) Die Absätze 1 und 2 gelten nicht für personenbezogene Daten, die deshalb gesperrt sind, weil sie auf Grund gesetzlicher Aufbewahrungsvorschriften nicht gelöscht werden dürfen, sowie für solche Daten, die ausschließlich zum Zwecke der Datensicherung oder Datenschutzkontrolle gespeichert werden.

Dritter Abschnitt
Rechte des Betroffenen

§ 17
Benachrichtigung und Auskunft

(1) Werden personenbezogene Daten in einer automatisierten Datei gespeichert, ist der Betroffene von dieser Tatsache zu benachrichtigen. Die Benachrichtigung umfaßt die nach § 6 Nr. 1-5 festzulegenden Angaben. Spätere Änderungen dieser Angaben sind ihm ebenfalls mitzuteilen.

(2) Werden personenbezogene Daten in einer Datei gespeichert, dann ist dem Betroffenen von der speichernden Stelle auf Antrag gebührenfrei Auskunft zu erteilen über

1. die zu seiner Person gespeicherten Daten,

2. den Zweck und die Rechtsgrundlage der Verarbeitung sowie

3. die Herkunft der Daten und die Empfänger regelmäßiger Übermittlungen.

In dem Antrag soll die Art der Daten, über die Auskunft erteilt werden soll, näher bezeichnet werden.

(3) Benachrichtigung und Auskunft sind schriftlich zu erteilen, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist.

(4) Sind personenbezogene Daten in Akten gespeichert, die zur Person des Betroffenen geführt werden, dann kann er bei der speichernden Stelle Einsicht in die von ihm bezeichneten Akten verlangen. Werden die Akten nicht zur Person des Betroffenen geführt, hat er Angaben zu machen, die das Auffinden der zu seiner Person gespeicherten Daten mit angemessenem Aufwand ermöglichen.
Die Einsichtnahme ist unzulässig, wenn die Daten des Betroffenen mit Daten Dritter oder geheimhaltungsbedürftigen nichtpersonenbezogenen Daten derart verbunden sind, daß ihre Trennung nicht oder nur mit unverhältnismäßig großem Aufwand möglich ist. In diesem Fall ist dem Betroffenen Auskunft nach Abs. 1 zu erteilen. Im übrigen kann ihm statt Einsicht Auskunft gewährt werden.

(5) Abs. 1, 2 und 4 gelten nicht, soweit eine Abwägung ergibt, daß die dort gewährten Rechte des Betroffenen hinter dem öffentlichen Interesse an der Geheimhaltung oder an dem überwiegenden Geheimhaltungsinteresse Dritter zurücktreten müssen. Die Entscheidung trifft der Leiter der speichernden Stelle oder dessen Stellvertreter. Werden Auskunft oder Einsicht nicht gewährt, ist der Betroffene darauf hinzuweisen, daß er sich an den Hessischen Datenschutzbeauftragten wenden kann.

(6) Abs. 1, 2 und 4 gelten nicht für Berufungsverfahren von Professoren und berufungsähnliche Verfahren. Sie gelten außerdem nicht für datenverarbeitende Stellen, soweit sie sich privatrechtlich betätigen. Bei Prüfungsverfahren gelten sie erst nach deren Abschluß.

(7) Einer Begründung für die Ablehnung der Auskunft bedarf es gegenüber dem Betroffenen dann nicht, wenn durch die Mitteilung der Gründe, auf die die Entscheidung gestützt wird, der mit der Auskunftsverweigerung verfolgte Zweck gefährdet würde. Unterbleibt die Begründung, so sind die wesentlichen Gründe für diese Entscheidung aufzuzeichnen.

(4) Die Absätze 1 und 2 gelten nicht für Daten, die ausschließlich zum Zweck der Datensicherung oder Datenschutzkontrolle gespeichert werden.

(5) Sind personenbezogene Daten in Akten gespeichert, die zur Person des Betroffenen geführt werden, dann kann er bei der speichernden Stelle Einsicht in die Akten verlangen. Werden die Akten nicht zur Person des Betroffenen geführt, hat er besondere Umstände darzulegen, die die Annahme rechtfertigen, daß Daten zu seiner Person gespeichert sind. Er kann Einsicht verlangen, soweit dadurch keine berechtigten Geheimhaltungsinteressen Dritter berührt sind. § 29 des Hessischen Verwaltungsverfahrensgesetzes vom 1. Dezember 1976 bleibt unberührt.

(6) Die Absätze 1, 2 und 5 gelten nicht, soweit im Einzelfall nach Feststellung der obersten Landesbehörde das Wohl des Bundes oder des Landes gefährdet würde. In diesen Fällen sind die wesentlichen Gründe für die Entscheidung aufzuzeichnen. Der Hessische Datenschutzbeauftragte ist zu unterrichten. Der Betroffene ist darauf hinzuweisen, daß er sich an diesen wenden kann.

(7) Bei öffentlich-rechtlichen Kreditinstituten und Versicherungen gelten die Absätze 1, 2 und 5 nicht, wenn das Bekanntwerden personenbezogener Daten die Geschäftszwecke der speichernden Stelle erheblich gefährden würde und berechtigte Interesssen des Betroffenen nicht entgegenstehen. Gewähren diese Stellen keine Auskunft, zeichnen sie die wesentlichen Gründe für die Entscheidung auf. Der Betroffene ist darauf hinzuweisen, daß er sich an den Hessischen Datenschutzbeauftragten wenden kann.

§ 19
Berichtigung, Sperrung und Löschung

(1) Personenbezogene Daten sind zu berichtigen, wenn sie unrichtig sind.

(2) Personenbezogene Daten sind zu sperren, wenn

1. ihre Richtigkeit vom Betroffenen bestritten wird und sich weder die Richtigkeit noch die Unrichtigkeit feststellen läßt,

2. ihre Kenntnis für die speichernde Stelle zur rechtmäßigen Erfüllung der in ihrer Zuständigkeit liegenden Aufgaben nicht mehr erforderlich ist oder

3. ihre Verarbeitung unzulässig war und der Betroffene anstelle der Löschung die Sperrung verlangt.

In automatisierten Dateien ist die Sperrung grundsätzlich durch technische Maßnahmen sicherzustellen; im übrigen ist ein entsprechender Vermerk anzubringen.

Gesperrte Daten dürfen über die Speicherung hinaus nicht mehr verarbeitet werden, es sei denn, daß die Verarbeitung zur Behebung einer bestehenden Beweisnot oder aus sonstigen im überwiegenden Interesse der speichernden Stelle oder eines Dritten liegenden Gründen unerläßlich ist oder der Betroffene in die Verarbeitung eingewilligt hat.

(3) Personenbezogene Daten können gelöscht werden, wenn ihre Kenntnis für die speichernde Stelle zur rechtmäßigen Erfüllung der in ihrer Zuständigkeit liegenden Aufgaben nicht mehr erforderlich ist und kein Grund zu der Annahme besteht, daß durch die Löschung schutzwürdige Belange des Betroffenen beeinträchtigt werden.

(4) Personenbezogene Daten sind zu löschen, wenn ihre Verarbeitung unzulässig ist oder wenn es in den Fällen des Abs. 2 Satz 1 Nr. 2 der Betroffene verlangt.

§ 18
Berichtigung, Sperrung und Löschung

(1) Personenbezogene Daten sind zu berichtigen, wenn sie unrichtig sind.

(2) Personenbezogene Daten sind zu sperren, wenn ihre Richtigkeit vom Betroffenen bestritten wird und sich weder die Richtigkeit noch die Unrichtigkeit feststellen läßt. Gesperrte Daten sind mit einem entsprechenden Vermerk zu versehen; sie dürfen über die Speicherung hinaus nicht mehr verarbeitet werden, es sei denn, daß die Verarbeitung zur Behebung einer bestehenden Beweisnot unerläßlich ist oder der Betroffene in die Verarbeitung eingewilligt hat.

(3) Personenbezogene Daten sind zu löschen, wenn ihre Verarbeitung unzulässig ist. Sie sind auch zu löschen, wenn ihre Kenntnis für die datenverarbeitende Stelle zur rechtmäßigen Erfüllung der in ihrer Zuständigkeit liegenden Aufgaben nicht mehr erforderlich ist und kein Grund zu der Annahme besteht, daß durch die Löschung schutzwürdige Belange des Betroffenen beeinträchtigt werden.

(4) Von der Berichtigung gemäß Absatz 1 sowie von der Sperrung gemäß Absatz 2 und der Löschung gemäß Absatz 4 sind unverzüglich die Stellen zu verständigen, denen die Daten im Rahmen regelmäßiger Datenübermittlungen übermittelt werden; im übrigen kann die Verständigung unterbleiben, wenn schutzwürdige Belange des Betroffenen sie nicht gebieten.

(5) Von der Berichtigung nach Abs. 1 sowie von der Sperrung nach Abs. 2 Satz 1 Nr. 1 und 3 und der Löschung nach Abs. 4 sind unverzüglich die Stellen zu unterrichten, denen die Daten übermittelt wurden. Die Unterrichtung kann unterbleiben, wenn sie einen unverhältnismäßigen Aufwand erfordern würde und keine Anhaltspunkte bestehen, daß dadurch schutzwürdige Belange des Betroffenen beeinträchtigt werden können.

(6) Sind personenbezogene Daten in Akten gespeichert, ist die Sperrung nach Abs. 2 Satz 1 Nr. 2 nur durchzuführen, wenn die gesamte zur Person des Betroffenen geführte Akte zur Erfüllung der dort genannten Aufgaben nicht mehr erforderlich ist. Die Löschung nach Abs. 4 2. Halbsatz kann der Betroffene in diesem Fall nicht verlangen. Die Abs. 1 bis 4 gelten nicht für Stellen, die Akten nur vorübergehend beigezogen haben.

(7) In den Fällen des Abs. 2 Satz 1 Nr. 2 und des Abs. 3 kann die speichernde Stelle die Daten anstelle der dort vorgeschriebenen Sperrung oder Löschung dem zuständigen staatlichen oder kommunalen Archiv zur Übernahme anbieten; im übrigen ist unter Beachtung der Sperrungsvorschriften des Abs. 2 Satz 1 Nr. 1 und 3 die Übergabe an das Archiv zulässig, soweit die Daten zur Aufgabenerledigung nicht mehr benötigt werden und eine Löschung nicht vorgeschrieben ist.

§ 20
Schadensersatz

(1) Wird der Betroffene durch eine unzulässige oder unrichtige automatisierte Verarbeitung personenbezogener Daten in seinen Rechten nach § 1 Nr. 1 beeinträchtigt, so hat ihm der Träger der datenverarbeitenden Stelle den daraus entstehenden Schaden zu ersetzen. In schweren Fällen kann der Betroffene auch wegen des Schadens, der nicht Vermögensschaden ist, eine billige Entschädigung in Geld verlangen. Der Ersatzpflichtige haftet jedem Betroffenen für jedes schädigende Ereignis bis zu einem Betrag von 250.000 Deutsche Mark.

(2) § 254 des Bürgerlichen Gesetzbuches gilt entsprechend.

(3) Der Schadensersatzanspruch verjährt in drei Jahren von dem Zeitpunkt an, in welchem der Betroffene von dem Schaden und von der zur Entschädigung verpflichteten Stelle Kenntnis erlangt, ohne Rücksicht auf diese Kenntnis in 30 Jahren von der Entstehung des Anspruchs an.

(4) Weitergehende sonstige Schadensersatzansprüche bleiben unberührt.

(5) Sind personenbezogene Daten in Akten gespeichert, hat die Löschung, nach Absatz 3 durch Vernichtung der Akten zu erfolgen. Diese ist nur durchzuführen, wenn die gesamte zur Person des Betroffenen geführte Akte zur Erfüllung der dort genannten Aufgaben nicht mehr erforderlich ist.

(6) Absatz 3 gilt nicht, soweit Rechtsvorschriften die Übergabe der gespeicherten Daten an staatliche oder kommunale Archive anordnen und eine Nutzung der archivierten Daten zu Verwaltungszwecken ausschließen.

§ 19
Folgenbeseitigung und Schadensersatz

(1) Der Betroffene kann verlangen, daß eine rechtswidrige Beeinträchtigung seines Rechts auf informationelle Selbstbestimmung unterlassen oder beseitigt wird, wenn diese nach der Berichtigung, Sperrung oder Löschung andauert.

(2) Entsteht dem Betroffenen durch eine unzulässige oder unrichtige Verarbeitung personenbezogener Daten ein Schaden, so hat ihm der Träger der datenverarbeitenden Stelle Ersatz zu leisten. Auch für Nichtvermögensschäden ist eine Entschädigung in Geld zu gewähren.

(3) Ein Verschulden des Betroffenen ist bei der Gewährung des Schadensersatzes zu berücksichtigen.

(4) Der Schadensersatzanspruch verjährt in drei Jahren von dem Zeitpunkt an, in welchem der Betroffene von dem Schaden und von der zur Entschädigung verpflichteten Stelle Kenntnis erlangt, ohne Rücksicht auf diese Kenntnis in 30 Jahren von der Entstehung des Anspruchs an.

(5) Weitergehende sonstige Schadensersatzansprüche bleiben unberührt.

(6) Auf öffentlich-rechtliche Unternehmen, die am Wettbewerb teilnehmen, finden Abs. 1 bis 4 keine Anwendung.

Zweiter Teil

Hessischer Datenschutzbeauftragter

§ 21
Rechtsstellung

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

(2) Der Präsident des Landtags verpflichtet den Hessischen Datenschutzbeauftragten vor dem Landtag, sein Amt gerecht zu verwalten und die Verfassung des Landes Hessen und das Grundgesetz für die Bundesrepublik Deutschland getreulich zu wahren.

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

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

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

§ 22
Unabhängigkeit

Der Hessische Datenschutzbeauftragte ist unbeschadet seiner Verpflichtungen aus den §§ 24 bis 31 und 39 unabhängig und frei von Weisungen.

Zweiter Teil

Hessischer Datenschutzbeauftragter

§ 20
Rechtsstellung

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

(2) Der Präsident des Landtags verpflichtet den Hessischen Datenschutzbeauftragten vor dem Landtag, sein Amt gerecht zu verwalten und die Verfassung des Landes Hessen und das Grundgesetz für die Bundesrepublik Deutschland getreulich zu wahren.

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

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

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

§ 21
Unabhängigkeit

Der Hessische Datenschutzbeauftragte ist unbeschadet seiner Verpflichtungen aus den §§ 23 bis 31 unabhängig und frei von Weisungen.

§ 23
Verschwiegenheitspflicht

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

§ 24
Aufgaben

(1) Der Hessische Datenschutzbeauftragte überwacht die Einhaltung der Vorschriften dieses Gesetzes sowie anderer Vorschriften über den Datenschutz bei den datenverarbeitenden Stellen, ausgenommen die Gerichte, soweit sie nicht in Verwaltungsangelegenheiten tätig werden. Zu diesem Zwecke kann er Empfehlungen zur Verbesserung des Datenschutzes geben; insbesondere kann er die Landesregierung und einzelne Minister sowie die übrigen datenverarbeitenden Stellen in Fragen des Datenschutzes beraten. Der Hessische Datenschutzbeauftragte kontrolliert die Einhaltung der Datenschutzvorschriften auch bei den Stellen, die sich und soweit sie sich nach § 4 Abs. 2 Satz 1 seiner Kontrolle unterworfen haben.

(2) Der Hessische Datenschutzbeauftragte beobachtet die Auswirkungen der automatisierten Datenverarbeitung auf die Arbeitsweise und die Entscheidungsbefugnisse der datenverarbeitenden Stellen. Er hat insbesondere darauf zu achten, ob sie zu einer Verschiebung in der Gewaltenteilung zwischen den Verfassungsorganen des Landes, zwischen den Organen der kommunalen Selbstverwaltung und zwischen der staatlichen und der kommunalen Selbstverwaltung führen. Er soll Maßnahmen anregen, die ihm geeignet erscheinen, derartige Auswirkungen zu verhindern.

(3) Der Hessische Datenschutzbeauftragte arbeitet mit den Behörden und sonstigen Stellen, die für die Kontrolle der Einhaltung der Vorschriften über den Datenschutz im Bund und in den Ländern zuständig sind, sowie mit den Aufsichtsbehörden nach § 30 des Bundesdatenschutzgesetzes zusammen.

§ 22
Verschwiegenheitspflicht

(1) Der Hessische Datenschutzbeauftragte ist auch nach Beendigung seines Amtsverhältnisses verpflichtet, über die ihm bei seiner amtlichen Tätigkeit bekanntgewordenen Angelegenheiten Verschwiegenheit zu wahren. Dies gilt nicht für Mitteilungen im dienstlichen Verkehr oder über Tatsachen, die offenkundig sind oder ihrer Bedeutung nach keiner Geheimhaltung bedürfen.

(2) Der Hessische Datenschutzbeauftragte ist oberste Dienstbehörde im Sinne des § 96 der Strafprozeßordnung in der Fassung vom 7. Januar 1975 und trifft die Entscheidung nach § 75 und § 76 des Hessischen Beamtengesetzes in der Fassung vom 14. Dezember 1976 für sich und die ihm zugewiesenen Bediensteten in eigener Verantwortung.

§ 23
Aufgaben

(1) Der Hessische Datenschutzbeauftragte überwacht die Einhaltung der Vorschriften dieses Gesetzes sowie anderer Vorschriften über den Datenschutz bei den in § 3 Abs. 1 genannten Behörden und Stellen, ausgenommen die Gerichte, soweit sie nicht in Verwaltungsangelegenheiten tätig werden. Er kann Empfehlungen zur Verbesserung des Datenschutzes geben; insbesondere kann er die Landesregierung und einzelne Minister sowie die übrigen in § 3 Abs. 1 genannten Behörden und sonstigen Stellen in Fragen des Datenschutzes beraten. Der Hessische Datenschutzbeauftragte kontrolliert die Einhaltung der Datenschutzvorschriften auch bei den Stellen, die sich nach § 4 Abs. 2 seiner Kontrolle unterworfen haben oder nach § 4 Abs. 3 seiner Kontrolle unterstellt sind.

(2) Der Hessische Datenschutzbeauftragte beobachtet die Entwicklung und die Auswirkungen der automatisierten Datenverarbeitung sowie der Informations- und Kommunikationstechniken auf die Arbeitsweise und die Entscheidungsbefugnisse der in § 3 Abs. 1 genannten Stellen. Er hat insbesondere darauf zu achten, ob sie zu einer Verschiebung in der Gewaltenteilung zwischen den Verfassungsorganen des Landes, zwischen den Organen der kommunalen Selbstverwaltung und zwischen der staatlichen und der kommunalen Selbstverwaltung führen. Er soll Maßnahmen anregen, die ihm geeignet erscheinen, derartige Auswirkungen zu verhindern.

(3) Der Hessische Datenschutzbeauftragte arbeitet mit den Behörden und sonstigen Stellen, die für die Kontrolle der Einhaltung der Vorschriften über den Datenschutz im Bund und in den Ländern zuständig sind, sowie mit den Aufsichtsbehörden nach § 30 des Bundesdatenschutzgesetzes zusammen.

§ 25
Gutachten und Untersuchungen in Datenschutzfragen

Der Landtag und die Landesregierung können den Hessischen Datenschutzbeauftragten mit der Erstattung von Gutachten und der Durchführung von Untersuchungen in Datenschutzfragen betrauen.

§ 26
Register

(1) Die speichernde Stelle ist verpflichtet, dem Hessischen Datenschutzbeauftragten die Beschreibung ihrer Dateien (§ 6) vorzulegen. Der Hessische Datenschutzbeauftragte führt ein Register dieser Dateien. Das Register kann von jedem eingesehen werden.

(2) Abs. 1 Satz 3 gilt nicht für

1. Dateien des Landesamtes für Verfassungsschutz,

2. Dateien, die der Gefahrenabwehr oder der Strafverfolgung dienen,

3. Dateien der Landesfinanzbehörden, soweit sie personenbezogene Daten zur Erfüllung der gesetzlichen Aufgaben im Anwendungsbereich der Abgabenordnung zur Überwachung und Prüfung enthalten.

4. Dateien der in § 3 Abs. 9 genannten Stellen,

wenn die speichernde Stelle eine Einsichtnahme mit der Erfüllung ihrer Aufgaben für unvereinbar erklärt.

(3) Der Hessische Datenschutzbeauftragte führt ein Verzeichnis der Geräte, mit denen personenbezogene Daten automatisiert gespeichert und weiterverarbeitet werden. Die datenverarbeitende oder in ihrem Auftrag tätige Stelle, die solche Geräte betreibt, hat ihm den Typ und die Art der Geräte, ihren Hersteller sowie ihre Anzahl, das verwendete Betriebssystem sowie die Möglichkeiten zur Datenverarbeitung oder Datenübertragung zu melden. Weitere in das Verzeichnis der Geräte aufzunehmende Angaben bestimmt die Landesregierung durch Rechtsverordnung nach Anhörung des Hessischen Datenschutzbeauftragten.

§ 24
Gutachten und Untersuchungen in Datenschutzfragen

Der Landtag und die Landesregierung können den Hessischen Datenschutzbeauftragten mit der Erstattung von Gutachten und der Durchführung von Untersuchungen in Datenschutzfragen betrauen.

§ 25
Dateienregister

(1) Die datenverarbeitenden Stellen sind verpflichtet, dem Hessischen Datenschutzbeauftragten die Beschreibung ihrer Dateien (§ 6) vorzulegen. Der Hessische Datenschutzbeauftragte führt ein Register dieser Dateien. Das Register kann von jedem eingesehen werden.

(2) Abs. 1 Satz 3 gilt nicht für

1. Dateien des Landesamtes für Verfassungsschutz

2. Dateien der Staatsanwaltschaft und der Vollzugspolizei

3. Dateien der Steuerfahndung,

wenn und soweit diese Stellen eine Einsichtnahme mit der Erfüllung ihrer Aufgaben für unvereinbar erklären.

(3) Der Hessische Datenschutzbeauftragte führt ein Verzeichnis der Geräte, mit denen personenbezogene Daten automatisiert gespeichert und weiterverarbeitet werden. Die öffentlichen Stellen, die solche Geräte betreiben, haben ihm den Typ und die Art der Geräte, ihren Hersteller, ihre Anzahl, die verwendete Betriebssoftware sowie die Verbindungsmöglichkeiten zu anderen Geräten, die zur Datenfernverarbeitung oder Datenfernübertragung verwendet werden können, zu melden. Weitere in das Verzeichnis der Geräte aufzunehmende Angaben bestimmt die Landesregierung durch Rechtsverordnung nach Anhörung des Hessischen Datenschutzbeauftragten.

§ 27
Beanstandungen durch den Hessischen Datenschutzbeauftragten

(1) Stellt der Hessische Datenschutzbeauftragte Verstöße gegen die Vorschriften dieses Gesetzes oder gegen andere Datenschutzbestimmungen oder sonstige Mängel bei der Verarbeitung personenbezogener Daten fest, so beanstandet er dies

1. bei der Landesverwaltung gegenüber der zuständigen obersten Landesbehörde,

2. bei den Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts sowie bei Vereinigungen solcher Körperschaften, Anstalten und Stiftungen gegenüber dem Vorstand oder dem sonst vertretungsberechtigten Organ

und fordert zur Stellungnahme innerhalb einer von ihm zu bestimmenden Frist auf. In den Fällen von Satz 1 Nr. 2 unterrichtet der Hessische Datenschutzbeauftragte gleichzeitig auch die zuständige Aufsichtsbehörde.

(2) Der Hessische Datenschutzbeauftragte kann von einer Beanstandung absehen oder auf eine Stellungnahme der betroffenen Stelle verzichten, wenn es sich um unerhebliche Mängel handelt.

(3) Mit der Beanstandung kann der Hessische Datenschutzbeauftragte Vorschläge zur Beseitigung der Mängel und zur sonstigen Verbesserung des Datenschutzes verbinden.

(4) Die gemäß Abs. 1 abzugebende Stellungnahme soll auch eine Darstellung der Maßnahmen enthalten, die auf Grund der Beanstandung des Hessischen Datenschutzbeauftragten getroffen worden sind. Die in Abs. 1 Satz 1 Nr. 2 genannten Stellen leiten der zuständigen Aufsichtsbehörde eine Abschrift ihrer Stellungnahme an den Hessischen Datenschutzbeauftragten zu.

§ 26
Beanstandungen durch den Hessischen Datenschutzbeauftragten

(1) Stellt der Hessische Datenschutzbeauftragte Verstöße gegen die Vorschriften dieses Gesetzes oder gegen andere Datenschutzbestimmungen oder sonstige Mängel bei der Verarbeitung personenbezogener Daten fest, so beanstandet er dies

1. bei der Landesverwaltung gegenüber der zuständigen obersten Landesbehörde,

2. bei den Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts sowie bei Vereinigungen solcher Körperschaften, Anstalten und Stiftungen gegenüber dem Vorstand oder dem sonst vertretungsberechtigten Organ

und fordert zur Stellungnahme innerhalb einer von ihm zu bestimmenden Frist auf. In den Fällen von Satz 1 Nr. 2 unterrichtet der Hessische Datenschutzbeauftragte gleichzeitig auch die zuständige Aufsichtsbehörde.

(2) Der Hessische Datenschutzbeauftragte kann von einer Beanstandung absehen oder auf eine Stellungnahme der betroffenen Stelle verzichten, wenn es sich um unerhebliche Mängel handelt.

(3) Mit der Beanstandung kann der Hessische Datenschutzbeauftragte Vorschläge zur Beseitigung der Mängel und zur sonstigen Verbesserung des Datenschutzes verbinden.

(4) Die gemäß Abs. 1 abzugebende Stellungnahme soll auch eine Darstellung der Maßnahmen enthalten, die auf Grund der Beanstandung des Hessischen Datenschutzbeauftragten getroffen worden sind. Die in Abs. 1 Satz 1 Nr. 2 genannten Stellen leiten der zuständigen Aufsichtsbehörde eine Abschrift ihrer Stellungnahme an den Hessischen Datenschutzbeauftragten zu.

§ 28
Anrufung des Hessischen Datenschutzbeauftragten

Jedermann kann sich an den Hessischen Datenschutzbeauftragten wenden, wenn er annimmt, bei der Verarbeitung seiner personenbezogenen Daten durch datenverarbeitende Stellen, ausgenommen die Gerichte, soweit sie nicht in Verwaltungsangelegenheiten tätig werden, in seinen Rechten verletzt worden zu sein.

§ 29
Auskunftsrecht des Hessischen Datenschutzbeauftragten

(1) Alle datenverarbeitenden Stellen sind verpflichtet, den Hessischen Datenschutzbeauftragten bei der Erfüllung seiner Aufgaben zu unterstützen. Ihm ist dabei insbesondere

1. Auskunft zu seinen Fragen sowie Einsicht in alle Unterlagen zu gewähren, die in Zusammenhang mit der Verarbeitung personenbezogener Daten stehen.

2. Zutritt in alle Diensträume zu gewähren.

Satz 2 gilt nicht, soweit die oberste Landesbehörde im Einzelfall feststellt, daß die Einsicht in Unterlagen und Akten die Sicherheit des Bundes oder eines Landes gefährdet.

(2) Es ist sicherzustellen, daß der Hessische Datenschutzbeauftragte über Verfahrensentwicklungen und Gesetzesvorhaben im Zusammenhang mit der automatisierten Verarbeitung personenbezogener Daten unterrichtet wird.

§ 27
Anrufung des Hessischen Datenschutzbeauftragten

(1) Jedermann kann sich unmittelbar an den Hessischen Datenschutzbeauftragten wenden, wenn er annimmt, bei der Verarbeitung seiner personenbezogenen Daten durch die in § 3 Abs. 1 genannten Behörden und sonstigen Stellen in seinen Rechten verletzt worden zu sein.

(2) Bedienstete der in § 3 Abs. 1 genannten Behörden und sonstigen Stellen können sich ohne Einhaltung des Dienstweges an den Hessischen Datenschutzbeauftragten wenden.

(3) Abs. 1 findet keine Anwendung auf Gerichte, soweit sie rechtsprechende Tätigkeit ausüben.

§ 28
Benachteiligungsverbot

Niemand darf dafür gemaßregelt oder benachteiligt werden, daß er sich aufgrund von tatsächlichen Anhaltspunkten für einen Verstoß gegen dieses Gesetz oder andere Vorschriften über den Datenschutz an den Hessischen Datenschutzbeauftragten wendet.

§ 29
Auskunftsrecht des Hessischen Datenschutzbeauftragten

(1) Alle in § 3 Abs. 1 genannten Stellen sind verpflichtet, den Hessischen Datenschutzbeauftragten bei der Erfüllung seiner Aufgaben zu unterstützen. Ihm ist dabei insbesondere

1. Auskunft zu seinen Fragen sowie Einsicht in alle Unterlagen zu gewähren, die in Zusammenhang mit der Verarbeitung personenbezogener Daten stehen.

2. Zutritt in alle Diensträume zu gewähren.

(2) Der Hessische Datenschutzbeauftragte ist über Verfahrensentwicklungen und Gesetzesvorhaben im Zusammenhang mit der automatisierten Verarbeitung personenbezogener Daten rechtzeitig zu unterrichten.

§ 30
Berichtspflicht

(1) Bis zum 31. Dezember jeden Jahres hat der Hessische Datenschutzbeauftragte dem Landtag und der Landesregierung einen Bericht über das Ergebnis seiner Tätigkeit vorzulegen. Er gibt dabei auch einen Überblick über die technischen und organisatorischen Maßnahmen nach § 10 und regt Verbesserungen des Datenschutzes an. Zwischenberichte sind zulässig.

(2) Die Landesregierung legt ihre Stellungnahme zu dem Haupt- oder Zwischenbericht dem Landtag vor. Zusammen mit der Stellungnahme zum Hauptbericht gibt sie einen Bericht über die Tätigkeit der für den Datenschutz im nicht-öffentlichen Bereich zuständigen Aufsichtsbehörden.

§ 31
Personal- und Sachausstattung

(1) Dem Hessischen Datenschutzbeauftragten ist vom Präsidenten des Landtags die für die Erfüllung seiner Aufgaben notwendige Personal- und Sachausstattung zur Verfügung zu stellen; sie ist im Einzelplan des Landtags in einem eigenen Kapitel auszuweisen.

(2) In Personalangelegenheiten hat der Hessische Datenschutzbeauftragte ein Vorschlagsrecht. Die Bediensteten unterstehen seinen Weisungen.

Dritter Teil
Besonderer Datenschutz

§ 32
Datenverarbeitung für Planungszwecke
(vgl. § 33 Entwurf des Hessischen Datenschutzbeauftragten)

(1) Für Zwecke der öffentlichen Planung können personenbezogene Daten gesondert verarbeitet werden. Die Verarbeitung soll von der übrigen Verwaltung personell und organisatorisch getrennt erfolgen.

(2) Die zu Planungszwecken gespeicherten personenbezogenen Daten dürfen nicht für andere Verwaltungszwecke genutzt werden. Sobald es der Zweck der Planungsaufgabe erlaubt, sind die zu diesem Zweck verarbeiteten personenbezogenen Daten so zu verändern, daß sie sich weder auf eine bestimmte Person beziehen, noch eine solche erkennen lassen. Eine Übermittlung von Daten, aus denen Rückschlüsse auf Einzelpersonen gezogen werden können, ist unzulässig.

§ 30
Berichtspflicht

(1) Der Hessische Datenschutzbeauftragte hat dem Landtag und der Landesregierung jährlich einen Bericht über seine Tätigkeit vorzulegen. Er gibt dabei auch einen Überblick über die technischen und organisatorischen Maßnahmen nach § 10 und regt Verbesserungen des Datenschutzes an. Zwischenberichte sind zulässig.

(2) Die Landesregierung legt ihre Stellungnahme zu dem Haupt- oder Zwischenbericht dem Landtag vor. Zusammen mit der Stellungnahme zum Hauptbericht gibt sie einen Bericht über die Tätigkeit der für den Datenschutz im nicht-öffentlichen Bereich zuständigen Aufsichtsbehörden.

§ 31
Personal- und Sachausstattung

(1) Dem Hessischen Datenschutzbeauftragten ist vom Präsidenten des Landtags die für die Erfüllung seiner Aufgaben notwendige Personal- und Sachausstattung zur Verfügung zu stellen; sie ist im Einzelplan des Landtags in einem eigenen Kapitel auszuweisen.

(2) Die Bediensteten werden auf Vorschlag des Hessischen Datenschutzbeauftragten ernannt. Ihr Dienstvorgesetzter ist der Hessische Datenschutzbeauftragte, an dessen Weisungen sie ausschließlich gebunden sind.

Dritter Teil
Besonderer Datenschutz

§ 33
Datenverarbeitung für wissenschaftliche Zwecke

(1) Zum Zweck unabhängiger wissenschaftlicher Forschung dürfen datenverarbeitende Stellen personenbezogene Daten ohne Einwilligung des Betroffenen nur für bestimmte Forschungsarbeiten übermitteln, soweit dessen schutzwürdige Belange wegen der Art der Daten, wegen ihrer Offenkundigkeit oder wegen der Art der Verwendung nicht beeinträchtigt werden. Der Einwilligung des Betroffenen bedarf es auch nicht, wenn das öffentliche Interesse an der Durchführung des Forschungsvorhabens die schutzwürdigen Belange des Betroffenen erheblich überwiegt und der Zweck der Forschung nicht auf andere Weise erreicht werden kann. Bei Stellen des Landes bedarf die Übermittlung der vorherigen Genehmigung der obersten Landesbehörde oder einer von dieser bestimmten Stelle. Die Genehmigung muß den Empfänger, die Art der zu übermittelnden personenbezogenen Daten, den Kreis der Betroffenen und das Forschungsvorhaben bezeichnen und ist dem Hessischen Datenschutzbeauftragten mitzuteilen.

(2) Sobald der Forschungszweck dies erlaubt, sind die Merkmale, mit deren Hilfe ein Personenbezug hergestellt werden kann, gesondert zu speichern; die Merkmale sind zu löschen, sobald der Forschungszweck erreicht ist.

(3) Eine Verarbeitung der nach Abs. 1 übermittelten Daten zu anderen als Forschungszwecken ist unzulässig. Die nach Abs. 1 Satz 2 übermittelten Daten dürfen nur mit Einwilligung des Betroffenen weiterübermittelt werden.

(4) Soweit die Vorschriften dieses Gesetzes auf den Empfänger keine Anwendung finden, dürfen personenbezogene Daten nur übermittelt werden, wenn sich der Empfänger verpflichtet, die Vorschriften der Abs. 2 und 3 einzuhalten und sich der Kontrolle des Hessischen Datenschutzbeauftragten unterwirft.

(5) Unter den Voraussetzungen des Abs. 1 darf die datenverarbeitende Stelle personenbezogene Daten ohne Einwilligung des Betroffenen selbst zum Zwecke wissenschaftlicher Forschung verarbeiten.

§ 32
Datenverarbeitung für wissenschaftliche Zwecke

(1) Zum Zwecke unabhängiger wissenschaftlicher Forschung können für ein bestimmtes Forschungsvorhaben die in § 3 Abs. 1 genannten Behörden und öffentlichen Stellen mit Einwilligung des Betroffenen personenbezogene Daten übermitteln.

(2) Der Einwilligung bedarf es nicht, soweit schutzwürdige Belange des Betroffenen wegen der Art der Daten, wegen ihrer Offenkundigkeit oder wegen der Art der Verwendung nicht beeinträchtigt werden. Der Einwilligung des Betroffenen bedarf es auch nicht, wenn das öffentliche Interesse an der Durchführung des Forschungsvorhabens die schutzwürdigen Belange des Betroffenen erheblich überwiegt und der Zweck der Forschung nicht auf andere Weise erreicht werden kann. Die Übermittlung bedarf der vorherigen Genehmigung der obersten Landesbehörde oder einer von dieser bestimmten Stelle. Die Genehmigung muß den Empfänger, die Art der zu übermittelnden personenbezogenen Daten, den Kreis der Betroffenen und das Forschungsvorhaben bezeichnen und ist dem Hessischen Datenschutzbeauftragten mitzuteilen.

(3) Sobald der Forschungszweck dies erlaubt, sind die Merkmale, mit deren Hilfe ein Personenbezug hergestellt werden kann, gesondert zu speichern; die Merkmale sind zu löschen, sobald der Forschungszweck erreicht ist.

(4) Eine Nutzung der nach Abs. 1 und 2 übermittelten Daten zu anderen als Forschungszwecken ist unzulässig. Die nach Abs. 2 Satz 2 übermittelten Daten dürfen nur mit Einwilligung des Betroffenen weiterübermittelt werden.

(5) Soweit die Vorschriften dieses Gesetzes auf den Empfänger keine Anwendung finden, dürfen personenbezogene Daten nach Maßgabe der Absätze 1 und 2 nur übermittelt werden, wenn sich der Empfänger verpflichtet, die Vorschriften der Absätze 3 und 4 einzuhalten und sich der Kontrolle des Hessischen Datenschutzbeauftragten unterwirft.

§ 34
Datenschutz bei Dienst- und Arbeitsverhältnissen
(vgl. § 35 Entwurf des Hessischen Datenschutzbeauftragten)

(1) Öffentliche Stellen dürfen Daten ihrer Beschäftigten nur verarbeiten, wenn dies zur Eingehung, Durchführung, Beendigung oder Abwicklung des Dienst- oder Arbeitsverhältnisses oder zur Durchführung innerdienstlicher organisatorischer, sozialer und personeller Maßnahmen erforderlich ist oder eine Rechtsvorschrift, ein Tarifvertrag oder eine Dienstvereinbarung es vorsieht.

(2) Abweichend von § 16 Abs. 1 ist eine Übermittlung der Daten von Beschäftigten an Personen und Stellen außerhalb des öffentlichen Bereichs nur zulässig, wenn der Empfänger ein rechtliches Interesse darlegt, der Dienstverkehr es erfordert oder der Betroffene eingewilligt hat. Die Datenübermittlung an einen künftigen Dienstherrn oder Arbeitgeber ist nur mit Einwilligung des Betroffenen zulässig.

(3) Das Auskunftsrecht nach § 18 Abs. 1 Satz 1 umfaßt auch die Art der automatisierten Auswertung der Daten des Beschäftigten. § 18 Abs. 5 findet keine Anwendung.

(4) Im Falle des § 19 Abs. 2 Satz 1 Nr. 2 sind die Daten der Beschäftigten zu löschen. Daten, die vor der Eingebung eines Dienst- oder Arbeitsverhältnisses erhoben wurden, sind unverzüglich zu löschen, sobald feststeht, daß ein Dienst- oder Arbeitsverhältnis nicht zustande kommt. Dies gilt nicht, wenn Grund zu der Annahme besteht, daß durch die Löschung schutzwürdige Belange des Betroffenen beeinträchtigt werden.

(5) Eine automatisierte Verarbeitung von Daten der Beschäftigten darf erst eingeführt, angewendet, geändert oder erweitert werden, wenn dem Hessischen Datenschutzbeauftragten die Dateibeschreibung nach § 6 zur Stellungnahme vorgelegen hat. Hat er eine Stellungnahme abgegeben, so ist sie zusammen mit der Dateibeschreibung der zuständigen Personalvertretung im Rahmen des personalvertretungsrechtlichen Beteiligungsverfahrens zuzuleiten. Bei öffentlichen Stellen des Landes ist die Genehmigung der obersten Landesbehörde erforderlich.

§ 33
Datenverarbeitung für Planungszwecke
(vgl. § 32 Regierungsentwurf)

(1) Für Zwecke der Landes- und Kommunalplanung können personenbezogene Daten für bestimmte Planungsvorhaben in gesondert eingerichteten Informationssystemen verarbeitet werden, die von der übrigen Verwaltung personell und organisatorisch getrennt sind. Ein Informationssystem zu Planungszwecken (Planungsinformationssystem) im Sinne dieses Gesetzes kann nur bei solchen Stellen errichtet werden, die eine Trennung der Planung von anderen Verwaltungseinheiten gewährleisten können. Vor der Einrichtung ist der Hessische Datenschutzbeauftragte anzuhören.

(2) Die in den Planungsinformationssystemen gespeicherten personenbezogenen Daten dürfen nicht für andere Verwaltungszwecke genutzt werden. Sobald es der Zweck des einzelnen Planungsvorhabens erlaubt, sind die zu diesem Zweck verarbeiteten personenbezogenen Daten so zu verändern, daß sie sich weder auf eine bestimmte Person beziehen, noch eine solche erkennen lassen (zu anonymisieren). Vor jeder Übermittlung von Planungsdaten hat die Stelle, bei der das Planungsinformationssystem eingerichtet ist, sicherzustellen, daß die Daten anonymisiert sind.

(3) Jedermann hat über § 29 des Hessischen Verwaltungsverfahrensgesetzes hinaus Anspruch auf Auskunft über Planungsdaten, die keinen Personenbezug mehr aufweisen. Auskünfte dürfen nicht erteilt werden, wenn ihnen ein gesetzliches Verbot entgegensteht. Das Auskunftsrecht des Landtags und der kommunalen Vertretungsorgane gemäß § 36 bleibt unberührt.

(6) Dienst- und arbeitsrechtliche Beurteilungen sowie medizinische und psychologische Befunde des Beschäftigten dürfen nicht automatisiert verarbeitet werden.

(7) Daten der Beschäftigten, die im Rahmen der Durchführung der technischen und organisatorischen Maßnahmen nach § 10 Abs. 3 gespeichert werden, dürfen nicht zu Zwecken der Verhaltens- oder Leistungskontrolle ausgewertet werden.

(8) Daten der Beschäftigten dürfen zu Planungszwecken nach Maßgabe von § 32 verarbeitet werden. Eine automatisierte Verarbeitung ist nur zulässig, wenn sichergestellt ist, daß sie von der übrigen Verwaltung personell und organisatorisch getrennt erfolgt. Der Hessische Datenschutzbeauftragte ist vor der Einführung des automatisierten Verfahrens zu hören.

§ 35
Datenübermittlung an öffentlich-rechtliche Religionsgesellschaften
(vgl. § 15 Entwurf des Hessischen Datenschutzbeauftragten)

Die Übermittlung personenbezogener Daten an Stellen der öffentlich-rechtlichen Religionsgesellschaften ist in entsprechender Anwendung der Vorschriften über die Datenübermittlung an öffentliche Stellen zulässig, sofern sichergestellt ist, daß bei dem Empfänger ausreichende Datenschutzmaßnahmen getroffen werden.

§ 36
Fernmessen und Fernwirken

Wer eine Datenverarbeitungs- oder Übertragungseinrichtung zu dem Zweck nutzt, bei einem Betroffenen insbesondere in der Wohnung oder in den Geschäftsräumen ferngesteuert Messungen vorzunehmen oder andere Wirkungen auszulösen, bedarf dessen Einwilligung.

§ 34
Fernmessen und Fernwirken

Wer eine Datenverarbeitungs- oder Übertragungseinrichtung zu dem Zweck nutzt, bei einem Betroffenen insbesondere in der Wohnung oder in den Geschäftsräumen ferngesteuert Messungen vorzunehmen oder andere Wirkungen auszulösen, bedarf dessen Einwilligung.

§ 37
Datenschutzbeauftragter des Hessischen Rundfunks
(entfällt im Entwurf des Hessischen Datenschutzbeauftragten)

(1) Der Rundfunkrat des Hessischen Rundfunks bestellt für die Dauer von jeweils vier Jahren einen Beauftragten für den Datenschutz. Wiederbestellung ist zulässig. Nach dem Ende der Amtszeit bleibt der Beauftragte für den Datenschutz bis zur Neuwahl im Amt. Vor Ablauf seiner Amtszeit kann der Beauftragte für den Datenschutz nur abberufen werden, wenn Tatsachen vorliegen, die bei einem Beamten die Entlassung aus dem Dienst rechtfertigen. Er kann jederzeit von seinem Amt zurücktreten.

(2) Zum Beauftragten für den Datenschutz darf nur bestellt werden, wer die zur Erfüllung seiner Aufgaben erforderliche Fachkunde und Zuverlässigkeit besitzt.

(3) Der Beauftragte für den Datenschutz ist bei der Ausübung seines Amtes frei von Weisungen; die Dienstaufsicht obliegt dem Verwaltungsrat. Dies gilt nicht, soweit der Beauftragte für den Datenschutz sonstige Aufgaben der Anstalt wahrnimmt. Er darf wegen der Erfüllung seiner Aufgaben als Beauftragter für den Datenschutz nicht benachteiligt werden. § 23 gilt mit der Maßgabe, daß die Aussagegenehmigung der Intendant erteilt.

(4) Der Beauftragte für den Datenschutz überwacht die Ausführung dieses Gesetzes sowie anderer Vorschriften über den Datenschutz.

(5) Jedermann kann sich an den Beauftragten für den Datenschutz wenden, wenn er annimmt, bei der Verarbeitung seiner personenbezogenen Daten durch den Hessischen Rundfunk in seinen Rechten verletzt worden zu sein.

(6) Für Beanstandungen durch den Beauftragten für den Datenschutz gilt § 27 mit der Maßgabe, daß an die Stelle der in § 27 Abs. 1 Satz 1 Nr. 1 und 2 genannten Behörden der Intendant und an die Stelle der Aufsichtsbehörde der Rundfunkrat treten.

(7) Der Beauftragte für den Datenschutz erstattet dem Rundfunkrat und dem Verwaltungsrat jedes Jahr einen Bericht über seine Tätigkeit.

§ 35
Datenschutz bei Dienst- oder Arbeitsverhältnissen
(vgl. § 34 Regierungsentwurf)

(1) Öffentliche Stellen dürfen Daten ihrer Beschäftigten nur verarbeiten, wenn dies zur Eingehung, Durchführung oder Beendigung des Dienst- oder Arbeitsverhältnisses erforderlich ist oder eine Rechtsvorschrift es vorsieht.

(2) Abweichend von § 15 Abs. 1 ist eine Übermittlung der Daten von Beschäftigten an Stellen außerhalb des öffentlichen Bereichs nur mit Einwilligung des Betroffenen zulässig. Dies gilt auch für Datenübermittlungen an einen künftigen Dienstherrn oder Arbeitgeber des Betroffenen.

(3) Das Auskunftsrecht nach § 17 Abs. 2 Satz 1 umfaßt auch die Art der automatisierten Auswertung der Daten des Beschäftigten. § 17 Abs. 4, 6 und 7 findet keine Anwendung.

(4) Daten, die vor der Eingehung eines Dienst- oder Arbeitsverhältnisses erhoben wurden, sind unverzüglich zu löschen, sobald feststeht, daß ein Dienst- oder Arbeitsverhältnis nicht zustande kommt.

(5) Für automatisierte Verfahren zur Verarbeitung der Daten von Beschäftigten ist die Genehmigung der obersten Landesbehörde erforderlich.

(6) Automatisierte Verfahren dürfen erst eingerichtet werden, wenn dem Hessischen Datenschutzbeauftragten die Dateibeschreibung nach § 6 zur Stellungnahme vorgelegen hat. Hat er eine Stellungnahme abgegeben, so ist sie zusammen mit der Dateibeschreibung dem Personalrat im Rahmen des Beteiligungsverfahrens nach dem Hessischen Personalvertretungsgesetz vom 2. Januar 1979 zuzuleiten.

(7) Dienst- und arbeitsrechtliche Beurteilungen sowie medizinische und psychologische Daten des Beschäftigten dürfen nicht automatisiert verarbeitet werden.

(8) Daten der Beschäftigten, die im Rahmen der Durchführung der technischen und organisatorischen Maßnahmen nach § 10 und der Anlage dazu gespeichert werden, dürfen nicht zu Zwecken der Verhaltens- oder Leistungskontrolle ausgewertet werden.

Vierter Teil
Rechte des Landtags und der kommunalen Vertretungsorgane

§ 38
Auskunftsrecht des Landtags und der kommunalen Vertretungsorgane

(1) Die Hessische Zentrale für Datenverarbeitung, die Kommunalen Gebietsrechenzentren und die Landesbehörden, die Datenverarbeitungsanlagen betreiben, sind verpflichtet, dem Landtag, dem Präsidenten des Landtags und den Fraktionen des Landtags die von diesen im Rahmen ihrer Zuständigkeiten verlangten Auskünfte auf Grund der gespeicherten Daten zu geben, soweit Programme zur Auswertung vorhanden sind. Die Auskünfte dürfen keine personenbezogenen Daten enthalten. Den Auskünften darf ein gesetzliches Verbot oder ein öffentliches Interesse nicht entgegenstehen; dem Auskunftsrecht des Landtags steht ein öffentliches Interesse in der Regel nicht entgegen. Der Landtag hat Zugriff zu den Daten, soweit durch technische Maßnahmen sichergestellt ist, daß die Grenzen der Sätze 1 bis 3 eingehalten werden.

(2) Der Landtag kann von der Landesregierung Auskünfte über die bestehenden Daten verlangen, die für Auskünfte oder den Zugriff nach Abs. 1 geeignet sind. Das Auskunftsverlangen kann sich erstrecken auf:

1. Name des Verfahrens mit kurzer Funktionsbeschreibung,

2. vorhandene Dateien,

3. Aufbau der Datensätze mit Angaben über den Inhalt und die Ordnungskriterien,

4. vorhandene Auswertungsprogramme,

5. zuständige Behörde.

(3) Das Auskunftsrecht des Abs. 1 steht im Rahmen ihrer Zuständigkeiten den Gemeindevertretungen und den Kreistagen sowie deren Fraktionen und den entsprechenden Organen anderer in § 3 Abs. 1 genannten Körperschaften und Anstalten Gegenüber der Hessischen Zentrale für Datenverarbeitung, dem zuständigen Kommunalen Gebietsrechenzentrum und den Behörden der Gemeinden und Gemeindeverbände zu, die Datenverarbeitungsanlagen betreiben. Der Antrag der Fraktionen ist in den Gemeinden über den Gemeindevorstand, in den Kreisen über den Kreisausschuß zu leiten.

Vierter Teil
Recht des Landtags und der kommunalen Vertretungsorgane

§ 36
Auskunftsrecht des Landtags und der kommunalen Vertretungsorgane

(1) Die Hessische Zentrale für Datenverarbeitung, die Kommunalen Gebietsrechenzentren und die Landesbehörden, die Datenverarbeitungsanlagen betreiben, sind verpflichtet, den Landtag, dem Präsidenten des Landtags und den Fraktionen des Landtags die von diesen im Rahmen ihrer Zuständigkeiten verlangten Auskünfte auf Grund der gespeicherten Daten zu geben, soweit Programme zur Auswertung vorhanden sind. Die Auskünfte dürfen keine personenbezogenen Daten enthalten. Den Auskünften darf ein gesetzliches Verbot oder ein öffentliches Interesse nicht entgegenstehen; dem Auskunftsrecht des Landtags steht ein öffentliches Interesse in der Regel nicht entgegen. Der Landtag hat Zugriff zu den Daten, soweit durch technische Maßnahmen sichergestellt ist, daß die Grenzen der Sätze 1 bis 3 eingehalten werden.

(2) Der Landtag kann von der Landesregierung Auskünfte über die bestehenden Daten verlangen, die für Auskünfte oder den Zugriff nach Abs. 1 geeignet sind. Das Auskunftsverlangen kann sich erstrecken auf:

1. Name des Verfahrens mit kurzer Funktionsbeschreibung,

2. vorhandene Dateien,

3. Aufbau der Datensätze mit Angaben über den Inhalt und die Ordnungskriterien,

4. vorhandene Auswertungsprogramme,

5. zuständige Behörde.

(3) Das Auskunftsrecht des Abs. 1 steht im Rahmen ihrer Zuständigkeiten den Gemeindevertretungen und den Kreistagen sowie deren Fraktionen und den entsprechenden Organen anderer in § 3 Abs. 1 genannten Körperschaften und Anstalten gegenüber der Hessischen Zentrale für Datenverarbeitung, dem zuständigen Kommunalen Gebietsrechenzentrum und den Behörden der Gemeinden und Gemeindeverbände zu, die Datenverarbeitungsanlagen betreiben. Der Antrag der Fraktionen ist in den Gemeinden über den Gemeindevorstand, in den Kreisen über den Kreisausschuß zu leiten.

§ 39
Untersuchungen für den Landtag und die kommunalen Vertretungsorgane

Der Landtag, der Präsident des Landtags und die in § 38 Abs. 3 genannten Vertretungsorgane können verlangen, daß der Hessische Datenschutzbeauftragte untersucht, aus welchen Gründen Auskunftsersuchen nicht oder nicht ausreichend beantwortet wurden.

Fünfter Teil
Schlußvorschriften

§ 40
Straftaten

(1) Wer entgegen den Vorschriften dieses Gesetzes in Dateien gespeicherte personenbezogene Daten, die nicht offenkundig sind,

1. übermittelt, verändert, zum Abruf bereithält oder löscht,

2. abruft, einsieht oder sich aus in Behältnissen verschlossenen Dateien verschafft oder durch Vortäuschung falscher Tatsachen ihre Übermittlung an sich oder einen Dritten veranlaßt,

wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft.

(2) Handelt der Täter gegen Entgelt oder in der Absicht, einen anderen zu schädigen oder sich oder einen anderen zu bereichern, so ist die Strafe Freiheitsstrafe bis zu zwei Jahren oder Geldstrafe.

(3) Abs. 1 und 2 finden nur Anwendung, soweit die Tat nicht in anderen Vorschriften mit Strafe bedroht ist.

(4) Die Tat wird nur auf Antrag verfolgt.

§ 37
Untersuchungen für den Landtag und die kommunalen Vertretungsorgane

Der Landtag, der Präsident des Landtags und die in § 38 Abs. 3 genannten Vertretungsorgane können verlangen, daß der Hessische Datenschutzbeauftragte untersucht, aus welchen Gründen Auskunftsersuchen nicht oder nicht ausreichend beantwortet werden.

Fünfter Teil
Schlußvorschriften

§ 38
Straftaten

(1) Wer entgegen den Vorschriften dieses Gesetzes in Dateien gespeicherte personenbezogene Daten, die nicht offenkundig sind,

1. übermittelt, verändert, zum Abruf bereithält oder löscht,

2. abruft, einsieht oder sich aus in Behältnissen verschlossenen Dateien verschafft oder durch Vortäuschung falscher Tatsachen ihre Übermittlung an sich oder einen Dritten veranlaßt,

wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft.

(2) Handelt der Täter gegen Entgelt oder in der Absicht, einen anderen zu schädigen oder sich oder einen anderen zu bereichern, so ist die Strafe Freiheitsstrafe bis zu zwei Jahren oder Geldstrafe.

(3) Abs. 1 und 2 finden nur Anwendung, soweit die Tat nicht in anderen Vorschriften mit Strafe bedroht ist.

(4) Die Tat wird nur auf Antrag verfolgt.

§ 41
Ordnungswidrigkeiten

(1) Ordnungswidrig handelt, wer vorsätzlich oder fahrlässig entgegen § 16 Abs. 2 Daten nicht nur für den Zweck verwendet, zu dessen Erfüllung sie ihm übermittelt wurden.

(2) Die Ordnungswidrigkeit kann mit einer Geldbuße bis zu fünfzigtausend Deutsche Mark geahndet werden.

§ 42
Übergangsvorschrift
(vgl. § 40 Entwurf des Hessischen Datenschutzbeauftragten)

(1) Waren personenbezogene Daten vor Inkrafttreten dieses Gesetzes in automatisierten Dateien gespeichert, dann hat die Benachrichtigung nach § 18 Abs. 2 innerhalb von zwei Jahren nach dem Inkrafttreten zu erfolgen.

(2) Auf Akten, die bei Inkrafttreten des Gesetzes vorhanden waren, ist § 19 Abs. 1, 4 und 6 nur anwendbar, wenn die speichernde Stelle die Voraussetzungen für die Berichtigung, Löschung oder Sperrung bei der Erfüllung ihrer laufenden Aufgaben feststellt.

§ 39
Ordnungswidrigkeiten

(1) Ordnungswidrig handelt, wer vorsätzlich oder fahrlässig

1. entgegen § 13 Abs. 1 personenbezogene Daten für einen anderen Zweck nutzt, übermittelt oder sonst braucht, als den, für den sie erhoben oder gespeichert worden sind,

2. entgegen § 15 Abs. 2 die ihm übermittelten Daten für einen anderen Zweck verwendet, als den, für dessen Erfüllung sie ihm übermittelt wurden,

(2) Die Ordnungswidrigkeit kann mit einer Geldbuße bis zu 50.000 DM geahndet werden.

§ 40
Aufhebung bisherigen Rechts
(vgl. § 43 Regierungsentwurf)

Das Hessische Datenschutzgesetz vom 31. Januar 1978 (GVBl. I S. 96), geändert durch Gesetz vom 14. Oktober 1980 (GVBl. I S. 377), sowie die Hessische Verordnung über die Veröffentlichung der Angaben über gespeicherte personenbezogene Daten vom 01. November 1978 (GVBl. I S. 553) und die Hessische Verordnung über die von dem Hessischen Datenschutzbeauftragten zu führenden Dateienregister vom 08. Dezember 1978 (GVBl. I S. 682) werden aufgehoben.

§ 43
Aufhebung bisherigen Rechts
(vgl. § 40 Entwurf des Hessischen Datenschutzbeauftragten)

Das Hessische Datenschutzgesetz vom 31. Januar 1978 (GVBl. I S. 96), geändert durch Gesetz vom 14. Oktober 1980 (GVBl. I S. 377), sowie die Hessische Verordnung über die Veröffentlichung der Angaben über gespeicherte personenbezogene Daten vom 01. November 1978 (GVBl. I S. 553) und die Hessische Verordnung über die von dem Hessischen Datenschutzbeauftragten zu führenden Dateienregister vom 08. Dezember 1978 (GVBl. I S. 682) werden aufgehoben.

§ 44
Inkrafttreten

Dieses Gesetz tritt am in Kraft.

§ 41
Übergangsvorschrift
(vgl. § 42 Regierungsentwurf)

Waren personenbezogene Daten vor Inkrafttreten dieses Gesetzes in automatisierten Dateien gespeichert, dann hat die Benachrichtigung nach § 17 Abs. 1 innerhalb von zwei Jahren nach dem Inkrafttreten zu erfolgen.

§ 42
Inkrafttreten

Dieses Gesetz tritt am in Kraft.

11. Recht auf Information/"Freedom of Information"

11.1
Freedom of Information

11.1.1
Datenschutz und Recht auf Information

Die Diskussion über den Datenschutz hat sich in den letzten Jahren verständlicherweise auf die Bedingungen der Verarbeitung personenbezogener Daten konzentriert. Der Datenschutz wurde deshalb nahezu durchweg mit einer Abwehr der nicht zuletzt unter dem Einfluß der technologischen Entwicklung entstandenen Gefahren gleichgesetzt. Spätestens seit der Entscheidung des Bundesverfassungsgerichts zum Volkszählungsgesetz steht aber fest, daß noch so konsequenter Datenschutz immer nur Teil einer Informationsregelung ist, die auch und gerade das Recht des einzelnen auf Information umfaßt. Um noch einmal auf das Bundesverfassungsgericht zurückzukommen: Wenn das Grundrecht auf informationelle Selbstbestimmung zu den elementaren Voraussetzungen einer demokratischen Gesellschaft zählt, dann müssen Datenschutz und Recht auf Information immer zugleich bedacht werden.

Auf den ersten Blick scheinen Datenschutz und ein Recht auf Information, wie beispielsweise das amerikanische Freedom of Information-Gesetz von 1974 oder das entsprechende französische Gesetz vom 17. Juli 1978 es dem Bürger gewähren, einander auszuschließen: Während man bei dem Stichwort "Datenschutz" vor allem an ein Abwehrrecht des Bürgers denkt, also an das Recht, bestimmte Informationsflüsse zu verhindern, geht es bei dem Recht auf Information/"Freedom of Information" darum, dem Bürger einen Zugang zu den bei Behörden vorhandenen Informationen (Akten und auf Datenträgern gespeicherten Daten) zu eröffnen, also einen Informationsfluß zu ermöglichen. So heißt es auch in einem Papier der Organisation für wirtschaftliche Zusammenarbeit und Entwicklung (OECD): "Die Beziehung zwischen Datenschutz und Bestimmungen über ein Zugangsrecht zu Akten ist problematisch. Der freie Zugang könnte durch Datenschutzbestimmungen eingeschränkt, der Datenschutz in seinem Umfang durch Bestimmungen über ein Zugangsrecht gehindert werden" (vgl. OECD: "Legislation on Access to Administrative Documents and the Protection of privacy", Paris, March 1984, Seite 4). Unbestreitbar ist jedenfalls, daß es sowohl beim Datenschutz wie bei einem Recht auf Information um die Regelung von Informationsströmen innerhalb unserer Gesellschaft geht, also um eine Art von "Datenverkehrsordnung".

Das Hessische Datenschutzgesetz hat von Anfang an bereits in seiner ersten Fassung vom 7. Oktober 1970 Datenschutz nicht nur als "Abwehrrecht" des einzelnen verstanden (wie später das Bundesdatenschutzgesetz), sondern auch als Kontrolle von Informationsflüssen in der Gesellschaft. Dies zeigen vor allem seine Vorschriften über den Schutz des Informationsgleichgewichts zwischen den Staatsgewalten (§ 10 Abs. 2) und die Vorschriften über das Informationsrecht des Landtags sowie der kommunalen Vertretungsorgane (§ 6). Das derzeit gültige Hessische Datenschutzgesetz vom 31. Januar 1978 baut auf dem Konzept des ersten Hessischen Datenschutzgesetzes auf und hat dies dadurch verdeutlicht und präzisiert, daß es in § 1 (Aufgabe und Gegenstand) beide Aspekte, den Schutz des Individuums und den Schutz des Informationsgleichgewichtes, als Aufgaben des Datenschutzes bezeichnet. Es ist deshalb nur folgerichtig, wenn Überlegungen zur Weiterentwicklung des Datenschutzes in Hessen insbesondere den Aspekt der Regelung von Informationsflüssen in der Gesellschaft aufgreifen und in ihren Komplementärbeziehungen zueinander zu präzisieren versuchen.

11.1.2
Regelungen im Ausland

Im Hinblick auf das oben genannte Ziel empfiehlt sich eine genauere Betrachtung der Entstehungsgeschichte und der Ausprägung des Rechts auf Information (Freedom of Information), wie es sich gegenwärtig in verschiedenen Ländern darstellt. Am 19. März 1985 wurde im Europäischen Parlament ein Resolutionsentwurf über "Freedom of Information" eingebracht. Er nimmt Bezug auf eine im Jahre 1970 von der Beratenden Versammlung des Europarats einstimmig angenommene Empfehlung, daß die in Artikel 10 der Europäischen Menschenrechtskonvention garantierten Rechte um das Recht auf Informationsfreiheit erweitert werden sollten: "... um ein Recht auf freien Informationszugang ... mit einer entsprechenden Pflicht öffentlicher Behörden, Informationen über Angelegenheiten von öffentlichem Interesse zugänglich zu machen, unter angemessenen Einschränkungen". Unter Hinweis darauf, daß seit 1970 eine Reihe von Staaten auf Bundes- oder Länderebene Gesetze über freien Zugang zu öffentlichen Akten erlassen haben, fordert der Resolutionsentwurf die Mitgliedstaaten des Europäischen Parlaments, die dies nicht schon verwirklicht haben, dazu auf, ein gesetzliches Recht auf Zugang zu bei Regierungsstellen vorhandenen Informationen zu schaffen, und zwar spätestens bis zum 30. Juni 1986 (Transnational Data Report, 1985, Seite 202).

Das Recht auf "Freedom of Information" läßt sich zurückverfolgen auf die schwedische "Druckfreiheitsverordnung" von 1766. Das daraus entwickelte Prinzip der Aktenöffentlichkeit ist ein Verfassungsgrundsatz des schwedischen Rechts. In der heute gültigen Fassung vom 1. Januar 1978 lautet dieser Grundsatz wie folgt:

"Kapitel 2: Über den öffentlichen Charakter offizieller Akten

§ 1 Zur Förderung eines freien Meinungsaustausches und einer allseitigen Orientierung ist jeder schwedische Staatsbürger zur Einsichtnahme in offizielle Akten befugt.

§ 2 Das Recht auf Einsichtnahme in offizielle Akten darf nur dann beschränkt werden, wenn dies erforderlich ist aus Rücksicht auf

1. die Sicherheit des Reiches oder auf dessen Verhältnis zu einer fremden Macht oder zwischenstaatlichen Organisation,

2. die zentrale Finanz- und Währungspolitik,

3. die Tätigkeit einer Behörde zu Inspektion, Kontrolle oder anderer Aufsicht,

4. das Interesse an der Vorbeugung und Verfolgung von Verbrechen,

5. das wirtschaftliche Interesse der Allgemeinheit,

6. den Schutz der berechtigten persönlichen oder finanziellen Verhältnisse des Einzelnen,

7. das Interesse an der Bewahrung von Tier- oder Pflanzenarten."

Wie sich aus der Entstehungsgeschichte des schwedischen Rechts auf Aktenöffentlichkeit ergibt, diente es dem Bürger dazu, sich durch rechtzeitige Einsicht in die Planungen und Vorhaben der staatlichen Bürokratie vor Beeinträchtigung seiner eigenen Interessen zu schützen. Als weitaus bedeutsamer als dieser individuelle Aspekt des Prinzips der Aktenöffentlichkeit hat sich allerdings der Aspekt des Schutzes der sogenannten "kollektiven Freiheitsrechte" erwiesen: Die Druckfreiheitsverordnung von 1766 sollte es hauptsächlich der Gesamtheit der Bürger, also "dem Volk", ermöglichen, dem König und seinen Räten "in die Karten zu sehen", d.h. also durch die Kenntnis seiner Absichten und deren Verwirklichung durch seine Verwaltung eine Grundlage für die Mitsprache der Bürger ("Parlament") zu erhalten.

Die historischen Voraussetzungen haben sich zwar geändert, aber auch für die parlamentarische Demokratie bleibt der freie Aktenzugang von zentraler Bedeutung. Auf sehr vielen Gebieten des öffentlichen Lebens sind die Gesetze so kompliziert, die Zusammenhänge zwischen sozialen, wirtschaftlichen, rechtlichen, finanziellen und anderen Aspekten so unüberschaubar und die Beteiligung der verschiedensten Behörden und öffentlichen Stellen so zahlreich geworden, daß die für das Funktionieren des parlamentarischen Systems lebenswichtige Beiligung des Bürgers genauso wie die Kontrolle der Exekutive durch das Parlament immer mehr in Gefahr gerät, ineffektiv zu werden. Gerade deshalb gebühren den Überlegungen zur Einführung eines Rechts auf Freedom of Information besondere Beachtung.

Eine Freedom of Information-Gesetzgebung besteht gegenwärtig in sechs europäischen und drei außereuropäischen Ländern, nämlich den skandinavischen Ländern Schweden, Finnland, Norwegen und Dänemark, außerdem in Frankreich und in den Niederlanden. An außereuropäischen Ländern sind zu nennen: die USA und Kanada sowie Australien. Ein Überblick über diese Gesetzgebung läßt sich am leichtesten gewinnen mit Hilfe einer kurzen Darstellung der Rechtslage zu Freedom of Information in Schweden und einer daran anschließenden Übersicht über wesentliche Unterschiede in der Gesetzgebung der anderen Länder.

11.1.2.1
Schweden

Für Schweden gilt: "Offizielle Akten, die ausgehändigt werden dürfen, sind sofort oder so bald wie möglich an Ort und Stelle gebührenfrei demjenigen zur Verfügung zu stellen, der davon Kenntnis zu nehmen wünscht, so daß die Akten gelesen, abgehört oder auf andere Weise verstanden werden können. Akten dürfen auch abgeschrieben, abgebildet oder zur Tonübertragung in Anspruch genommen werden. Können Akten nicht zur Verfügung gestellt werden, ohne daß ein Teil davon, der nicht ausgeliefert werden darf, bekannt gemacht wird, sind die übrigen Teile dem Antragsteller in Abschriften oder Kopien zugänglich zu machen." (Kapitel 2 § 12 der Druckfreiheitsverordnung, zitiert nach Schwan "Amtsgeheimnis oder Aktenöffentlichkeit?" S. 125). Über die Praxis wird berichtet: "Täglich pflegen Journalisten und Nachrichtenagenturen den Schriftverkehr bedeutenderer Behörden, vor allem in der Hauptstadt Stockholm, systematisch durchzugehen; eine ganze Reihe von Zentralbehörden legt ihrerseits die eingehende Post vor der Bearbeitung für einige Stunden in einem eigens der Presse zugänglichen Raum zur Einsichtnahme aus" (Conradi, Das Öffentlichkeitsprinzip in der schwedischen Verwaltung, Dissertation, Berlin 1969).

Auch wenn das Informationsrecht des Bürgers in der schwedischen Praxis offenbar nur indirekt, nämlich durch die Presse, wahrgenommen wird, darf man nicht verkennen, welche Bedeutung diese Praxis für den Informationsfluß von der Verwaltung zum Bürger hat, ganz besonders auf lokaler Ebene. Aber auch für die kommunale Selbstverwaltung kann es von großer Bedeutung sein, über das Aktenöffentlichkeitsprinzip frühzeitig über Projekte der Zentralregierung informiert zu sein, die Gemeindeinteressen betreffen. Das Prinzip kann also auch für die "vertikale Gewaltenteilung" eine Rolle spielen.

Die Einschränkungen des Aktenzugangsrechts ergeben sich aus dem Geheimhaltungsgesetz vom 28. Mai 1937 i.d.F. vom 1. Juli 1982 und der dazu ergangenen Geheimhaltungsverordnung. Grundgedanke der Geheimhaltungsbestimmungen ist, daß ohne die Geheimhaltung bestimmter Vorgänge der Allgemeinheit oder dem einzelnen ein Schaden entstehen würde. Die in Kapitel 2 § 2 Druckfreiheitsverordnung genannten möglichen Einschränkungen des Akteneinrichtsrechts (siehe oben) bilden die verschiedenen Gruppen, nach denen die Geheimhaltung im Geheimhaltungsgesetz und der dazu ergangenen Verordnung im einzelnen festgelegt worden ist.

Von Interesse ist noch, daß nach den schwedischen Geheimhaltungsbestimmungen die Pflicht zur Geheimhaltung zeitlich begrenzt ist, und zwar auf Zeiträume zwischen 50 Jahren (für Privatgeheimnisse) und 20 Jahren (für Geheimnisse der öffentlichen Verwaltung).

11.1.2.2
Finnland

Da Finnland bis zum Jahre 1809 eine staatliche Einheit mit Schweden bildete, galt dort ebenso wie in Schweden die Druckfreiheitsverordnung von 1766. In der Folgezeit, als Finnland ein Bestandteil des Zarenreiches wurde, änderte sich dies zu Gunsten der noch in der heutigen Sowjetunion geltenden Geheimhaltung. Nach Finnlands Erlangung der Unabhängigkeit wurde die Aktenöffentlichkeit nicht erneut geregelt. Erst 1951 erließ Finnland das "Gesetz über die Öffentlichkeit allgemeiner Akten" vom 9. Februar 1951. Es ist der schwedischen Druckfreiheitsverordnung sehr ähnlich, hat jedoch nicht wie diese Verfassungsrang.

11.1.2.3
Norwegen

Norwegen hat erst am 19. Juni 1970 das "Gesetz über die Öffentlichkeit in der Verwaltung" angenommen, das am 1. Juli 1971 in Kraft getreten und im Jahre 1982 novelliert worden ist.
In § 2 des Gesetzes heißt es: "Die Sachakten der Verwaltung sind öffentlich, soweit keine Ausnahmen durch Gesetz oder aufgrund eines Gesetzes gemacht worden sind. Jeder kann von der zuständigen öffentlichen Behörde verlangen, Einblick in den Inhalt einer öffentlichen Sachakte aus einem bestimmten Verfahren zu bekommen". Die üblichen Ausnahmen von dem Öffentlichkeitsgrundsatz sind, ähnlich wie in Schweden, in § 6 des Gesetzes geregelt. Bemerkenswert ist, daß § 5 eine Art "Kernbereich" der Regierung ebenfalls von dem Öffentlichkeitsgrundsatz ausnimmt: "Vorschläge, Entwürfe, Gutachten und andere ähnliche Arbeitsunterlagen, Untersuchungen oder Berichte, die das öffentliche Organ selbst erarbeitet oder, ohne hierzu gesetzlich verpflichtet zu sein, zur Verwendung bei einer internen Behandlung einer Sache einholt".

11.1.2.4
Dänemark

Auch Dänemark hat erst am 10. Juni 1970 ein Gesetz über die Öffentlichkeit der Verwaltung erlassen. Es bestimmt in § 1: "Jedermann kann verlangen, die Akten in Sachen, die von der öffentlichen Verwaltung behandelt werden oder behandelt worden sind, einzusehen". Die Ausnahmen sind ähnlich denen des norwegischen Gesetzes und enthalten ebenfalls den Schutz von Entwürfen, Konzepten und behördeninternen Briefwechseln.

Außerhalb der skandinavischen Länder verbreitete sich der Grundsatz des "Freedom of Information" in Europa erst Ende der siebziger Jahre, während in außereuropäischen Ländern schon Mitte der siebziger Jahre eine entsprechende Gesetzgebung entstand.

11.1.2.5
Frankreich

Wie in den meisten zentraleuropäischen Ländern galt auch in Frankreich noch bis in die jüngste Zeit der Grundsatz, daß alle Verwaltungsvorgänge, soweit sie nicht ausdrücklich als dem einzelnen oder der Öffentlichkeit zugänglich bezeichnet waren, geheimzuhalten seien. Diese Tradition wurde durch zwei im Jahre 1978 erlassene Gesetze, die mehr Bürgernähe der Verwaltung bewirken sollten, geradezu auf den Kopf gestellt: Grundsätzlich gilt das Prinzip der Aktenöffentlichkeit mit Ausnahme der Fälle, die im Gesetz ausdrücklich genannt sind. Bei den

genannten Gesetzen handelt es sich einmal um das französische Datenschutzgesetz vom 6. Januar 1978 und um das Gesetz vom 17. Juli 1978 "Über verschiedene Maßnahmen zur Verbesserung der Beziehungen zwischen der Verwaltung und der Öffentlichkeit und verschiedene Maßnahmen auf administrativem, sozialem und fiskalischem Gebiet". Während das Datenschutzgesetz in Art. 3 das Recht des Betroffenen auf Auskunft über die über ihn gespeicherten personenbezogenen Daten regelt, enthält das Gesetz vom 17. Juli 1978 die Bestimmungen über den allgemeinen Aktenzugang: Soweit es sich nicht um personenbezogene Daten handelt, garantiert Art. 1 jedermann ein unbeschränktes Recht auf Aktenzugang. Ausnahmen von diesem Recht bestimmt Art. 6, und zwar für den Fall, daß durch die Auskunft eine Gefahr eintritt für

- das Entscheidungsgeheimnis der Regierung oder anderer Stellen der Exekutivgewalt;
- das Geheimnis der nationalen Verteidigung und der Außenpolitik;
- die Währung und den öffentlichen Kredit, die Staats- und die öffentliche Sicherheit;
- den Ablauf von Verfahren oder Vorverfahren vor den Gerichten;
- den Schutz der Privatsphäre, das Personal- bzw. das Patientengeheimnis;
- Geschäfts- und Industriegeheimnisse;
- die Zoll- und Steuerfahndung, und, ganz allgemein, für gesetzlich geschützte Geheimnisse.

Die Einsichtnahme in Akten ist kostenlos. Lediglich für Anfertigung von Kopien darf eine Gebühr verlangt werden, die jedoch die entstandenen Kosten nicht übersteigen darf.

11.1.2.6
Niederlande

In den Niederlanden ist am 1. Mai 1980 ein Gesetz über die Verwaltungsöffentlichkeit in Kraft getreten. Damit sind die Niederlande das einzige Land in der europäischen Gemeinschaft, das zwar ein Gesetz über den Zugang zu öffentlichen Akten besitzt, aber noch kein Datenschutzgesetz. In den meisten EG-Ländern, die Datenschutzgesetze haben, fehlt es umgekehrt bisher an einer "Freedom of Information"-Regelung.

Nach § 1 des Gesetzes über die Verwaltungsöffentlichkeit hat jedermann das Recht gegenüber Behörden, Informationen über den Inhalt offizieller Akten zu verlangen. Darüber hinaus verpflichtet Art. 2 des Gesetzes die Behörden, die Öffentlichkeit über geplante und verwirklichte Maßnahmen regelmäßig zu unterrichten.

Ausnahmen von dem Grundsatz der Verwaltungsöffentlichkeit sind zulässig zum Schutz der Privatsphäre sowie in den Fällen, in denen eine Auskunft eine Gefahr bildet

- für die Einheit des Reiches
- die Staatssicherheit
- die Beziehungen mit anderen Nationen
- die Strafverfolgung oder im Namen der Regierung durchgeführte Kontrollmaßnahmen
- die wirtschaftlichen und finanziellen Interessen des Staates und anderer öffentlicher Stellen (Art. 4 des Gesetzes).

Bezüglich des Verfahrens zur Auskunftserteilung kann die Behörde wählen zwischen Erteilung von Einsicht in Akten und Dokumente und der Übermittlung vollständiger oder teilweiser Kopien sowie Inhaltsangaben über die Akten.

Eine dafür besonders eingesetzte Bewertungskommission soll die bisherige Praxis beim Zugang des Bürgers zu öffentlichen Akten untersuchen.

11.1.2.7
USA

Das heute in Kraft befindliche Freedom of Information-Gesetz (5 USC para. 552) von 1974 stammt in seiner ersten Fassung aus dem Jahre 1966. Es war das erste derartige Gesetz außerhalb Schwedens. In den USA gibt es nicht nur auf Bundes-, sondern auch auf Staatenebene entsprechende Gesetzgebung: Nach einer - allerdings nicht auf dem neuesten Stand befindlichen - Aufstellung haben nur drei von fünfzig Staaten keine Freedom of Information-Gesetzgebung (vgl. Access Reports, Dec. 1975, Washington). Die entsprechenden Gesetze der Einzelstaaten ergingen in der Regel im Anschluß an die Bundesgesetzgebung. Aus dieser Entwicklung in den USA läßt sich der Schluß ziehen, daß das Recht des Bürgers auf Zugang zu öffentlichen Akten in den USA einen hohen politischen Wert besitzt. Stellvertretend für die zahlreichen amerikanischen Einzelgesetze zu Freedom of Information wird hier das Bundesgesetz von 1974 betrachtet. Es richtet sich an alle Bundesbehörden und andere Stellen des Bundes, ausgenommen die Gerichte und das Parlament und betrifft alle Akten ("records") der Bundesverwaltung, inklusive Datenträger und sogar Computerprogramme. Auf Antrag eines Bürgers hat die betreffende Bundesstelle innerhalb von zehn Tagen über die Gewährung von Einsicht zu entscheiden. Bei negativer Entscheidung ist der Klageweg gegeben. Die Einschränkung des Freedom of Information-Gesetzes betrifft neun Gruppen:

1. Informationen, die die nationale Verteidigung oder die Außenpolitik betreffen,
2. Informationen, die interne Personalangelegenheiten der Behörden betreffen,
3. gesetzlich von der Veröffentlichung ausgenommene Informationen,
4. Geschäftsgeheimnisse sowie Informationen über wirtschaftliche oder finanzielle Verhältnisse,
5. Informationen, die zwischen Behörden oder innerhalb von Behörden ausgetauschte Memoranden oder Briefe betreffen, die im Prozeß nicht vorgelegt zu werden brauchen,
6. Personal- und medizinische Akten und ähnliche Unterlagen, die die Privatsphäre einer Person betreffen,
7. bestimmte Akten des Ermittlungsverfahrens,
8. Informationen im Zusammenhang mit der Rechnungsprüfung,
9. geologische oder geophysische Informationen einschließlich Landkarten über Quellen.

In Zweifelsfällen entscheidet über das Vorliegen eines oder mehrerer Ausschlußgründe das Gericht.

11.1.2.8
Australien

Etwa zur gleichen Zeit, als in den USA das Freedom of Information-Gesetz in Kraft trat (1966/1967), begann in Australien die öffentliche Diskussion und die parlamentarische Debatte über die Einführung ähnlicher Gesetzgebung. Bis zum Erlaß eines entsprechenden Gesetzes dauerte es aber mehrere Jahre: Das australische Gesetz über Freedom of Information trat am 1. Dezember 1982 in Kraft. Bereits am 1. Januar 1984 wurde der Anwendungsbereich des Gesetzes durch eine Novelle erheblich erweitert. Auch in Australien existiert nicht nur auf Bundesebene, sondern in verschiedenen Einzelstaaten eine entsprechende Gesetzgebung. Grundsätzlich sind nach dem Bundesgesetz alle Akten der Bundesverwaltung für die öffentliche Einsicht zugänglich. Ausgenommen sind interne, insbesondere der Vorbereitung von Entscheidungen dienende Papiere, Kabinettsprotokolle und Vorlagen sowie solche Dokumente, die von der zuständigen Behörde als geheim eingestuft worden sind. Daneben gilt die Ausnahme von der Veröffentlichung für Akten, die die öffentliche Sicherheit, das Finanzwesen oder Regierungseigentum betreffen, solche, die das Strafverfahren, Geschäfts- oder Berufsgeheimnisse betreffen, sowie solche, die dem Schutz der Privatsphäre unterliegen. Außer der Möglichkeit, sich bei Verweigerung einer Einsichtnahme an die nächsthöhere Behörde oder das zuständige Gericht zu wenden, hat der Bürger die Möglichkeit, sich mit einer Beschwerde an den - mit Gesetz von 1970 installierten - Ombudsman zu wenden.

11.1.2.9
Kanada

Das kanadische Freedom of Information-Gesetz stammt vom 7. Juli 1982 und trat 1 Jahr später in Kraft. Außerdem gibt es in verschiedenen kanadischen Provinzen Freedom of Information - Gesetzgebung, die sich nach der amerikanischen ausgerichtet hat. Kanada ist das erste Land der Welt, das die Zusammenhänge zwischen Freedom of Information und Datenschutz dadurch verdeutlicht hat, daß es sie gleichzeitig (in zwei parallel erlassenen Gesetzen) geregelt hat. Die Provinz Quebec war sogar so konsequent, Datenschutz und Freedom of Information in einem einzigen Gesetz zu regeln.

Nach dem Bundesgesetz hat der Bürger grundsätzlich das Recht auf Zugang zu Behördenakten, z.B. "...jegliche Korrespondenz, Memorandum, Buch, Plan, Karte, Zeichnung, Diagramm, bildliche oder grafische Darstellung, Fotografie, Film, Mikrofiche, Schallaufzeichnung, Videoband, maschinenlesbare Daten und alles andere dokumentarische Material und jede Kopie davon, einerlei in welcher physischen Form oder Charakteristik (sie vorhanden sind)" (§ 3 des Gesetzes; eigene Übersetzung). Auch hier wieder sind eine größere Zahl von Ausnahmetatbeständen im Gesetz genau umschrieben. Entscheidend für die Verwirklichung des Rechts des Bürgers ist, daß die kanadischen Gesetze die Einrichtung eines "Information Commissioner" (Beauftragten für Informationsfreiheit) vorsehen, der sein Amt parallel zu dem des Datenschutzbeauftragten ausübt. An ihn kann sich der Bürger wenden, wenn ihm im Einzelfall die Information verweigert wird.

11.1.3
Zur gegenwärtigen Diskussion in der Bundesrepublik

Dem kanadischen Konzept, den Grundsatz des Freedom of Information mit dem Recht auf Datenschutz in einem Gesetz oder in einer wenigstens klar abgestimmten Gesetzgebung zu behandeln, kommt erhebliche Bedeutung auch für die weitere Entwicklung in der Bundesrepublik zu. Spätestens mit der Entscheidung des Bundesverfassungsgerichts zum Volkszählungsgesetz ist die Dringlichkeit einer Novellierung der Datenschutzgesetze offenkundig. Damit sind aber auch die Voraussetzungen für eine gleichzeitige Diskussion des Rechts auf informationelle Selbstbestimmung und des Rechts auf Information gegeben. Dies umso mehr, als die in der oben erwähnten Entschließung des Europäischen Parlaments enthaltene Frist bald abläuft.

Besondere Aufmerksamkeit verdient in diesem Zusammenhang die Forderung nach einem Einsichtsrecht in Umweltakten. Zwar wird damit ein gerade aus der Perspektive des Bürgers besonders wichtiger Bereich angesprochen. Gerade die Erfahrungen der letzten Jahre legen es nahe, sich bei der Diskussion über Voraussetzungen und Grenzen des Rechts auf Information auf einen aus der Sicht des einzelnen erwiesenermaßen zentralen Problembereich zu konzentrieren. Dies umso mehr, als die Auseinandersetzung um das Recht auf Information nicht zuletzt an der Abstraktion der Diskussion gelitten hat. Was ein solches Recht genau bedeutet, welche Chancen und welche Gefahren mit ihm verknüpft sind, läßt sich erst verläßlich abschätzen, wenn man es im Zusammenhang mit einem konkreten Gebiet diskutiert.

Die Schwierigkeiten sind aber nicht zu übersehen. Schon die Definition des Anwendungsbereichs ist kompliziert. Zum "Umweltschutz" gehören beispielsweise nicht nur die nach landläufigem Verständnis darunter einzuordnenden Gegenstände wie Luft- und Gewässerreinhaltung, Entsorgung, Lärmbekämpfung - um nur die wichtigsten zu nennen - sondern auch weite Gebiete des Verbraucherschutzes und der Verbraucheraufklärung, der Lebensmittelherstellung und Kontrolle, des Naturschutzes, der Medizin und Pharmazie, des Transportwesens, der Landwirtschaft und vieles andere mehr.

Ebenso schwer fällt es, die Verwaltungsverfahren exakt zu beschreiben und abzugrenzen, die in "Umweltschutzangelegenheiten" geführt werden. Dazu gehören nämlich nicht nur die allgemein bekannten Genehmigungen für Atomanlagen, Kraftwerke und Mülldeponien, sondern auch Verfahren wie die Erteilung einer Baugenehmigung, die straßenverkehrsrechtliche Zulassung von Kraftfahrzeugen, luftverkehrsrechtliche Genehmigungen, die Führung und der Ausbau von Straßen, Rad- und Fußwegen, die Genehmigung von Sprühmitteln in der Landwirtschaft, die Genehmigung von Medikamenten, ja selbst die Erlaubnis für die Überschreitung der Polizeistunde bei einem öffentlichen Tanzvergnügen, um einige Beispiele für die Vielzahl der denkbaren Möglichkeiten zu geben.

Die Hauptschwierigkeit einer gesetzlichen Regelung eines Rechts auf Information im Bereich des Umweltschutzes wird demnach darin liegen, bei den vielen notwendigen Definitionen und Abgrenzungen noch anschaulich und für den Bürger überschaubar zu bleiben.

11.2
Archivgesetz

11.2.1
Notwendigkeit eines Landesarchivgesetzes

Der von der Bundesregierung vorgelegte Entwurf eines Gesetzes über die Sicherung und Nutzung von Archivgut des Bundes (Bundesarchivgesetz - BArchG) vom 26. März 1985 (Bundestags-Drucks. 10/3072) hat der Diskussion um die Notwendigkeit von Archivgesetzen einen neuen Anstoß gegeben.

In der Vergangenheit habe ich mehrfach auf die Notwendigkeit eines Landesarchivgesetzes hingewiesen (vgl. 10. Tätigkeitsbericht, Ziff. 2.3; 12. Tätigkeitsbericht, Ziff. 4.1; 13. Tätigkeitsbericht, Ziff. 4.1.7). Der Hessische Landtag hat die Forderung aufgegriffen und die Landesregierung gebeten, ihm einen Vorschlag für ein Archivgesetz zu unterbreiten (vgl. Beschluß Nr. 17 zu meinem 12. Tätigkeitsbericht, Drucks. 11/1551 i.V.m. Protokoll der 22. Plenarsitzung vom 5. Juli 1984, S. 1378). Nach wie vor liegt allerdings kein Entwurf vor. Nicht zuletzt im Hinblick darauf kommt für die weitere Diskussion in Hessen dem Entwurf der Bundesregierung besondere Bedeutung zu.

Die Auseinandersetzung um den Gesetzentwurf der Bundesregierung veranlaßt mich, noch einmal an die zentralen Argumente zu erinnern. Dies umso mehr, als der Zusammenhang der Überlegungen zum Archivgesetz mit der Diskussion um Freedom of Information immer deutlicher wird.

Bei der Archivierung geht es auch und gerade um die Aufbewahrung personenbezogener Daten auf Dauer. Dem Betroffenen war und ist aber mit der Archivierung seiner Daten die Möglichkeit genommen, selbst über die weitere Nutzung der sich auf seine Person beziehenden Angaben zu entscheiden. Diese Feststellung ist um so gravierender, als die zweckgebundene und deshalb auch zwangsläufig zeitlich begrenzte Verwendung personenbezogener Daten zu den zentralen Grundsätzen des Datenschutzes zählt. Erinnert sei lediglich an die in jedem Datenschutzgesetz enthaltenen Löschungsvorschriften. "Computer müssen vergessen können", jene Maxime, die den Datenschutz von Anfang an begleitet hat, steht so gesehen in einem grellen Kontrast zu der Lückenlosigkeit eines umfassenden historischen Gedächtnisses.

Spätestens seit der Entscheidung des Bundesverfassungsgerichts zum Volkszählungsgesetz steht nun fest, daß eine derartige Einschränkung des Rechts auf informationelle Selbstbestimmung nur aufgrund einer bereichsspezifischen, mithin eindeutig auf die Archivierung bezogenen Regelung erfolgen darf. Daran mangelt es nach wie vor. Die Abgabe von Unterlagen an die Archive und die Benutzung der Archivalien erfolgt aufgrund von Registraturanweisungen oder Aktenordnungen sowie Benutzungsordnungen. Über die Verarbeitung eindeutig personenbezogener Daten bestimmen also reine Verwaltungsvorschriften. Damit nicht genug: Viele von den Behörden abgegebene Unterlagen enthalten Daten, die besonderen gesetzlich angeordneten Geheimhaltungsvorschriften unterliegen. Steuer- und Sozialdaten sind nur zwei besonders markante Beispiele dafür. Ganz gleich aber, wie man zu der gesetzlich angeordneten Geheimhaltung steht, Ausnahmen davon kann niemand sonst als der Gesetzgeber selbst festlegen.

Ohne Zweifel bereitet nun die gesetzliche Regelung Schwierigkeiten: Der einzelne hat unstreitig ein verfassungsrechtlich garantiertes Interesse an einer für ihn überschaubaren und kontrollierbaren sowie von Anfang an zeitlich begrenzten Verarbeitung der ihn betreffenden Daten. Ebensowenig läßt sich aber übersehen, daß die Funktionsfähigkeit einer demokratischen Gesellschaft von der Publizität der Regierungs- und Verwaltungstätigkeit und damit von einer korrekten und vollständigen Archivierung der Entscheidungsvorgänge abhängt. In der Diskussion über das Archivgesetz wiederholen sich insofern Fragestellungen, wie sie schon aus den Überlegungen zu dem Verhältnis zwischen Datenschutz und wissenschaftlicher Forschung oder auch der Datenschutzgesetze zu den vielfachen Bestrebungen, einen freien Informationszugang sicherzustellen, bekannt sind.

Am Beispiel des Archivgesetzes erweist sich einmal mehr, daß überzeugende Lösungen nur im Rahmen einer Regelung gefunden werden können, die sich an den Grundsätzen einer gesellschaftlich notwendigen und verfassungsrechtlich geforderten Verteilung von Informationen orientiert. So wenig sich freilich eine Einschränkung des Rechts auf informationelle Selbstbestimmung vermeiden läßt, so sehr kommt es darauf an, ihren Anwendungsbereich sowie ihre möglichen Auswirkungen genau zu regeln. Vorweg gilt es soviel zu bedenken: Die veränderten Verarbeitungsmethoden verändern auch radikal das potentielle Archivmaterial. Je mehr Aktenvorgänge automatisiert werden, je mehr also die automatische Verarbeitung zum selbstverständlichen Arbeitsinstrument der öffentlichen Verwaltung wird, desto leichter fällt es, Material aufzubewahren und insoweit auch für eine Archivierung bereitzustellen. Bislang hat es als selbstverständlich gegolten, daß tendenziell die gesamten Unterlagen der öffentlichen Verwaltung auch für eine Archivierung in Betracht kommen müssen. Sollte man diesen Grundsatz so aufrecht erhalten, dann würde mit Rücksicht auf die veränderte Arbeitsweise der Verwaltung das Archivmaterial um ein vielfaches zunehmen. Gerade im Hinblick auf die steigende Informationsverarbeitungskapazität der öffentlichen Verwaltung muß sich der Gesetzgeber die Frage stellen, ob Grenzen bei der Archivierung gezogen werden müssen, und nach welchen Kriterien sie im einzelnen zu bestimmen sind.

Abgesehen davon gibt die Archivierung die Verwendungsschranken in gesellschaftlich besonders sensiblen Bereichen auf und ermöglicht eine weitere Nutzung selbst dort, wo der Gesetzgeber bislang gewollt und gezielt eine Löschung angestrebt hat. Man denke nur an den Bereich der Sicherheitsbehörden oder der Sozialverwaltung. Es kann daher nicht der Sinn eines Archivgesetzes sein, diese wohlüberlegte und für die Funktionsfähigkeit einer demokratischen Gesellschaft unerläßlichen Schranken einfach aufzuheben und eine Information, die nicht mehr zugänglich sein darf, gleichsam zu verewigen.

An diesen beiden Beispielen zeigt sich, wie wichtig im Zusammenhang mit einem Archivgesetz der auch vom Bundesverfassungsgericht ausdrücklich hervorgehobene Grundsatz der funktionalen Trennung ist. Die Archivierung ist keine Verlängerung des Gedächtnisses der Behörden und kein willkommener Ausweg, um unzugängliche Daten doch wieder zugänglich zu machen. Sie ist vielmehr die Herstellung der Öffentlichkeit historischer Akten und Unterlagen. Insoweit stellt das Archivgesetz strenge organisatorische Anforderungen, ohne deren strikte Einhaltung jeder Versuch einer Archivierung von vornherein verfassungswidrig wäre.

Gemessen an diesen Erwartungen bedeutet der Entwurf der Bundesregierung einen entscheidenden Fortschritt gegenüber der bisherigen Lage. Keineswegs nur im Hinblick auf die angestrebte gesetzliche Regelung, sondern auch aus inhaltlichen Gründen. Der Entwurf bringt in Kenntnis der sich aus dem Datenschutz ergebenden Anforderungen eine Regelung, die weitgehend auch den Erwartungen der historischen Forschung Rechnung trägt. Auch wenn zuweilen die öffentliche Diskussion den Eindruck vermittelte, das Archivgesetz würde die Forschung behindern, muß objektiv das Gegenteil festgestellt werden. Gleichwohl bleibt eine Reihe kritischer im Zusammenhang mit jeder Archivregelung zu bedenkender Punkte.

11.2.2
Anonymisierungsproblem

Besonders hinzuweisen ist dabei auf die Anonymisierungsproblematik:

Vor allem gegen die Anonymisierung von Unterlagen vor Abgabe an das Archiv richtet sich die Kritik der historischen Forschung. Dabei bezieht sich dieses Anonymisierungsgebot nur auf solche Unterlagen, die das Archiv nach geltendem Recht überhaupt nicht erhalten dürfte. Diese Unterlagen werden in der Regel von der Ursprungsbehörde vernichtet. Jedenfalls sind sie bisher für die Archive nicht zugänglich gewesen. Diese Form der Anonymisierung bezweckt daher nicht eine Verschlechterung des Datenzugangs, sondern dessen Verbesserung. Allerdings muß genau dargelegt werden, was unter dieser Form von Anonymisierung zu verstehen ist. Auf keinen Fall darf die Authentizität der Archivalien gefährdet werden. Dies versucht § 2 Abs. 3 Ziff. 2 zu gewährleisten: Wird die Archivwürdigkeit durch vorherige Anonymisierung beeinträchtigt, so sind die Unterlagen unverändert zu übergeben, wenn die schutzwürdigen Belange Betroffener auf funktional äquivalente Weise gewahrt werden können. Im übrigen kann im Einvernehmen mit der abgebenden Stelle die Schutzmaßnahme, d.h. auch die Anonymisierung, aufgehoben oder verändert werden. Nach meinem Verständnis kommt daher eine Anonymisierung nur bei Massendaten in Betracht, die besonderen Geheimhaltungsbestimmungen unterliegen und dies auch nur dort, wo nicht andere Maßnahmen den gleichen Schutz gewähren können.

Ein Zensurvorwurf ist in diesem Zusammenhang völlig unangebracht: Schließlich wurde bisher normativ anhand geschichtswissenschaftlicher Kriterien und Prognosen über die Archivwürdigkeit bestimmter Unterlagen entschieden und damit zugleich über die Vernichtung des weitaus überwiegenden Restbestands an Akten irreversibel verfügt. Kurzum: Die Kehrseite der archivischen Tätigkeit ist immer auch die Vernichtung einer großen Anzahl historischer Quellen.

Ganz anders hingegen ist die Frage der Anonymisierung auf Intervention des historisch Betroffenen hin zu beurteilen (§ 4 Abs. 1). Jede solche Regelung stellt letztlich das historische Geschehen zur Disposition der am historischen Prozeß Beteiligten. Ein Ergebnis, das im Hinblick auf die Bedeutung der Archivierung nicht hingenommen werden kann. Für einen angemessenen Schutz des Betroffenen reicht ein Gegendarstellungsrecht aus, das die Authentizität der historischen Quellen unverändert läßt, gleichwohl aber die subjektive Sicht des Beteiligten als zusätzlichen Gesichtspunkt garantiert.

Bleibt die Frage der Anonymisierung bei der Benutzung von Archivmaterial vor Ablauf der Sperrfristen zu betrachten (§ 5 Abs. 4). Dabei geht es nicht um die Veränderung der historischen Quelle, sondern um die Bedingungen, unter denen im Hinblick auf die Bedeutung der wissenschaftlichen Forschung die Nutzung von an und für sich unzugänglichen Unterlagen ermöglicht werden soll. Mit Rücksicht auf die Situation der Betroffenen ist hier eine Verkürzung der Information hinzunehmen, entweder durch die Beschränkung auf Auszüge oder die Unkenntlichmachung von Namen. Auch dies ist letztlich nichts Neues. Ähnliche Verfahren sind schon lange vor Inkrafttreten der Datenschutzgesetze praktiziert worden.

Eine gesetzliche Regelung muß - im Gegensatz zum Entwurf - Bestimmungen über die Übernahme automatisierter Dateien oder Datenbanken enthalten; schon deshalb, weil beide die Eigenschaft haben, nicht zu veralten. Automatisierte Dateien und Datenbanken werden im Prinzip ständig aktualisiert und bereinigt. Die Funktionsweise moderner Informationssysteme hat also zur Folge, daß keine historischen Quellen wie bei den mit Akten arbeitenden traditionellen Verwaltungen entstehen können. Notwendig sind also Bestimmungen darüber, wie der aktuelle Status einer Datenbank zu einem bestimmten Stichtag an ein Archiv abgegeben werden kann und dort den Schutzvorkehrungen der Datenschutzgesetze entsprechend aufzubewahren ist.

Eine solche Regelung wäre allerdings undenkbar ohne eine starke Betonung der funktionellen Trennung von Archiven und öffentlicher Verwaltung. Damit ist zunächst weniger eine institutionelle Trennung angesprochen, als eine Einschränkung der Benutzung aller Unterlagen für die Behörden, bei denen das Archivgut entstanden ist. Die Verwaltung muß, jedenfalls solange es sich nicht um eine Zwischenlösung handelt, allen anderen Benutzern gleichgestellt werden.

12. Parlamentsinformation

Die Forderung des HDSG, das Informationsgleichgewicht sicherzustellen, trifft ohne Zweifel den Kern des parlamentarischen Selbstverständnisses. Wenn und soweit die parlamentarische Arbeit Kritik und Auseinandersetzung mit der Regierungspolitik ist, dann gerät diese Aufgabe dort zur Illusion, wo das Parlament nicht auch über die Informationsgrundlagen verfügt, die Inhalt und Ziele der von der Regierung angestrebten Entscheidung bestimmen. Insofern spricht in der Tat zunächst alles dafür, das Problem einer kontinuierlichen und verläßlichen Information des Parlaments zunächst einmal unter dem Gesichtspunkt des Informationsgleichgewichts anzugehen. Und ebensowenig überraschen die Widerstände und Schwierigkeiten, die in dem Augenblick zutage traten, in dem das Parlament mit seinem gesetzlich abgesicherten Anspruch, an den der Regierung zur Verfügung stehenden Informationen beteiligt zu werden, Ernst machte. Es genügt, an die sofort geäußerte Erwartung der Regierung zu erinnern, wenn schon die Datenbestände zugänglich gemacht werden sollten, dann doch sofort und genau über den Inhalt und das Ziel der jeweiligen Anfrage unterrichtet zu werden.

Doch die Intensität der seinerzeitigen Diskussion steht, so viel läßt sich heute feststellen, in keinem Verhältnis zu ihrem Ergebnis. Genaugenommen ist es bei den damaligen mehr prinzipiellen Überlegungen geblieben, keineswegs also zu einer ebenso kontinuierlichen wie konsequenten Inanspruchnahme der Information durch das Parlament gekommen. Insofern liegt es nahe, zu fragen, was denn eigentlich die Abgeordneten zu dieser Zurückhaltung veranlaßt. Die Frage ist um so berechtigter, als ähnliche Erfahrungen aus einem ganz anderen Bereich vorliegen. Fast gleichzeitig mit dem Aufbau der staatlichen Datenbanken haben auch die Bemühungen eingesetzt, ein eigenes Parlamentsinformationssystem zu entwickeln, das vor allem dazu verhelfen sollte, auf die mit der parlamentarischen Arbeit zusammenhängenden Informationen jederzeit zurückzugreifen. Der Hessische Landtag verfügt mittlerweile über alle Voraussetzungen dazu. Wiederum steht aber die Benutzungsfrequenz in keinem Verhältnis zu den Erwartungen, die mit dem System ausdrücklich verknüpft worden sind, eine Feststellung, die übrigens keineswegs nur für Hessen zutrifft.

Eines ändert sich trotzdem nicht: Das Ziel, den Abgeordneten zu ermöglichen, alle für ihre Arbeit erforderlichen Informationen zu bekommen, bleibt richtig. Nur läßt es sich offensichtlich auf dem bisher eingeschlagenen Weg nicht erreichen. Insofern überrascht es nicht, wenn, wie sich an der Entwicklung in den Vereinigten Staaten, seit kurzem aber auch an den im Bundestag angestellten Überlegungen zeigt, der Akzent sich mehr und mehr auf die Arbeitsbedingungen der Abgeordneten verschiebt. Damit ist zunächst eine wirklich genaue Auseinandersetzung mit den konkreten Informationserwartungen der Abgeordneten gemeint. Statt ihnen also abstrakt den Zugang zu bestimmten Informationen anzubieten, gilt es sich zunächst einmal zu vergewissern, was denn eigentlich in Kenntnis ihrer Erfahrungen und unter Berücksichtigung der Besonderheiten ihrer Arbeit aus ihrer Perspektive an Informationen notwendig erscheint. Konkret: Sicherlich bereitet es technisch letztliche keine Schwierigkeiten, den Abgeordneten einen direkten Zugang zu den verschiedensten, längst automatisierten Fachinformationssystemen zu verschaffen. Die Liste ist lang und eindrucksvoll, und genausowenig läßt sich die Bedeutung dieser Systeme bestreiten. Doch daraus folgt noch lange nicht, daß sie auch für die Abgeordneten von unmittelbarem Interesse sind. So imponierend die Vernetzung einer ständig steigenden Zahl von vor allem naturwissenschaftlichen Datenbanken auch sein mag, so wenig kommt es darauf an, den Abgeordneten die vielfältigen Chancen einer konsequent genutzten Informationstechnik zu demonstrieren, einen Eindruck, den man unweigerlich bekommt, schaut man sich die im Bundestag diskutierten Unterlagen näher an.

Entscheidend kann und darf vielmehr allein der Zugang zu einer bestimmten, von vornherein beschränkten, eindeutig parlamentsspezifischen Information sein. Insofern traf und trifft es zu, daß die Informationsinteressen der Abgeordneten primär auf politisch-administrative, in aller Regel von der öffentlichen Verwaltung verarbeitete Daten gerichtet sind.

Hinzu kommt eine weitere Überlegung: So offensichtlich sich die Informationserwartungen der Abgeordneten zunächst an der parlamentarischen Arbeit überhaupt orientieren, so wenig lassen sie sich von der engen Verbindung der Abgeordneten zu ihrem Wahlkreis trennen. Wenn deshalb Überlegungen zur Inanspruchnahme der durch die Informationstechnik gebotenen Möglichkeiten durch die Abgeordneten einen Sinn haben sollen, dann nur unter einer doppelten Voraussetzung: Zum einen kommt es entscheidend darauf an, ob und in welchem Umfang die jeweils zugänglichen Daten in wahlkreisbezogene Informationen umgesetzt werden können, zum anderen erscheint es genauso wichtig, die Informationstechnik zu nutzen, um die Kommunikation mit dem Wahlkreis zu verbessern, also auch und vor allem die aus dem Wahlkreis eingehenden Informationen unmittelbar und konsequent zu verarbeiten.

Je deutlicher sich aber die Überlegungen auf die spezifischen Informationsinteressen des Abgeordneten konzentrieren, desto klarer wird auch, daß seine Arbeitsbedingungen der Schlüssel zu einer wirklichen Inanspruchnahme der Informationsmöglichkeiten sind. So trivial es auch klingen mag: Niemandem ist letztlich mit einem noch so perfekten Informationssystem und einem noch so offenen Zugang zu den jeweils gewünschten Daten genutzt, solange der Abgeordnete nicht an seinem Arbeitsplatz oder jedenfalls in dessen unmittelbarer Nähe über einen Anschluß verfügt und die Daten möglichst selbst und ohne technische Komplikationen bekommen kann.

Ehe deshalb weitere komplizierte Betrachtungen über den Inhalt und den Nutzen von Informationssystemen angestellt werden, gilt es alle Aufmerksamkeit auf eine verläßliche Arbeitsplatzanalyse zu richten. Ihr Ziel muß es sein, eine technische Infrastruktur zu schaffen, die von der Textverarbeitung bis zum Zugriff auf die für die parlamentarische Arbeit relevanten Daten reicht. Zugespitzt formuliert, statt in den höheren Sphären abstrakter Reflexion über die Bedeutung der Information und die Fortschritte der Informationstechnik zu verharren, gilt es sich zunächst einmal in die Niederungen der alltäglichen Arbeit und ihrer Erschwernisse zu begeben. Wohlgemerkt, keineswegs geht es darum, Neuland zu betreten. Es gibt durchaus eine ganze Reihe konkreter Überlegungen, die in diese Richtung weisen, und auch an ersten Erfahrungen fehlt es nicht. Beides gilt es zu verwerten. Nur dann kann es letzlich gelingen, die Realität parlamentarischer Arbeit mit der Forderung des Gesetzes nach Informationsgleichgewicht in Einklang zu bringen.

13. Bilanz

13.1
Beschlüsse des Hessischen Landtags zum 13. Tätigkeitsbericht

Die Arbeitsgruppe "Datenschutz und Datenverarbeitung" des Innenausschusses des Hessischen Landtags hat auf ihren Sitzungen vom 17. September und vom 12. November 1985 den 13. Tätigkeitsbericht diskutiert und Beschlußempfehlungen formuliert. Diese lagen dem Innenausschuß auf seiner Sitzung vom 13. November vor und wurden dort als Beschlußempfehlungen an das Plenum des Parlaments verabschiedet. Der Landtag schließlich hat am 14. November zu den folgenden Punkten Beschlüsse gefaßt (vgl. Beschlußempfehlung und Bericht des Innenausschusses, Drucks. 11/4696 i.V.m. Nr. 9 des Beschlußprotokolls der 63. Plenarsitzung vom 14. November 1985):

13.1.1
Zu Ziff. 2.2.2 "Ausschluß vom Schöffenamt aufgrund pauschaler Datenübermittlung"

Ein Bewerber um das Amt eines Schöffen war aufgrund einer Mitteilung der Polizei abgelehnt worden, die sich auf ein eingestelltes Ermittlungsverfahren aus dem Jahr 1966 bezog und im polizeilichen Informationssystem (HEPOLIS) längst hätte gelöscht sein müssen. Dieser Fall war für mich Anlaß, zum wiederholten Mal zu kritisieren, daß die Bereinigung der Aktensammlungen und Datenbestände der Polizei nicht ausreichend und rechtzeitig erfolgt. Zu bemängeln war auch, daß die Polizei pauschal ihre Erkenntnisse auch dann übermittelt, wenn sie mit den persönlichen Voraussetzungen für die Ernennung zum Schöffen nichts zu tun haben.

Der Landtag hat hierzu folgenden Beschluß gefaßt:

"1. Die Landesregierung wird um Auskunft darüber gebeten, wie der gegenwärtige Stand der Aussonderung nicht mehr aktueller Datenbestände der kriminalpolizeilichen Sammlungen ist, welche organisatorischen Vorkehrungen getroffen sind, um die Übermittlung nicht mehr aktueller Daten zu verhindern, welchen finanziellen und organisatorischen Aufwand es erfordern würde, alle bei den Polizeibehörden gespeicherten Daten hinsichtlich der Löschungsfristen dem gesetzlichen Stand anzupassen."

Durch Erlaß vom 27. November 1985 hat der Innenminister nunmehr angeordnet, daß die Polizei in Zukunft nur noch solche Daten übermittelt, die einer Ernennung zum Schöffen tatsächlich entgegenstehen.

13.1.2
Zu Ziff. 2.2.3 "Sicherheitsüberprüfungen durch den Verfassungsschutz: Mangelnde Transparenz für den Betroffenen"

Ich hatte darüber berichtet, daß die Bewerbung einer Studentin um ein Praktikum in einer Justizvollzugsanstalt aufgrund von Erkenntnissen des Verfassungsschutzes bei der Sicherheitsüberprüfung abgelehnt worden war, ohne daß die Betroffene zu den Ablehnungsgründen ordnungsgemäß gehört worden war. In diesem Zusammenhang hatte ich eine gesetzliche Regelung der Sicherheitsüberprüfung gefordert, die eine rechtsstaatliche und für den Betroffenen transparente Verfahrensweise gewährleistet. Diese gesetzliche Regelung gehört in das zu novellierende Verfassungsschutzgesetz, das die Befugnisse der Verfassungsschutzbehörden bei der Erhebung und Verwendung personenbezogener Informationen präzise festlegen soll.

Der Hessische Landtag hatte schon anläßlich der Beratung meines 12. Tätigkeitsberichts die Landesregierung gebeten, bis zum Frühjahr 1985 den Entwurf für bereichsspezifische Datenschutzregelungen für diesen Nachrichtendienst vorzulegen, um damit die Konsequenz aus dem Regelungsauftrag des Bundesverfassungsgerichts im "Volkszählungs-Urteil" vom 15. Dezember 1983 zu ziehen (vgl. Nr. 3 der Beschlußempfehlung des Innenausschusses, Drucks. 11/1551 i.V.m. Protokoll der 22. Plenarsitzung vom 5. Juli 1984, S. 1378). Einen solchen Entwurf hat die Landesregierung aus verschiedenen Gründen bis heute nicht erarbeitet.

Der Landtag hat daher folgenden Beschluß zu diesem Thema gefaßt:

"2. Die Landesregierung wird erneut gebeten, so bald wie möglich einen Entwurf für bereichsspezifische Datenschutzregelungen im Verfassungsschutzgesetz vorzulegen.

Der Landtag geht davon aus, daß im Zusammenhang mit der Novellierung des Verfassungsschutzgesetzes auch die Regelung der Sicherheitsüberprüfung überarbeitet wird.

Die Landesregierung wird gebeten, über den Stand der Diskussion der Novellierung des Bundesverfassungsschutzgesetzes und über ihre Bewertung der bisher vorhandenen Vorlagen und ihre entsprechenden Initiativen zu berichten."

13.1.3
Zu Ziff. 3.3.1 "Bildschirmtext"

Die Deutsche Bundespost weigert sich nach wie vor, die in Art. 9 des Staatsvertrags über den Bildschirmtext (GVBl. I 1983, 91) enthaltenen Datenschutzregelungen für die Teilnehmer an diesem Postdienst in entsprechende bundesrechtliche Rechtsvorschriften zu übernehmen, wie es die Datenschutzbeauftragten der Länder für notwendig halten. Insoweit ist der Sachstand gegenüber den Ausführungen im letzten Tätigkeitsbericht bis heute unverändert. Auch der im Dezember vorgelegte Entwurf für eine Telekommunikationsordnung (vgl. oben Ziff. 7.1) enthält insoweit keine neuen Gesichtpunkte. Eine Reihe von Mängeln und Defiziten bei der Datensicherung von Bildschirmtext hat die Deutsche Bundespost zum Anlaß genommen, bestimmte Verfahren zu ändern und sie bei der anstehenden Softwareumstellung zu berücksichtigen.

Im Hinblick auf die rechtlich nach wie vor unbefriedigende Situation hat der Landtag folgenden Beschluß gefaßt:

"3. Die Landesregierung wird um eine erneute Stellungnahme gebeten, welche rechtlichen Schritte zur Verwirklichung eines wirksamen Datenschutzes im Bereich Bildschirmtext möglich und geboten sind."

13.1.4
Zu Ziff. 3.2.2 "Volkszählung" und Ziff. 4.1.6 "Landes- und Kommunalstatistik"

Das neue "Volkszählungsgesetz 1987" ist am 15. November 1985 in Kraft getreten (vgl. BGBl. I, S. 2078). Es berücksichtigt weitgehend die verfassungsrechtlichen Vorgaben des "Volkszählungs-Urteils" vom 15. Dezember 1983 (vgl. zum VZG '87, insbesondere zu den verbleibenden Kritikpunkten, im einzelnen in diesem Bericht Ziff. 5.3.1). In den o.a. Abschnitten meines letzten Tätigkeitsberichts hatte ich erneut meine Auffassung unterstrichen, daß eine verfassungsgemäße Durchführung der nächsten Volkszählung mit der gründlichen Novellierung des einschlägigen Bundesgesetzes allein nicht gewährleistet werden kann. Die organisatorische und personelle "Abschottung" der Erhebungsstellen (vgl. § 9 VZG '87) ebenso wie der kommunalen Statistikämter - wenn sie Einzelangaben aus der Volkszählung erhalten wollen (vgl. § 14 VZG '87) - bedingt das Vorhandensein landesrechtlicher Rechtsvorschriften für die Landes- und Kommunalstatistik.

Über die Erforderlichkeit eines Landesstatistikgesetzes besteht prinzipiell Konsens; die Landesregierung hat diese Frage bereits in ihrem Bericht vom 30. Oktober 1984 an den Landtag (vgl. dessen Prüfauftrag in Beschluß Nr. 5 zu meinem 12. Tätigkeitsbericht, Drucks. 11/1551 i.V.m. Protokoll der 22. Plenarsitzung vom 5. Juli 1984, S. 1378) ebenfalls bejaht. Dagegen bestanden zwischen der Landesregierung und mir unterschiedliche Vorstellungen darüber, zu welchem Zeitpunkt dieses Gesetz verabschiedet sein muß. Der Landtag hat sich meiner Position angeschlossen, daß dies vor Durchführung der Volkszählung geschehen muß und kein zeitlicher Spielraum bis zur voraussichtlichen Übermittlung von Ergebnissen aus der Zählung an die Kommunen besteht (so aber die Landesregierung in ihrer Stellungnahme zu meinem 13. Tätigkeitsbericht, Drucks. 11/3951, S. 13).

Der Beschluß des Landtags lautet wie folgt:

"4. Der Landtag bittet die Landesregierung, ihm baldmöglichst den Entwurf für ein Landesstatistikgesetz vorzulegen.

Der Landtag ist der Auffassung, daß aufgrund des Urteils des Bundesverfassungsgerichts zur Volkszählung landesgesetzliche Regelungen über die Landes- und Kommunalstatistik auf jeden Fall vor Durchführung der Volkszählung erforderlich sind.

Der Landtag bittet die Landesregierung darum, bis Ende dieses Jahres einen Bericht über den derzeitigen Stand um den weiteren Ablauf der Organisation der Volkszählung, insbesondere auf Gemeindeebene, vorzulegen."
Der Bericht der Landesregierung liegt noch nicht vor.

13.1.5
Zu Ziff. 3.2.3 "Mikrozensus"

Mein hauptsächlicher Kritikpunkt am Mikrozensus war und ist die bußgeldbewehrte Auskunftspflicht der für die Befragung ausgewählten Bürger (vgl. bereits meine Ausführungen im 9. Tätigkeitsbericht, Ziff. 2.3.3). Meine Bedenken habe ich auch am 25. Februar 1985 bei einer Anhörung im Deutschen Bundestag zum Entwurf des neuen Mikrozensusgesetzes (Bundestags-Drucks. 10/2600) vorgetragen und begründet. Das "Gesetz zur Durchführung einer Repräsentativstatistik über die Bevölkerung und den Arbeitsmarkt" ist am 14. Juni 1985 in Kraft getreten (vgl. BGBl. I, S. 955) und war Grundlage für die anschließend durchgeführte Erhebung. Das neue Gesetz hält prinzipiell an der Auskunftspflicht fest; davon sind einige Angaben ausgenommen, deren Mitteilung freiwillig ist. Darüber hinaus sind Testerhebungen mit freiwilliger Auskunftserteilung vorgesehen, um beispielhaft zu prüfen, ob künftig nicht generell bei Bundesstatistiken auf den Auskunftszwang verzichtet werden kann. Der Deutsche Bundestag hat diese Zielsetzung in einer Entschließung vom 14. Mai 1985, die mit der Verabschiedung des Mikrozensusgesetzes gefaßt wurde, wie folgt formuliert:
"2.1 Die im vorliegenden Mikrozensusgesetz enthaltenen freiwilligen Befragungsteile (Angaben zum Eheschließungsjahr, zu Urlaubs- und Erholungsreisen sowie zur Gesundheit) sind ein wichtiger Schritt für die methodische Weiterentwicklung der Bundesstatistik.

Der eingeschlagene Weg, Bevölkerungsbefragungen als Bundesstatistiken auf freiwilliger Grundlage durchzuführen, sollte konsequent mit dem Ziel fortgesetzt werden, die Freiwilligkeit der Beantwortung möglichst auf alle Sachverhalte zu erstrecken" (vgl. Bundestags-Drucks. 10/3328).

Der Landtag hat beschlossen, sich dieser Position anzuschließen (Beschluß Nr. 5). Ein ergänzender Antrag der F.D.P.-Fraktion, die Auskunftspflicht als angemessenes Mittel zur Gewinnung statistischer Erkenntnisse zu bezeichnen, wurde abgelehnt (vgl. Drucks. 11/4696, S. 3 lit. a).

13.1.6
Zu Ziff. 4.1.4 "Hinweis- und Spurendokumentationssysteme"

Zum wiederholten Mal mußte ich im letzten Tätigkeitsbericht kritisieren, daß die Verwendung von Hinweis- und Spurendokumentationssystemen (HIDOK bzw. SPUDOK) in der polizeilichen Ermittlungsarbeit zur überlangen Datenspeicherung, insbesondere von unbeteiligten Personen, führt. Schon bei den Beratungen zu meinem vorletzten Tätigkeitsbericht hatte der Landtag die Landesregierung gebeten, derartige Systeme nur aufgrund jeweils spezieller Errichtungsanordnungen zu betreiben und dabei eine ständige Überprüfung und Bereinigung der Datenbestände vorzusehen (vgl. Beschluß Nr. 9 zum 12. Tätigkeitsbericht, Drucks. 11/1551 i.V.m. Protokoll der 22. Plenarsitzung vom 5. Juli 1984, S. 1378).

In ihrer Stellungnahme zum 13. Tätigkeitsbericht hat die Landesregierung Entwürfe für Errichtungsanordnungen vorgelegt. Diese Entwürfe bringen einige datenschutzrechtliche Verbesserungen, sie lösen jedoch die von mir dargelegten zentralen Probleme nicht. Zudem enthält die Antwort der Landesregierung keine präzisen Informationen über die Einsatzplanungen und die zukünftigen Anwendungsstätten dieser Systeme, so daß die praktischen Konsequenzen der vorgelegten Entwürfe nicht hinreichend klar sind (vgl. Drucks. 11/3951, S. 23 ff).

Der Landtag hat hierzu folgenden Beschluß gefaßt:

"6. Der Landtag bittet den Datenschutzbeauftragten, zu den Errichtungsanordnungen HIDOK und SPUDOK eine Stellungnahme vorzulegen.

Die Landesregierung wird gebeten, über den derzeitigen und zurückliegenden Einsatz der Systeme HIDOK und SPUDOK sowie über deren zukünftige Anwendungsbereiche aufgrund der vorgelegten Errichtungsanordnungen zu berichten".

13.1.7
Zu Ziff. 4.1.3 "PIOS-Datei 'Staatsgefährdung'" bzw. "Innere Sicherheit" (APIS)

Die Errichtungsanordnung für die "Arbeitsdatei PIOS-Innere Sicherheit" - APIS - (zunächst war die Datei PIOS-"Staatsgefährdung" bezeichnet worden), die bundesweit beim Bundeskriminalamt geführt wird und über die Daten der bisherigen PIOS-Datei "Terrorismus" hinaus erhebliche weitere Bereiche des polizeilichen Staatsschutzes umfassen soll, liegt seit dem letzten Jahr vor. Die Hessische Landesregierung hat dieser Errichtungsanordnung bisher als einzige nicht zugestimmt. Motiv war u.a. der Beschluß des Landtags zu meinem 12. Tätigkeitsbericht, die Landesregierung um einen Bericht zum Ausbaustand und zur Planung von APIS sowie darum zu bitten, dabei auf meine geäußerten Bedenken einzugehen.

Schwerpunkt meiner Kritik ist zum einen die grundsätzliche Konzeption der Datei. Die Notwendigkeit einer Erweiterung der bisherigen Datei PIOS-Terrorismus auf nahezu den gesamten Bereich des Staatsschutzes ist bisher nicht überzeugend dargelegt worden (s. hierzu auch Ziff. 4.1.2). Zum anderen richtet sich meine Kritik gegen die unklare Festlegung des einzuspeichernden Personenkreises (Hintermann, Mitglied, Unterstützer, sog. "andere Personen") in Verbindung mit dem vage definierten Katalog von in Betracht kommenden Straftaten. Dabei geht es vor allem um die Ziff. 2.1.10 der Errichtungsanordnung, wonach auch Bagatelldelikte bzw. deren Täter gespeichert werden können, sofern nur "die Angriffsrichtung" oder "das Motiv" des Delinquenten den Verdacht einer Zielsetzung im terroristischen oder "staatsgefährdenden" Bereich wecken. Ferner erscheinen mir die vorgesehenen Speicherungsfristen zu lang. Mit Schreiben vom 8. Oktober 1985 hat mir der Innenminister mitgeteilt, daß er meine Bedenken hinsichtlich der zuletzt genannten drei Punkte teilt und sich für eine Abänderung der Errichtungsanordnung einsetzen wird. Zufriedenstellende Lösungsvorschläge liegen mir nicht vor.

Der Landtag hat sich meinen Einwänden angeschlossen und folgenden Beschluß gefaßt:

"8. Der Landtag stellt aufgrund des derzeitigen Beratungsstandes in der Innenministerkonferenz fest, daß die bisher erhobenen Bedenken gegen die Errichtungsanordnung zur Arbeitsdatei PIOS- Innere Sicherheit (APIS) fortbestehen."

Die F.D.P.-Fraktion hatte einen weniger weitgehenden Antrag vorgelegt, nachdem die Landesregierung unverzüglich der APIS-Errichtungsanordnung zustimmen solle, wegen der berechtigten Bedenken zu Ziff. 2.1.10 (s.o.) bis zur Konkretisierung dieses Punktes keine Daten zu "anderen Straftaten" im Sinne dieser Ziffer in die APIS-Datei eingeben solle.

Dieser Antrag wurde von der Landtagsmehrheit abgelehnt.

13.2
Sonstige Bereiche

13.2.1
Studentendaten (13. Tätigkeitsbericht, Ziff. 2.4.2)

Die auch von der Landesregierung nicht bestrittene Notwendigkeit, die Verarbeitung von Studentendaten und deren Umfang gesetzlich zu regeln, hat über die entsprechenden Erklärungen hinaus keine Tätigkeit des Verordnungsgebers, geschweige denn des Gesetzgebers, zur Folge gehabt. Diese Untätigkeit kann schwerwiegende administrative Probleme für die Hochschulen des Landes nach sich ziehen, zumal dann, wenn die bisherige Praxis der Verarbeitung von Studentendaten einer gerichtlichen Überprüfung unterworfen würde. Ich selbst habe in der Vergangenheit immer wieder auf die rechtliche Problematik hingewiesen und im Vertrauen auf die vom Minister für Wissenschaft und Kunst zugesagte Initiative bisher davon abgesehen, Beanstandungen auszusprechen. Nach dem Volkszählungsurteil des Bundesverfassungsgerichts vom 15. Dezember 1983 ist eine gesetzliche Regelung unabweisbar geworden und zwischenzeitlich auch vordringlich.

13.2.2
Gebührenpflicht für Auskunft (13. Tätigkeitsbericht, Ziff. 2.5)

Wenn Behörden den Bürgern, die bei ihnen eine Datenauskunft beantragen, dafür eine Gebühr abverlangen, wirkt sich dies als Hemmnis für die Geltendmachung der Informations- und ggf. Berichtigungsrechte des einzelnen ebenso wie für die notwendige Transparenz von Datenspeicherungen und Datenflüssen im allgemeinen aus. Das Hessische Datenschutzgesetz erklärt die Auskunftserteilung deshalb für kostenlos (§ 18 Abs. 4 HDSG). Doch unterliegen nicht alle öffentlichen Stellen der Landes-, der Kommunal- und der Sozialverwaltung den Regelungen des HDSG, sondern einige - zumindest teilweise - denen des Bundesdatenschutzgesetzes (BDSG). Das BDSG ist jedoch in diesem Punkt weniger bürgerfreundlich; es erlaubt sowohl den (Bundes-) Behörden als auch den privaten Unternehmen, Vereinen usw., eine Gebühr bzw. ein Entgelt für die Auskunft zu erheben (vgl. § 13 Abs. 4 und § 26 Abs. 3 BDSG).

Anhand zweier Beispielsfälle hatte ich im letzten Tätigkeitsbericht (Ziff. 2.5) auf solche Relikte der Gebührenpflicht auch in Hessen aufmerksam gemacht. Für beide Fälle lassen sich positive Lösungen vermelden. Die formal noch bestehende Entgeltlichkeit der Auskunft an die Beschäftigten in hessischen öffentlichen Dienststellen (Ziff. 2.5.1) soll bei der anstehenden Novellierung des HDSG abgeschafft werden. Nach dem Gesetzentwurf der Landesregierung für ein Hessisches Datenschutzgesetz (Drucks. 11/4749 vom 26. November 1985) wird der Datenschutz bei Dienst- und Arbeitsverhältnissen künftig im HDSG selbst und nicht mehr durch Verweisung auf das BDSG geregelt (§ 34 des Entwurfs). Damit greift auch für die Arbeitnehmerauskunft die in § 18 festgelegte Gebührenfreiheit.

Zum zweiten Fall (Ziff. 2.5.2): Die Landesversicherungsanstalt Hessen hat mir inzwischen mitgeteilt, daß künftig sowohl sie wie auch die übrigen Rentenversicherungsträger auf die nach § 13 Abs. 4 BDSG mögliche Erhebung einer Auskunftsgebühr verzichten werden. Damit ist in einem großen Bereich der Sozialverwaltung die Kostenlosigkeit der Auskunft an den Bürger klargestellt.

Doch kann diese - sicherlich begrüßenswerte - freiwillige Selbstbeschränkung einiger großer Sozialversicherungsträger insgesamt nicht befriedigen. Vielmehr gehört - das habe ich zu wiederholten Malen gefordert - die Gebührenpflicht auch im BDSG endgültig abgeschafft, was sich im übrigen nach dem derzeitigen Vorbereitungsstand der überfälligen BDSG-Novellierung inzwischen abzeichnet. Wird die Gebührenpflicht in § 13 Abs. 4 BDSG gestrichen, entfällt sie darüber hinaus für alle Sozialleistungsträger auch auf Landes- und kommunaler Ebene, für die derzeit noch wegen der Verweisung in § 79 Abs. 1 und 3 SGB X diese Bestimmung Gültigkeit hat.

13.2.3
TEMEX (13. Tätigkeitsbericht, Ziff. 3.1.2)

Mit dem TEMEX-Dienst der Deutschen Bundespost ist das Fernwirken und Fernmessen im einzelnen Haushalt über das Telefonnetz möglich. Die Datenschutzbeauftragten sind übereinstimmend der Auffassung, daß die datenschutzrechtlichen Probleme dieses technischen Systems, das Messungen und Beobachtungen in einer Wohnung von außen erlaubt, eine bereichsspezifische gesetzliche Regelung für den Einsatz von TEMEX zwingend erfordern. Meinen im letzten Tätigkeitsbericht gemachten Vorschlag, eine entsprechende Norm in die Novelle zum Hessischen Datenschutzgesetz aufzunehmen, hat die Landesregierung aufgegriffen (vgl. § 36 des Entwurfs, Drucks. 11/4749). Im Hinblick auf die technische Datensicherung bei TEMEX bleiben die Ergebnisse von Betriebs- und Systemversuchen in verschiedenen Bundesländern abzuwarten, die von einer Arbeitsgruppe der jeweils zuständigen Landesdatenschutzbeauftragten gemeinsam mit dem Bundesbeauftragten für den Datenschutz begleitet und ausgewertet werden.

13.2.4
Der maschinenlesbare Personalausweis (13. Tätigkeitsbericht, Ziff. 3.5.3)

In den beiden letzten Tätigkeitsberichten (12. Tätigkeitsbericht Ziff. 3.1, 13. Tätigkeitsbericht Ziff. 3.5.3) habe ich mich ausführlich mit der geplanten Einführung eines maschinenlesbaren Personalausweises beschäftigt und dabei auf einige grundsätzliche Bedenken gegen dessen Einführung hingewiesen:

1. Ein Grund, warum der Ausweis in maschinenlesbarer Form eingeführt werden soll, ist bisher nicht hinreichend dargetan. Eine Beschleunigung und Vermehrung der Kontrollen im Inland und an den Grenzen könnte das einzige Motiv sein. Weder der Bundesinnenminister noch die Innenbehörden der Länder haben jedoch bisher in ausreichendem Umfang dargelegt, inwieweit der Ausweis dafür in Zukunft genutzt werden soll, zumal allem Anschein nach das Bestreben, Grenzkontrollen abzubauen, im Vordergrund politischer Überlegungen steht.

2. In Übereinstimmung mit meinen Kollegen der Länder und des Bundes habe ich gefordert, daß die Verwendung des Ausweises durch die Sicherheitsbehörden an die Schaffung bereichsspezifischer Vorschriften für die personenbezogene Datenverarbeitung bei den Sicherheitsbehörden zu knüpfen ist. Für einen konsequenten Datenschutz können dabei bloße Entwürfe nicht ausreichen.
   Die Datenschutzbeauftragten haben immer wieder betont, und der Bundestag hat dies in seiner Entschließung anläßlich der Verabschiedung des Personalausweisgesetzes am 17. Januar 1980 aufgegriffen (vgl. Bundestags-Drucks. 8/3498), daß es entscheidend darauf ankommt, daß zum Zeitpunkt der Einführung des maschinenlesbaren Ausweises die durch die Benutzung des Ausweises auftretenden Gefahren durch gezielte gesetzliche Regelungen aufgefangen sind.

3. Außerdem habe ich kritisiert, daß die Verwendung des Ausweises nicht klar auf den Bereich der Identitätsüberprüfung durch die Polizei beschränkt ist. So besteht die Gefahr, daß die Personalausweisregister zu "Parallelmelderegistern" entwickelt und einer Vielzahl von öffentlichen Stellen als Auskunftsquelle dienen werden. Damit ist die Zweckbindung der für die Erstellung und Verwaltung des Ausweises gespeicherten Daten nicht gewährleistet.

4. Ein weiterer wichtiger Einwand ergab sich daraus, daß der Ausweis zur Einrichtung oder Erschließung polizeilicher Dateien maschinell gelesen werden darf, soweit diese für die "Fahndung aus Gründen der Strafverfolgung und der Gefahrenabwehr durch die hierfür zuständigen Behörden betrieben werden". Zu kritisieren war hier, daß die in der Gesetzesformulierung verwendeten Begriffe unklar und präzisierungsbedürftig sind, insbesondere aber auch die Speicherung sogenannter Negativanfragen, d.h. Anfragen, die keine Anzeichen für eine Belastung des betroffenen Bürgers aufgrund bereits über ihn gespeicherter Daten ergeben haben, für bestimmte Fallkonstellationen ohne klare Begrenzung zugelassen werden soll.

Die seitherige Diskussion hat meine Bedenken nicht zerstreut. Die nunmehr von den Koalitionsparteien beschlossene Fassung des Personalausweisgesetzes läßt Tendenzen erkennen, die die Bedenken noch verschärfen. Das gilt insbesondere für die faktische Auflösung des Junktims: fertige Begleitgesetze für die Datenverarbeitung im Sicherheitsbereich werden nicht mehr vorausgesetzt; die bloßen Gesetzentwürfe sollen schon ausreichen. Dieses Ergebnis wäre umso bedenklicher, als - wie in den jüngsten Entwürfen geplant - spätere Sonderregelungen für den automatisierten Abruf und die Speicherung personenbezogener Daten durch die Polizei zulässig sein sollen.

13.2.5
Das Zentrale Verkehrsinformationssystem des Kraftfahrtbundesamtes (ZEVIS) (13. Tätigkeitsbericht, Ziff. 3.5.4)

Der in meinem 13. Tätigkeitsbericht erörterte Entwurf einer Änderung des Straßenverkehrsgesetzes, mit dem das Zentrale Verkehrsinformationssystem (ZEVIS) des Kraftfahrtbundesamtes sowie die Datenverarbeitung bei den Kraftfahrzeugzulassungsstellen auf eine bereichsspezifische Rechtsgrundlage gestellt werden sollen, hat noch zu keiner endgültigen Regelung geführt. Auch in diesem Zeitraum legte der Bundesverkehrsminister eine Reihe von Neufassungen dieses Entwurfs vor, ohne daß darin eine grundsätzliche Neuorientierung zu erkennen wäre. Offensichtlich hält die Bundesregierung an der Grundkonzeption des Informationssystems fest. Die in meinem 13. Tätigkeitsbericht geltend gemachten Bedenken - insbesondere die weitgehenden Zugriffsmöglichkeiten der Polizei auf dieses System, die mangelnde Zweckbindung der Straßenverkehrsregister und die umfassende Nutzung auch durch Nachrichtendienste und Justizbehörden - bestehen weitgehend fort.

Lediglich die Bestrebungen, im zentralen Fahrzeugregister allgemein für Zwecke der Strafverfolgung oder Strafvollstreckung durch die hierfür zuständigen Behörden, d.h. Staatsanwaltschaften und Gerichte, Suchvermerke und Steckbriefnachrichten über Beschuldigte oder Verurteilte, deren Aufenthalt unbekannt ist, zu speichern, sind aufgegeben worden. Unverändert soll die Polizei über die Eingabe von Fahrzeugdaten zur Feststellung des Halters und umgekehrt über die Eingabe von Halterdaten zur Feststellung des Fahrzeugs eine automatisierte Zugriffsmöglichkeit besitzen. Die bisherige Zurückhaltung den Nachrichtendiensten gegenüber ist aufgegeben worden. Diese sollen nun uneingeschränkt in den Empfängerkreis einbezogen werden. Gleiches gilt auch für die Übermittlungen im Zusammenhang mit Ordnungswidrigkeitsverfahren. Auch hier wurden die bisherigen berechtigten Bedenken zurückgestellt.

Nur in einem Punkt ist der Kritik an den umfassend vorgesehenen Direktzugriffsverfahren gefolgt worden: Dort, wo Direktabrufe möglich sind, sieht der Entwurf für einen ausgewählten Teil der Abrufe vor, daß durch die abrufende Stelle oder das Kraftfahrtbundesamt Aufzeichnungen anzufertigen sind, die sich auf den Anlaß des Abrufs erstrecken und die Feststellung der für den Abruf verantwortlichen Personen ermöglichen. Diese Regelung, die eine Aufzeichnungspflicht über die allgemein im Zusammenhang mit den Abrufen vorzunehmenden Aufzeichnungen (sie sollen lediglich die zur Durchführung der Abrufe selbst verwendeten Daten, den Tag und die Uhrzeit der Abrufe, die Kennung der abrufenden Dienststelle und die abgerufenen Daten enthalten) hinaus vorsieht, um damit auch den Grund des Abrufs nachvollziehen zu können, ist sicherlich ein Fortschritt. Die grundsätzlichen Bedenken gegen die Einführung der P-Abfrage (vgl. hierzu 13. Tätigkeitsbericht, Ziff. 3.5.4.4) kann diese gesetzlich vorgesehene Maßnahme nicht relativieren. Ich sehe deshalb keinen Grund für eine Änderung meines Standpunktes.

13.2.6 Zweckbindung der Beihilfedaten (13. Tätigkeitsbericht, Ziff. 4.2.2.2; 12. Tätigkeitsbericht, Ziff. 2.1.6.2; 11. Tätigkeitsbericht, Ziff. 5.2.2)

Die im letzten Tätigkeitsbericht erwähnte Änderung der Verwaltungsvorschriften zu § 107 Hessisches Beamtengesetz ist inzwischen vom Hessischen Minister des Innern erlassen und im Staatsanzeiger veröffentlicht worden (vgl. Erlaß vom 16. September 1985, StAnz. Nr. 40/1985, S. 1810). Mit der Einfügung eines neuen Abschnitts Va in die Verwaltungsvorschriften ist nach jahrelangem Hin und Her endlich klargestellt, daß Beihilfeunterlagen strikt zweckgebunden für die Prüfung und Berechnung der Beihilfe zu verwenden sind, daß sie für dienstrechtliche Angelegenheiten ohne Zustimmung des Bediensteten von der Personalabteilung nicht eingesehen werden dürfen und daß die Beihilfeakten getrennt von den übrigen Personalakten zu führen sind. Rechtsverbindlich sind diese Verwaltungsvorschriften zwar nur für die Behörden der Landesverwaltung; in Ziff. VI des Erlasses vom 26. März 1984 (StAnz. Nr. 16/1984, S. 779) wird den Kommunen und sonstigen Körperschaften des öffentlichen Rechts lediglich "empfohlen", die Verwaltungsvorschriften zu § 107 HBG ebenfalls anzuwenden. Da die Neuregelung für die Beihilfedaten jedoch das verfassungsrechtliche Gebot der strikten Zweckbindung bei der Datenverwendung konkretisiert und nur ihre Beachtung das Patientengeheimnis der im öffentlichen Dienst Beschäftigten wahrt, erwarte ich, daß auch die Gemeinden und sonstigen öffentlichen Stellen die neuen Vorschriften beachten werden.

Hinzuweisen ist in diesem Zusammenhang auf § 34 Abs. 6 des Entwurfs der Landesregierung zur Änderung des Hessischen Datenschutzgesetzes (Drucks. 11/4749), der die automatisierte Verarbeitung medizinischer Befunde der Bediensteten untersagt und damit für die Zukunft die Nutzung der ADV für die Verarbeitung von Beihilfedaten, jedenfalls insoweit Diagnosen, ärztliche Beurteilungen usw. betroffen sind, ausschließt.

13.2.7
Krebsregister (12. Tätigkeitsbericht, Ziff. 2.1.4)

Im 12. Tätigkeitsbericht hatte ich über die Rechtsprobleme der Datenspeicherung bei epidemiologischen und klinischen Krebsregistern sowie über den Ausbaustand der hessischen Tumorzentren berichtet. Inzwischen sind die Tumorzentren Frankfurt und Marburg/Gießen in Betrieb. Die Landesregierung hat ihre Einschätzung und Planung in der Antwort auf eine Große Anfrage der SPD-Fraktion betr. Krebsregister (Drucks. 11/3565 zu Drucks. 11/1037) dargelegt. Dazu habe ich gegenüber dem Landtag aufgrund seines Beschlusses vom 14. November 1985 (vgl. Nr. 7, Drucks. 11/4696) meinen Standpunkt erläutert und dabei auf die weitgehende Übereinstimmung zwischen Landesregierung und mir in Bezug auf die rechtlichen Rahmenbedingungen eines epidemiologischen Krebsregisters hingewiesen. In Anbetracht des Ausbaus der klinischen Tumordokumentation habe ich angeregt, die sich auch dafür abzeichnende Regelungsnotwendigkeit sowie den geeigneten Regelungsort zu überprüfen und gemeinsam zu erörtern.

Wiesbaden, den 23. Januar 1986

gez. Prof. Dr. Simitis

14. Materialien

14.1
Beschluß der Konferenz der Datenschutzbeauftragten des Bundes und der Länder zu den Anforderungen an Datenschutzregelungen im Polizeirecht vom 24. Januar 1985.

I. Notwendigkeit bereichsspezifischer Regelungen

1.
Die Datenschutzbeauftragten des Bundes und der Länder haben seit Jahren auf die Notwendigkeit präziser gesetzlicher Regelungen für die Datenverarbeitung durch die Vollzugspolizei hingewiesen. Einzelne Maßnahmen wie zum Beispiel die Polizeiliche Beobachtung oder die Verarbeitung von Daten Unbeteiligter stehen weitgehend im Widerspruch zum geltenden Polizei- und Strafverfahrensrecht. Gesetzlich nicht hinreichend abgedeckt sind insbesondere die Erhebung und Nutzung personenbezogener Daten zu Zwecken der vorbeugenden Bekämpfung von Straftaten.

Spätestens seit dem Urteil des Bundesverfassungsgerichts zum Volkszählungsgesetz ist eine bereichsspezifische Regelung der polizeilichen Informationsverarbeitung unerläßlich. Dabei kann es nicht darum gehen, die derzeitige, durch eine Ausweitung der Datenverarbeitung gekennzeichnete Praxis der Datenverarbeitung festzuschreiben, sie muß vielmehr überprüft und der Umfang zulässiger Informationsverarbeitung durch spezielle Befugnisnormen konkret bestimmt und begrenzt werden.

2.
Eine solche Regelung muß zumindest die nachfolgenden Grundsätze beachten. Diese Grundsätze sollten - evtl. differenziert je nach spezifischer Aufgabenzuweisung - sowohl in den Polizeigesetzen des Bundes und der Länder als auch in der Strafprozeßordnung, soweit es um gleichartige Maßnahmen geht, berücksichtigt werden.

II. Grundsätze polizeilicher Informationsverarbeitung

1.
Allgemeine Prinzipien

1.1
Die gesetzlichen Regelungen über die Informationsverarbeitung müssen die polizeilichen Befugnisse klar und rechtsstaatlich umschreiben. Dies bedeutet

- dem Gebot der Normenklarheit entsprechende Spezialregelungen und damit die Zurückdrängung von Generalklauseln,
- Beachtung des Grundsatzes der Verhältnismäßigkeit,
- prinzipielle Beschränkung auf die Aufgaben Gefahrenabwehr und Strafverfolgung,
- Beachtung des Grundsatzes der Zweckbindung der Daten.

1.2
In Übereinstimmung mit dem vom Bundesverfassungsgericht anerkannten Recht auf informationelle Selbstbestimmung müssen die Regelungen jede Art und Form der Verarbeitung personenbezogener Daten durch die Polizei erfassen.

Sowohl die Erhebung als auch jede Nutzung von Daten sind in die Regelung mit einzubeziehen.

Die Form der Verarbeitung ist bei der Intensität der einzelnen Regelung zu berücksichtigen.

Die Speicherung personenbezogener Merkmale wie Krankheit oder besonderer Verhaltensweisen, insbesondere mit Hilfe automatischer Verfahren, ist nur zulässig, wenn die möglichen Verwendungen in einem angemessenen Verhältnis zu den Gefahren für die schutzwürdigen Belange der Betroffenen stehen. Durch die Automatisierung darf keine Verzerrung oder unangemessene Verkürzung des Sachverhalts entstehen.

2.
Für die Datenverarbeitung sollten folgende Grundsätze Beachtung finden:

2.1
Zum Erheben und Speichern personenbezogener Daten

2.1.1
Grundsätze
Die Verarbeitung von Daten muß grundsätzlich der Abwehr einer im einzelnen Fall bestehenden (konkreten) Gefahr oder der Aufklärung einer konkreten Straftat dienen.

- Eine darüber hinausgehende Verarbeitung kann nur in eng begrenzten Fällen zugelassen werden. Insbesondere bedürfen Befugnisse zur vorbeugenden Bekämpfung von Straftaten einer klaren abschließenden Umschreibung im Gesetz.

- Für die Erfüllung spezialgesetzlich zugewiesener Aufgaben stehen der Polizei nur die jeweiligen spezialgesetzlichen Befugnisse zu.

- Der Bürger muß - wie zuletzt auch das Bundesverfassungsgericht im Volkszählungsurteil festgestellt hat - grundsätzlich unbeobachtet von staatlichen Stellen an Versammlungen teilnehmen können. Bei Befugnissen zur Informationserhebung in Versammlungen ist stärker als in der bisherigen Praxis dem Grundrecht der Versammlungsfreiheit Rechnung zu tragen.

Werden personenbezogene Informationen in Dateien gespeichert, müssen die Herkunft und die Richtigkeit der Informationen in Akten oder anderen Unterlagen nachweisbar sein. Werden Bewertungen gespeichert, muß erkennbar sein, wer die Bewertungen vorgenommen hat und wo die Erkenntnisse gespeichert sind, die ihnen zugrunde liegen.

2.1.2

Datenerhebung und -speicherung

- Die Gewinnung von Informationen muß grundsätzlich offen geschehen; heimliche Informationserhebung ist nur dann zulässig, wenn dies zur Aufgabenerfüllung im Einzelfall unerläßlich ist.

- Die Erhebung durch selbsttätige Lese- und Aufzeichnungsgeräte ist gesetzlich zu regeln.

- Bei Erhebung von Daten unter Mitwirkung des Betroffenen ist dieser in der Regel auf seine Aussage- oder Mitwirkungspflicht oder auf die Freiwilligkeit hinzuweisen.

- Werden heimlich erhobene Daten gespeichert, ist der Betroffene grundsätzlich nach Wegfall der Zweckgefährdung zu informieren.

- Die Anfertigung und Aufbewahrung erkennungsdienstlicher Unterlagen muß präziser und restriktiver geregelt werden. Vorschriften über die Anfertigung und Verarbeitung von erkennungsdienstlichen Unterlagen dürfen nicht durch eine technische Möglichkeit umgangen werden (z.B. Überwachung bestimmter Orte durch Videogeräte, automatische Stimmerkennung).

- Die Übernahme der in Strafermittlungsverfahren erhobenen Informationen in Unterlagen für Zwecke der Gefahrenabwehr und vorbeugenden Bekämpfung von Straftaten ist an strenge Voraussetzungen zu knüpfen.

- Der Abgleich von oder mit Fremddatenbeständen darf künftig nur zur Abwehr erheblicher gegenwärtiger Gefahren sowie zur Aufklärung abschließend festgelegter schwerer Straftaten zugelassen werden. Die hierbei gewonnenen Daten müssen einer strengen Zweckbindung unterliegen. Voraussetzungen, Art und Umfang des Abgleichs, Verwertung und Dauer der Aufbewahrung sind im Gesetz abschließend zu regeln.

- Der Einsatz besonderer Verfahren, die über ein Aktenhinweissystem hinausgehen (z.B. Spurendokumentationsverfahren) bedarf einer gesetzlichen Regelung.

- Personenbezogene Daten dürfen grundsätzlich nur bei der sachbearbeitenden Dienststelle in kriminalpolizeilichen Sammlungen oder entsprechenden Dateien gespeichert werden. Die Speicherung dieser personenbezogenen Daten bei polizeilichen Zentralstellen ist nur aufgrund ausdrücklicher gesetzlicher Regelung zulässig.

- Erkenntnisanfragen oder Bitten um Amtshilfe dürfen bei den angefragten Stellen grundsätzlich nicht zur Anlage kriminalpolizeilicher Personenakten oder -dateien führen. Gleiches muß für bloße Unterrichtungen gelten.

2.2
Übermittlung von Daten

2.2.1
Die zu polizeilichen Zwecken gewonnenen Daten sind grundsätzlich zweckgebunden zu verwerten.

2.2.2
Bei der Übermittlung an Polizeibehörden ist hinsichtlich Art und Inhalt nach der konkreten polizeilichen Funktion und Zuständigkeit zu unterscheiden. Die Datenübermittlung an zentrale Stellen ist restriktiv zu regeln; das gilt auch für Erkenntnisanfragen und deren Beantwortung.

2.2.3
Eine Übermittlung an andere als Polizeibehörden und sonstige öffentliche Stellen sowie an Privatpersonen ist nur im Einzelfall zulässig und nur

- zur Abwendung einer konkreten Gefahr, einer erheblichen sozialen Notlage oder

- zur Verfolgung von öffentlich-rechtlichen oder zivilrechtlichen Ansprüchen in Fällen von Beweisnot,

und nur, wenn hierfür eine ausdrückliche gesetzliche Regelung besteht. Bei Anfragen, deren Beantwortung in die Zuständigkeit anderer Stellen fällt, hat die Polizei grundsätzlich an diese Stellen zu verweisen. Die Vorschriften des Bundeszentralregistergesetzes dürfen nicht durch polizeiliche Auskunft unterlaufen werden.

Eine Datenübermittlung an Nachrichtendienste darf wegen der verfassungsrechtlich gebotenen Trennung von polizeilicher und nachrichtendienstlicher Tätigkeit entgegen der derzeitigen Praxis nur in engen Grenzen zugelassen werden. Ein geeigneter Maßstab sind die Übermittlungsregelungen nach dem Gesetz zu Art. 10 GG.

Bei der Übermittlung an ausländische Stellen ist durch geeignete Absprachen und durch die Vereinbarung internationaler Regelungen sicherzustellen, daß die innerstaatlichen Grundsätze des Datenschutzes nicht gefährdet werden.

2.2.4
Vor jeder Übermittlung hat die auskunftgebende Stelle grundsätzlich die Richtigkeit der vorhandenen Unterlagen und deren Erforderlichkeit für die eigene Aufgabenerfüllung zu überprüfen. Wenn ein Verfahren noch nicht abgeschlossen ist, ist darauf hinzuweisen. Eine Übermittlung hat zu unterbleiben, wenn die Unterlagen zu vernichten sind.

2.2.5
Tatsache und Inhalt der Übermittlung sind in der Akte festzuhalten. Bei Veränderung wesentlicher Gesichtspunkte (z.B. Löschung) hat die übermittelnde Stelle die Änderung nachzuberichten, soweit dadurch nicht schutzwürdige Belange des Betroffenen beeinträchtigt werden.

2.3
Löschungs- und Überprüfungsvorschriften

Für die Aufbewahrung der Daten muß der Gesetzgeber differenzierte Löschungs- und Überprüfungsvorschriften gesetzlich vorsehen. Insbesondere ist zu unterscheiden

- nach Alter des Betroffenen,

- nach der Schwere der Gefahr und der Straftat,

- nach der Art der Tatbegehung,

- nach der Art der Daten,

- nach dem Ausgang des Verfahrens.

Die gegenwärtig praktizierten Regelfristen (für Kinder 2 Jahre, für Jugendliche 5 Jahre, für Erwachsene 10 Jahre) dürfen nicht verlängert werden.

Daten, die allein zur Personenfeststellung erhoben wurden, sind unmittelbar nach Zweckerreichung zu vernichten.

2.4
Transparenz

Entsprechend der verfassungsmäßigen Garantie des Rechtsweges (Art. 19 Abs. 4 GG) hat der einzelne grundsätzlich ein Recht auf vollständige Auskunft.
Dieses umschließt

- die zu seiner Person gespeicherten Informationen,

- Zweck, Rechtsgrundlage und vorgesehene Dauer der Speicherung,

- Art der Gewinnung oder Herkunft der Informationen,

- die Tatsache und den Inhalt der Übermittlung an andere Stellen.

Ausnahmen hiervon sollten nur dann zulässig sein, wenn hierdurch die Erfüllung polizeilicher oder anderer Sicherheitsaufgaben gefährdet oder erheblich erschwert wird, überwiegende Interessen Dritter entgegenstehen oder die Erfüllung des Auskunftsanspruchs nur mit unverhältnismäßigem Aufwand möglich wäre.

Die Bearbeitung von Auskunftsersuchen muß getrennt von polizeilichen Informationssammlungen erfolgen. Die Tatsache der Antragstellung darf nicht zum Nachteil des Betroffenen verwertet werden.

2.5
Notwendige organisatorische Maßnahmen

Für die Anlage neuer und für die Überprüfung vorhandener personenbezogener Sammlungen sowie für Verbunddateien muß der Erlaß von Errichtungsanordnungen gesetzlich vorgesehen werden, die Regelungen enthalten über

1. die Bezeichnung, den Zweck und die Rechtsgrundlage der Sammlung,

2. den in die Sammlung aufzunehmenden Personenkreis,

3. die Art und den Umfang der zu speichernden Informationen, die der Erschließung dienen können,

4. die Übermittlung von Informationen,

5. die Dauer der Aufbewahrung der Informationen und

6. die zuständige Stelle für die Anlage und Führung von Sammlungen.

Diese Errichtungsanordnungen sind zu veröffentlichen.

Daten, die zur Vorgangsverwaltung oder nur zum Nachweis polizeilichen Handelns geführt werden, sind von Datensammlungen zur Gefahrenabwehr und Strafverfolgung zu trennen.

14.2

Beschluß der Konferenz der Datenschutzbeauftragten des Bundes und der Länder zu den Anforderungen der Datenschutzregelungen für den Verfassungsschutz vom 16. September 1985

I. Notwendigkeit bereichsspezifischer Regelungen

1.
Gerade für die Datenverarbeitung der Verfassungsschutzbehörden sind präzise gesetzliche Grundlagen erforderlich, da sie in besonderem Maße in das informationelle Selbstbestimmungsrecht eingreift, weil sie fast vollständig im Geheimen und somit unter Ausschluß der Öffentlichkeit und der Kontrolle durch den Betroffenen stattfindet.

Ebenso wie im Polizeirecht kann es auch beim Verfassungsschutz nicht darum gehen, die derzeitige Praxis gesetzlich festzuschreiben. Vielmehr muß der Umfang zulässiger Informationsverarbeitung der Verfassungsschutzbehörden auf der Grundlage des Volkszählungsgesetzurteils des BverfG überprüft und durch spezielle Aufgaben- und Befugnisnormen konkretisiert und begrenzt werden. Die Neuregelung muß zumindest die nachfolgenden Grundsätze beachten.

2.
Ähnliche Regelungen für den MAD und den BND sind unter Berücksichtigung der Besonderheiten der jeweiligen Aufgabenstellung geboten.

II. Allgemeine Grundsätze der Datenverarbeitung durch den Verfassungsschutz

1.
Die Regelung der Informationsverarbeitung durch den Verfassungsschutz muß den Anforderungen der Normenklarheit entsprechen. Da über die Datenverarbeitung im Einzelfall meist nichts bekannt wird, ist es für den Bürger von besonderer Bedeutung, daß er den gesetzlichen Bestimmungen entnehmen kann, aus welchem Anlaß, in welcher Form und zu welchem Zweck der Verfassungsschutz personenbezogene Daten verarbeiten darf.

2.
Diese Vorschriften müssen zwischen den unterschiedlichen Aufgaben der Verfassungsschutzbehörden differenzieren. Was beispielsweise für die Abwehr von Spionen vertretbar ist, ist nicht auch für die Mitwirkung an Sicherheitsüberprüfungen angemessen.

3.
Der Grundsatz der Zweckbindung gilt auch für die Verfassungsschutzbehörden. Das bedeutet: Angesichts der Vielfalt ihrer Aufgaben reicht eine pauschale Bindung an "Zwecke des Verfassungsschutzes" nicht aus. Vielmehr dürfen die für die unterschiedlichen Aufgaben erhobenen Daten grundsätzlich nur für die jeweilige Aufgabe verwendet werden.

4.
Die Regelung der Verarbeitung personenbezogener Daten durch den Verfassungsschutz muß die Erhebung sowie jegliche andere Art der Verarbeitung und Verwendung einbeziehen.

5.
Regelungsbedürftig sind auch die Voraussetzungen für die jeweilige Form der Datenverarbeitung: Wesentliche Schritte der Automatisierung sollten beispielsweise nur zugelassen werden, wenn diese für die Erfüllung der jeweiligen Aufgabe gerechtfertigt sind und hierdurch schutzwürdige Belange der Betroffenen nicht unverhältnismäßig beeinträchtigt werden. Dies gilt insbesondere für Systeme der Datenverarbeitung, die über einen Aktennachweis hinausgehen oder durch Übernahme von Akteninhalten neue Verwendungs- und Verknüpfungsmöglichkeiten eröffnen.

6.
Für jede automatisierte oder manuelle Datei ist eine detaillierte Errichtungsanordnung zu erlassen.

III. Erheben und Sammeln personenbezogener Daten

1.
Der Einsatz nachrichtendienstlicher Mittel muß klar geregelt sein. Dies gilt sowohl für die Voraussetzungen der Anwendung als auch für die Frage, gegen wen nachrichtendienstliche Mittel eingesetzt werden dürfen. Die nachrichtendienstlichen Mittel sollten soweit wie möglich gesetzlich festgelegt werden. Zumindest sollten die Verfassungsschutzbehörden verpflichtet werden, alle in Frage kommenden Mittel im einzelnen intern zu beschreiben und ihren Einsatz zu dokumentieren. Die Anwendung nachrichtendienstlicher Mittel entbindet nicht von der Beachtung der allgemeinen Rechtsordnung.

2.
Holt der Verfassungsschutz bei anderen Behörden Auskünfte ein, so soll er sein Ersuchen begründen, wenn nicht besondere Gründe entgegenstehen (z.B. schutzwürdige Belange des Betroffenen oder Sicherheitsinteressen des Staates). Entfällt danach die Begründung, so sind die Gründe des Ersuchens intern zu dokumentieren. Für Kontrollzwecke sollte ein eigenes Verzeichnis eingerichtet werden.

3.
Eine Verpflichtung anderer Behörden, dem Verfassungsschutz von sich aus Informationen zu übermitteln, muß auf solche Bestrebungen beschränkt werden, die auf Anwendung von Gewalt oder geheimdienstliche Tätigkeit gerichtet sind. Darüber hinaus dürfen Behörden von sich aus nur unter weiteren gesetzlich festzulegenden Einschränkungen den Verfassungsschutz über personenbezogene Vorgänge informieren. Übermittlungen "auf Verdacht" sind unzulässig und können sich schädlich für das Verhältnis des Bürgers zu den Behörden auswirken.

4.
Bei der Regelung der Informationsbeziehungen zwischen Polizei und Verfassungsschutz ist das verfassungskräftige Trennungsgebot zu beachten, das inhaltlicher ebenso wie organisatorischer Natur ist. Der Verfassungsschutz darf deshalb die Polizei z.B. nicht um Maßnahmen ersuchen, die die Anwendung polizeilicher Befugnisse erfordern. Online-Verbindungen zwischen Polizei und Verfassungsschutz sind mit dem Trennungsgebot nicht vereinbar. Ein geeigneter Maßstab für Datenübermittlungen der Polizei an den Verfassungsschutz im Einzelfall sind die Verwertungsregelungen nach dem Gesetz zu Art. 10 GG.

5.
Es ist sicherzustellen, daß spezielle Verwertungsbestimmungen - z.B. des Strafverfahrensrechts - beachtet werden; dies gilt z.B. für Erkenntnisse, die im Rahmen der Telefonüberwachung oder bei Durchsuchungen gewonnen wurden.

IV. Speichern personenbezogener Daten

1.
Die Befugnis zur Speicherung ist differenziert nach den unterschiedlichen Aufgabenbereichen zu regeln.

So muß der Extremismusbezug in der Person desjenigen erfüllt sein, dessen Daten personenbezogen auswertbar im Rahmen der Extremismusbeobachtung gespeichert werden sollen. Hierbei ist außerdem zu beachten, daß Personendaten nur gespeichert werden dürfen, wenn dies zum Zwecke der Beobachtung extremistischer Bestrebungen erforderlich ist. Der Praxis, die immer mehr von der Beobachtung von Organisationen zur Erfassung von Einzelpersonen übergeht, muß entgegengewirkt werden.

2.
Die Gründe für eine Speicherung müssen aus den Unterlagen des Verfassungsschutzes nachvollziehbar sein. Werden Bewertungen gespeichert, so muß erkennbar sein, wer sie vorgenommen hat und welche Unterlagen ihnen zugrundeliegen.

3.
Es sind gesetzliche Regelfristen für die Überprüfung und Löschung der gespeicherten Daten festzulegen. Dabei ist zwischen den einzelnen Aufgabenbereichen (etwa Extremismusbeobachtung/Spionageabwehr), nach der Relevanz der einzelnen Informationen (etwa: vager Verdacht/gesicherte Informationen) sowie nach dem Alter der Betroffenen zu differenzieren. Dies gilt auch für die Speicherung in Akten.

V. Mitwirkung an Personenüberprüfungen (Sicherheitsüberprüfungen - § 3 Abs. 2 BVerfSchG)

1.
Im Rahmen von Sicherheitsüberprüfungen werden sowohl beim Verfassungsschutz als auch bei einer Reihe weiterer Stellen Daten erhoben und verarbeitet. Hierfür sind besondere gesetzliche Grundlagen erforderlich.

2.
Für die Mitwirkung des Verfassungsschutzes sind folgende Prinzipien zu beachten:

- Die Sicherheitsüberprüfungen sind auf das erforderliche Maß zu beschränken. Dies gilt insbesondere für die Intensität der Prüfung, die sich nach der Gefährdung im Einzelfall richten muß.

- Die Sicherheitsüberprüfung soll erst durchgeführt werden, wenn nur noch davon die Aufnahme der sicherheitsrelevanten Tätigkeit abhängig ist. Für den personellen Sabotageschutz ist zudem die exakte Beschreibung der sicherheitsempfindlichen Bereiche und die Begrenzung der Überprüfung auf tatsächlich in diesem Bereich eingesetzte Personen zu fordern.

- Die Verfahrensregelungen müssen andere Ermittlungsformen ausschließen.
- Im Rahmen der Sicherheitsüberprüfung ist es nicht Aufgabe des Verfassungsschutzes, die Auskünfte aller beteiligten Stellen zu koordinieren.
- Die Voraussetzungen, unter denen im Rahmen der Sicherheitsüberprüfung auch Nachforschungen über Dritte angestellt werden dürfen, sind gesetzlich festzulegen. Soweit Dritte, z.B. Ehegatten, einbezogen werden, ist deren Einwilligung erforderlich. Die Speicherung von Daten über diese Personen ist auf ein Minimum zu beschränken und darf grundsätzlich nicht personenbezogen erschließbar sein.
- Das Verfahren muß für die Betroffenen (einschließlich der Dritten) transparent sein. Sie sind über die Tatsache, den Ablauf, die beteiligten Stellen und das Ergebnis der Sicherheitsüberprüfung zu unterrichten. Im Fall von Sicherheitsbedenken ist dem Überprüften Gelegenheit zur Stellungnahme zu geben. Ausnahmen von dieser Unterrichtungspflicht sind eng zu fassen. Auch Auskunftspersonen sind über den Zweck der Befragung zu unterrichten, um Fehlschlüsse zu Lasten des Betroffenen zu vermeiden, und auf die Freiwilligkeit ihrer Angaben hinzuweisen.
- Stellt der Betroffene einen Auskunftsantrag nach den Datenschutzgesetzen, so ist diesem zu entsprechen, soweit die Speicherung im Rahmen der Sicherheitsüberprüfung erfolgt ist.
- Die speziell für die Sicherheitsüberprüfung beim Betroffenen oder bei anderen Stellen erhobenen Daten dürfen i.d.R. nur für diesen Zweck verwendet werden. Die Trennung von Sicherheits- und Personalakten ist strikt zu wahren.

VI. Übermittlung von Daten durch Verfassungsschutzbehörden

1.
Verfassungsschutzbehörden dürfen untereinander personenbezogene Daten nur austauschen, soweit dies zu ihrer jeweiligen gesetzlich festgelegten Aufgabenerfüllung erforderlich und verhältnismäßig ist.

2.
Die Übermittlung personenbezogener Daten durch den Verfassungsschutz an andere Sicherheitsbehörden (z.B. Polizei, Staatsanwaltschaft, BND u.a.) muß unter Beachtung des Zweckbindungsgrundsatzes präziser und restriktiver als in den derzeit praktizierten Zusammenarbeitsrichtlinien in Staatsschutzsachen geregelt werden. Die Voraussetzungen einer Übermittlung müssen konkret festgelegt werden. Allein die Begründung, daß die Übermittlung mit "dem Zweck des Verfassungsschutzes" vereinbar sei, ist nicht ausreichend. An Strafverfolgungsbehörden darf der Verfassungsschutz Informationen, die er mit nachrichtendienstlichen Mitteln erlangt hat, nur weitergeben, wenn tatsächliche Anhaltspunkte für die Einleitung eines Ermittlungsverfahrens wegen einer Straftat der in § 7 Abs. 3 Gesetz zu Art. 10 GG genannten Art vorliegen.

3.
Eine Übermittlung an andere Behörden kann nur zur Erfüllung eigener Aufgaben des Verfassungsschutzes in Betracht kommen. Ausnahmen bedürfen einer gesetzlichen Regelung.

4.
Eine Übermittlung von personenbezogenen Daten an private Stellen (z.B. Firmen, Gewerkschaften, Parteien) ist nur im Rahmen der gesetzlich vorgesehenen Sicherheitsüberprüfungen und nur in dem dafür unerläßlichen Rahmen oder aus Gründen der Spionage- und Terrorismusabwehr zulässig. Bei Übermittlungen außerhalb der Sicherheitsüberprüfung ist außerdem die Zustimmung der obersten Dienstbehörde einzuholen.

5.
Eine Übermittlung an ausländische Dienststellen einschl. der Nachrichtendienste ist an besonders enge Voraussetzungen zu knüpfen. Es ist - längerfristig durch völkerrechtliche Übereinkommen - zu gewährleisten, daß im Inland geltende Schutzrechte des Betroffenen nicht gefährdet werden.

6.
Vor jeder Übermittlung hat die auskunftgebende Verfassungsschutzbehörde die Richtigkeit der vorhandenen Unterlagen und deren Erforderlichkeit für die eigene Aufgabenerfüllung zu überprüfen. In allen Fällen ist die Übermittlung personenbezogen zu dokumentieren. Über die Änderung wesentlicher Gesichtspunkte ist die Empfängerbehörde zu unterrichten, soweit dadurch nicht schutzwürdige Belange des Betroffenen beeinträchtigt werden.

7.
Eine Unterrichtung der Öffentlichkeit über personenbezogene Erkenntnisse des Verfassungsschutzes ist grundsätzlich ausgeschlossen.

VII. Auskunft an den Betroffenen

Die Verfassungsschutzbehörden dürfen Auskunftsersuchen der Bürger nicht, wie dies derzeit die meisten Ämter handhaben, schematisch ablehnen. Der Gesetzgeber sollte daher von folgenden Grundsätzen ausgehen:

Die Auskunft ist zu erteilen

- in aller Regel, wenn die Speicherung nur auf einer Sicherheitsüberprüfung beruht,
- im übrigen nach Abwägung im Einzelfall.

Im Falle einer Auskunftsverweigerung sind die Gründe im einzelnen zu dokumentieren.

Die Bearbeitung von Auskunftsersuchen muß getrennt von anderen Informationssammlungen erfolgen. Die Tatsache der Antragstellung darf nicht zum Nachteil der Betroffenen verwertet werden.

VIII. Rechte der Datenschutzbeauftragten

Die Kontrollkompetenz der Datenschutzbeauftragten erstreckt sich auf die gesamte Datenverarbeitung der Verfassungsschutzbehörden und umfaßt auch Akten und sonstige Unterlagen. Auch die Datenverarbeitung im Rahmen des Gesetzes zu Art. 10 GG muß der Kontrolle der Datenschutzbeauftragten unterliegen. Dies ist unerläßlich für die Durchsetzung des Rechts auf informationelle Selbstbestimmung gerade im Bereich des Verfassungsschutzes.