12. Wahlperiode

Drucksache **12/1742**

HESSISCHER LANDTAG

26. 02. 88

Sechzehnter Tätigkeitsbericht des Hessischen Datenschutzbeauftragten

Professor Dr. Spiros Simitis

vorgelegt zum 31. Dezember 1987
gemäß § 30 des Hessischen Datenschutzgesetzes vom 11. November 1986

Eingegangen am 26. Februar 1988 · Ausgegeben am 15. März 1988

Herstellung: Johannes Weisbecker, 6000 Frankfurt am Main · Auslieferung: Kanzlei des Hessischen Landtags · Postf. 3240 · 6200 Wiesbaden 1

12/1742

INHALTSVERZEICHNIS

KERNPUNKTE DES 16. TÄTIGKEITSBERICHTS

1. Die Verabschiedung bereichsspezifischer gesetzlicher Regelungen für die Verarbeitung personenbezogener Daten durch die Sicherheitsbehörden läßt sich nicht mehr aufschieben. Die Übergangsfrist läuft Ende 1988 ab (Ziff. 1.2.1).
2. Das am Jahresanfang 1987 in Kraft getretene neue Hessische Datenschutzgesetz hat zu einer Reihe von Auslegungsproblemen geführt. Geklärt wurden Interpretationsfragen u.a. zum Anwendungsbereich, zur Benachrichtigungspflicht und zur Bestellung behördeninterner Datenschutzbeauftragter (Ziff. 2).
3. Die Volkszählung 1987 ist zwar ausreichend gesetzlich geregelt; bei der Durchführung haben sich jedoch gravierende Mängel gezeigt (Ziff. 3).
4. Der Hessische Rundfkunk ist seinen gesetzlichen Verpflichtungen nicht nachgekommen. Er hat für die journalistisch-redaktionelle Datenverarbeitung keinen Beauftragten für den Datenschutz bestellt und bestreitet dem Hessischen Datenschutzbeauftragten die Kontrollbefugnis für die nicht zu publizistischen Zwecken verwendeten Datenbestände (Ziff. 2.6).
5. Die Diskussion um ein landesweites Kommunikationsnetz kann nur sinnvoll geführt werden, wenn die Landesregierung zuvor ein Gesamtkonzept vorlegt, in dem die Informationsströme klar definiert und das Netz- sowie Datenschutzkonzept detailliert beschrieben sind (Ziff. 4.4).
6. Bei Umfragen beachten die Gemeinden oft die datenschutzrechtlichen Anforderungen nicht oder nicht ausreichend (Ziff. 5.1).
7. Beschäftigte öffentlicher Stellen können sich ohne Einhaltung des Dienstwegs direkt an den Hessischen Datenschutzbeauftragten wenden, gleichgültig, ob es um ihre eigenen Daten oder um Daten Dritter geht (Ziff. 5.2).
8. Automatisierte Abrufverfahren innerhalb der Gemeinde dürfen nur aufgrund einer förmlichen Entscheidung des Magistrats oder Oberbürgermeisters eingeführt werden; darin sind festzulegen: Datenempfänger, Datenarten, Zweck des Abrufs und die Maßnahmen zur Datensicherung und Kontrolle (Ziff. 5.4).
9. Aids-Tests dürfen im Krankenhaus grundsätzlich nicht ohne Wissen und Willen des Betroffenen durchgeführt werden (Ziff. 6.1.1).
10. Die Erforderlichkeit der Speicherung personenbezogener Aids- Hinweise in polizeilichen Informationssystemen ist bislang nicht ausreichend begründet (Ziff. 6.1.2).
11. Die Polizei darf keine Kenntnisse über einzelne Aids-Infizierte an das Gesundheitsamt weitergeben (Ziff. 6.1.3).
12. Gegen die in der Laborberichtsverordnung vorgeschriebene anonyme Meldepflicht für HIV-Bestätigungstests bestehen keine datenschutzrechtlichen Bedenken (Ziff. 6.1.4.2).
13. Es ist nicht zulässig, daß Landkreise Kopien der Sozialhilfebescheide an die Wohnsitzgemeinde des Sozialhilfeempfängers schicken, damit dort die Angaben des Antragstellers überprüft werden können (Ziff. 7.1).
14. Ein externer Prüfer oder das Rechnungsprüfungsamt der Gemeinde, die in einem Sozialamt eine Organisations- und Wirtschaftlichkeitsuntersuchung durchführen, dürfen dort keine Unterlagen mit personenbezogenen Sozialdaten einsehen (Ziff. 7.2).
15. Die Sozialämter können auch ohne die Weitergabe personenbezogener Sozialdaten die Wohlfahrtsverbände bei der Verteilung der EG-Butter für Kälteopfer organisatorisch unterstützen (Ziff. 7.3).
16. Die Personalnachrichten im Staatsanzeiger für das Land Hessen verstoßen teilweise gegen das Hessische Datenschutzgesetz (Ziff. 8.1).
17. In die „Richtlinien für die Führung Kriminalpolizeilicher personenbezogener Sammlungen" muß umgehend ein differenziertes System für Aussonderungsprüffristen aufgenommen werden (Ziff. 9.1).
18. Die in früheren Tätigkeitsberichten geäußerten Bedenken, daß sich die Staatsschutzdatei „Arbeitsdatei PIOS - Innere Sicherheit" (APIS) zu einem Register für politisch motivierte Straftaten von geringer Bedeutung entwickelt, haben sich bestätigt (Ziff. 9.2).
19. Die generelle Weigerung des Landesamts für Verfassungsschutz, Bürgern Auskunft darüber zu geben, ob es Daten über sie gespeichert hat oder nicht, ist nur für einige wenige Fallgruppen akzeptabel (Ziff. 9.3).
20. Die Bundesdruckerei muß durch ein geeignetes Kontrollsystem sicherstellen, daß nicht Personalausweise mit derselben Seriennummer ausgegeben werden (Ziff. 10).
21. Gerichte und Staatsanwaltschaften sollten ohne besondere Aufforderung die Polizei regelmäßig über den Ausgang eines Strafverfahrens unterrichten (Ziff. 11).
22. Die Fragebogen-Aktion zur Durchführung der Milch-Garantiemengen-Verordnung verstieß gegen das Hessische Datenschutzgesetz (Ziff. 12).

1. Zur Situation

1.1
Erste Erfahrungen mit dem neuen Hessischen Datenschutzgesetz

1987 war das Jahr der Volkszählung, aber auch der ersten Erfahrungen mit dem neuen Hessischen Datenschutzgesetz. Beides steht verständlicherweise im Vordergrund des Tätigkeitsberichts. Kein anderes Ereignis hat das Interesse am Datenschutz so geweckt wie die Volkszählung. Niemals sonst sind die Notwendigkeit genauso wie die Grenzen einer rechtlichen Regelung der Verarbeitung personenbezogener Angaben derart intensiv und unter so großer öffentlicher Anteilnahme diskutiert worden. Nie zuvor hat schließlich die Auseinandersetzung um den Datenschutz so nachhaltige Folgen für seine weitere Entwicklung gehabt. Spätestens seit der Entscheidung des Bundesverfassungsgerichts zum Volkszählungsgesetz von 1983 läßt sich am untrennbaren Zusammenhang zwischen verbindlichen, rechtlich abgesicherten Vorgaben an die Adresse jeder öffentlichen oder privaten Stelle, die personenbezogene Daten verarbeiten möchte und der Existenz einer demokratischen Gesellschaft nicht mehr zweifeln. Spätestens seit diesem Zeitpunkt steht aber auch die Verpflichtung des Gesetzgebers fest, gezielt einzugreifen, um die Einhaltung der verfassungsrechtlichen Minimalanforderungen an die Verarbeitung sicherzustellen, angefangen bei der Beteiligung und Information des Betroffenen, über die strikte Zweckbindung bis hin zur Garantie einer unabhängigen Kontrolle.

Vor genau diesem Hintergrund ist das neue Hessische Datenschutzgesetz entstanden. Anders als etwa noch die jüngsten Reformvorschläge zum Bundesdatenschutzgesetz hat der Hessische Gesetzgeber seine Aufgabe keineswegs darin gesehen, die Novellierung auf wenige, unvermeidliche Korrekturen zu beschränken und im übrigen die Chance zu nutzen, um vor allem die lästige Kontrolle soweit wie nur möglich zurückzudrängen. Das 3. HDSG knüpft zwar an die legislativen Erfahrungen seit 1970 an, versucht aber zugleich einen neuen, konsequent an der Verwirklichung des Datenschutzes orientierten Weg zu gehen. Daraus erklärt sich die breite Resonanz des Gesetzes. Es hat inzwischen nicht nur die Reformbestrebungen anderer Landesgesetzgeber entscheidend beeinflußt, sondern gilt mittlerweile weit über die Grenzen der Bundesrepublik hinaus als der wohl wichtigste Beitrag zur Fortentwicklung des Datenschutzes.

So gut es aber gelungen ist, den Eckwerten einer verfassungskonformen Regelung Rechnung zu tragen, etwa mit der unmißverständlich festgehaltenen Verpflichtung, keine Daten am Betroffenen vorbei zu erheben oder der Einbeziehung der Akten und dem folgerichtigen Ausbau der Kontrollbefugnisse des Datenschutzbeauftragten, so wenig kann das Gesetz für sich beanspruchen, durchweg Lösungen anzubieten, die eine komplikationslose Anwendung des Datenschutzes sichern. Manche Anwendungsschwierigkeiten, wie zum Beispiel die Auseinandersetzungen um das Recht der Beschäftigten öffentlicher Stellen, sich ohne Einhaltung des Dienstwegs an den Datenschutzbeauftragten zu wenden (vgl. Ziff. 5.2) oder um die Modalitäten der Benachrichtigung (vgl. Ziff. 2.3), spiegeln Meinungsverschiedenheiten wider, die sich schon im Gesetzgebungsprozeß abzeichneten; andere, wie etwa die genaue Abgrenzung der Fälle, in denen dem Datenschutzbeauftragten zu einer automatisierten Verarbeitung von Daten der Beschäftigten Gelegenheit zur Stellungnahme gegeben werden muß (vgl. Ziff. 8.2.1), sind erst im Verwaltungsalltag aufgetreten.

Für jede dieser Schwierigkeiten gilt freilich: Lösungen lassen sich nur durch eine Interpretation der jeweiligen Vorschriften finden, die sich strikt an die Vorgaben hält, welche auch die Entstehung und die Ziele des Gesetzes bestimmt haben. Die Auslegung der gesetzlichen Bestimmungen darf mit anderen Worten nicht den Rückzug in Positionen einläuten, die das HDSG bewußt verworfen hat.

Konkret: Ein konsequenter Datenschutz verträgt sich nur mit einer eindeutig aufgabenorientierten, streng zweckgebundenen Verarbeitung. Eben deshalb hat der Datenschutz schon sehr früh dazu geführt, sich bei der Definition der speichernden Stellen nicht nach den bislang akzeptierten formalen Einheiten zu richten, sondern ausschließlich nach den spezifischen Funktionen der jeweiligen Stellen. Nur unter dieser Voraussetzung kann die Verarbeitung von vornherein auf ganz bestimmte Aufgaben bezogen und auf den für sie typischen Bereich beschränkt bleiben. Just dieser „funktionale Stellenbegriff" ist erst jüngst vom Bundesverfassungsgericht bestätigt worden (Beschluß der 1. Kammer des Ersten Senats des Bundesverfassungsgerichts vom 18.12.1987 -1 BvR 962/87 - unter Ziff. II 4). An ihm gilt es daher auch bei der Anwendung des HDSG unbedingt festzuhalten, auch wenn zuweilen die Schwierigkeiten, etwa im kommunalen Bereich, nicht zu übersehen sind. Nichts anderes gilt für die Benachrichtigung. Der Gesetzgeber hat sich eben keineswegs mit dem Recht des Betroffenen zufriedengegeben, Auskunft über die zu seiner Person verarbeiteten Angaben zu verlangen. So unverzichtbar ein solches Recht ist, so schnell gerät es zur Fiktion, wenn der Betroffene keinen Anhaltspunkt darüber hat, wer überhaupt in welchem Umfang und mit welchen Zielen Informationen über ihn sammelt. Der Schritt über das Auskunftsrecht hinaus auf die Benachrichtigung zu bringt deshalb den Wunsch zum Ausdruck, die Chancen des Betroffenen zu verbessern, Kenntnis von der Verarbeitung zu bekommen und seine Rechte auszuüben. Selbst wenn daher die vom HDSG verlangte Benachrichtigung die Behörden belastet, kann und darf die Auslegung des Gesetzes nicht als Mittel verstanden werden, um die Benachrichtigungsfälle, so weit es nur geht, einzuschränken. Der Gesetzgeber ist ohne Zweifel zu Kompromissen bereit gewesen, und zwar im Hinblick auf diese immer wieder angeführte Belastung. Keiner dieser Kompromisse rechtfertigt es jedoch, die Gesetzesanwendung zu nutzen, um die Einschränkungen zu erweitern. Die Interpretation muß im Gegenteil das Ziel verfolgen, eine um der Betroffenen willen eingeführte Aufgabe sicherzustellen, alle Möglichkeiten also auszuloten, um die Information der Betroffenen auszubauen. Es sind ihre Daten, die verarbeitet werden, ihnen steht deshalb auch der gesetzlich bekräftigte Anspruch zu, am Verarbeitungsprozeß beteiligt zu werden. Die Benachrichtigung ist, so gesehen, kein überflüssiges Beiwerk, sie zählt zu den Grundvoraussetzungen einer

Datenschutzregelung, die eine Verarbeitung personenbezogener Daten grundsätzlich nur so lange duldet, wie sie sich nicht am Betroffenen vorbei vollzieht.

1.2
Anwendungsbereich des HDSG

1.2.1
Vorrang bereichsspezifischer Regelungen

Der Anwendungsbereich des HDSG ist dreifach begrenzt. Die ersten Anwendungsschranken ergeben sich aus der Vorgeschichte sowie den Zielen der gesetzlichen Regelung. Es ist in einer Zeit entstanden, in der die einst für selbstverständlich hingenommene Erwartung, mit einem Gesetz auf alle Verarbeitungssituationen reagieren zu können, längst brüchig, ja hinfällig geworden war. Das Bundesverfassungsgericht hat dann die letzten Zweifel ausgeräumt: Eine ebenso verfassungskonforme wie wirksame Verarbeitungsregelung setzt in erster Linie bereichsspezifische Vorschriften voraus. Obgleich also auf allgemeine gesetzliche Bestimmungen nach wie vor nicht verzichtet werden kann, hat sich ihre Funktion von Grund auf verändert. Sie sind eben nicht mehr der ausschließliche, sondern immer nur ein ergänzender Regelungsansatz.

Der Gesetzgeber muß infolgedessen auf zwei deutlich voneinander getrennten Ebenen operieren. Er kann sich nicht auf die einmal im Rahmen des HDSG getroffenen Entscheidungen zurückziehen, sondern ist genauso gehalten, einzelne Verarbeitungskomplexe aufzugreifen und durch eigens darauf zugeschnittene Vorschriften anzusprechen. Der Hessische Landtag war sich dessen durchaus bewußt, wie sich allein schon an der Aufforderung an die Landesregierung zeigt, die Voraussetzungen für eine möglichst baldige gesetzliche Regelung der Verarbeitung personenbezogener Daten im Rahmen des Umweltschutzes zu schaffen. Die Verabschiedung des HDSG verleitet aber offensichtlich leicht dazu, sich immer wieder mit einer allgemeinen Verweisung auf die generellen Bestimmungen abzufinden und so der Notwendigkeit aus dem Weg zu gehen, bereichsspezifische Regeln zu formulieren. Die Novellierung des Hochschulgesetzes ist ein recht bezeichnendes Beispiel für solche Tendenzen (vgl. Ziff. 13.3). Manches spricht dafür, daß sich genau diese Bestrebungen auch beim geplanten Krankenhausgesetz durchzusetzen drohen. Erst recht gilt es deshalb festzuhalten: Dem Gesetzgeber steht es nicht einfach frei, sich entweder auf die allgemeinen Bestimmungen zurückzuziehen oder zusätzliche, eindeutig bereichsspezifisch orientierte Vorschriften zu verabschieden. Die Verfassung legt vielmehr eine klare Abfolge fest. Nur die bereichsspezifische Regelung vermag dem Betroffenen wirklich jene auch vom Bundesverfassungsgericht unmißverständlich verlangte Klarheit darüber zu verschaffen, welche Ziele hinter der angestrebten Verarbeitung stehen und unter welchen Voraussetzungen sich diese genau abspielen soll. Der bereichsspezifischen Regelung gebührt daher der Vorrang, und zwar in jedem Fall dort, wo sich der Betroffene von vornherein in einer Situation befindet, die ihm gar nicht erst die Wahl läßt, die verlangte, sich auf seine Person beziehende Information zu geben oder zu verweigern. Die Krankenhausgesetzgebung ist ein Musterbeispiel dafür. Ebensowenig gilt es zu übersehen, daß der Gesetzgeber die Entscheidung keineswegs beliebig hinauszögern kann. Die allgemeinen Regeln sind immer nur eine kurzfristig tolerable Übergangslösung, vor allem dann, wenn die Angaben, wie im Sicherheitsbereich ohne Rücksicht auf die Einstellung des Betroffenen, ja an ihm vorbei erhoben werden. Was aber schon der 15. Tätigkeitsbericht (Ziff. 1.1.2) festgestellt hat, ist inzwischen von zahlreichen Gerichten, weit über Hessen hinaus, bestätigt worden: Die Übergangsfrist läuft ab. Sollte es deshalb bis zum Ende des Jahres 1988 zu keiner gesetzlichen Regelung der polizeilichen Datenverarbeitung kommen, dann werden sich von diesem Zeitpunkt an die Polizeibehörden dem berechtigten Einwand ausgesetzt sehen, bei jeder Verarbeitung personenbezogener Daten rechtswidrig zu handeln. Mehr denn je kommt es daher darauf an, Klarheit darüber zu gewinnen, wo genau bereichsspezifische Vorschriften vonnöten sind sowie eine entsprechende Prioritätenliste für den Entscheidungsprozeß des Gesetzgebers aufzustellen. Unter just diesem Aspekt gilt es an das Verfassungsschutz-, das Archiv- oder auch das Krebsregistergesetz zu erinnern, um einige der wichtigsten, unter Prioritätsgesichtspunkten allerdings sehr unterschiedlich einzuschätzende Bestandteile dieser Liste anzugeben.

1.2.2
Hessischer Rundfunk

Die zweite Anwendungsgrenze ist im Gesetz selbst angelegt. Der Gesetzgeber hat in einer Reihe ausdrücklich aufgezählter Fälle die Anwendung des HDSG entweder völlig ausgeschlossen oder weitgehend eingeschränkt. Mit das wichtigste Beispiel ist die Verarbeitung personenbezogener Daten durch den Hessischen Rundfunk. Ohne Zweifel kann gerade die Datenverarbeitung durch die Medien weitreichende Folgen für den jeweils Betroffenen haben. Insofern war und ist es durchaus verständlich, wenn im Gesetzgebungsverfahren eine Einbeziehung des Hessischen Rundfunks nachdrücklich gefordert wurde. Der Gesetzgeber hat sich aber diesen Bestrebungen zu Recht widersetzt. Freilich: Zur Debatte steht nicht die Notwendigkeit einer Datenschutzregelung, sondern lediglich der Weg, der dabei beschritten werden muß. So gesehen, ist gerade die Verarbeitung durch die Medien im allgemeinen und den Rundfunk im besonderen eines der Hauptbeispiele für die Erforderlichkeit einer bereichsspezifischen Regelung. Nur mit ihrer Hilfe läßt sich ein Differenzierungsgrad erreichen, der sowohl den Betroffenen ein Höchstmaß an Schutz bietet als auch der Presse- und Rundfunkfreiheit Rechnung trägt, in erster Linie also jeden Versuch ausschließt, die Datenschutzregelung in ein Zensurinstrument umzuwandeln. Das HDSG beläßt es deshalb zunächst bei der schon früher getroffenen, mittlerweile allgemein akzeptierten Unterscheidung zwischen einer Inanspruchnahme personenbezogener Daten für journalistisch-redaktionelle Zwecke einerseits und einer Verarbeitung für alle anderen, insbesondere also für administrative Zwecke andererseits. Bei den ersteren begnügt es sich mit einigen allgemeinen Grundsätzen und schreibt darüber hinaus die Bestellung eines internen Datenschutzbeauftragten vor, dem die

Kontrolle über die Einhaltung dieser Grundsätze obliegt. Die allgemein gehaltenen Formulierungen erklären sich nicht zuletzt aus der im Gesetzgebungsverfahren ausdrücklich geäußerten Erwartung, eine eingehende Regelung zu einem späteren Zeitpunkt im Rahmen einer Novellierung des Pressegesetzes zu treffen. Soweit jedoch nicht dieser originär journalistische Bereich berührt ist, spricht sich das HDSG für eine uneingeschränkte Anwendung seiner Vorschriften aus. Der Hessische Rundfunk muß infolgedessen die materiellen und organisatorischen Verarbeitungsanforderungen beachten und untersteht insoweit der Kontrolle des Hessischen Datenschutzbeauftragten (vgl. Ziff. 2.6). Genaugenommen, ist auch dies keine Novität. Genauso verfährt das Bundesdatenschutzgesetz.

Freilich: Keine der vom Gesetzgeber geäußerten Erwartungen ist bis jetzt erfüllt worden, im Gegenteil, der Hessische Rundfunk hat sich in jeder Beziehung über die Anforderungen des HDSG hinweggesetzt. Weder im journalistischen noch im administrativen Bereich ist der Datenschutz gesichert. Nach wie vor und allen Nachfragen zum Trotz ist der für die journalistische Tätigkeit allein zuständige interne Beauftragte nicht bestellt. Nach wie vor weigert sich der Hessische Rundfunk aber auch, die Voraussetzungen für eine korrekte Gesetzesanwendung bei allen übrigen Verarbeitungsfällen zu erfüllen. Er ist nicht einmal bereit, die Verarbeitungssituation offenzulegen und damit nicht zuletzt eine auch in seinem Interesse liegende Abgrenzung der beiden unterschiedlich geregelten Bereiche zu ermöglichen. Nicht weniger schwer wiegt die an die Adresse des Hessischen Datenschutzbeauftragten geäußerte Erwartung, die bei einer Kontrolle gewonnenen Erfahrungen aus seinem Tätigkeitsbericht auszunehmen, um damit jede öffentliche, also auch und gerade parlamentarische Diskussion über einen Teil jedenfalls der rundfunkinternen Verarbeitung, gleichviel ob sie sich auf die Hörer oder auf die Arbeitnehmer bezieht, auszuschließen.

Nie zuvor ist in der Geschichte des Datenschutzes die Geltung der gesetzlichen Bestimmungen so offen und unumwunden in Frage gestellt worden. Nie zuvor ist zudem so klar dem Gesetzgeber das Recht bestritten worden, die Verarbeitung personenbezogener Angaben an bestimmte, gesetzlich fixierte Bedingungen zu binden. Wohlgemerkt: Die Weigerung, das Gesetz anzuwenden, richtet sich nicht gegen einen Gesetzgeber, der die verfassungsrechtlich garantierte Freiheit des Rundfunks mißachtet, sondern gegen einen Gesetzgeber, der im Gegenteil alles getan hat, um jede Gefährdung dieser Freiheit zu vermeiden und gerade deshalb die ihm durchaus zustehenden Regelungsmöglichkeiten nicht einmal voll ausgeschöpft hat.

1.2.3
Bundesrecht

Eine dritte Anwendungsgrenze folgt schließlich aus den Kompetenzschranken des Landesgesetzgebers. Seine Zuständigkeit endet unstreitig dort, wo Bundesrecht das Handeln der öffentlichen Stellen des Landes abschließend regelt. Für den Hessischen Datenschutzbeauftragten ergibt sich die Verpflichtung, sorgfältig zu unterscheiden. Je nachdem, ob die kontrollierte Stelle Landes- oder Bundesrecht anwendet, wechselt auch der Kontrollmaßstab. Solange sich freilich die Verarbeitungsanforderungen decken, kommt dieser Feststellung weiter keine Bedeutung zu. Sobald sie aber auseinanderfallen, kann es durchaus zu einer, gerade im Hinblick auf die Glaubwürdigkeit sowie die Wirksamkeit des Datenschutzes überaus bedenklichen Entwicklung kommen.

Daß diese Gefahr alles andere als eine rein theoretische Spekulation ist, zeigen die jüngsten Vorschläge zur Novellierung des Bundesdatenschutzgesetzes. Sie sehen unter anderem eine empfindliche Einschränkung der Rechte des Bundesbeauftragten für den Datenschutz vor und nehmen im übrigen die Akten ausdrücklich von der Anwendung der revidierten Datenschutzvorschriften aus. Die Folgen lassen sich unschwer beschreiben. Der Betroffene kann dann, wenn Landesrecht angewendet wird, ohne weiteres mit einer gleich intensiven Kontrolle jeder Verarbeitung seiner Daten rechnen, ohne Rücksicht also darauf, ob sie in einer automatisch gesteuerten Datei oder in einer einfachen Akte enthalten sind. Sollte es jedoch um die Verarbeitungspraxis einer Behörde gehen, die zugleich Bundesrecht ausführt und dabei personenbezogene Angaben in Akten aufnimmt, verringern sich sofort die Kontrollmöglichkeiten. In bestimmten Fällen, wie etwa bei der Verarbeitung durch die Finanzämter, wird die Überwachung sogar generell erschwert. Die Reformvorschläge akzeptieren eine Kontrolle nur, wenn der Betroffene nicht widersprochen hat. Und um jeden Zweifel an der Tragweite dieser Aussage auszuschließen, fügt die Begründung hinzu, daß dem Betroffenen selbstverständlich Gelegenheit gegeben werden muß, sich rechtzeitig zu äußern. Dem Datenschutzbeauftragten wird damit von vornherein die Möglichkeit genommen, just den Weg zu gehen, der bislang als der einzig erfolgversprechende galt. Er könnte gar nicht mehr den gesamten Bestand an verarbeiteten Daten in seine Überwachung einbeziehen, um dann über einzelne unter Umständen interessierende individuelle Fälle hinaus, generelle Feststellungen über die Art und Weise, wie die Verarbeitung im jeweiligen Verwaltungszweig erfolgt, zu machen. Die besonders betonte Notwendigkeit einer vorherigen Information gibt zudem der Behörde die Chance, die Überwachung immer wieder hinauszuschieben und ihr damit jede Aktualität sowie letztlich jegliche Aussagekraft zu nehmen. Während es also dem Landesgesetzgeber ganz besonders darauf ankam, die Kontrollbefugnisse des Datenschutzbeauftragten zu stärken und eine lückenlose Überwachung zu sichern, zielen die Reformvorschläge zum Bundesdatenschutzgesetz eindeutig darauf ab, die Position des Datenschutzbeauftragten zu schwächen, ihm also selbst die Rechte, jedenfalls teilweise zu nehmen, die ihm das geltende Recht zugesteht.

Wie wichtig den Verfassern des Entwurfes gerade diese Korrektur zu Lasten des Datenschutzes ist, zeigt sich an der ausdrücklichen Feststellung, daß die von ihnen vorgesehenen Kontrollvoraussetzungen auch von den Landesdatenschutzbeauftragten zu beachten sind, soweit sie Verarbeitungsvorgänge kontrollieren, die im Zusammenhang mit der Ausführung von Bundesrecht stehen. Sieht man einmal von den verfassungsrechtlichen Bedenken auch und gerade gegen diese letzte Vorschrift ab, dann kann an den Folgen kein Zweifel bestehen: Einem konsequent auf die

Verwirklichung des Datenschutzes bedachten Landesdatenschutzgesetz würde in Zukunft ein ebenso konsequent auf die Einschränkung des Datenschutzes abzielendes Bundesdatenschutzgesetz gegenüberstehen. Die Verarbeitung müßte sich nach Kriterien richten, die sich nicht nur voneinander unterscheiden, sondern sogar offen widersprechen. Mit dem Übergang zur Ausführung von Bundesrecht würde auch der Datenschutz zurückweichen und der Betroffene weitgehend den im Anwendungsbereich des Hessischen Datenschutzgesetzes selbstverständlichen Schutz verlieren. Wenn aber die vom Bundesverfassungsgericht formulierten und vom Hessischen Landtag bestätigten Anforderungen an eine Gesetzgebung, die der Bedeutung des Datenschutzes für die Funktionsfähigkeit „eines auf die Handlungs- und Mitwirkungsfähigkeit seiner Bürger begründeten freiheitlichen demokratischen Gemeinwesens", um mit dem Bundesverfassungsgericht zu sprechen, wirklich Rechnung trägt, dann darf diese Entwicklung nicht hingenommen werden. Das Ziel muß im Gegenteil eine Regelung sein, die auf Landes- und Bundesebene ein gleich hohes Maß an Datenschutz sicherstellt.

1.3
Volkszählung 1987

Die Volkszählung gibt zu drei Feststellungen Anlaß. Zunächst: An der Verfassungsmäßigkeit ihrer gesetzlichen Grundlage gab und gibt es keinen Zweifel. Man kann sicher über manche Einzelheit des Volkszählungsgesetzes streiten. Nur läßt sich daraus nicht eine wie immer begründete Verfassungswidrigkeit der gesetzlichen Regelung ableiten. Darauf haben schon die früheren Tätigkeitsberichte hingewiesen. Sowohl der Hessische Verwaltungsgerichtshof als auch das Bundesverfassungsgericht haben inzwischen diese Meinung bestätigt (vgl. Ziff. 3.2.2.2). Im Unterschied freilich zu der in letzter Zeit wiederholt geäußerten Meinung, das Bundesverfassungsgericht habe mit diesen Entscheidungen zugleich seine ursprüngliche Position korrigiert, gilt es festzuhalten: Keine der bisher vorliegenden Aussagen ändert auch nur das Geringste an dem Ende 1983 zum seinerzeitigen Volkszählungsgesetz ergangenen Urteil. Es bleibt die nach wie vor verbindliche Richtlinie sowohl für die Regelung statistischer Erhebungen als auch für die Datenschutzgesetzgebung. Zur Debatte stand ausschließlich die Frage, ob das gegenwärtig geltende Volkszählungsgesetz den Anforderungen dieses Urteils entsprach, und nur darauf bezieht sich jede der späteren Entscheidungen.

Die Verfassungsmäßigkeit der gesetzlichen Regelung besagt, zweitens, noch nichts über die Rechtmäßigkeit der Durchführung der Volkszählung. Mit genau dieser Frage galt es, sich in den vergangenen Monaten immer wieder auseinanderzusetzen, und sie wird auch weiterhin im Vordergrund der Kontrollaufgaben des Datenschutzbeauftragten stehen. Um noch einmal das Bundesverfassungsgericht zu zitieren: Den Datenschutzbeauftragten und der Verwaltungsgerichtsbarkeit obliegt es, der Frage nachzugehen, ob und in welchem Umfang die Volkszählung korrekt abgelaufen ist (Entscheidung vom 28. September 1987 - 1 BvR 1063/87 unter Ziff. 3).

1.3.1
Defizite bei der Durchführung

Die Kontrolle hat, wie sich unschwer an den im Tätigkeitsbericht geschilderten Erfahrungen ablesen läßt, nicht das immer wieder propagierte Bild eines problemlosen Verlaufs der Volkszählung bestätigt (vgl. Ziff. 3.4). Im Gegenteil, so wenig im Prinzip gegen das Gesetz zu sagen ist, so viel läßt sich gegen seine Durchführung vorbringen. Sie war von Anfang äußerst problematisch, ganz gleich im übrigen, ob es um die Auswahl der Zähler, die Organisation der Erhebungsstellen, die Übermittlung der für ihre Tätigkeit notwendigen Angaben oder die Befragung der Betroffenen ging. So gesehen, überrascht es nicht, wenn sich unter diesen Umständen die Durchführung als ein äußerst kompliziertes und mühseliges Verfahren erwies, bei dem es fortlaufend Korrekturen anzubringen galt und bei dem trotzdem immer wieder neue Schwierigkeiten auftauchten. Viele der überprüften Erhebungsstellen waren nicht in einer den rechtlichen Anforderungen entsprechenden Weise organisiert. Oft bedurfte es der Intervention des Datenschutzbeauftragten, um einen gesetzeskonformen Ablauf sicherzustellen.

Gewiß, das Gesetz hat besonders an die Kommunen erhebliche Anforderungen gestellt und vor allem organisatorische Vorkehrungen verlangt, die sich häufig nicht komplikationslos realisieren ließen. Ebensowenig läßt sich bestreiten, daß es fast immer, zuweilen allerdings erst nach der Intervention der Aufsichtsbehörde, gelungen ist, die Mängel zu korrigieren. Nur darf man sich nicht mit dieser Feststellung zufrieden geben. Vielmehr gilt es, noch einmal an die Entscheidung des Bundesverfassungsgerichts zum Volkszählungsgesetz von 1983 zu erinnern. Das Gericht hat sich keineswegs darauf beschränkt, die Grundsätze einer verfassungskonformen statistischen Erhebung anzugeben. Es hat auch, und genau darauf kommt es hier an, ausdrücklich darauf hingewiesen, daß der Erfolg der Erhebung entscheidend vom Vertrauen der Bürger in eine die strikte Einhaltung einer streng zweckgebundenen Erhebung gewährleistenden Organisation der Volkszählung abhängt. Solange dieses Vertrauen nicht besteht, nutzen alle sonstigen Anstrengungen nichts. Eben deshalb wäre es unbedingt notwendig gewesen, so rechtzeitig mit den Vorbereitungen zu beginnen, daß die später aufgetretenen Mängel hätten verhindert werden können. Nichts hätte beispielsweise näher gelegen, als die Organisationsmodalitäten schon zu einem sehr frühen Zeitpunkt in einem Modell durchzuspielen und so beizeiten die erst im nachhinein festgestellten Defizite zu korrigieren. Statt dessen konnte und kann man sich des Eindrucks nicht erwehren, daß die viel zu spät begonnene Vorbereitung weitgehend planlos verlief, immer wieder ins Stocken geriet sowie wegen der fortlaufend auftretenden Mängel stets revidiert werden mußte. Der Preis für jeden dieser Mängel war ein Verlust an Glaubwürdigkeit. Dort wo die Bürger auch und gerade in Anbetracht der Entscheidung des Bundesverfassungsgerichts allen Anlaß hatten, eine einwandfreie Organisation zu erwarten, mußten sie zur Kenntnis nehmen, daß selbst elementare Vorkehrungen für eine korrekte Durchführung der Volkszählung unterlassen worden waren. Allzu leicht und allzu schnell wird aber dieser weit über

die gegenwärtige Zählung hinaus wirkende Vertrauensverlust durch die mittlerweile üblichen und ständig wiederholten Hinweise auf die Zahl der ausgefüllten Fragebögen verdrängt.

1.3.2
Zukünftige Zählungen

Beides, sowohl die verfassungsrechtlichen Anforderungen an statistische Erhebungen als auch die konkreten Erfahrungen mit der Durchführung der Volkszählung, zwingt drittens dazu, sich jetzt schon mit den Voraussetzungen sowie dem Ablauf zukünftiger Zählungen auseinanderzusetzen. Das Bundesverfassungsgericht hatte es bei aller Bereitschaft, die unter den gegenwärtigen Bedingungen stattfindende Volkszählung für verfassungsmäßig anzusehen, ausdrücklich abgelehnt, die jetzige Form als die einzig mögliche und deshalb auch für alle Zukunft beizubehaltende zu akzeptieren. Das Gericht hat vielmehr den Gesetzgeber unmißverständlich aufgefordert, sich intensiv mit anderen Erhebungsmöglichkeiten zu beschäftigen. So viel steht deshalb fest: Eine Erhebung, die sich wie jetzt auf eine gesetzlich vorgeschriebene Auskunftspflicht gründet, ist nur eine vorübergehend akzeptable Regelung. Dahinter steht die schon erwähnte, vom Bundesverfassungsgericht bekräftigte Überlegung, daß, so notwendig statistische Erhebungen sind, ihr Erfolg, noch genauer ihre Aussagekraft vom Vertrauen der Bürger, also von deren Bereitschaft abhängt, die gewünschten Informationen zur Verfügung zu stellen. Nur dort, wo der Bürger von der Notwendigkeit der Erhebung überzeugt ist, weil er ihre Ziele kennt und sich auch darauf verlassen kann, daß die Daten ausschließlich für die ihm bekannten Zwecke verarbeitet werden, hat es Sinn, mit seiner Kooperation zu rechnen sowie sich auf seine Aussagen zu verlassen. Anders ausgedrückt: Es genügt nicht, noch so nachdrücklich darauf hinzuweisen, daß die Erhebung für den Bürger erfolgt, sie muß auch mit ihm geschehen und von ihm getragen werden. Unter diesen Umständen muß nicht der Zwang, sondern die Freiwilligkeit das auch rechtlich abzusichernde Fundament jeder Erhebung sein. Ganz in diesem Sinn hatte sich früher schon der Bundestag ausgesprochen. Der Hessische Landtag ist noch einen Schritt weitergegangen. Das Landesstatistikgesetz räumt als erste gesetzliche Regelung der Freiwilligkeit eindeutig den Vorrang ein.

Wie sehr damit eine Position eingenommen wird, die auch der Überzeugung der Bürger entspricht, zeigen, so seltsam es zunächst klingen mag, auch die Erfahrungen mit der Volkszählung. Selbst wenn gegenwärtig kein Zweifel am Beteiligungszwang besteht, verpflichtet das Gesetz die Betroffenen keineswegs, die von ihnen gewünschten Informationen in Gegenwart der Zähler und als Antwort auf die von diesen gestellten Fragen zu geben. Der Gesetzgeber ist im Gegenteil, was allerdings oft vergessen wird, dem ausdrücklichen Hinweis des Bundesverfassungsgerichts gefolgt und hat es den Auskunftspflichtigen freigestellt, den Fragebogen allein auszufüllen sowie selbst zu verschicken.

Gewiß, mit einer freiwilligen Teilnahme hat diese Regelung nichts zu tun. Sie bringt aber deutlich die Intention zum Ausdruck, eine selbständige Beteiligung wenigstens für einen Teil des Verfahrens anzuerkennen. Welchen Wert die Betroffenen gerade darauf legen, erweist sich an der hohen, wahrscheinlich von kaum jemandem erwarteten Zahl derjenigen, die es vorgezogen haben, den Fragebogen selbst zu versenden. Und dies, obgleich es nicht an Hindernissen gefehlt hat. So scheinen etlichen Erhebungsstellen die Briefumschläge sehr bald ausgegangen zu sein. Um so bemerkenswerter ist die entschiedene Inanspruchnahme der gesetzlich vorgesehenen Alternative bei der Ausfüllung. Sie rechnet zu den wahrscheinlich wichtigsten Erfahrungen, und zwar auch und gerade deshalb, weil sie deutlich demonstriert, wie sehr es den Betroffenen auf Verfahren ankommt, die ihre Entscheidungsfreiheit respektieren und ihnen daher den höchstmöglichen Entscheidungsspielraum garantieren. Just dieses Ziel läßt sich aber am ehesten und besten über eine freiwillige Teilnahme erreichen.

Nach wie vor fehlt es, ohne Zweifel, an überzeugenden Vorschlägen für eine freiwillige Erhebung, mit deren Hilfe es gelingen könnte, die mit der Volkszählung angestrebten Informationsziele zu erreichen. Ebensowenig ist jedoch zu übersehen, daß bislang weit mehr Wert darauf gelegt wurde, die Unentbehrlichkeit des jetzigen Verfahrens zu betonen als auf den Versuch, Alternativen auszumachen. Für Statistiker scheint es weitgehend unvorstellbar zu sein, daß ein solange praktiziertes, von ihnen mittlerweile für selbstverständlich gehaltenes Verfahren plötzlich nicht mehr akzeptabel sein soll. Insofern verwundert es nicht, wenn ihre Argumentation immer wieder darauf hinausläuft, zu beteuern, wie gut bisher alles funktioniert habe und wie unangebracht, ja von Grund auf verfehlt sämtliche Zweifel seien. Genausowenig überraschen die kritischen, zuweilen unverhohlen disqualifizierenden Bemerkungen über das Recht der Auskunftspflichtigen, Fragebögen selbst auszufüllen. Die amtliche Statistik soll eben durch amtliche Zähler in der amtlich verordneten Art und Weise vollzogen werden. Jede Abweichung erscheint unter diesen Umständen als ein gefährlicher, durch nichts zu rechtfertigender Störfaktor. Der Betroffene verliert eben seinen Wert als „Informationsschuldner" von dem Augenblick an, in dem er die amtliche Statistik all den Risiken aussetzt, die mit einer aktiven persönlichen Beteiligung einhergehen.

Zweierlei bleibt dabei unbeachtet. Die Auseinandersetzung um die Volkszählung war und ist zuvörderst eine Diskussion über die Notwendigkeit sowie die Grenzen einer strikt zweckgebundenen Verarbeitung. Konsequenterweise richteten sich die verfassungsrechtlichen Einwände gegen das frühere Volkszählungsgesetz in erster Linie gegen den vom Gesetzgeber geduldeten, ja ausdrücklich anerkannten Zugriff anderer Behörden auf die Daten durchaus identifizierbarer Personen. So gesehen stand seinerzeit nicht die Statistik zur Debatte, sondern die Zweckentfremdung der für statistische Ziele erhobenen Angaben.

Die Kritik richtet sich insofern vor allem gegen eine Verwaltung, die nicht zuletzt vor dem Hintergrund der durch die Informationstechnologie gebotenen Verarbeitungsmöglichkeiten meinte, das mit Hilfe der Volkszählung gewonnene Informationsmaterial auch für administrative Zwecke nutzen zu können.

Das Bundesverfassungsgericht hat freilich zugleich klargestellt, daß der bloße Hinweis auf die Notwendigkeit statistischer Erhebungen keineswegs ausreicht, um jeden Informationswunsch zu rechtfertigen. Vielmehr gilt hier wie sonst der Grundsatz der Erforderlichkeit. Seine Folgen sind verständlicherweise verschieden, je nachdem welche Ziele durch die jeweilige statistische Erhebung verfolgt werden. Eines ändert sich dennoch nicht: Auch bei der Volkszählung kann, ja muß gefragt werden, welche Daten genau im Hinblick auf die spezifischen Zwecke einer solchen generellen Erhebung wirklich benötigt werden. Nichts anderes verbirgt sich hinter der Diskussion um den exakten Gehalt jener „Grunddaten" auf die immer wieder verwiesen wird, wenn die Unverzichtbarkeit der Volkszählung zur Diskussion steht.

Schließlich: Spätestens seit der Verabschiedung der Datenschutzgesetze steht fest, daß eine zwangsweise Erhebung personenbezogener Daten weder selbstverständlich ist, noch beliebig angeordnet werden kann. Solange der sich unmittelbar aus der Verfassung ergebende Grundsatz der informationellen Selbstbestimmung wirklich ernstgenommen wird, muß eine Erhebung ohne Zustimmung des Betroffenen die seltene, stets besonders zu rechtfertigende Ausnahme bleiben. Es gibt deshalb keinen Bereich der öffentlichen Verwaltung, der für sich in Anspruch nehmen kann, die für seine Aufgaben erforderlichen Daten durchweg ohne Rücksicht auf die Einstellung der Betroffenen, ja unter Umständen auch ohne deren Kenntnis erheben zu können. Jeder Verwaltungszweig ist im Gegenteil zunächst verpflichtet, alles zu unternehmen, um die Kenntnis, aber auch die Beteiligung der Betroffenen zu sichern. Gerade diese Feststellung gewinnt im Zusammenhang mit statistischen Untersuchungen deshalb eine besondere Bedeutung, weil, um das schon mehrfach genannte Argument in Erinnerung zu rufen, deren Verläßlichkeit entscheidend von der Kooperationsbereitschaft sowie dem Vertrauen der Betroffenen abhängen.

Die Statistischen Ämter sehen sich daher mit einer überaus konkreten Erwartung konfrontiert. Es ist ihre ureigenste Aufgabe, Mittel und Wege anzugeben, die es ermöglichen, die Auskunftspflicht durch eine freiwillige Information zu ersetzen. Was also von ihnen verlangt wird, ist nicht die Vorzüge der bisherigen Verfahren zu beschreiben und wissenschaftlich attestieren zu lassen, sondern umgekehrt, die Impulse für neue Verfahren zu liefern, die den veränderten normativen Rahmenbedingungen entsprechen. Kurzum, Ziel aller Anstrengungen muß es sein, die Auskunftspflicht in die Geschichte der Statistik zu verweisen und einen neuen auf die Freiwilligkeit gegründeten und durch sie legitimierten Abschnitt in der Entwicklung der Statistik einzuleiten.

1.4
Aids

Aids war bereits im 15. Tätigkeitsbericht als eine zentrale, wenn nicht sogar die gegenwärtig wichtigste Datenschutzfrage bezeichnet worden. An dieser Einschätzung hat sich nichts geändert. Im Gegenteil, die Befürchtung hat sich bewahrheitet, daß Aids schnell und oft dazu führen könnte, die ansonsten akzeptierten Datenschutzgrundsätze in Frage zu stellen, vor allem also personenbezogene Angaben an den Betroffenen vorbei und ohne jede rechtliche Grundlage zu erheben oder zu übermitteln. Bezeichnend dafür ist schon die Diskussion über Aids-Tests im Krankenhaus (vgl. Ziff. 6.1.1.1). Die Selbstverständlichkeit, mit der in einer Vielzahl von Fällen entsprechende Untersuchungenvorgenommen worden sind, ohne zuvor die Betroffenen zu unterrichten, dokumentiert nicht etwa eine bedauerliche Nachlässigkeit, sondern die weit verbreitete Überzeugung, daß gerade bei Aids alle sich bietenden Gelegenheiten genutzt werden müssen, um Aids-Infizierte zu identifizieren. Über die Konsequenzen, die ein positives Ergebnis haben kann, wird folglich gar nicht erst weiter nachgedacht, der Aids-Test erscheint als notwendige, routinemäßig durchzuführende Maßnahme.

Genauso signifikant sind die Versuche, einzelne Personengruppen gezielt zu untersuchen. Ganz gleich, ob es sich um die Angehörigen bestimmter Berufe, Asylbewerber oder Insassen von Haftanstalten handelt, immer wieder mußte daran erinnert werden, daß der Test eben grundsätzlich nicht ohne Kenntnis der Betroffenen sowie ohne ihr Einverständnis durchgeführt werden darf (vgl. Ziff. 6.1.1.2 und 6.1.1.3). Die korrekte rechtliche Abfolge kehrt sich offensichtlich um: Statt sich grundsätzlich an der Entscheidung der Betroffenen zu orientieren und lediglich für die möglicherweise notwendigen wenigen Ausnahmefälle nach einer besonderen Begründung zu suchen, wird mehr und mehr eine Begründung für die Information des Betroffenen sowie die Verpflichtung verlangt, seine Einwilligung einzuholen. Selbst dort, wo auf den ersten Blick durchaus die Bereitschaft besteht, die Betroffenen einzuschalten, bleibt letzlich, wie das Beispiel der Haftanstalten zeigt, kaum noch etwas davon übrig. Wer den Betroffenen mitteilt, auf ihre Einwillung werde durchaus Wert gelegt, zugleich aber erklärt, sie seien zur Teilnahme am Test rechtlich verpflichtet, verwandelt das Einverständnis in nutzloses Beiwerk.

In die gleiche Richtung weisen schließlich Forderungen wie etwa die nach einer Eintragung eines besonderen Aids-Vermerks in die polizeilichen Register (vgl. Ziff. 6.1.2). Wiederum bleiben die Reaktionen der Betroffenen genauso außer acht wie die Konsequenzen der Registrierung. Und erneut genügt offenbar der Hinweis auf die besondere Gefährlichkeit von Aids, um alle Bedenken gegen die Eintragung zu zerstreuen. Gewiß, wann immer Skepsis und Kritik auftauchen, pflegt auf die Fürsorgepflicht verwiesen zu werden. Nur: Kaum ein anderes Argument eignet sich besser dazu, nahezu alle Betroffenen ohne jede Rücksicht auf ihre Einstellung zu registrieren. Zur Fürsorge ist jeder Arbeitgeber verpflichtet. Wo es deshalb ausreicht, sich auf die Fürsorgepflicht zu berufen, um eine Eintragung vorzunehmen oder auch eine Übermittlung zuzulassen, muß jeder Arbeitnehmer mit der Registrierung rechnen, und zwar ohne Rücksicht darauf, ob er von einer öffentlichen oder einer privaten Stelle beschäftigt wird. Insofern verwundert es nicht, wenn mittlerweile bei Aids-Tests in Krankenhäusern genauso von der Fürsorgepflicht die Rede ist, wie bei der Diskussion über generelle Untersuchungen in Schulen. Der rasche Rückgriff auf die Fürsorgepflicht verdeckt zudem, daß sich der beabsichtigte Schutz, etwa bei der Polizei, auf diesem Weg gar nicht

erreichen läßt. Genau darin liegt aber einer der unter Datenschutzgesichtspunkten wichtigsten Einwände. Vor jedem Zugriff auf personenbezogene Angaben gilt es, sich Gewißheit darüber zu verschaffen, ob deren Verarbeitung im konkret zur Debatte stehenden Zusammenhang erforderlich ist. Der Zugang zu den personenbezogenen Daten bleibt mit anderen Worten solange versperrt, wie nicht einwandfrei dargetan worden ist, daß ein bestimmtes, rechtlich abgesichertes Ziel nur mit Hilfe einer personenbezogenen Information verwirklicht werden kann. Wohlgemerkt, niemand verkennt die schwierige Situation, in der sich gerade Polizeibeamte befinden, und ebenso vermessen wäre es, die Angst zu ignorieren, die jeder empfindet, der in eine vergleichbare Lage gerät. Gerade deshalb kommt es aber besonders darauf an, nicht mit falschen Mitteln falsche Hoffnungen zu wecken. Die Erinnerung an die Verpflichtung, stets die Erforderlichkeit nachzuweisen, ist, so gesehen, mehr als Abwehr einer willkürlichen Stigmatisierung, sie zwingt zugleich dazu, ausschließlich Regelungen zur Diskussion zu stellen, von denen ernsthaft ein Beitrag zur Eindämmung der Gefahren von Aids erwartet werden kann.

Aus diesem Grund zählt die Erforderlichkeit zu den Gesichtspunkten, die es zuvördert zu bedenken gilt, wenn von einer Meldepflicht die Rede ist. Sicher, die Bestrebungen, eine personenbezogene Meldepflicht einzuführen, haben sich bislang nicht durchgesetzt. Die unstreitig notwendigen epidemiologischen Untersuchungen lassen sich eben auch mit anonymisierten Angaben durchführen. So wenig daher auf eine ebenso kontinuierliche, wie zentralisierte Information verzichtet werden kann, so deutlich lassen sich die rechtlich gebotenen Informationsgrenzen angeben. Die Erfahrungen mit der Laborberichtsverordnung (vgl. Ziff. 6.1.4.2) unterstreichen jedoch, daß sich die Datenschutzprobleme nicht einfach durch die Bereitschaft erledigen, es bei einer anonymen Berichtspflicht zu belassen. Vielmehr gilt es genauso intensiv die Bedingungen zu untersuchen, unter denen die Angaben zusammengetragen werden. Wer beispielsweise von den Labors Informationen verlangt, die sie weder haben können noch haben dürfen, begünstigt eine unzulässige Verbreitung hochsensibler personenbezogener Daten. Genau deshalb geht es nicht an, Informationswege zu beschreiten, die faktisch den Übermittlungsdruck verstärken. Die Laborberichtsverordnung hat diese Gefahr nicht gebannt. Hinzu kommt ein weiteres: Die Übereinstimmung darüber, daß für eine Verarbeitung lediglich anonymiserte Angaben in Betracht kommen, darf keineswegs dazu führen, die Zahl der gesammelten Informationen gleichsam beliebig zu steigern, nicht zuletzt mit Rücksicht auf die bereits erwähnten Gefahren im Vorfeld der Anonymisierung. Die Informationsanforderung läßt sich nicht von der Reflexion über die Informationsziele trennen. Erst deren exakte Umschreibung erlaubt es auch, Gewißheit über das erforderliche Material zu gewinnen, schränkt also zugleich die Informationswünsche und dadurch die Verbreitungsgefahr ein.

Vor diesem Hintergrund gewinnt die im Hessischen Landtag aus Anlaß des CDU-Antrages vom September 1987 geführte Debatte eine ganz besondere Bedeutung. Sie hat die Priorität einer Information des Betroffenen sowie die Notwendigkeit seines Einverständnisses deutlich unterstrichen und zugleich klar zu erkennen gegeben, wie wichtig es ist, einheitliche Grundsätze für die Verwaltungstätigkeit festzulegen. Genauso gilt es, an die Feststellung des Hessischen Sozialministeriums zu erinnern. Sie sprechen sich gegen routinemäßige, zumal in Unkenntnis des Betroffenen durchgeführte Untersuchungen, aber auch gegen die Tendenzen einer generalisierten Registrierung aus. Diese Ansatzpunkte müssen jetzt konsequent weiter verfolgt und ausgebaut werden, nicht zuletzt mit Hilfe der zu erwartenden, vom Landtag ausdrücklich angesprochenen Richtlinien der Landesregierung.

1.5
Umfragen

Datenschutzprobleme, die mit Umfragen zusammenhängen, waren in früheren Tätigkeitsberichten eher sparsam behandelt worden. Nicht etwa, weil es keine Schwierigkeiten gab. Erst jetzt haben sich jedoch die Komplikationen in einem Maße zugespitzt, das eine sehr viel eingehendere Behandlung erforderlich erscheinen läßt. Der diesjährige Tätigkeitsbericht greift zwei der wichtigsten Fälle auf. Sie sind in mehrfacher Hinsicht typisch für den Problemwandel, aber auch für die in der Tat oft recht schwierigen Anwendungsprobleme, die bei Umfragen auftreten. Bisher richtete sich die Aufmerksamkeit vor allem auf Umfragen im Rahmen einzelner sozialwissenschaftlicher oder medizinischer Forschungsprojekte. Mittlerweile gewinnen aber die von den Kommunen durchgeführten oder auch veranlaßten Umfragen, um etwa die Reaktion auf die verschiedenen von ihnen angebotenen Leistungen besser ermessen zu können, an Bedeutung. Zudem haben früher mehr oder weniger umfangreiche schriftliche Umfragen im Mittelpunkt der Aufmerksamkeit gestanden. An die Stelle der Fragebögen tritt, zumindest in einzelnen Bereichen, mehr und mehr die telefonische Umfrage.

Zweierlei ist dabei bemerkenswert, zum einen die offensichtlich immer längere Dauer der telefonischen Befragung und zum anderen die wachsende Tendenz, aus dem Ausland anzurufen. Beides scheint nicht zuletzt eine Reaktion auf die als zunehmend hinderlich empfundenen Datenschutzvorkehrungen zu sein. Die telefonische Umfrage macht es, jedenfalls auf den ersten Blick, sehr viel leichter, sich über die ohnehin ständig kritisierte Forderung nach einer im Prinzip schriftlichen Einwilligung der Befragten hinwegzusetzen. Die Verlegung ins Ausland erlaubt es, zumindest zunächst, auf einen ganz anderen, eben nicht mit vergleichbaren Datenschutzbestimmungen belasteten rechtlichen Hintergrund zu verweisen.

Beide Annahmen beruhen freilich auf einem Trugschluß. Am Geltungsanspruch der auch bisher uneingeschränkt zu beachtenden Datenschutzvorschriften ändert sich nicht das Geringste. Nach wie vor gilt es, beispielsweise, von den Vorstellungen auszugehen, die den Gesetzgeber veranlaßt haben, die Verarbeitung personenbezogener Daten von einer grundsätzlich schriftlichen Einwilligung abhängig zu machen. Der Betroffene soll zunächst und vor allem präzise erfahren, was zu den einzelnen Fragen führt, und wie mit den Antworten verfahren werden soll, um dann selbst, und zwar in einer Form, die jedes Mißverständnis ausschließt, zu entscheiden. Eben deshalb kann es nicht

weiter wichtig sein, ob ihm ein Fragebogen übergeben, vorgelesen oder zugeschickt oder ob ihm die jeweilige Frage telefonisch gestellt wird. Spätestens an der Dauer des Telefongesprächs zeigt sich, daß sich zwar die Befragungsform verändert hat, der Betroffene aber vor genau den Problemen steht, die zur gesetzlichen Regelung geführt haben. Der süffisante Hinweis auf die Möglichkeit des Betroffenen, den Hörer aufzulegen, verfälscht das Bild der Befragungssituation. Die Betroffenen unterbrechen eben nicht das Gespräch, weil es ineiner Art und Weise eingeleitet wird, die seine Länge, seinen Inhalt und seine Tragweite nicht erkennen läßt. Die Entscheidung für eine Telefonumfrage befreit deshalb nicht von der Verpflichtung, sich von den Betroffenen eine schriftliche Einwilligung geben zu lassen. Das schriftlich formulierte Einverständnis bleibt vielmehr die unabdingbare Voraussetzung einer Verarbeitung der jeweils erhobenen Daten. Gewiß, Ausnahmen von der Schriftlichkeit kann es nach dem geltenden Recht geben, sie finden aber keine Anwendung auf die hier zur Debatte stehenden Umfragen, und zwar vor allem mit Rücksicht auf deren Umfang und Inhalt.

Soweit es nun um Anrufe aus dem Ausland geht, wird allzu schnell übersehen, daß die personenbezogenen Daten im Inland erhoben werden. Insofern ist es gleichgültig, von wo aus die Frage jeweils gestellt wird. Die Datenschutzvorschriften sind in jedem Fall zu beachten, ganz gleich also ob die gesetzlichen Anforderungen an die Form oder an die vom Gesetzgeber festgehaltenen inhaltlichen Verarbeitungsbedingungen zur Debatte stehen. Soweit diese Erwartungen außer acht bleiben, kommt es zu einer illegalen Verarbeitung. Ihre Ergebnisse dürfen insofern, zumindest im Bereich der Bundesrepublik, nicht verwendet werden. Trotzdem läßt sich nicht leugnen, daß gerade das Einwilligungserfordernis unter Umständen Schwierigkeiten bereitet, die das Ziel des Gesetzes in Frage stellen, den Betroffenen die Chance einzuräumen, Einfluß auf den Verarbeitungsprozeß zu nehmen. Eine strikt am Wortlaut orientierte Anwendung legt den Schluß nahe, daß die Einwilligung vor der Befragung erteilt werden muß. Jede solche Interpretation hindert aber letztlich den Betroffenen daran, seine Entscheidung vor dem Hintergrund einer genauen Information über Zweck und Inhalt der Befragung zu treffen. Wenn er sich wirklich über beides zunächst Gewißheit verschaffen soll, dann kann er nicht umhin, sich erst die Fragen anzuhören, sich über sie zu unterhalten und dabei auch einen Eindruck über das Umfeld sowie die möglichen Auswirkungen der Befragung zu gewinnen. Den Grundvorstellungen der gesetzlichen Regelung entspricht es deshalb bei längeren und komplizierten Befragungen weit eher, die Entscheidung über eine mögliche Verarbeitung nach der Befragung zu fällen. Eines sollte jedoch klar sein: Keine einzige vor Abschluß des Gesprächs erteilte Information darf verarbeitet werden, wenn die Einwilligung ausbleibt. Was immer an Daten auch mitgeteilt worden sein mag, eignet sich nicht für eine Verwertung. Wo deshalb die Angaben in irgend einer Form festgehalten worden sind, müssen sie vernichtet werden. Noch einmal aber: Ziel einer solchen Interpretation der entsprechenden gesetzlichen Bestimmungen ist es ausschließlich, die vom Gesetz gewollte Information des Betroffenen besser zu verwirklichen. An den gesetzlich vorgeschriebenen Verarbeitungsbedingungen ändert sich deshalb dadurch überhaupt nichts.

1.6
Landesautomation

Der 15. Tätigkeitsbericht (Ziff. 9) war ausführlich auf die Konsequenzen eingegangen, die sich aus der zunehmenden Verbreitung der Personal-Computer für den Datenschutz ergeben. Der diesjährige Bericht beschäftigt sich genauso eingehend mit den Auswirkungen einer sich immer mehr zum selbstverständlichen Arbeitsinstrument der öffentlichen Verwaltung entwickelnden Informationstechnologie (vgl. Ziff. 4). Hessen ist zwar nicht, wie etwa Baden-Württemberg, den Weg einer breit angelegten, langfristig im voraus geplanten Automatisierung der Landesverwaltung gegangen. Insofern fehlt es an einem ähnlich klar umrissenen Anknüpfungspunkt für eine Auseinandersetzung mit den Folgen der Automatisierung. Allerdings läßt sich kaum übersehen, daß inzwischen vielerorts eine technische Infrastruktur entstanden ist und auch konsequent weiter ausgebaut wird, die alle Voraussetzungen für zentralisierte Informationssysteme mit sich bringt. Unter diesem Gesichtspunkt darf nicht abgewartet werden, bis es etwa zu Vernetzungen kommt, um die einzelnen Datenschutzaspekte aufzugreifen. Vielmehr gilt es, just diese Fragen bereits in dem Augenblick aufzuwerfen, in dem die Entscheidung für eine die automatisierte Datenverarbeitung ermöglichende Bürokommunikation gefällt wird. Ebensowenig kann die Tatsache von Belang sein, daß es einstweilen jedenfalls noch weitgehend offen ist und letztlich von der Initiative der einzelnen Stellen abhängt, ob und in welchem Umfang das für eine Automatisierung notwendige Instrumentarium angeschafft wird. Mit seiner Installation ist zumindest technisch der Weg für spätere Verbindungen geebnet. Ziel aller Datenschutzgesetze ist es aber von Anfang gewesen, einen freien Umlauf personenbezogener Angaben zu verhindern und nur eine auf bestimmte, klar identifizierbare Zwecke beschränkte Verarbeitung zuzulassen. Deshalb war und ist beispielsweise eine Online-Verbindung allenfalls unter gewissen gesetzlich geregelten Bedingungen hinzunehmen. Und aus dem gleichen Grund kann es nicht gleichgültig sein, daß, sei es auch nur technisch, die Möglichkeit einer uneingeschränkten Zirkulation der Daten entsteht. Der Datenschutz beginnt schon bei den einzelnen Bausteinen der Vernetzung. Deshalb läßt sich die Antwort auf die im Tätigkeitsbericht aufgeworfenen Fragen nicht hinausschieben. Nur wenn sie jetzt diskutiert und beantwortet werden, kann es gelingen, die weitere Entwicklung an eine präventive Intervention zu knüpfen und sich nicht auf letzlich aussichtslose punktuelle Korrekturen eines in seiner Struktur nicht mehr korrigierbaren Informationsystems zu beschränken.

1.7
Perspektive

Gerade weil der Tätigkeitsbericht einzelne Problembereiche in den Vordergrund rückt, zwingt er auch dazu, sich immer wieder zu fragen, ob es nicht Gebiete gibt, die sehr viel mehr als bisher beachtet werden müßten. Zwei Beispiele drängen sich sofort auf. Das eine erinnert an einen der gleichsam klassischen Verarbeitungsbereiche, die Verwertung

personenbezogener Daten durch die Finanzämter. Sicher, Bemerkungen dazu finden sich in einer ganzen Reihe von Tätigkeitsberichten. Nicht zuletzt die gerade in letzter Zeit intensivierten Ansätze für einen internationalen Datenaustausch sind Anlaß genug, um sich erneut und intensiv mit den Bedingungen auseinanderzusetzen, unter denen auf personenbezogene Angaben für steuerliche Zwecke zurückgegriffen wird. Ein weiterer, nicht minder wichtiger Grund ist die offensichtliche Tendenz, Informationen, die für ganz bestimmte Steuerzwecke zur Verfügung gestellt werden, auch in anderen, davon völlig unabhängigen Zusammenhängen zu nutzen. Neu ist das Problem, genaugenommen, nicht. Nur gilt es hier wie sonst zu fragen, wo denn genau die Grenzen einer durch den jeweiligen Verarbeitungszweck legitimierten Verwendung der Angaben verlaufen.

Das zweite Beispiel lenkt die Aufmerksamkeit auf einen Verarbeitungskomplex, der erst jüngst in den Anwendungsbereich des Hessischen Datenschutzgesetzes einbezogen worden ist: die Verarbeitung personenbezogener Daten durch die öffentlich-rechtlichen Kreditinstitute. Mehr als eine erste Annäherung an die damit verbundenen Probleme konnte in der kurzen Zeit seit dem Inkrafttreten des Gesetzes nicht geleistet werden. Eines steht trotzdem fest: In kaum einem anderen Bereich werden personenbezogene Angaben so intensiv und unter einer so konsequenten Nutzung aller durch die Entwicklung der Informationstechnologie gebotenen Möglichkeiten verwertet. Um keine Mißverständnisse aufkommen zu lassen: Weder die Verarbeitungsziele noch die Verarbeitungsprobleme sind ausschließlich typisch für die öffentlich-rechtlichen Kreditinstitute, sondern im Gegenteil kennzeichnend für Zwecke, die im Kreditbereich überhaupt verfolgt werden und für Fragen, die dort generell auftauchen. So sehr aber gerade dieser Aspekt immer wieder betont werden muß, so wenig darf die Verarbeitung durch die öffentlich-rechtlichen Kreditinstitute vernachlässigt werden. Sie zählt im Gegenteil zu den Verarbeitungsfällen, die mehr und mehr in den Vordergrund der Tätigkeit des Datenschutzbeauftragten gerückt werden müssen, und zwar sowohl im Hinblick auf die innovative Nutzung der Informationstechnologie, wie sich allein schon am Beispiel der intelligenten Karten zeigt, als auch mit Rücksicht auf das offenkundig hohe Interesse der Bürger an einer Information in einem für sie tagtäglich relevanten Bereich.

Umgekehrt gilt es einmal mehr vor der Trivialisierung des Datenschutzes zu warnen. Längst ist es offenbar zur Gewohnheit geworden, sich jedem für unangenehm empfundenen Informationswunsch durch einen ebenso entschlossenen wie kurzen Hinweis auf den Datenschutz zu entziehen. Je mehr das Interesse am Datenschutz zugenommen hat, je deutlicher seine Bedeutung durch die Rechtsprechung, zumal durch das Bundesverfassungsgericht unterstrichen worden ist, desto größer scheint die Versuchung zu sein, sich auf ihn ohne jede Rücksicht auf den Hintergrund und die Details der jeweils gestellten Frage zu berufen. So muß der Datenschutz herhalten, um die Weigerung zu rechtfertigen, die Daten längst verstorbener Personen mitzuteilen, obgleich nicht der mindeste Zweifel daran bestehen kann, daß kein einziges Datenschutzgesetz auch nur im entferntesten die Angaben über nicht mehr lebende Personen in seinen Anwendungsbereich mit einbezieht. Mit der gleichen Selbstverständlichkeit pflegt man den Datenschutz heranzuziehen, um mit allem Nachdruck die Einrichtung von „Diskretionszonen" vor den Schaltern von Banken oder Postämtern zu fordern, etwas weniger verschroben ausgedrückt, von deutlichen Markierungen, die die einzelnen Kunden daran hindern sollen, sich jeweils über die Schulter zu schauen. So verständlich solche Erwartungen sind, der Datenschutzvorschriften bedarf es dafür nicht. Wer sich schon auf juristische Argumentationen einlassen will, kann auch mit den ebenso traditionellen wie respektablen Regeln des Vertragsrechts auskommen. Nun könnte man durchaus meinen, daß es vollkommen überflüssig ist, sich mit solchen Erscheinungen zu beschäftigen, so bedauerlich sie im übrigen seien. Wer allerdings so argumentiert, unterschätzt die Folgen. Der genauso unvermittelte wie durch nichts begründete Hinweis auf den Datenschutz verblüfft nicht nur, er stellt die Glaubwürdigkeit aller Anstrengungen in Frage, die Verarbeitung personenbezogener Angaben an strenge Bedingungen zu binden, und zwar sehr oft gerade bei denjenigen, die durchaus von der Notwendigkeit von Datenschutzvorschriften überzeugt sind. Offenkundig deplacierte Hinweise auf den Datenschutz führen ebenso wie eine banalisierte Anwendung der gesetzlichen Bestimmungen schnell dazu, die Datenschutzanforderungen nicht mehr sonderlich ernst zu nehmen und in ihnen eine von vielen eher überflüssigen Regelungen zu sehen. Sich für den Datenschutz konsequent einsetzen, heißt deshalb auch, sich in aller Deutlichkeit und Schärfe gegen alle Trivialisierungstendenzen zu wenden.

2.
Das neue Hessische Datenschutzgesetz - die ersten Erfahrungen, die wichtigsten Auslegungsfragen

2.1
Auswirkungen der Novellierung

Das neue Hessische Datenschutzgesetz (HDSG) vom 11. November 1986 hat die Novellierungsdiskussion in Bund und Ländern nachhaltig belebt. Dies belegen die zahlreichen Überlegungen in anderen Bundesländern, das Landesdatenschutzgesetz zu novellieren. Zu erwähnen sind in diesem Zusammenhang vor allem das am 1. Oktober 1987 in Kraft getretene Bremische Datenschutzgesetz (Gesetzblatt der Freien Hansestadt Bremen 1987 S. 235), sowie der Entwurf der rheinland-pfälzischen SPD-Fraktion (Landtags-Drucks. 11/18 vom 4. Juni 1987). Beide Vorschläge sind deutlich geprägt durch das HDSG. Dagegen soll anscheinend die fällige Novellierung des Bundesdatenschutzgesetzes - ein offizieller Referenten- oder gar Regierungsentwurf ist in dieser Legislaturperiode noch nicht vorgelegt worden - weit hinter den Standards, die das HDSG setzt, zurückbleiben.

In meiner Dienststelle hat das neue HDSG zu einer Flut von Anfragen der Bürger und Behörden geführt. Erste Auslegungsfragen habe ich bereits in meinem letzten Tätigkeitsbericht (Ziff. 2.2) und in der Broschüre „Hessisches

Datenschutzgesetz" beantwortet. Von dieser Broschüre sind 21.000 Stück verteilt oder versandt worden. In einer Vielzahl von Schreiben, Telefonaten, Dienstbesprechungen und Fortbildungsveranstaltungen habe ich zu Interpretationsproblemen Stellung genommen.

Dabei ging es der Verwaltung - insbesondere den Kommunen - in erster Linie um die behördenorganisatorischen Konsequenzen. Sie wollten vor allem wissen, welcher Personenkreis für die Bestellung zum behördlichen Datenschutzbeauftragten in Betracht kommt und welche Anforderungen an den Funktionsinhaber zu stellen sind (§ 5 Abs. 2 HDSG, vgl. dazu Ziff. 2.2).

Auch zu den Modalitäten der Benachrichtigungspflicht nach § 18 Abs. 2 HDSG gab es zahlreiche Anfragen (dazu Ziff. 2.3). Bei den öffentlich-rechtlichen Wettbewerbsunternehmen und den Krankenhäusern stellten sich Fragen zum Anwendungsbereich des HDSG im Verhältnis zum BDSG (§ 3 Abs. 7 HDSG, vgl. Ziff. 2.4). Bei der Auftragsdatenverarbeitung (§ 4 HDSG) tauchten Zweifel an der Abgrenzung der gegenseitigen Pflichten zwischen Auftraggeber und Auftragnehmer auf (vgl. Ziff. 2.5). Mit dem Hessischen Rundfunk schließlich ist eine Kontroverse über die verfassungsrechtliche Zulässigkeit meiner - d.h. einer externen - Kontrollbefugnis im Hinblick auf die Staatsfreiheit entstanden (dazu Ziff. 2.6).

In den folgenden Abschnitten wird im einzelnen zu diesen Problemen Stellung genommen. Aber auch die anderen Beiträge dieses Berichts behandeln z.T. Auslegungsfragen und zwar u.a.:

- die Reichweite des Rechtes jedes öffentlichen Bediensteten, sich ohne Einhaltung des Dienstweges an den Hessischen Datenschutzbeauftragten zu wenden (§ 28 Abs. 2 HDSG, dazu Ziff. 5.2),
- die Geltung des § 15 HDSG für gemeindeinterne online-Anschlüsse (dazu Ziff. 5.4),
- zur pauschalen Auskunftsverweigerung durch den Verfassungsschutz (§ 18 Abs. 5 HDSG, dazu Ziff. 9.3),
- zu § 34 Abs. 5 HDSG, wonach mir vor Einführung oder Änderung der automatisierten Verarbeitung von Beschäftigtendaten eine Dateibeschreibung vorzulegen ist (dazu Ziff. 8.2.1).

2.2
Behördlicher Datenschutzbeauftragter (§ 5 Abs. 2 HDSG)

2.2.1
Kommunen

Das neue Hessische Datenschutzgesetz verpflichtet in § 5 Abs. 2 jede datenverarbeitende Stelle, einen behördeninternen Beauftragten für den Datenschutz zu bestellen (zur Sondersituation der Bestellungspflicht für die kommunale Sozialverwaltung nach § 79 Abs. 1 SGB X in Verbindung mit §§ 28, 29 BDSG vgl. 11. Tätigkeitsbericht Ziff. 6.1.4.2). Für die Kommunen ist das Problem, welche Beschäftigten für diese Funktion in Frage kommen - nimmt man die Zahl der Anfragen zum Maßstab -, besonders schwierig.

Das Hessische Datenschutzgesetz (§ 5 Abs. 2) nennt sowohl ein positives als auch ein negatives Auswahlkriterium. Zum einen muß der Bedienstete die zur Erfüllung seiner Aufgaben erforderliche Sachkenntnis und Zuverlässigkeit besitzen. An die Sachkenntnis sind sicherlich unterschiedlich hohe Anforderungen zu stellen, je nachdem, ob es sich um eine Großstadtverwaltung mit eigener EDV- Abteilung oder um eine kleine Gemeinde handelt. Zum anderen darf der Bedienstete durch die Tätigkeit als Datenschutzbeauftragter keinem Interessenkonflikt mit sonstigen dienstlichen Aufgaben ausgesetzt sein. Damit soll verhindert werden, daß Personen Datenschutzbeauftragte werden, deren Umgang mit personenbezogenen Daten gerade besonders intensiver Kontrolle und Beratung bedarf.

Das Gesetz definiert nicht, wann ein Interessenkonflikt besteht. Dafür läßt sich auch kein abschließender Kriterienkatalog aufstellen: Die Beurteilung hängt vielfach von der spezifischen Konstellation in der jeweiligen Kommune ab. Ein Interessenkonflikt liegt allerdings eindeutig vor bei Mitarbeitern, die über die Einführung, Anwendung, Änderung oder Erweiterung von automatisierter Verarbeitung zu entscheiden haben oder derartige Entscheidungen wesentlich beeinflussen. Mitglieder des Gemeindevorstands oder des Magistrats können daher nicht gleichzeitig Datenschutzbeauftragte ihrer Kommune sein. Das gleiche gilt in der Regel für die Amtsleiter und die Beschäftigten im Organisationsamt.

Dagegen besteht im Grundsatz kein Interessenkonflikt bei Leitern und Mitarbeitern von Ämtern mit Querschnittsfunktionen, wie etwa dem Rechnungsprüfungsamt. Diese Bediensteten werden häufig sogar aus ihrer Kontrolltätigkeit die Organisationsabläufe und Verarbeitungsbedingungen in der gesamten Kommune besonders gut kennen. Auch bei Beschäftigten des Rechtsamts sind Interessenkonflikte kaum zu befürchten.

Wegen der in § 5 Abs. 2 HDSG vorausgesetzten Autorität und Durchsetzungsfähigkeit des oder der Beauftragten gegenüber den Fachämtern, aber auch gegenüber Vorgesetzten, nicht zuletzt aber auch im Hinblick auf die gebotene Sachkenntnis in juristischen Datenschutzfragen empfiehlt es sich, möglichst keine Mitarbeiter außerhalb des höheren oder gehobenen Dienstes zu bestellen.

2.2.2
Kommunale Krankenhäuser

Zu der Frage, ob kommunale Krankenhäuser von dem Datenschutzbeauftragten der jeweiligen Gemeinde bzw. des Landkreises „mitbetreut" werden können oder einen eigenen bestellen müssen, habe ich auf mehrere Anfragen hin folgende Auffassung vertreten:

Kommunale Krankenhäuser sind selbständige „datenverarbeitende Stellen" im Sinne des HDSG (vgl. zur Anwendbarkeit des HDSG auf öffentliche Krankenhäuser Ziff. 2.4.2). Soweit sie Behandlungsaufgaben wahrnehmen, gelten sie nach allgemeiner Auffassung als öffentlich-rechtliche Wettbewerbsunternehmen. Insoweit unterliegen sie nach § 3 Abs. 7 HDSG den materiellen Vorschriften des Bundesdatenschutzgesetzes. Nach § 28 BDSG sind sie daher verpflichtet, wie Privatunternehmen einen Beauftragten für den Datenschutz zu bestellen, dessen Aufgaben sich aus § 29 BDSG ergeben.

Sofern die Krankenhäuser über die Patientenbehandlung hinaus andere Aufgaben wahrnehmen, bei denen kein „Wettbewerb" besteht - etwa medizinische Forschung -, gilt insoweit uneingeschränkt das HDSG. Für diesen Bereich greift daher die Verpflichtung nach § 5 Abs. 2 HDSG, wie Behörden einen internen Beauftragten zu benennen. Die Tätigkeit nach § 28 BDSG und § 5 Abs. 2 HDSG kann von einer Person ausgeübt werden, wenn auch beide Vorschriften einen etwas abweichenden Funktionskatalog enthalten.

Entscheidend ist, daß mit dieser separaten Bestellungspflicht der kommunalen Krankenhäuser sichergestellt wird, daß „vor Ort" ein Mitarbeiter für die Einhaltung des Datenschutzes mitverantwortlich ist, der genaue Kenntnisse von Organisation und Arbeitsweise seines Hauses hat und als Ansprechpartner für Bedienstete und Betroffene aus der Verwaltung und dem ärztlichen Bereich zur Verfügung steht.

Aus dieser recht komplizierten Rechtslage in öffentlichen Krankenhäusern helfen nur konkrete bereichsspezifische Regelungen für Datenverarbeitung und Datenschutz im Krankenhaus. Diese habe ich nicht nur im Interesse von Transparenz und Rechtssicherheit, sondern auch wegen der sich aus dem Volkszählungsurteil des Bundesverfassungsgerichtes für den Krankenhausbereich ergebenden Normierungspflichten zu wiederholten Malen angemahnt (vgl. zuletzt 15. Tätigkeitsbericht, Ziff. 4.1.2). Einen entsprechenden Entwurf hatte die vorige Landesregierung vorgelegt. Ich hoffe, daß die neue Landesregierung möglichst bald den Entwurf eines neuen Krankenhausgesetzes bzw. datenschutzrechtliche Regelungen für diesen Bereich vorlegen wird.

2.3
Benachrichtigung (§ 18 Abs. 2 HDSG)

2.3.1
Regelungsziel und Praxiserfahrungen

Das novellierte HDSG sieht in § 18 Abs. 2 vor, daß jeder Betroffene, dessen personenbezogene Daten automatisiert gespeichert werden, darüber schriftlich zu benachrichtigen ist. Eine für die Verwaltung bislang beispiellose Regelung, die dem nur für private Unternehmen geltenden § 26 Abs. 1 des Bundesdatenschutzgesetzes nachgebildet ist.

Im Gesetzgebungsverfahren war die Benachrichtigungspflicht einer der am intensivsten diskutierten Punkte. Entscheidend für die Aufnahme in das neugefaßte HDSG war für den Gesetzgeber das Argument, daß die Transparenz der Datenverarbeitung - unverzichtbarer Bestandteil des informationellen Selbstbestimmungsrechts - mit dem bloßen Recht auf Auskunft über die gespeicherten Daten nicht ausreichend hergestellt werden kann, daß vielmehr der einzelne von den datenverarbeitenden Stellen zuerst einmal über Art und Umfang der Datenaufzeichnung unterrichtet werden muß, um dann sein Recht auf Auskunft sowie auf Berichtigung, Sperrung und Löschung geltend zu machen. Mit der Benachrichtigung erhält der Bürger also keinen „Datenkontoauszug", sondern nur einen Hinweis darauf, daß und welche Daten über ihn in eine bestimmte automatisierte Datei aufgenommen worden sind, welchem Zweck diese Datei dient, wem regelmäßig Daten übermittelt werden und wie lange die Sperrungs- und Löschungsfristen laufen.

Wie die ersten Erfahrungen zeigen, bereitet die Benachrichtigungspflicht für personenbezogene Daten, die erstmals nach dem Inkrafttreten des neuen HDSG am 1. Januar 1987 gespeichert werden, keine besonderen Probleme. Erleichterung bietet die in § 18 Abs. 2 HDSG vorgesehene Möglichkeit, den Bürger schon bei der Erhebung auf die spätere automatisierte Speicherung hinzuweisen. So kann beispielsweise die Benachrichtigung in Antragsformulare aufgenommen werden.

Für „Alt-Dateien", die bei Inkrafttreten des HDSG bereits - in automatisierter Form - angelegt waren, gilt ebenfalls die Benachrichtigungspflicht. Allerdings gewährt § 42 Abs. 1 HDSG hierfür eine Frist von zwei Jahren, d.h. bis zum 31. Dezember 1988.

Die gesetzliche Regelung ist eindeutig und läßt keinen Spielraum für einschränkende Interpretationen. Ausnahmen gibt es nur, wo die Informationspflichten in Einzelgesetzen abschließend geregelt sind, wie z.B. im Hessischen Meldegesetz. Darüber hinaus besteht keine Möglichkeit, etwa wegen hoher Kosten oder aus praktischen Gründen von der Pflicht zur Benachrichtigung auch und gerade bei „Alt-Dateien" abzugehen. Ich habe daher, beispielsweise für

den Bereich der Kraftfahrzeugzulassung, gegenüber den beteiligtenRessorts darauf bestanden, daß § 18 Abs. 2 i.V.m. § 43 Abs. 1 HDSG strikt eingehalten wird und die Kraftfahrzeughalter unterrichtet werden. Bei Halterwechsel innerhalb der Zwei-Jahres-Frist besteht ohnehin Gelegenheit zur Benachrichtigung.

Ich verkenne nicht, daß für die Verwaltungen beträchtliche Kosten entstehen können. Daher kann im Einzelfall geprüft werden, ob z.B. mehrere Benachrichtigungen zusammengefaßt, oder ob die Benachrichtigungen mit sonstigen dem Bürger regelmäßig zugestellten Bescheiden verbunden werden können. Aber noch einmal: Das Kostenargument ist im Gesetzgebungsverfahren ausführlich behandelt worden; das zeigt sich schon daran, daß der Hessische Rundfunk aus Kostengründen von der Benachrichtigungspflicht für die „Alt-Daten" ausgenommen worden ist (§ 42 Abs. 1 Satz 2 HDSG). Hohe Kosten berechtigen nicht, auf die Benachrichtigung zu verzichten.

2.3.2
Dateien der Staatsanwaltschaften

2.3.2.1
Kein vorrangiges Bundesrecht

Immer mehr Staatsanwaltschaften automatisieren ihre allgemeinen Namens- und Aktenzeichenregister. Die Dateien enthalten Namen und Vornamen der Betroffenen, im Einzelfall auch Geburtsdaten, den Deliktsvorwurf in Kurzform und das Aktenzeichen. Sie dienen der internen Registrierung und Erschließung der Aktenbestände und werden in der Regel nicht für Auskünfte an andere Stellen genutzt.

Ob die Betroffenen gem. § 18 Abs. 2 HDSG über die Speicherung ihrer Daten in dieser Datei zu benachrichtigen sind, ist zwischen dem Hessischen Justizministerium, dem Hessischen Innenministerium und mir umstritten. Nach Ansicht der beiden Ministerien hat der Landesgesetzgeber keine Befugnis, die staatsanwaltschaflichen Dateien zu regeln. Für diese sei allein die bundesrechtliche Strafprozeßordnung maßgeblich, die jedoch keine Benachrichtigung vorsieht.

Dem ist entgegenzuhalten, daß sowohl das Strafrecht als auch das Strafprozeß- und das Strafvollstreckungsrecht der konkurrierenden Gesetzgebung unterliegen (Art. 74 Nr. 1 Grundgesetz). Das bedeutet, „solange und soweit der Bund von seinen Gesetzgebungsrechten keinen Gebrauch macht", haben die Länder die Gesetzgebungsbefugnis (Art. 72 Grundgesetz). Die Strafprozeßordnung regelt nirgends die Führung und Auswertung staatsanwaltlicher Akten. Sie enthält auch keine Bestimmungen über die Einrichtung und Nutzung automatisierter oder manueller Dateien. Das ist jedoch nicht deshalb geschehen, weil der Bundesgesetzgeber hierfür überhaupt keine gesetzlichen Vorschriften wollte, vielmehr hat er es den Ländern überlassen, dies zu regeln.

Auch der Hessische Landtag ist davon ausgegangen. Das ergibt sich eindeutig aus § 3 Abs. 3 Satz 2 HDSG, wenn dort u.a. die Anwendung des § 18 HDSG für „die Verarbeitung personenbezogener Daten in Akten durch die Staatsanwaltschaften bei der Verfolgung von Straftaten und der Strafvollstreckung" ausgenommen wird. Die Datenverarbeitung in Akten soll ausgenommen sein, nicht die automatisierte Datenverarbeitung. Der Landesgesetzgeber hat sehr wohl das Problem der Verarbeitung personenbezogener Informationen in staatsanwaltschaftlichen Unterlagen gesehen und ausdrücklich nur für Akten eine Ausnahme von der Benachrichtigungspflicht gewollt. Die Regelung des § 18 Abs. 2 HDSG gilt deshalb zweifellos für automatisierte staatsanwaltschaftliche Dateien.

2.3.2.2
Zeitpunkt der Benachrichtigung

Der Betroffene muß allerdings nicht unmittelbar, nachdem die Anzeige eingegangen und der Name erfaßt ist, benachrichtigt werden. Das ergibt sich aus § 18 Abs. 5 HDSG. Danach ist abzuwägen, ob das Benachrichtigungsrecht des Betroffenen hinter dem öffentlichen Interesse an der Geheimhaltung oder einem überwiegenden Geheimhaltungsinteresse Dritter zurücktreten muß. Diese Interessenabwägung ist jedoch erst dann möglich, wenn alle Umstände bekannt sind. Das heißt: Erst mit Abschluß des Ermittlungsverfahrens kann festgestellt werden, welche Interessen Dritter oder öffentliche Interessen betroffen sind und ob somit einer Benachrichtigung Belange Dritter entgegenstehen. Damit ist die Befürchtung der Staatsanwaltschaft weitgehend entkräftet, die Benachrichtigung störe den Rechtsfrieden, da der Betroffene auch über unberechtigte Anzeigen informiert würde, von denen er nach dem bisherigen Verfahren nichts erfahre. Bis die Entscheidung nach § 18 Abs. 5 HDSG getroffen werden kann, wird im allgemeinen der Beschuldigte gehört worden sein und damit von der Anzeige erfahren haben.

Die Benachrichtigung hat für den Betroffenen zudem Vorteile: Sollte er über die Anzeige und die Speicherung in staatsanwaltschaftlichen Unterlagen in Fällen Mitteilung erhalten, in denen er bisher nicht darüber informiert war, so erlaubt ihm diese Neuerung eine bessere Wahrung seiner Rechte.

2.4
Anwendungsbereich des HDSG (§ 3 Abs. 7 HDSG)

2.4.1
Öffentlich-rechtliche Wettbewerbsunternehmen

Für die öffentlich-rechtlichen Unternehmen, die am Wettbewerb teilnehmen, hat sich die Rechtssituation durch das neue HDSG geändert. Die öffentlich-rechtlichen Kreditinstitute (vor allem also die Sparkassen) und Versicherungs-

unternehmen unterliegen jetzt der Kontrollbefugnis des Hessischen Datenschutzbeauftragten. Die bisher für diese Gruppe von Wettbewerbsunternehmen geltende Sonderregelung, wonach die Aufsichtsbehörden für den privaten Bereich (in Hessen also die Regierungspräsidenten) für die Datenschutzüberwachung zuständig waren (§ 3 Abs. 2 Satz 2 des alten HDSG), wurde aufgehoben.

Modifikationen gibt es auch im Hinblick auf das von den öffentlich-rechtlichen Wettbewerbsunternehmen zu beachtende materielle Recht.

Nach § 3 Abs. 7 des neuen HDSG gelten die materiellen Vorschriften des Bundesdatenschutzgesetzes für öffentlich-rechtliche Unternehmen nur, „soweit (sie) am Wettbewerb teilnehmen". Dieser Vorbehalt ist wörtlich zu verstehen: Der Gesetzgeber wünscht - das haben die Beratungen bei der Novellierung des HDSG deutlich gemacht -, daß öffentlich- rechtliche Unternehmen grundsätzlich dem HDSG unterliegen sollen. Nur für den Bereich ihrer Tätigkeit, mit dem sie am Wettbewerb teilnehmen, sollen sie anderen, privatwirtschaftlich arbeitenden Unternehmen datenschutzrechtlich gleichgestellt werden. Nur für dieses Segment ihrer Aktivitäten gilt die Verweisung auf die Vorschriften des Bundesdatenschutzgesetzes. Auslegungsfragen, die nach dem alten Recht (vgl. § 3 Abs. 2 HDSG a.F.) diskutiert wurden (...öffentlich-rechtliche Unternehmen, die am Wettbewerb teilnehmen...), sind damit gegenstandslos. Die Kontrollbefugnis des Hessischen Datenschutzbeauftragten besteht freilich auch für diesen Bereich.

Ob und inwieweit die von § 3 Abs. 7 HDSG vorausgesetzte Konkurrenzsituation gegeben ist, läßt sich nur im Einzelfall feststellen. Bei öffentlichen Energieversorgungs-Unternehmen z.B. läßt sich die Beteiligung am Wettbewerb nicht abstrakt am jeweiligen Energieträger festmachen. Vielmehr kommt es auf die spezifische Konkurrenzsituation im Einzugsgebiet des jeweiligen Unternehmens an.

Sicherlich kann es aufgrund dieser Rechtslage zu einer Zersplitterung des Datenschutzes dadurch kommen, daß für verschiedene Geschäftszweige kommunaler Unternehmen unterschiedliches Recht, entweder das HDSG oder das BDSG, anzuwenden ist. Dies ist aber nur die Konsequenz aus dem Motiv des Gesetzgebers, öffentlich-rechtliche Unternehmen zunächst wie andere Behörden der Verwaltung zu behandeln und ihnen Sonderkonditionen nur dort einzuräumen, wo im Verhältnis zu privaten Konkurrenten andernfalls Wettbewerbsnachteile zu befürchten sein könnten.

2.4.2
Kommunale Krankenhäuser

Eine Reihe von Anfragen zum Anwendungsbereich des neuen HDSG betraf auch die kommunalen Krankenhäuser. Diese haben zwar in der Regel keine eigene Rechtspersönlichkeit (vgl. § 1 Eigenbetriebsgesetz), sie sind jedoch ein organisatorisch und wirtschaftlich selbständiger Betrieb mit einer besonderen Aufgabe. Aus diesem Grunde sind sie als „datenverarbeitende Stelle" im Sinne des Hessischen Datenschutzgesetzes (§ 2 Abs. 3) anzusehen.

Da die kommunalen Krankenhäuser nach allgemeiner Auffassung als öffentlich-rechtliche Wettbewerbsunternehmen einzustufen sind, soweit sie Behandlungsaufgaben wahrnehmen, gelten für sie nach § 3 Abs. 7 HDSG jedoch lediglich der Zweite Teil sowie die §§ 34 und 36 des HDSG. Im übrigen haben sie sich - mit Ausnahme der Vorschriften über die Aufsichtsbehörde - nach den Normen des Bundesdatenschutzgesetzes über die Zulässigkeit der Datenverarbeitung, die Pflicht zur Bestellung eines internen Datenschutzbeauftragten (dazu ausführlich Ziff. 2.2.2) usw. zu richten. Sofern Krankenhäuser über die Behandlung der Patienten hinaus andere Tätigkeitsbereiche ohne Wettbewerbscharakter haben - z.B. Forschung -, gilt für sie insoweit in vollem Umfang das HDSG.

Auf meine Kontrollbefugnis hat jedoch die Frage des anwendbaren Rechts - BDSG oder HDSG - keinen Einfluß. Der Verweis auf den Zweiten Teil des HDSG in § 3 Abs. 7 zeigt, daß ich die Einhaltung des Datenschutzes auch dann zu überwachen habe, wenn die kommunalen Krankenhäuser das BDSG zu beachten haben.

2.5
Auftragsdatenverarbeitung: Rechte und Pflichten des Auftragnehmers bei rechtswidrigen Datenverarbeitungsaufträgen (§ 4 Abs. 1 HDSG)

Der Magistrat einer Kleinstadt wollte im Zusammenhang mit der Volkszählung 1987 das Kommunale Gebietsrechenzentrum (KGRZ) mit einer bestimmten Datenverarbeitungsmaßnahme beauftragen und erkundigte sich zuvor beim Hessischen Datenschutzbeauftragten nach deren Zulässigkeit. Das Vorhaben war offensichtlich rechtswidrig, was dem Magistrat mitgeteilt wurde. Dessen Reaktion: Er beauftragte das KGRZ trotzdem mit der Durchführung. Das KGRZ antwortete dem Magistrat, die Maßnahme sei zwar rechtswidrig, werde aber dennoch ausgeführt. Auf meine Intervention hin wies die oberste Aufsichtsbehörde den Magistrat daraufhin an, die beabsichtigte Verarbeitung zu unterlassen.

Der Fall interessiert hier nicht wegen des seltsamen Verhaltens des Magistrats, sondern weil er die Frage aufwirft, ob der Auftragnehmer einen Auftrag, von dessen Rechtswidrigkeit er überzeugt ist, ausführen muß. Das KGRZ begründete sein Verhalten damit, es sei in jedem Fall an die Weisungen des Auftraggebers gebunden, dieser sei allein für die Einhaltung der Datenschutzvorschriften verantwortlich. Das Hessische Datenschutzgesetz verpflichte den Auftragnehmer lediglich, denAuftraggeber auf die Rechtswidrigkeit der Maßnahme hinzuweisen. Vom KGRZ um

Stellungnahme gebeten, hat das Hessische Innenministerium diese Auffassung bekräftigt. Soweit der Auftraggeber datenschutzrechtliche Vorschriften verletze, sei es Sache der zuständigen Aufsichtsbehörde, das Erforderliche zu veranlassen.

Die Ansicht des KGRZ und des Innenministeriums beruht auf einer falschen Auslegung des § 4 Abs. 1 HDSG. Nach dieser Vorschrift darf der Auftragnehmer nur im Rahmen der Weisungen des Auftraggebers handeln und hat den Auftraggeber auf Rechtsverstöße hinzuweisen. Damit hat der Gesetzgeber für die Auftragsdatenverarbeitung im öffentlichen Bereich Pflichten des Auftragnehmers konkretisiert, die für das privatrechtliche Auftragsverhältnis schon seit langem ähnlich gesetzlich geregelt (Weisungsgebundenheit in § 665 Bürgerliches Gesetzbuch) oder durch die Rechtsprechung anerkannt sind (BGHZ 23, 222; 33, 293 zur Belehrungs- und Warnungspflicht des Auftragnehmers).

Obgleich nicht besonders im Zusammenhang mit dem Auftragsverhältnis geregelt, ist es privatrechtlich selbstverständlich, daß der Auftragnehmer rechtswidrige Aufträge nicht ausführen muß und Aufträge, die zudem gegen ein gesetzliches Verbot verstoßen - und daher i.d.R. nichtig sind (§ 134 BGB) - nicht ausführen darf. Um es an einem drastischen Beispiel zu verdeutlichen: Der Auftrag zu einem Diebstahl muß und darf nicht ausgeführt werden. Nicht einzusehen ist, warum gerade dieses Rechtsprinzip nicht gelten soll, wenn eine öffentliche Stelle eine andere mit der Verarbeitung personenbezogener Daten beauftragt; zumal hier ein rechtswidriger Auftrag immer auch gegen ein gesetzliches Verbot verstößt, denn die Verarbeitung personenbezogener Daten ist grundsätzlich verboten und nur unter den gesetzlich festgelegten Voraussetzungen zulässig (§ 7 Abs. 1 HDSG).

Nur darauf vertrauen zu müssen, die Aufsichtsbehörde des Auftraggebers werde die Ausführung rechtswidriger Datenverarbeitungsaufträge verhindern - so das Innenministerium - ist jedenfalls keine gleichwertige Alternative. Zumeist wird nämlich die Aufsichtsbehörde von dem Datenverarbeitungsvorhaben überhaupt nichts erfahren. Der Auftragnehmer muß schließlich nach dem Gesetz nicht die Aufsichtsbehörde, sondern nur den Auftraggeber auf die Rechtswidrigkeit hinweisen.

Festzuhalten bleibt: Der Auftragnehmer muß und darf Datenverarbeitungsaufträge, die er für rechtswidrig hält, nicht ausführen. Allerdings muß er andererseits Aufträge und Weisungen nicht ausführlich rechtlich überprüfen.

2.6
Kontrollbefugnis beim Hessischen Rundfunk (§§ 3 Abs. 6, 24, 37 Abs. 2 HDSG)

2.6.1
Von der internen zur externen Überwachung des Datenschutzes

Für die Datenverarbeitung und den Datenschutz beim Hessischen Rundfunk hat das neue HDSG eine wichtige Rechtsänderung gebracht. Nach dem alten Recht kontrollierte die Einhaltung der Datenschutzbestimmungen ausschließlich ein hausinterner Beauftragter, der vom Rundfunkrat bestellt und diesem Gremium sowie dem Verwaltungsrat berichtspflichtig war (§ 31 HDSG a.F.). Die Vorschriften über die Zulässigkeit der Speicherung, Übermittlung usw. - mit Ausnahme der Datensicherheitsbestimmungen in § 10 - galten nicht für die ausschließlich zu eigenen publizistischen Zwecken verarbeiteten personenbezogenen Daten. Die nicht dieser Kategorie zugehörigen Daten des Rundfunks unterlagen dagegen uneingeschränkt dem HDSG.

Nach dem neuen Gesetz bleibt es, was die materiellen Datenschutznormen angeht, bei der bisherigen Zweiteilung zwischen ausschließlich zu eigenen journalistisch-redaktionellen Zwecken verarbeiteten Daten einerseits und nicht-publizistischen Angaben andererseits. Die Kontrollkompetenz ist jedoch neu geordnet: Für den Datenschutz im redaktionellen Bereich ist nach wie vor ein vom Rundfunkrat zu bestellender interner Beauftragter zuständig. Für die Überwachung der Einhaltung des Datenschutzes bei den übrigen Datenbeständen hat der Gesetzgeber dem Hessischen Datenschutzbeauftragten die Kontrollbefugnis eingeräumt (§§ 3 Abs. 6, 24, 37 Abs. 2 HDSG). Eine keinesfalls einmalige Regelung, denn das Bundesdatenschutzgesetz gewährt dem Bundesdatenschutzbeauftragten die gleiche Kontrollkompetenz gegenüber dem Deutschlandfunk und der Deutschen Welle.

Über Umfang und Art der Ausübung der Kontrollbefugnis besteht eine Kontroverse zwischen mir und dem Intendanten des Hessischen Rundfunks. Der Intendant befürchtet Eingriffe in die Staatsfreiheit des Rundfunks und hat verfassungsrechtliche Bedenken gegen eine externe Datenschutzkontrolle auch dann, wenn sie sich - wie nach dem neuen HDSG - auf den Bereich der Administration der Rundfunkanstalt und deren Datenverarbeitung beschränkt. Verfassungsrechtlich vertretbar ist nach seiner Ansicht die Kontrolle durch den Hessischen Datenschutzbeauftragten allenfalls, wenn sie in einem „anstaltsautonomen Zusammenhang" erfolgt. Dazu sei erforderlich, daß ich weder die Landesregierung in Fragen berate, die den Hessischen Rundfunk berühren (§ 24 Abs. 1 HDSG), noch entsprechende Gutachtenaufträge von Landtag und Regierung entgegennehme (§ 25 HDSG). Außerdem müsse auf eine detaillierte Berichterstattung im jährlichen Tätigkeitsbericht verzichtet werden.

2.6.2
Verfassungsmäßigkeit der Kontrollzuständigkeit - Mißverständnis über die „Staatsfreiheit"

Ich habe die Forderungen des Intendanten abgelehnt und in einem Schreiben vom Mai 1987 meinen Standpunkt ausführlich erläutert. Der Datenschutzbeauftragte kann nicht mit einzelnen öffentlichen Stellen über Einschränkungen seiner Kontrollbefugnisse und gesetzlichen Pflichten gegenüber Parlament und Regierung verhandeln.

Die teilweise Änderung der Kontrollkompetenz für den Datenschutz beim Hessischen Rundfunk beruht nicht auf einer Kritik an der Effektivität des bisherigen rundfunkinternen Kontrollmodells. Dem vom Parlament gewählten Datenschutzbeauftragten sollte vielmehr im öffentlichen Bereich eine generelle Zuständigkeit eingeräumt werden. Nur aus zwingenden verfassungsrechtlichen Gründen ist der Gesetzgeber von diesem Grundsatz abgewichen. Dementsprechend unterliegen z.B. die unabhängigen Gerichte in ihrer justiziellen Tätigkeit nicht der Kontrollbefugnis des Datenschutzbeauftragten (§ 24 Abs. 1 Satz 1 HDSG). Auch der Hessische Rundfunk ist ausgenommen, insoweit er personenbezogene Daten ausschließlich zu eigenen journalistisch-redaktionellen Zwecken verarbeitet (§ 3 Abs. 6 HDSG).

Natürlich muß die Staatsfreiheit des Rundfunks gewahrt bleiben. Der Hessische Rundfunk hat jedoch weder während des Gesetzgebungsverfahrens noch später überzeugend dargestellt, inwiefern die Kontrollbefugnis des unabhängigen Datenschutzbeauftragten im Bereich der nicht-publizistischen Datenverarbeitung die Staatsfreiheit des Rundfunks gefährden könnte. Pauschale Behauptungen genügen hier ebensowenig wie Hinweise auf die zahlreichen Entscheidungen des Bundesverfassungsgerichts zur Rundfunkautonomie. Dabei ist die Notwendigkeit, diese Datenbestände von den Informationen abzugrenzen, die ausschließlich zur Erfüllung des journalistisch- redaktionellen Rundfunkauftrages erhoben und verwendet werden, keineswegs neu, vielmehr fordern alle Datenschutzgesetze diese Trennung. Auch schon nach dem alten HDSG war diese Unterscheidung unverzichtbar, um festzustellen, auf welchen Teil der Datenverarbeitung die materiellen Bestimmungen des Gesetzes Anwendung finden (§ 3 Abs. 3 des alten HDSG).

Im übrigen gibt es große Unterschiede zwischen einer Staatsaufsicht und der Stellung bzw. den Aufgaben des Hessischen Datenschutzbeauftragten. Er ist kein Organ der Staatsaufsicht, er kann keine Verwaltungsakte im Wege der Fach- oder Rechtsaufsicht erlassen, sondern soll hauptsächlich beraten und Empfehlungen geben (vgl. § 24 Abs. 1 Satz 2 HDSG). Auch mit dem weitestgehenden Mittel, der förmlichen Beanstandung, kann er die öffentliche Stelle nur zu datenschutzgerechtem Verhalten auffordern und die Aufsichtsbehörde einschalten, nicht aber selbst Maßnahmen untersagen. Seine Sonderrolle kommt auch darin zum Ausdruck, daß er vom Parlament gewählt, in seiner Tätigkeit unabhängig und keiner Ministerverantwortlichkeit unterworfen ist. Das Bundesverfassungsgericht hat im Volkszählungsurteil auch und gerade im Hinblick auf diese von den übrigen staatlichen Instanzen unabhängige Position dem Datenschutzbeauftragten eine besondere Funktion bei der Sicherung des informationellen Selbstbestimmungsrechts der Bürger zugeschrieben.

2.6.3
Grenzen verfassungskonformer Auslegung

Es mag notwendig sein, in Zweifelsfällen die Datenbestände des Hessischen Rundfunks zum rundfunkautonomen und nicht zum Verwaltungsbereich zu rechnen, eine „verfassungskonforme Auslegung" des HDSG kann jedoch unter keinen Umständen dazu führen, daß meine gesetzlichen Kontrollbefugnisse oder gar Ansprüche anderer Verfassungsorgane - insbesondere des Landtags - auf mein Tätigwerden eingeschränkt werden.

Dementsprechend kann dem Hessischen Rundfunk auch nicht die gewünschte pauschale Sonderstellung in den Punkten Entgegennahme von Beratungs- und Gutachtenaufträgen sowie Erwähnung im Tätigkeitsbericht zugestanden werden. Ganz sicher kann ich die Landesregierung oder einzelne Ministerien nach § 24 Abs. 1 HDSG nicht in Einzelfragen der Datenverarbeitung beim Rundfunk beraten, für die die Ressorts nicht zuständig sind. Doch geht die Konsultationsaufgabe des Datenschutzbeauftragten über die konkrete Verarbeitungssituation in der jeweiligen Behörde weit hinaus. So würde ich beispielsweise selbstverständlich gegenüber der Landesregierung dann Stellung nehmen oder Anregungen geben, wenn im Rahmen der Vorbereitung einer Änderung des Rundfunkgesetzes Regelungsvorschläge zur Verbesserung des Datenschutzes zu beurteilen bzw. zu formulieren wären. Ähnliches gilt für Gutachten- oder Untersuchungsaufträge nach § 25 HDSG.

Meine Berichtspflicht nach § 30 HDSG besteht uneingeschränkt, gleich ob es den Hessischen Rundfunk oder irgendeine andere öffentliche Stelle betrifft. Das Parlament hat Anspruch darauf, über die wichtigsten Aktivitäten im Berichtsjahr informiert zu werden. Im übrigen besteht mein Bericht nicht nur in der Darstellung und Bewertung von Einzelproblemen bei datenverarbeitenden Stellen, sondern auch und gerade in der Anregung gesetzgeberischer Verbesserungen. Sicherlich habe ich bei der Ausgestaltung des Berichts ein gewisses „Auswahlermessen", das jedoch in keinem Fall zugunsten irgendei- ner Stelle pauschal beschränkt werden kann. Dabei ist es für mich selbstverständlich, vor jeder Publikation im Jahresbericht den jeweils betroffenen datenverarbeitenden Stellen Gelegenheit zur Stellungnahme zu meinen Bewertungen oder Kritikpunkten zu geben.

2.6.4
Tragweite der Kontroverse

Nach meinem Schreiben vom Mai habe ich mehrmals dem Intendanten ein Gespräch vorgeschlagen, in dem es zunächst um eine Abgrenzung der journalistisch-redaktionellen von den zu anderen Zwecken genutzten Datensammlungen des Hessischen Rundfunks gehen sollte. Nur wenn diese Zuordnung zumindest versucht wird, lassen sich mögliche Konflikte zwischen Datenschutzaufsicht und Rundfunkautonomie überhaupt erst erkennen. Der Intendant hat diese notwendige Kategorisierung abgelehnt, erneut auf seine Vorschläge zur „verfassungskonformen" Anwendung des HDSG verwiesen und darauf beharrt, daß vorrangig die „grundsätzlichen Fragen" geklärt werden müßten. Ein letztes Gesprächsangebot, das ich in einem Schreiben vom 27. November 1987 unterbreitet habe, ist völlig ohne Antwort geblieben. Jetzt ist es Sache des Hessischen Landtags, sich dazu zu äußern und der Geltung des Gesetzes Respekt zu verschaffen.

3. Volkszählung 1987

Die Volkszählung war im vergangenen Jahr nicht nur Dauerthema in den Medien, sondern hat in nie dagewesenem Ausmaß auch den Hessischen Datenschutzbeauftragten beschäftigt. In der nunmehr 16jährigen Geschichte der Institution des Hessischen Datenschutzbeauftragten ist die Volkszählung 1987, so viel läßt sich ohne Übertreibung sagen, zweifellos das größte und komplexeste Datenverarbeitungsprojekt. Wenn die Erhebung abgeschlossen ist, werden 426 bei den Gemeinden in Hessen eingerichtete Erhebungsstellen die Daten von voraussichtlich mehr als 5 Millionen Personen beschafft und an das Hessische Statistische Landesamt zur statistischen Aufbereitung weitergeleitet haben.

3.1 Rollenverständnis

Bei meiner Tätigkeit im Zusammenhang mit der Volkszählung ging es keineswegs nur um die übliche Wahrnehmung gesetzlich zugewiesener Aufgaben, sondern auch um die Erfüllung einer ausdrücklichenForderung des Bundesverfassungsgerichts. Das Gericht hat den Datenschutzbeauftragten eine besondere Rolle bei der Volkszählung zugewiesen. Mit Hinweis auf die Dimension und Komplexität der Volkszählung sowie die für den Bürger damit verbundene erschwerte Durchschaubarkeit der Datenverarbeitung hat es in seinem Volkszählungsurteil eine frühzeitige Beteiligung der Datenschutzbeauftragten bei der Gestaltung des Verarbeitungsprozesses und eine effektive Kontrolle der Datenverarbeitung durch die Datenschutzbeauftragten verlangt (BVerfGE 65, 46, 60).

Es ist schwer zu sagen, ob es allein die Forderung des Bundesverfassungsgerichts war, die Gesetzgeber, Landesregierung, Hessisches Statistisches Landesamt, Gemeinden, Erhebungsstellen und Rechenzentren bisher veranlaßt hat, in der Regel den Hessischen Datenschutzbeauftragten rechtzeitig zu beteiligen. Erkennbar war häufig auch das durchaus legitime Interesse, die Datenschutzbeauftragten in die Verantwortung einzubinden und unter Hinweis auf deren Stellungnahmen oder Äußerungen die Akzeptanz der Volkszählung bei den Bürgern zu fördern. So berief sich etwa die Landesregierung in der Landtagsdebatte, die am 10. Juni 1987 zur Durchführung der Volkszählung stattfand, auf die Konferenz der Datenschutzbeauftragten des Bundes und der Länder, die „ohne Abstriche" das Volkszählungsgesetz für verfassungsmäßig halte (Protokoll der 3. Plenarsitzung vom 10. Juni 1987, S 377). Die Bundesregierung zitierte in einer Bundestagsdebatte zum gleichen Thema den Bundesdatenschutzbeauftragten, der mehrfach erklärt habe, daß bei der Volkszählung für keinen Bürger Anlaß bestehe, sich Sorgen zu machen und nach menschlichem Ermessen alles getan worden sei, um den Datenschutz zu gewährleisten (Verhandlungen des Deutschen Bundestags, 10. Wahlperiode, 10. Sitzung vom 7. Mai 1987, S. 611). Auch das Statistische Bundesamt warb in seinem Informationsblatt „So zählt unser Land" unter Berufung auf die Datenschutzbeauftragten um das Vertrauen der Bürger. Gleich zu Beginn erfolgte der Hinweis, das Volkszählungsgesetz habe die einmütige Zustimmung der Bundestagsfraktionen sowohl der CDU/CSU, der F.D.P. als auch der SPD gefunden. Außerdem hätten „alle Bundesländer zugestimmt, ebenso die Datenschutzbeauftragten von Bund und Ländern". Das speziell für Studenten herausgegebene Informationsblatt des Statistischen Bundesamtes mit der Überschrift „Keine wissenschaftliche Forschung ohne statistische Daten" zitiert im Abschnitt „Datenschutz in vollem Umfang gewährleistet" neben dem Bundesdatenschutzbeauftragten auch den Hessischen Datenschutzbeauftragten, wobei mir der Satz zugeschrieben wird: „Diesmal wird man nicht nein sagen können."

Es ist durchaus verständlich, wenn mit Äußerungen des Datenschutzbeauftragten geworben wird, nur darf darüber nicht vergessen werden, daß die Verantwortung für die Rechtmäßigkeit der Datenverarbeitung nicht bei ihm liegt, sondern bei den datenverarbeitenden Stellen und den Aufsichtsbehörden (§§ 4 Abs. 1, 5 Abs. 1 Hessisches Datenschutzgesetz). Der Hessische Datenschutzbeauftragte hat nicht die Funktion eines technischen Überwachungsvereins; er gibt keinen Unbedenklichkeitsstempel für ein bestimmtes Datenverarbeitungsprojekt. Seine gutachtlichen Stellungnahmen und Kontrollen entlassen die für die Durchführung der Volkszählung zuständigen Stellen nicht aus der Verpflichtung, selbst zunächst für die Einhaltung der Datenschutzvorschriften zu sorgen - gefordert war und ist mit anderen Worten zuallererst die Initiative dieser Stellen. Daran mangelte es jedoch mitunter, was insbesondere das unbefriedigende Ergebnis meines landesweiten Prüfprogramms bei den örtlichen Erhebungsstellen (dazu Ziff. 3.4.2.2 und 3.4.2.3) belegt.

3.2
Regelungssystem

3.2.1
Übersicht

Es gab und gibt kein Datenverarbeitungsvorhaben, das derart detailliert und umfassend geregelt ist wie die Volkszählung 1987. Das zeigt allein die Zahl der verschiedenen Vorschriften. Insgesamt 14 Gesetze, Rechtsverordnungen und Verwaltungsvorschriften sind maßgebend. Zum größten Teil handelt es sich um Spezialvorschriften, die ausschließlich die Volkszählung 1987 regeln, zum Teil sind es aber auch allgemeinere Gesetze, die Bedingungen für die Durchführung der Volkszählung festlegen. In der folgenden Übersicht sind die Vorschriften in der Reihenfolge formelle Gesetze, Rechtsverordnungen und Verwaltungsvorschriften aufgelistet.

a) Gesetze
Gesetz über eine Volks-, Berufs-, Gebäude-, Wohnungs- und Arbeitsstättenzählung (Volkszählungsgesetz 1987) vom 8. November 1985 (BGBl. I S. 2078)

Gesetz über die Statistik für Bundeszwecke (Bundesstatistikgesetz - BStatG) vom 22. Januar 1987 (BGBl. I S. 462)

Gesetz über Ordnungswidrigkeiten i.d.F. vom 19. Februar 1987 (BGBl. I S. 603)

Gesetz über die Statistik im Land Hessen (Hessisches Landesstatistikgesetz - HessLStatG) vom 19. Mai 1987 (GVBl. I S. 67)

Hessisches Datenschutzgesetz (HDSG) vom 11. November 1986 (GVBl. I S. 309)

Hessisches Verwaltungsverfahrensgesetz vom 1. Dezember 1976 (GVBl. I S. 454, ber. 1977 I, S. 95)

b) Verordnungen

Hessische Ausführungsverordnung zu § 9 Abs. 3 des Volkszählungsgesetzes 1987 über die Erhebungsstellen und deren Aufgaben vom 26. Juni 1986 (GVBl. I S. 229) i.V.m. Verordnung zur Änderung der Hessischen Ausführungsverordnung zu § 9 Abs. 3 des Volkszählungsgesetzes 1987 über die Erhebungsstellen und deren Aufgaben vom 11. März 1987 (GVBl. I S. 40)

Verordnung über Zuständigkeiten nach dem Bundesstatistikgesetz vom 11. März 1987 (GVBl. I S. 39)

c) Erlasse usw.

Anleitung für die Gemeinde und die Erhebungsstelle

Anleitung für Zählerin und Zähler (Zähleranleitung)

Gemeinsamer Runderlaß des Hessischen Ministerpräsidenten (Staatskanzlei), Hessischen Ministers des Innern und Hessischen Ministers der Finanzen zur Durchführung der Volkszählung 1987 vom 2. September 1986 (StAnz. 1986, S. 1774)

Gemeinsamer Runderlaß des Hessischen Ministerpräsidenten (Staatskanzlei) und Hessischen Ministers des Innern zur Durchführung der Volkszählung 1987 vom 27. April 1987 (StAnz. 1987, S. 1064)

Bekanntmachung des Bundesministers des Innern vom 25. März 1987, Volkszählung 1987, hier: Verhältnis Volkszählungsgesetz 1987 zum Bundesstatistikgesetz (GMBl. 1987, S. 163)

Festsetzung der Abgabefrist für Erhebungsvordrucke in der Volkszählung 1987 vom 27. Mai 1987 (StAnz. 1987, S. 1332)

Nicht enthalten in dieser Übersicht sind die inzwischen 11 Rundschreiben des Hessischen Statistischen Landesamtes an die Gemeinden mit Anweisungen zur Durchführung der Volkszählung. Unberücksichtigt geblieben sind außerdem die Dienstanweisungen der Gemeinden für das Personal in den örtlichen Erhebungsstellen.

3.2.2
Bewertung

3.2.2.1
Regelungsdichte

Natürlich läßt sich darüber streiten, ob nicht der eine oder andere ungeregelte Gegenstand doch hätte geregelt werden sollen, ob es nicht beispielsweise besser gewesen wäre - wie von mir gefordert -, den Mindestinhalt der Dienstanweisungen für die Beschäftigten in den Erhebungsstellen entweder in der Verordnung zur Durchführung der Volkszählung oder dem Gemeinsamen Runderlaß der obersten Aufsichtsbehörden festzulegen. Man mag auch darüber streiten, ob ein bestimmter geregelter Gegenstand statt in einer Verwaltungsvorschrift in einer Rechtsverordnung hätte geregelt werden müssen. Wie immer man zu den beiden Punkten steht, eines läßt sich nicht leugnen, daß nämlich insgesamt gesehen eine ausreichende Regelungsdichte für die Volkszählung vorhanden ist.

3.2.2.2
Verfassungsmäßigkeit des Volkszählungsgesetzes 1987

In Eingaben, die ich im vergangenen Jahr sowohl von einzelnen Bürgern wie Bürgerinitiativen, Verbänden und politischen Organisationen erhalten habe, ist immer wieder direkt oder implizit die Verfassungsmäßigkeit des Volkszählungsgesetzes 1987 bezweifelt worden. Zur Verfassungsmäßigkeit des Volkszählungsgesetzes 1987 habe ich mich bereits in den beiden vorangegangenen Tätigkeitsberichten geäußert (vgl. 14. Tätigkeitsbericht, Ziff. 5.3.1 und 15. Tätigkeitsbericht, Ziff. 8.2). Das Gesetz erfüllt die Anforderungen, die das Bundesverfassungsgericht im Volkszählungsurteil von 1983 gestellt hat.

Auch wenn noch keine Entscheidung eines Senats des Bundesverfassungsgerichts in Sachen Volkszählungsgesetz 1987 ergangen ist, so hat doch die 1. Kammer des Ersten Senats des Gerichts seit September 1987 in mehreren

Beschlüssen, in denen die Annahme von Verfassungsbeschwerden abgelehnt wurde, zu einer ganzen Reihe von Streitpunkten eindeutig Stellung genommen (vgl. 1 BvR 970/87, NJW 1987, S. 2085, 1 BvR 1063/87, 1 BvR 1122/87 und 1 BvR 962/87). Das Gericht sieht beispielsweise keinen Grund, an der Verhältnismäßigkeit der Totalerhebung mit Auskunftspflicht zu zweifeln und meint, der Gesetzgeber habe sich genügend mit dem Stand der Methodendiskussion auseinandergesetzt. Auch gegen das Erhebungsprogramm - einschließlich der Frage nach der Religionszugehörigkeit - hat das Gericht keine Einwände. In dem Sonderfall der selbständig Tätigen, deren Familienname im Namen der Ausbildungs- oder Arbeitsstätte enthalten oder deren Wohnanschrift mit der der Arbeits- oder Ausbildungsstelle identisch ist, genügt es den Verfassungsrichtern, wenn die Adresse der Arbeitsstätte nicht auf die für die maschinelle Weiterverarbeitung bestimmten Datenträger übernommen wird. Für die Dateien zur Abwicklung der Erhebung und für die Erhebungs(hilfs)papiere sind nach Ansicht des Gerichts keine besonderen gesetzlichen Regelungen notwendig. Ein Erhebungshilfspapier ist beispielsweise die Regionalliste, die die Erhebungsstelle für jeden Arbeitsbezirk eines Zählers anlegt und an das Statistische Landesamt weitergibt. Neben dem Namen des Haushalts enthält sie die Hausnummer des Gebäudes, die laufenden Nummern des Gebäudes, der Wohnung im Gebäude und des Haushalts in der Wohnung, die Zahl der Personen im Haushalt und die Nummer des Wohnungs- und Personenbogens sowie des Arbeitsstättenbogens. Der Namensteil wird allerdings im Statistischen Landesamt abgetrennt. Mit Hilfe der Regionalliste können die Einzelangaben aus den Erhebungsbogen einer von zwei Straßeneinmündungen begrenzten Straßenseite (Blockseite) zugeordnet werden. Das Bundesverfassungsgericht hält schließlich auch die Schutzvorschriften des Volkszählungsgesetz 1987, besonders den strafrechtlichen Schutz sowie die Trennungs- und Löschungsregelungen, für ausreichend.

Der Hessische Verwaltungsgerichtshof ist nach ausführlicher Prüfung gleichfalls zu der Ansicht gelangt, daß gegen das Volkszählungsgesetz 1987 keine verfassungsrechtlichen Bedenken bestehen (Beschluß vom 2. Oktober 1987 - 7 N 1273/87, unter Ziff. 1; vgl. dazu auch Ziff. 3.2.2.5.2 dieses Berichts).

3.2.2.3
Bundesstatistikgesetz

Über die Auseinandersetzung mit der Verfassungsmäßigkeit des Volkszählungsgesetzes 1987 geraten freilich allzu leicht die anderen Fragen, die sich im Zusammenhang mit der gesetzlichen Regelung der Volkszählung 1987 stellen oder gestellt haben, aus dem Blickfeld. Da ist zum einen das Problem, wie sich das neue Bundesstatistikgesetz zum Volkszählungsgesetz 1987 verhält.

Auf Drängen der Datenschutzbeauftragten hat der Bundesgesetzgeber noch vor dem Zählungsstichtag der Volkszählung 1987 das Bundesstatistikgesetz novelliert. Das neue Gesetz ist am 30. Januar 1987 in Kraft getreten und legt die allgemeinen Verarbeitungsbedingungen für sämtliche Bundesstatistiken fest, also für so unterschiedliche Statistiken wie Geflügelstatistik, Hochschulstatistik, Statistik der Fehlbildungen bei Neugeborenen und eben auch die Volkszählung. Da das Volkszählungsgesetz 1987 vom 8. November 1985 mit dem Bundesstatistikgesetz in der Fassungvom 14. März 1980 ein Regelungsprogramm bilden sollte, blieben durch die Novelle Interpretationsprobleme nicht aus.

Fraglich war auf einmal geworden, welche Regelungen für die Trennung und Löschung zu gelten hatten, die großzügigeren des neuen Bundesstatistikgesetzes oder die engeren des Volkszählungsgesetzes 1987. Nur nach dem Volkszählungsgesetz 1987 dürfen außerdem Zähler nicht in unmittelbarer Nähe ihrer Wohnung eingesetzt werden. Abweichungen gibt es auch bei den Übermittlungsvorschriften. Das novellierte Bundesstatistikgesetz erlaubt den Statistikämtern des Bundes und der Länder, statistische Einzelangaben zu Planungszwecken an oberste Landesbehörden zu übermitteln. Es gestattet zudem die Übermittlung faktisch anonymisierter Einzelangaben an Hochschulen und sonstige Einrichtungen mit der Aufgabe unabhängiger Forschung. Beides ist nach dem Volkszählungsgesetz 1987 unzulässig.

Das Problem ist juristisch nicht ungewöhnlich. Es ist die bekannte Methodenfrage, ob die ältere spezielle Regelung (Volkszählungsgesetz 1987 vom 8. November 1985) der jüngeren allgemeinen (Bundesstatistikgesetz vom 22. Januar 1987) vorgeht oder umgekehrt. Die Aufsichtsbehörden der Statistischen Landesämter und das Bundesinnenministerium als Aufsichtsbehörde des Statistischen Bundesamtes haben am 2./3. Februar 1987 das Verhältnis des Volkszählungsgesetzes 1987 zum Bundesstatistikgesetz vom 22. Januar 1987 „einvernehmlich und abschließend erörtert". Das Ergebnis ist vom Bundesbeauftragten für den Datenschutz „bestätigt" worden, dem Innenausschuß des Bundestages am 16. Februar 1987 „vorgetragen" und vom BMI anschließend bekanntgemacht worden (Volkszählung 1987, hier Verhältnis Volkszählungsgesetz 1987 zum Bundesstatistikgesetz - Bekanntmachung des BMI vom 25. März 1987 -, GMBl. 1987, S. 163). In den geschilderten Fällen bestätigt es jeweils den Vorrang des Volkszählungsgesetzes 1987.

Dazu sei hier nur angemerkt, daß es verfassungsrechtlich keineswegs zwingend ist, die Übermittlung von (faktisch anonymisierten) Einzelangaben für wissenschaftliche Zwecke zu untersagen. Das Volkszählungsgesetz 1983 erlaubte in § 9 Abs. 4 für wissenschaftliche Zwecke die Übermittlung von Einzelangaben ohne Namen und Anschrift. Diese Vorschrift hat das Bundesverfassungsgericht ausdrücklich für verfassungsmäßig erklärt (BVerfGE 65, 69).

Ob die Bekanntmachung des Bundesinnenministeriums ausreicht oder nicht eher eine von der Bundesregierung mit Zustimmung des Bundesrates zu erlassende norminterpretierende Verwaltungsvorschrift (Art. 84 Abs. 2 Grundgesetz) angebracht wäre, möchte ich hier dahingestellt sein lassen.

3.2.2.4
Landesstatistikgesetz

Überraschend verlief die Entwicklung bei einem anderen gesetzlichen Regelungsproblem, das sich im Zusammenhang mit der Volkszählung stellte: beim Landesstatistikgesetz. Das Volkszählungsgesetz 1987 erlaubt die Übermittlung statistischer Einzelangaben an die Kommunen nur, wenn durch Landesgesetz die Abschottung der gemeindlichen Statistikämter von anderen Verwaltungsstellen sichergestellt und das Statistikgeheimnis durch Organisation und Verfahren gewährleistet ist (§ 14 Abs. 1). Damit wird das Landesstatistikgesetz zum wesentlichen Bestandteil des Regelungsprogramms der Volkszählung.

Sowohl in meinem 13. Tätigkeitsbericht (Ziff. 4.1.6) als auch in meinem 14. Tätigkeitsbericht (Ziff. 5.3.1) hatte ich darauf hingewiesen, daß das Gesetz noch vor dem Zählungsstichtag, d.h. dem 25. Mai 1987, in Kraft getreten sein müsse. Auch der Landtag war dieser Meinung. In seinem einstimmigen Beschluß vom 14. November 1985 hat er die Auffassung vertreten, „daß aufgrund des Urteils des Bundesverfassungsgerichts zur Volkszählung landesrechtliche Regelungen über die Landes- und Kommunalstatistik auf jeden Fall vor Durchführung der Volkszählung erforderlich (seien)" (Drucks. 11/4696 i.V.m. Protokoll der 63. Plenarsitzung vom 14. November 1985, S. 3615). Der Grund dafür ist einfach: Der Bürger muß bereits vor der Erhebung erkennen können, was mit seinen Daten später geschieht.

Das Bundesverfassungsgericht hat in seinem Beschluß vom 25. September 1987 (1 BvR 936/87) die Frage, ob das vom Volkszählungsgesetz 1987 geforderte Landesgesetz bereits vor der Erhebung der Daten in Kraft getreten sein muß, allerdings noch offen gelassen.

Zunächst gab es, insbesondere nach dem einstimmigen Beschluß des Landtags, keinen Anlaß, an der rechtzeitigen Verabschiedung des Gesetzes zu zweifeln. Die damalige Landesregierung brachte spät, aber aus damaliger Sicht wohl nicht zu spät, am 24. Dezember 1986 den Entwurf eines Landesstatistikgesetzes im Landtag ein (Drucks. 11/7087). Doch bevor die Gesetzesvorlage beraten werden konnte, löste sich infolge der Regierungskrise zu Beginn des Jahres der Landtag am 17. Februar 1987 auf. Landtagsauflösung und Neuwahltermin am 5. April 1987 ließen die rechtzeitige Verabschiedung des Landesstatistikgesetzes plötzlich als sehr unwahrscheinlich erscheinen.

Die neue Landtagsmehrheit, die Fraktionen von CDU und F.D.P., brachte jedoch bereits am 23. April 1987 einen mit dem alten Regierungsentwurf übereinstimmenden Entwurf eines Landesstatistikgesetzes im neugewählten Landtag ein; mit der Begründung, das Gesetz solle rechtzeitig vor Durchführung der Volkszählung am 25. Mai 1987 in Kraft treten (Drucks. 12/33). Nach äußerst kurzer Beratung wurde das Gesetz am 13. Mai 1987 verabschiedet, so daß es am 23. Mai 1987 in Kraft treten konnte. Auch wenn nicht alle meine Vorstellungen in das Gesetz eingegangen sind (vgl. hierzu Ziff. 13.2 dieses Berichts), so kann dennoch festgestellt werden, daß es dem Landtag trotz schwieriger Umstände gelungen ist, ein schwerwiegendes gesetzliches Regelungsdefizit rechtzeitig zu beheben.

Mit der Feststellung, daß Landtag wie Bundestag das ihre für eine verfassungskonforme Volkszählung 1987 getan haben, wechselt allerdings der Blick zwangsläufig von der legislativen auf die administrative Ebene und da fällt die Bewertung keineswegs gleichermaßen positiv aus.

3.2.2.5
Hessische Verordnung zur Durchführung der Volkszählung 1987

3.2.2.5.1
Personal in den örtlichen Erhebungsstellen

Wie die örtliche Durchführung der Volkszählung 1987 inzwischen gezeigt hat, ist meine zentrale Kritik an der Hessischen Ausführungsverordnung zu § 9 Abs. 3 des Volkszählungsgesetzes 1987 vom 26. Juni 1986 (vgl. 15. Tätigkeitsbericht, Ziff. 8.2.1), die später durch die Änderungsverordnung vom 11. März 1987 in Hessische Verordnung zur Durchführung der Volkszählung 1987 umbenannt worden ist, nur zu berechtigt. Bemängelt habe ich vor allem, daß undifferenziert der Einsatz öffentlicher Bediensteter in der Erhebungsstelle zugelassen wird.

Die örtliche Durchführung der Volkszählung erfolgt grundsätzlich durch die Gemeinden, die zu diesem Zweck Erhebungsstellen einzurichten haben, die besonders in den großen Kommunen wahrscheinlich noch bis zum Frühjahr 1988 tätig sein werden, obgleich nach dem Zeitplan der Gemeindeanleitung bis Mitte August 1987 alle Erhebungsunterlagen an das Statistische Landesamt versandt sein sollten. Die Erhebungsstelle ist unter anderem verantwortlich für den Zählereinsatz. In der Erhebungsstelle werden sämtliche ausgefüllten Erhebungsbogen personenbezogen gesammelt, auf Vollzähligkeit und Vollständigkeit überprüft und unter Umständen Angaben nach Rücksprache mit dem Bürger ergänzt. Die Erhebungsstelle hat den Rücklauf der Erhebungsbogen zu kontrollieren und kann gegen Auskunftsverweigerer Verwaltungszwangsverfahren und/oder Bußgeldverfahren einleiten.

Von entscheidender Bedeutung für die Gewährleistung des verfassungsrechtlichen Gebots der Trennung von Statistik und Verwaltung und die Sicherung des Statistikgeheimnisses sind daher die Auswahlkriterien und Verhaltenspflichten für die in den Erhebungsstellen tätigen Personen. Zwar sind hierzu wichtige Sicherungen vorhanden: Die Bediensteten der Erhebungsstelle müssen die Gewähr für Zuverlässigkeit und Verschwiegenheit bieten. Sie sind auf die Wahrung des strafrechtlich gesicherten Statistikgeheimnisses und zur Verschwiegenheit zu verpflichten und dürfen während ihrer Tätigkeit in der Erhebungsstelle keine anderen Verwaltungsaufgaben wahrnehmen. Außerdem

besteht das Verbot, Erkenntnisse aus der Tätigkeit in der Erhebungsstelle in anderen Verfahren oder zu anderen Zwecken zu verwenden.

Auf eine zusätzliche, von mir vorgeschlagene Sicherungsvorkehrung ist jedoch verzichtet worden. Die Landesregierung ist nicht meinem Vorschlag gefolgt, solche Personen vom Einsatz in der Erhebungsstelle auszuschließen, bei denen die Gefahr besteht, daß sie ihre Kenntnisse aus der Tätigkeit in der Erhebungsstelle später zum Nachteil des Bürgers verwenden.

Für Zähler sieht das Volkszählungsgesetz eine entsprechende Regelung vor. Was für Zähler gilt, die nach dem Gesetz im übrigen auch das Statistikgeheimnis und das Verwertungsverbot zu beachtenhaben, muß in gleichem Maße für die Mitarbeiter der Erhebungsstelle gelten. Abgesehen davon, daß das Personal der Erhebungsstelle z.T. auch Zähleraufgaben wahrnimmt, da die Bürger die Erhebungsbogen im verschlossenen Umschlag direkt an die Erhebungsstelle schicken können, hat es Zugang zu weit mehr Daten als die Zähler. Während letztere nur einen kleinen Ausschnitt, nämlich die Angaben von maximal ca. 60 - 80 Haushalten erfahren können, haben die Mitarbeiter der Erhebungsstelle potentiell Zugang zu den Daten sämtlicher Einwohner der Gemeinde.

Die Gefahr einer Interessenkollision dürfte insbesondere bei Personen aus den Ordnungs-, Steuer-, Sozial- und Einwohnermeldeämtern bestehen. In etlichen Erhebungsstellen waren und sind Bedienstete aus diesen Bereichen tätig (vgl. Ziff. 3.4.2.2 b). Fälle, in denen der Leiter des Einwohnermeldeamtes oder des Ordnungsamtes zum Zählungsleiter bestellt worden ist, sind keineswegs selten. Es überrascht deshalb nicht, daß sich viele Bürger über die Besetzung der Erhebungsstelle ihrer Gemeinde bei mir beschwert haben; Bürger, denen insbesondere nicht einleuchten wollte, weshalb jemand nicht als Zähler tätig werden darf, aber in der Erhebungsstelle eingesetzt werden kann. Ich konnte jedoch nur auf den Dissens, der über diese Frage zwischen mir und der obersten Aufsichtsbehörde für die Durchführung der Volkszählung besteht, hinweisen.

3.2.2.5.2
Normenkontrollverfahren

Über die Gültigkeit der Hessischen Verordnung zur Durchführung der Volkszählung 1987 hatte im vergangenen Jahr der Hessische Verwaltungsgerichtshof in einem Normenkontrollverfahren zu entscheiden (Beschluß vom 20. Oktober 1987 - 7 N 1273/87). Nach Ansicht des Gerichts beruht die Verordnung auf einer wirksamen, d.h. verfassungskonformen, gesetzlichen Grundlage (Volkszählungsgesetz 1987) und verstößt auch nicht gegen höherrangiges Bundesrecht. Insbesondere sieht das Gericht keinen Grund zur Beanstandung des § 2 Abs. 1 der Hessischen Durchführungsverordnung, wonach die örtliche Durchführung der Volkszählung 1987 den Gemeinden mit 3.000 und mehr Einwohnern obliegt. Nach Auffassung des Gerichts sind Gemeinden mit 3.000 bis 100.000 Einwohnern objektiv in der Lage, die Anforderungen des Volkszählungsgesetzes 1987 zu erfüllen, und vermögen die zur Grundrechtssicherung erforderlichen Vorkehrungen zu treffen. Grundlage für diese Einschätzung war unter anderem auch meine auf Anforderung des Gerichts abgegebene Stellungnahme, in der ich die Ergebnisse der von mir in den Erhebungsstellen vorgenommenen Prüfungen dargestellt habe (zu den Prüfergebnissen vgl. Ziff. 3.4.2.2 und 3.4.2.3).

Obgleich der Hessische Verwaltungsgerichtshof es als verfassungsrechtlich zulässig ansieht, daß in Erhebungsstellen auch Personen eingesetzt werden können, die im Hinblick auf mögliche Interessenkollisionen von der Zählertätigkeit ausgeschlossen sind, übt er deutlich Kritik an der hessischen Regelung (Beschluß vom 20. Oktober 1987, unter Ziff. 1e und 2a). Nach Ansicht des Gerichts hätte es „- auch im Hinblick auf die Akzeptanz der Erhebung - nahegelegen, den Einsatz des Personals der Erhebungsstelle durch landesrechtliche Regelungen an einschränkende Bedingungen zu knüpfen".

Die 1. Kammer des Ersten Senats des Bundesverfassungsgerichts hat in ihren Beschlüssen vom 24. September 1987 (1 BvR 970/87) und 28. September 1987 (1 BvR 782/87) die Frage, ob es von Verfassungs wegen geboten ist, an die Mitarbeiter der Erhebungsstellen dieselben Maßstäbe anzulegen, wie sie § 10 Abs. 5 Volkszählungsgesetz 1987 für Zähler festlegt, noch offengelassen.

3.2.2.6
ADV in den Erhebungsstellen - Runderlaß vom 27. April 1987

In vielen der insgesamt 426 örtlichen Erhebungsstellen erfolgt die zur Durchführung der Volkszählung notwendige Datenverarbeitung (z.B. die Rücklaufkontrolle) mit Hilfe automatisierter Verfahren. Genaue Zahlen darüber liegen mir nicht vor. Ich habe die Staatskanzlei zwar bereits im November 1986 aufgefordert, mir eine Übersicht zur automatisierten Datenverarbeitung in den Erhebungsstellen vorzulegen, aber bis heute keine Antwort erhalten.

Die Datenverarbeitung, die in den Erhebungsstellen zur organisatorischen Durchführung der Volkszählung erforderlich ist, muß nicht mit Kladde und Federkiel erledigt werden. Es steht der amtlichen Statistik wie jedem anderen Zweig der Verwaltung selbstverständlich grundsätzlich frei, zur Erledigung ihrer Aufgaben automatisierte Verfahren einzusetzen. Ausreichende Rechtsgrundlagen hierfür sind im Volkszählungsgesetz 1987 und im Hessischen Datenschutzgesetz vorhanden. Ich teile deshalb nicht die geäußerten grundsätzlichen Zweifel an der Zulässigkeit des Einsatzes der EDV durch die Erhebungsstellen (vgl. auch 15. Tätigkeitsbericht, Ziff. 8.2.3). Im gleichen Sinne hat sich jüngst auch die 1. Kammer des Ersten Senats des Bundesverfassungsgerichts geäußert (Beschluß vom 28. September 1987 - 1 BvR 1063/87 - Ziff. 2). Damit ist allerdings nicht gesagt, daß keine Beschränkungen gelten.

Die technisch möglichen Verfahren für die Gestaltung der automatisierten Datenverarbeitung in den Erhebungsstellen reichen vom Einsatz „autonomer" Personalcomputer über die (Mitbe-)Nutzung gemeindeeigener Verwaltungsrechner bis hin zur Abwicklung der Datenverarbeitung in den Kommunalen Gebietsrechenzentren (KGRZ).

Für die Zulässigkeit der Nutzung externer Rechner durch die Erhebungsstellen ist entscheidend, daß die vom Bundesverfassungsgericht und vom Volkszählungsgesetz 1987 geforderte strikte Abschottung der Erhebungsstellen nicht beeinträchtigt wird. Besonders unter diesem Gesichtspunkt habe ich das von den Kommunalen Gebietsrechenzentren vorgelegte Konzept zusätzlicher Maßnahmen zur räumlichen, personellen und organisatorischen Datensicherung überprüft. Auf der Grundlage meiner Prüfergebnisse ist anschließend in Gesprächen mit der Staatskanzlei, dem Hessischen Statistischen Landesamt und den Kommunalen Gebietsrechenzentren eine akzeptable Lösung gefunden worden.

Das Ergebnis meiner Prüfungen und der Besprechungen ist die Verwaltungsvorschrift vom 27. April 1987 (StAnz. 1987, S. 1064), die ausschließlich die automatisierte Datenverarbeitung in den Erhebungsstellen regelt und den Kommunalen Gebietsrechenzentren zusätzliche Datensicherungs- und Abschottungsmaßnahmen aufgibt. Das betrifft z.B. die Löschung der gespeicherten Daten, den Druck und die Nachbereitung der Erhebungsunterlagen (nur außerhalb des Normalbetriebs), die Beschränkung der Zahl der Personen, die in den Kommunalen Gebietsrechenzentren Zugriff auf die Daten der Erhebungsstellen haben, den Einsatz besonderer Sicherungsprogramme oder etwa die Abwicklung des Transports der Erhebungsunterlagen vom Kommunalen Gebietsrechenzentrum zur Erhebungsstelle. Unter den in der Verwaltungsvorschrift festgelegten Bedingungen halte ich die DV-Unterstützung der Erhebungsstellen durch die Kommunalen Gebietsrechenzentren für vertretbar.

Dagegen sind die Datensicherungs- und Abschottungsprobleme bei der Verarbeitung von Volkszählungsdaten auf gemeindeeigenen Verwaltungsrechnern, auf denen gleichzeitig auch andere Verwaltungsdaten verarbeitet werden, nicht lösbar. Ich halte diese Form der Datenverarbeitung deshalb für unzulässig. Die Staatskanzlei hat sich dieser Auffassung angeschlossen und in Ziffer II des Erlasses ein entsprechendes Verbot erlassen.

Die Datenverarbeitung auf einem ohne Kommunikationsanschluß in der räumlich abgeschotteten Erhebungsstelle befindlichen Personalcomputer dürfte wahrscheinlich am wenigsten das Vertrauen der Bürger gefährden. Entsprechend läßt die Verwaltungsvorschrift bis auf einen Ausnahmefall nur Personalcomputer ohne Kommunikationsanschluß zu. Personalcomputer mit Kommunikationsanschluß zum Kommunalen Gebietsrechenzentrum dürfen nur als Datenendgeräte (Terminals) eingesetzt werden, was durch das KGRZ zu garantieren ist. Außerdem schreibt die Verwaltungsvorschrift noch weitere Datensicherungsmaßnahmen für den Einsatz von Personalcomputern vor. Die Nutzung privater Personalcomputer wird in diesem Zusammenhang ausdrücklich untersagt (Ziffer III).

Erwähnenswert ist schließlich noch die Klarstellung, daß die örtlichen Erhebungsstellen keine Angaben der Auskunftspflichtigen zu Erhebungsmerkmalen automatisiert speichern dürfen (Ziffer IV).

3.3
Anonymisierungs-Debatte

3.3.1
Werbung und Wirklichkeit

Als ob die Durchführung der Volkszählung 1987 nicht problembeladen genug wäre, stehen sich die Statistikämter manchmal zusätzlich selbst im Weg. Das wohl beste Beispiel hierfür ist die Diskussion um die Anonymität der Volkszählungsdaten.

Die Werbung der Statistikämter zielte bewußt oder unbewußt darauf, den Eindruck zu erwecken, als seien die Volkszählungsdaten anonym. Die Folge war eine relativ unergiebige öffentliche Debatte über Möglichkeiten, statistische Einzelangaben, die ohne Hilfsmerkmale wie Namen und Hausnummern in den Statistikämtern gespeichert sind, zu deanonymisieren. Auch in zahlreichen Eingaben, die ich erhalten habe, bezweifelten Bürger die Anonymität der Volkszählungsdaten. Beides wäre wahrscheinlich weitgehend unterblieben, wenn die amtlichen Statistiker rechtzeitig Klarheit geschaffen hätten.

In der Erhebungsphase sind die Daten unmittelbar personenbezogen zunächst bei den Erhebungsstellen und danach beim Statistischen Landesamt vorhanden. Dies ist notwendig, um die Teilnahme aller Auskunftspflichtigen feststellen und während der Vollzähligkeits- , Vollständigkeits- und Plausibilitätskontrolle bei Unstimmigkeiten Rückfragen vornehmen zu können. Auch nach der Vernichtung sämtlicher Erhebungsvordrucke (§ 15 Abs. 2 VZG '87) bleibt die Personenbeziehbarkeit der dann nur noch automatisiert gespeicherten Daten erhalten. Das Statistische Landesamt speichert die Einzelangaben dauerhaft zwar ohne Namen der Betroffenen und lediglich einem Straßenabschnitt (Blockseite) zugeordnet, damit sind die Daten aber nur dem griechischen Wortlaut nach „anonym" („ohne Namen"), nicht jedoch in dem Sinn, daß kein Personenbezug mehr hergestellt werden kann.

Um die Daten einer bestimmten Person zuzuordnen, ist nicht einmal ein unverhältnismäßig großer Aufwand an Zeit, Kosten und Arbeitskraft erforderlich, so daß sie auch nicht als faktisch anonymisiert gelten können. Für die Herstellung des Personenbezugs bedarf es auch nicht unbedingt der in den Medien hinlänglich beschriebenen Computerprogramme. Seltene Merkmalsausprägungen in einem Datensatz genügen. Der Beruf des Pfarrers, Arztes,

Rechtsanwalts, Journalisten oder Hochschullehrers, die griechische Staatsbürgerschaft oder jüdische Religion oder eine ungewöhnlich große Wohnfläche erlauben, ohne große Mühe und besondere Computerprogramme, aus den Daten einer kleinen Gemeinde den Betroffenen zu identifizieren.

3.3.2
Bewertung

Die fehlende Anonymität oder faktische Anonymität der Volkszählungsdaten macht jedoch die Volkszählung keineswegs verfassungswidrig. Davon, daß eine Reidentifizierung möglich ist, geht das Volkszählungsgesetz 1987 selbst aus, wie das Reidentifizierungsverbot in den §§ 17 Abs. 2, 18 zeigt, denn ein Verbot ist naturgemäß nur sinnvoll, wenn das Verbotene für möglich gehalten wird. Wenn § 15 Abs. 4 Volkszählungsgesetz 1987 vorschreibt, daß statistische Ergebnisse auf Blockseitenbasis, die zur Veröffentlichung bestimmt sind, keine Einzelangaben enthalten dürfen, die dem Betroffenen zuzuordnen sind, wird damit gleichfalls die Personenbeziehbarkeit der Daten selbst bei Aggregierung unterstellt.

Die Forderung, daß nur faktisch anonymisierte oder gar vollständig anonymisierte Einzeldaten zur statistischen Verarbeitung dauerhaft gespeichert werden dürfen, ließe sich, wie die o.g. Beispiele zeigen, ohne erheblichen Aussageverlust der Statistik kaum erfüllen. Da die rechtlichen Grundvoraussetzungen für die Durchführung der Volkszählung selbstverständlich gleichermaßen auch für jede andere amtliche Statistik, seien es nun Kommunal-, Landes- oder Bundesstatistiken, zu gelten haben, wären unter einer solchen Bedingung in vielen Fällen aussagefähige Sozial- und Wirtschaftsstatistiken nicht mehr möglich. Die in der Tat etwas unklaren Äußerungen des Bundesverfassungsgerichts im Volkszählungsurteil zur Frage der Anonymisierung lassen sich sinnvollerweise nur so verstehen, daß die Daten von den Statistikämtern nicht unmittelbar personenbezogen (d.h. mit Namen des Betroffenen) dauerhaft gespeichert werden dürfen.

Gegen die Gefahren, die sich daraus ergeben, daß Einzeldaten aus der Volkszählung unter Umständen einer bestimmten Person zugeordnet werden können, sind ausreichende gesetzliche Sicherungen vorhanden. Neben dem Abschottungsgebot für die Erhebungsstellen enthält das Volkszählungsgesetz 1987 beispielsweise das Verbot, Erkenntnisse aus der Zählertätigkeit oder der Tätigkeit in der Erhebungsstelle anderweitig zu verwenden und zu verwerten. Der Name ist unverzüglich nach Durchführung der Eingangskontrollen bei den Statistischen Landesämtern von den Angaben in den Personen- und Wohnungsbogen zu trennen und darf vom Statistischen Landesamt nicht auf die zur automatisierten Weiterverarbeitung bestimmten Datenträger übernommen werden. Das strafrechtlich gesicherte Statistikgeheimnis ist ergänzt durch ein gleichfalls strafbewehrtes Reidentifizierungsverbot. Schließlich dürfen die Statistischen Landesämter Einzeldaten aus der Volkszählung nur unter sehr eingeschränkten Voraussetzungen an Dritte weitergeben (d.h. nur an von der übrigen Verwaltung abgetrennte Statistikstellen der Gemeinden).

Inzwischen hat sich auch das Bundesverfassungsgericht unmißverständlich geäußert. Die 1. Kammer des Ersten Senats stellt in ihrem Beschluß vom 24. September 1987 (1 BvR 970/87, unter 2d) klar: „Für die Statistischen Landesämter bleiben die Daten allerdings durchgängig personenbezogen, weil personenbeziehbar." Das Gericht weist gleichzeitig darauf hin, daß dies bei einer auf Individualdaten aufbauenden, kleinräumig zu gliedernden Statistik unvermeidbar ist und der einzelne das verbleibende Reidentifizierungsrisiko als notwendige Folge einer im überwiegenden Allgemeininteresse angeordneten Statistik hinzunehmen hat.

Die 1. Kammer des Ersten Senats des Bundesverfassungsgerichts hat in einem anderen Beschluß vom 28. September 1987 (1 BvR 1063/87,unter Ziff. 5) in diesem Zusammenhang eine weitere wichtige Klarstellung getroffen: „Werden aggregierte, anonymisierte Daten zum Anlaß genommen, Verwaltungsmaßnahmen etwa durch gezielte Betrachtung bestimmter Personengruppen oder Gebiete, etwa einer Blockseite, vorzubereiten, widerspricht dies weder dem Grundsatz der Trennung von Statistik und Vollzug noch dem Gebot einer Zweckbindung der erhobenen Daten zu statistischen Zwecken ...".

3.4
Prüfbesuche und Programmkontrollen

3.4.1
Funktion

Ich habe immer wieder betont, daß, nachdem der Bundesgesetzgeber mit dem Volkszählungsgesetz 1987 eine verfassungskonforme Grundlage geschaffen hat (vgl. Ziff. 3.2.2.2), die Rechtmäßigkeit der Volkszählung sich an der Einhaltung der Durchführungsbestimmungen entscheidet. Verantwortlich für die Einhaltung der Vorschriften waren und sind neben den örtlichen Erhebungsstellen das Statistische Landesamt und als oberste Aufsichtsbehörde die Staatskanzlei.

Aufgabe des Datenschutzbeauftragten konnte und kann es nur sein, den rechtmäßigen Verwaltungsvollzug durch kontinuierliche, gleichwohl schon aus Kapazitätsgründen zwangsläufig stichprobenweise Kontrollen zu überwachen, Erhebungsstellen und Gemeinden auf Schwachstellen hinzuweisen sowie die Aufsichtsbehörden über Defizite zu informieren und zum Eingreifen aufzufordern.

In diesem Sinne habe ich 1987 ein umfangreiches Prüfprogramm durchgeführt. Betroffen waren alle Behörden, die mit der Bearbeitung und Auswertung von Erhebungsunterlagen befaßt sind. Überprüft wurden:

- Erhebungsstellen (Ziff. 3.4.2),
- Kommunale Gebietsrechenzentren (Ziff. 3.4.3 und 3.4.4),
- das Statistische Landesamt in Wiesbaden und seine Außenstelle in Korbach (Ziff. 3.4.5).

Überprüft habe ich außerdem die Datenverarbeitung der Sicherheitsbehörden im Zusammenhang mit der Volkszählung 1987 (Ziff. 3.4.6).

3.4.2
Prüfprogramm Erhebungsstellen

3.4.2.1
Ablauf, Prüfkriterien, Durchführungsprobleme

Von April bis Oktober 1987 haben meine Mitarbeiter hessenweit 47 der 426 Erhebungsstellen überprüft. Bei der Festlegung des Prüfkonzepts kam es mir nicht darauf an, möglichst viele Erhebungsstellen „abzuklappern", sondern gezielt einzelne möglichst repräsentativ ausgewählte Stellen intensiv und umfassend zu kontrollieren, um so auch die Aufsichtsbehörde auf typische Defizite hinweisen zu können. Die Kontrollbesuche fanden an ca. 30 Tagen statt, wobei eine Fahrstrecke von weit über 4.000 km zurückgelegt werden mußte.

Um die Beachtung der Durchführungsbestimmungen möglichst konkret und einheitlich feststellen zu können und damit alle Erhebungsstellen gleich zu behandeln, erfolgten die Prüfungen fast ausnahmslos ohne vorherige Ankündigung. Kontrolliert wurde in erster Linie, ob die rechtlichen Vorgaben für die räumliche, personelle und organisatorische Abschottung eingehalten wurden. Hierzu lag ein detaillierter Prüfkatalog vor, der gewährleistete, daß für alle Erhebungsstellen die gleichen Kriterien zugrunde gelegt wurden.

Die Kontrollen erfolgten immer in Anwesenheit des Zählungsleiters bzw. dessen Stellvertreters. Es wurden u.a. die Räume besichtigt, die Sicherungsvorkehrungen bewertet sowie die Verwaltungsmaßnamen bei der Einrichtung der Erhebungsstelle (Bestellung und Verpflichtung des Personals, Prüfung auf Interessenkollision usw.) kontrolliert.

Nach Abschluß der Prüfung haben meine Mitarbeiter das Ergebnis mit dem Leiter der Erhebungsstelle besprochen. Auf eindeutige Verstöße gegen die bestehenden Vorschriften wurden die Zählungsleiter sofort aufmerksam gemacht und - falls die Mängel noch behebbar waren - beraten, wie diese unter Berücksichtigung der jeweiligen Verhältnisse sofort beseitigt werden konnten, um eine ordnungsgemäße Durchführung der Volkszählung zu gewährleisten. In der Regel wurde nach drei Tagen telefonisch nachgefragt, ob die Änderungen erfolgt waren.

Die Zählungsleiter haben diese Form der Kontrolle „vor Ort" und die entsprechende Beratung in aller Regel positiv bewertet. Bei den Rückrufen wurde in fast allen Fällen die Beseitigung der festgestellten Mängel bestätigt.

Vereinzelt gab es allerdings Schwierigkeiten mit den jeweiligen Bürgermeistern, die sich in den direkten Kontakt mit den Verantwortlichen der Erhebungsstelle einschalten wollten und sich dabei offensichtlich fälschlicherweise als Fachvorgesetzte des Zählungsleiters und seiner Mitarbeiter verstanden. Vor Beginn der Überprüfung wurden zwar alle Erhebungsstellenleiter auf die Möglichkeit hingewiesen, den Bürgermeister in seiner Rolle als Dienstvorgesetzter hinzuzuziehen. Als Gesprächspartner kam jedoch nur der Zählungsleiter in Betracht, weil ausschließlich er die Erhebung zu leiten und die Aufsicht über das Personal der Erhebungsstelle zu führen hat (§ 4 HDO-VZG). Auf meine Aufforderung hin hat das Hessische Innenministerium alle Kommunalaufsichtsbehörden Anfang Juni entsprechend unterrichtet. Danach ist es zu keinen Zwischenfällen mehr gekommen.

Mängel, die nicht sofort von den Erhebungsstellen behoben werden konnten, habe ich dem Statistischen Landesamt und in gravierenden Fällen auch der Staatskanzlei mitgeteilt, verbunden mit der Aufforderung, in der Angelegenheit tätig zu werden. Eine Wiederholungskontrolle in der Erhebungsstelle konnte aus Kapazitätsgründen nur in Einzelfällen vorgenommen werden, insbesondere bei solchen Stellen, über die mehrfach Beschwerden eingingen.

Bei der Auswahl der Erhebungsstellen habe ich auf eine einigermaßen ausgewogene größenmäßige und regionale Verteilung der Gemeinden geachtet. Die 47 überprüften Erhebungsstellen verteilen sich wie folgt auf 7 Gemeindegrößenklassen:

unter	3.000 Einwohnern	7 Erhebungsstellen
3.000 -	6.000 Einwohnern	6 Erhebungsstellen
6.000 -	9.000 Einwohnern	5 Erhebungsstellen
9.000 -	20.000 Einwohnern	8 Erhebungsstellen
20.000 -	50.000 Einwohnern	10 Erhebungsstellen
50.000 -	100.000 Einwohnern	6 Erhebungsstellen
über	100.000 Einwohnern	5 Erhebungsstellen

Allerdings lassen sich die Ergebnisse nur unter gewissem Vorbehalt auf die Gesamtsituation in Hessen hochrechnen, weil nicht immer nach streng repräsentativen Kriterien vorgegangen werden konnte, sondern einige Erhebungsstellen aufgrund gezielter Hinweise auf Unregelmäßigkeiten kontrolliert werden mußten. Nicht auszuschließen ist daher, daß Verstöße gegen Durchführungsbestimmungen in den Prüforten häufiger waren als im Landesdurchschnitt.

3.4.2.2
Festgestellte Mängel

Die folgende Mängelliste bezieht sich auf die räumliche, personelle und organisatorische Abschottung der Erhebungsstellen, deren Anforderungen im einzelnen in den oben aufgelisteten Verordnungen und Erlassen (vgl. Ziff. 3.2.1) geregelt sind. Enthalten sind - um es noch einmal klarzustellen - nur Unregelmäßigkeiten, die meine Mitarbeiter „vor Ort" festgestellt haben, nicht aber die zahlreichen Mängel, die mir außerhalb des Prüfprogramms zusätzlich brieflich oder telefonisch mitgeteilt wurden. Die Grafik am Ende des Abschnitts Ziff. 3.4.2.3 enthält noch einmal die Häufigkeitsverteilung der wichtigsten Beanstandungspunkte.

a) Räumliche Abschottung:

- In siebzehn Erhebungsstellen war keine Empfangsstelle eingerichtet.
- In sieben im Erdgeschoß liegenden Erhebungsstellen waren die Fenster und Türen nicht ausreichend gesichert.
- In vierzehn Erhebungsstellen mit mehreren Zugängen fehlten die vorgeschriebenen Versiegelungen.
- In sieben Erhebungsstellen wurden die Volkszählungsunterlagen nicht in verschließbaren Schränken aufbewahrt.

b) Personelle Abschottung:

- In neun Fällen war versäumt worden, den Zählungsleiter und dessen Stellvertreter förmlich zu bestellen.
- In neun Erhebungsstellen waren die dort tätigen Personen nicht auf die Wahrung des Statistikgeheimnisses verpflichtet worden.
- In elf Erhebungsstellen waren Personen beschäftigt, die aus Ämtern kamen, bei denen die Besorgnis der Interessenkollision besteht (vgl. zu diesem Problem oben Ziff. 3.2.2.5.1).
- In vierzehn Fällen wurde Erhebungsstellenpersonal angetroffen, das gleichzeitig mit anderen Aufgaben des Verwaltungsvollzugs betraut war.
- Daß Zähler nach Abschluß ihrer Zählertätigkeit unzulässigerweise in der Erhebungsstelle beschäftigt wurden, habe ich dreimal festgestellt.

c) Organisation der Erhebungsstellen (einschließlich Zählereinsatz):

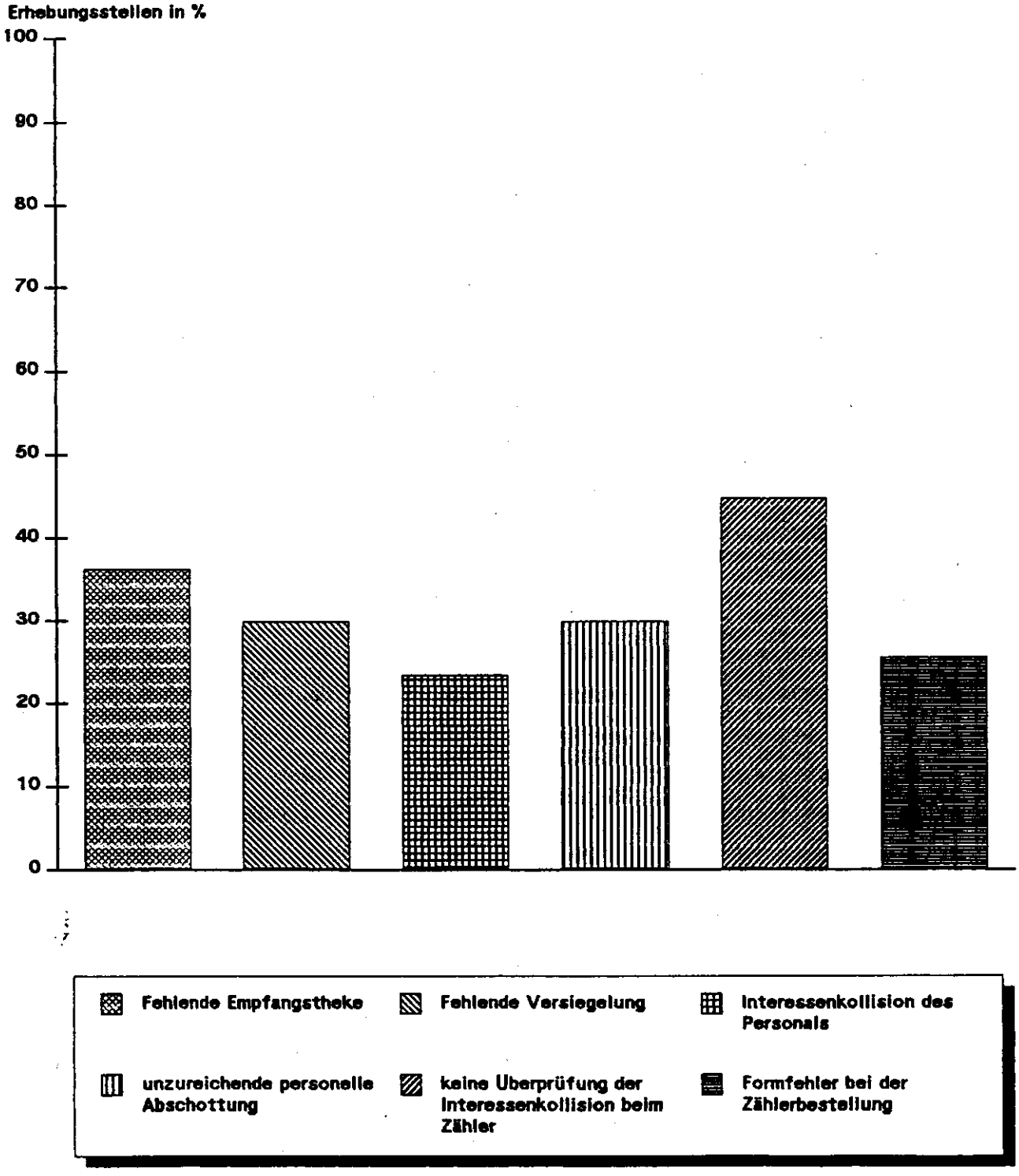
- In zwei Erhebungsstellen war nicht geregelt, wer von den dort tätigen Personen für die Zugangssicherung zuständig war.
- In zwölf Erhebungsstellen war die Zählerbestellung nicht korrekt bzw. nicht durch den Zählungsleiter erfolgt.
- In 21 Erhebungsstellen fehlte es an der Überprüfung einer möglichen Interessenkollision bei den Zählern.
- In vier Erhebungsstellen waren die Zähler nicht auf die Wahrung des Statistikgeheimnisses und zur Geheimhaltung solcher Erkenntnisse über die Auskunftspflichtigen schriftlich verpflichtet worden, die gelegentlich der Zählertätigkeit gewonnen werden.
- In einer Erhebungsstelle wurden Zähler aus dem Einwohnermeldeamt eingesetzt.
- Fünf Erhebungsstellen erhielten von den Einwohnermeldeämtern mehr Daten als nach § 11 Volkszählungsgesetz zulässig.
- In allen geprüften Erhebungsstellen in Gemeinden mit weniger als 3.000 Einwohnern mangelte es an dem Nachweis der Abschottung der Erhebungsstelle gegenüber der Kommunalaufsicht.

3.4.2.3
Bewertung

Was die Größe der Kommunen im Verhältnis zur Häufigkeit der Mängel angeht, läßt sich feststellen, daß bestimmte Defizite gehäuft bei kleineren Gemeinden, andere dagegen vorwiegend bei Kommunen mit größerer Einwohnerzahl

VOLKSZÄHLUNG 1987

Die häufigsten Mängel in den geprüften Erhebungsstellen



auftraten. Während bei den ersteren die Mängel vor allem im Bereich der räumlichen und organisatorischen Abschottung lagen, wurden in den Gemeinden zwischen 9.000 und 50.000 Einwohnern vermehrt die Anforderungen an die personelle Abschottung nicht eingehalten. In den kleineren Kommunen wurden die Probleme einer möglichen Interessenkollision des Personals der Erhebungsstelle in einer Reihe von Fällen schon dadurch vermieden, daß verwaltungsexterne Kräfte eingesetzt wurden. Diese Frage spielte auch in dem Normenkontrollverfahren vor dem Hessischen Verwaltungsgerichtshof eine zentrale Rolle (vgl. oben Ziff. 3.2.2.5.2). Dem VGH habe ich dementsprechend in meiner Stellungnahme mitgeteilt, daß meine Prüfergebnisse nicht den Schluß zulassen, in kleineren

Gemeinden könne das Abschottungsgebot schon aus organisatorischen Gründen gar nicht oder zumindest schlechter als in mittleren oder größeren Kommunen beachtet werden.

Insgesamt bewerte ich jedoch die administrative Umsetzung der Vorgaben für Datenschutz und Datensicherung bei den örtlichen Erhebungsstellen in Hessen als äußerst unbefriedigend. Das landesweite Prüfprogramm hat zum Teil gravierende Vollzugsdefizite aufgedeckt. Oft rechtfertigten sich die Zählungsleiter mit dem Hinweis auf die beschränkten organisatorischen und finanziellen Möglichkeiten der Gemeinde. Dem ist jedoch entgegenzuhalten, daß sich Gemeinden aller Größenklassen mit vorbildlich organisierten und abgeschotteten Erhebungsstellen nennen lassen, die belegen, daß bei entsprechender Vorausplanung und bei entsprechendem Einsatz der Behördenleitung die Durchführungsvorschriften problemlos eingehalten werden konnten.

3.4.3
Prüfprogramm Kommunale Gebietsrechenzentren - DV-Unterstützung der Erhebungsstellen

3.4.3.1
Eingesetzte Programme

Die Kommunalen Gebietsrechenzentren (KGRZ) des Hessischen DV-Verbundes haben drei verschiedene Programmversionen zur Unterstützung der Erhebungsstellen für die Volkszählung 1987 eingesetzt.

Die KGRZen Kassel und Gießen stellten den Erhebungsstellen ihres Einzugsbereiches Programme nur für die Vorbereitungsphase zur Verfügung. Dazu wurden die nach § 11 VZG zulässigen Daten aus den Verfahren „Kommunales Finanzwesen" (für die Gebäudevorerhebung) und „Grundstufe Einwohnerwesen" (für die Haupterhebung) zur weiteren Verarbeitung herausgefiltert. Anschließend wurden aus diesem Datenbestand Druckausgaben (Listen und Aufkleber) für die Erhebungsstellen erzeugt. Die Daten wurden nach Auslieferung der Listen und Aufkleber an die Erhebungsstellen nicht weiter in den Rechenzentren gespeichert. Es erfolgte keine automatisierte „Rücklaufkontrolle". Insgesamt hatte ich daher gegen dieses Verfahren keine Bedenken.

Die vom KGRZ Wiesbaden geschriebenen Programme sahen darüber hinaus die weitere Bearbeitung der Daten während der Gebäudevorerhebung und der Haupterhebung (Rücklaufkontrolle, Mahnungen, Zählerabrechnungen usw.) vor. Im Rahmen der automatisierten Rücklaufkontrolle konnten die Erhebungsstellen auch über Bildschirme auf diese Daten zugreifen und ggf. Änderungen durchführen. Das KGRZ stellte programmtechnisch sicher, daß jede Erhebungsstelle nur ihre eigenen Daten verarbeiten konnte.

Die mir vom KGRZ Wiesbaden zur Verfügung gestellten Programmbeschreibungen wurden geprüft. Nachdem die erforderlichen Änderungen durchgeführt waren, was mir auch schriftlich bestätigt wurde, gab es gegen den Einsatz der Programme keine Bedenken mehr.

In einem Fall aus dem Einzugsbereich des KGRZ Wiesbaden mußte ich allerdings eine förmliche Beanstandung aussprechen. Eine Gemeinde wollte ein im Einwohnermeldeamt stehendes Terminal für den Zugriff auf Volkszählungsdaten nutzen, was dem Abschottungsgebot und den Vorgaben des einschlägigen Erlasses vom 27. April 1987 (vgl. Ziff. 3.2.2.6 dieses Berichts) widersprach. Erst nach Intervention der Staatskanzlei wurde diese rechtswidrige Praxis noch vor dem Stichtag eingestellt.

Die Kommunalen Gebietsrechenzentren Starkenburg und Frankfurt stellten den Gemeinden sowohl für die Vorbereitungsphase als auch für die Gebäudevorerhebung und die Haupterhebung der Volkszählung 1987 Programme zur Verfügung, die durch den KOSIS-Verbund, einem Programmierverbund mehrerer deutscher Großstädte, entwickelt worden waren. Das fachliche Konzept für diese Programme hatten mehrere Kommunalverwaltungen in Zusammenarbeit mit einer Software-Firma erarbeitet.

Neben der automatisierten Rücklaufkontrolle und dem Direktzugriff durch die Erhebungsstellen bietet dieses Verfahren auch die Möglichkeit, die „Mahnungen" an säumige Auskunftspflichtige automatisiert zu erstellen.

3.4.3.2
Programm- und Dokumentationsmängel

Bei den mir von den Kommunalen Gebietsrechenzentren Darmstadt und Frankfurt übersandten Unterlagen handelte es sich lediglich um eine „Leistungsbeschreibung" des KOSIS-Verbundes, die für eine ordnungsgemäße datenschutzrechtliche Bewertung der Haupterhebung nicht ausreichte. Trotz wiederholter Mahnungen habe ich zu keinem Zeitpunkt die notwendigen prüffähigen Unterlagen (Programmbeschreibungen, Programmablaufpläne usw. entsprechend den DV-Leitsätzen) vollständig erhalten. Begründet wurde dies u.a. damit, daß die Rechenzentren keinen Einfluß auf die Erstellung und Dokumentation der Verfahren des KOSIS-Verbundes hätten; außerdem habe die Anwenderbetreuung Vorrang vor der Herstellung von „Formalien". Ich habe den Hessischen Ministerpräsidenten nachdrücklich darauf hingewiesen, daß sich ein solcher Vorgang, bei dem mir Programmbeschreibungen nur verspätet und unvollständig vorgelegt werden, auf keinen Fall wiederholen darf.

Trotz der Unzulänglichkeit der Unterlagen stellte ich mehrere Verstöße gegen die Durchführungsvorschriften fest. Die Mängel konnten durch Änderungen in den Programmen oder durch organisatorische Maßnahmen im Bereich

der Rechenzentren bzw. der einzelnen Erhebungsstellen teilweise behoben werden. Beispielsweise wurde sichergestellt, daß keine Speicherung des Merkmals „mehrere Wohnungen" und weiterer in § 11 VZG nicht zugelassener Angaben erfolgte. Verschiedene andere Mängel wurden jedoch nicht mehr beseitigt, da die Programme für einen bundesweiten Einsatz konzipiert und auf Hessen beschränkte Änderungen nicht möglich gewesen seien.

Aus diesen Vorgängen ergibt sich zwangsläufig die generelle Konsequenz, daß sich öffentliche Stellen - auch und gerade die Kommunalen Gebietsrechenzentren - nur an solchen Programmierverbünden beteiligen dürfen, bei denen sie eigenverantwortlich die Rechtmäßigkeit der Datenverarbeitung überprüfen und sicherstellen sowie einen ausreichenden Datensicherungsstandard gewährleisten können.

3.4.4
Prüfprogramm Kommunale Gebietsrechenzentren - Abschottung

Neben der Programmkontrolle kam es bei der Bewertung der Rechtmäßigkeit der Datenverarbeitung in den Kommunalen Gebietsrechenzentren mit begleitender DV-Unterstützung der Erhebungsstellen noch auf einen weiteren Punkt an. Die für die örtlichen Erhebungsstellen obligatorische Abschottung mußte auf die im Auftrag der Erhebungsstellen tätigen Rechenzentren „verlängert" werden. Es galt zu gewährleisten, daß der Zugriff auf Volkszählungsdaten technisch wie personell streng begrenzt wurde, um eine Vermischung mit den zahlreichen anderen in den Gebietsrechenzentren verarbeiteten Verwaltungsdaten zu verhindern.

Deshalb hatte ich schon vor dem Gemeinsamen Runderlaß zur Durchführung der Volkszählung 1987 vom 27. April 1987 (vgl. oben Ziff. 3.2.2.6) auf die Notwendigkeit von zusätzlichen technischen, organisatorischen und personellen Maßnahmen hingewiesen, denn das übliche Datensicherungs- und Abschottungskonzept der Kommunalen Gebietsrechenzentren reichte für die Volkszählung nicht aus.

Unter anderem habe ich folgende Vorkehrungen gefordert:

1. Technische Maßnahmen

- Zugriffe auf Volkszählungs-Daten sind zu protokollieren.
- Es ist eine spezielle Datenschutzsoftware einzusetzen.
- Die Warteschlangen für die Druckausgaben sind gegen unberechtigtes Lesen zu schützen.
- Verarbeitungsprogramme für die Volkszählung 1987 dürfen nur von dafür berechtigten Mitarbeitern gestartet werden, was maschinell zu überwachen ist.
- Durch Einsatz von entsprechenden Programmen ist sicherzustellen, daß die Mitarbeiter der örtlichen Erhebungsstellen nur Programme der Volkszählung 1987 aufrufen können und keinen Zugang zu anderen kommunalen Dateien haben.
- Alle temporären Dateien, die bei der Umsortierung von Datensätzen im Zusammenhang mit dem Ausdruck von Erhebungsunterlagen entstehen, sind nach Beendigung dieses Arbeitsganges unverzüglich zu löschen.

2. Organisatorische Maßnahmen

- Die Mitarbeiter mit Zugriffsberechtigung auf Volkszählungsdaten sind in einem gesonderten Dienstzimmer unterzubringen, das ständig verschlossen zu halten ist.
- Die Terminals dieser Mitarbeiter sind bei jedem Verlassen des Raumes abzuschalten (LOGOFF).
- Beim Druck der Erhebungsunterlagen und deren Nachbereitung hat das eingeteilte Maschinenpersonal sicherzustellen, daß außer den Anwendungsberatern keine weiteren Mitarbeiter des Rechenzentrums Zugriff auf die Bestände der Volkszählung 1987 haben.
- Die Erhebungsunterlagen sind in einem gesonderten Arbeitsgang getrennt vom übrigen Tagesgeschäft zu drucken und nachzubereiten.
- Der Kurierdienst des Rechenzentrums ist verpflichtet, die Unterlagen den örtlichen Erhebungsstellen unmittelbar zuzustellen. Die Zustellung an die allgemeine Posteingangsstelle der Gemeinde ist nicht zulässig.

3. Personelle Maßnahmen

- Es dürfen nur bestimmte, über ihre speziellen Pflichten belehrte Bedienstete Aufgaben für die Volkszählung 1987 wahrnehmen.
- Der Datenbankadministrator darf nur bei Datenbankfehlern nach Abstimmung mit dem zuständigen Abteilungsleiter lesend auf die Volkszählungsdaten zugreifen.

In den Kommunalen Gebietsrechenzentren Frankfurt, Darmstadt und Wiesbaden habe ich mich durch Prüfbesuche davon überzeugt, daß alle diese Vorgaben realisiert worden waren.

3.4.5
Prüfung des Statistischen Landesamts

Ergänzend zu den Prüfungen der Erhebungsstellen und der Kommunalen Gebietsrechenzentren habe ich die Datensicherheitsvorkehrungen im Statistischen Landesamt überprüft. Schwerpunkt war hierbei die Außenstelle in Korbach, an die sämtliche Erhebungsstellen ihr Material zu schicken haben und wo die Erhebungsunterlagen gelagert, auf Vollständigkeit und Vollzähligkeit geprüft, signiert, getrennt und zum gegebenen Zeitpunkt vernichtet werden. Bei zwei Ortsterminen konnte ich mich davon überzeugen, daß alle von mir angeregten bzw. in einem Gutachten des Landeskriminalamts vorgesehenen Maßnahmen getroffen waren.

In den Räumen des Statistischen Landesamts in Wiesbaden, in denen teilweise ebenfalls Volkszählungsunterlagen gelagert und bearbeitet werden - vor allem für die Arbeitsstättenzählung - habe ich mir ebenfalls mehrfach die Datensicherungsmaßnahmen zeigen lassen. Dem Präsidenten des Statistischen Landesamts habe ich mitgeteilt, daß noch Verbesserungen notwendig sind. Sie sollten zu Jahresbeginn 1988 endgültig festgelegt sein, damit sie bei Beginn der Aufbereitungsarbeiten realisiert sind.

3.4.6
Prüfung der Sicherheitsbehörden

Im Juni 1987 habe ich auch die Datenspeicherung der Sicherheitsbehörden im Zusammenhang mit der Volkszählung 1987 überprüft.

Das Landesamt für Verfassungsschutz teilte mir auf Anfrage mit, daß es Angaben über „Boykotteure" der Volkszählung nur speichere, wenn die Personen bereits aus anderen Gründen registriert worden seien - etwa als aktive Mitglieder von Organisationen, deren Tätigkeit das Landesamt beobachtet. Die Daten würden in diesen Fällen den bereits gespeicherten Informationen hinzugefügt.

Die meisten Datenspeicherungen, die die hessische Polizei im Zusammenhang mit der Volkszählung 1987 im bundesweiten polizeilichen Informationssystem APIS vorgenommen hatte, mußte ich beanstanden. Die Prüfung beim Landeskriminalamt ergab, daß mehr als 70 v. H. der Datensätze Bagatellfälle betrafen. In das für die Strafverfolgung und Gefahrenabwehr im Staatsschutzbereich geschaffene Informationssystem APIS gehören jedoch keine Angaben über Graffiti oder Plakat- und Flugblattaktionen, mit denen zum Boykott der Volkszählung aufgerufen wird. Es ist auch nicht zu erkennen, worin die Staatsgefährdung liegen soll, wenn jemand Plakate, auf denen für die Volkszählung geworben wird, beschädigt. Das mag anders sein bei Bombendrohungen oder Brandanschlägen auf Erhebungsstellen - nur wenige Datensätze bezogen sich allerdings auf solche Fälle. (Zu APIS und den datenschutzrechtlichen Anforderungen an die Speicherung von Daten in diesem System vgl. auch Ziff. 9.2 dieses Berichts).

3.5
Eingaben und Beschwerden der Bürger

3.5.1
Kritikpunkte

Die Volkszählung hat zu mehreren hundert schriftlichen und telefonischen Anfragen, Eingaben und Beschwerden bei meiner Dienststelle geführt. Dem zeitlichen Ablauf der Erhebung folgend ging es dabei zunächst darum, wer als Zähler verpflichtet und ob die Weigerung, als Zähler tätig zu werden, in der Personalakte vermerkt werden durfte. Als die Zähler mit dem Verteilen der Fragebogen begannen, beschwerten sich auch Bürger, daß ihr Zähler in der Nachbarschaft wohne oder durch seine berufliche Tätigkeit einem Interessenkonflikt ausgesetzt sei (Ziff. 3.5.2). Besorgnis löste in vielen Fällen die angeblich oder tatsächlich unzureichende räumliche, personelle und organisatorische Abschottung der örtlichen Erhebungsstelle aus, also die Punkte, die auch im Rahmen meines landesweiten Prüfprogramms festgestellt wurden (vgl. oben Ziff. 3.4.2.2). Neben Hinweisen auf Durchführungsmängel enthielten viele Briefe verfassungsrechtliche Zweifel an der Zulässigkeit der Totalerhebung sowie Kritik und Fragen zur einfachgesetzlichen Regelung der Volkszählung, etwa dem Verhältnis des Volkszählungsgesetzes 1987 zum neuen Bundesstatistikgesetz (vgl. oben Ziff. 3.2.2.2 und 3.2.2.3).

3.5.2
Zählereinsatz

Bei weitem die meisten Eingaben betrafen vermutete Verstöße gegen § 10 Abs. 5 Volkszählungsgesetz 1987. Nach dieser Vorschrift dürfen Zähler nicht in der Nachbarschaft eingesetzt werden und in keiner Interessenkollision sein. Es ging immer wieder um die Frage, wie der Rechtsbegriff der „unmittelbaren Nähe" zur Wohnung - so definiert das Gesetz „Nachbarschaft" - auszulegen ist und bei welchem Personenkreis eine zweckwidrige Verwendung von Informationen aus der Zählertätigkeit (Interessenkollision) zu befürchten sein könnte.

3.5.2.1
Nachbarschaft

Was unter „Nachbarschaft" zu verstehen ist, definiert die vom Hessischen Statistischen Landesamt herausgegebene Anleitung für die Erhebungsstellen wie folgt: Dies „hängt ... von den örtlichen Gegebenheiten ab. In jedem Fall darf der Zähler nicht in dem Zählbezirk eingesetzt werden, in dem er selbst wohnt. Wir empfehlen insbesondere kleineren Gemeinden, auch diejenigen Zählbezirke zur Nachbarschaft zu rechnen, die an den Zählerbezirk angrenzen, in dem der Zähler wohnt". Bedenkt man, daß ein Zählbezirk etwa 60 bis 80 Haushalte umfaßt, ergibt sich daraus, daß es nach den Vorgaben des Statistischen Landesamtes zulässig ist, daß Personen im gleichen Ortsteil oder Stadtbezirk ggf. nur eine Straße weiter zählten bzw. zählen, wenn diese Straße nicht mehr zum Zählbezirk gehört, in dem sie selbst wohnen.

Nach meinen Feststellungen wurden nur in wenigen Fällen entgegen der klaren Vorschrift Zähler in Bezirken eingesetzt, in denen sie wohnen. Dagegen haben sich leider die meisten Erhebungsstellen in kleineren Gemeinden nicht an die Empfehlung gehalten, auch die angrenzenden Zählbezirke zur „Nachbarschaft" zu rechnen. Selbst wo Zähler nicht in unmittelbarer Nähe ihrer Wohnung, aber noch innerhalb z.B. des gleichen Ortsteils eingesetzt wurden, haben sich immer wieder Bürger beschwert, daß ein Zähler erschienen war, den sie persönlich kannten.

Daß eine solche persönliche Bekanntschaft zwischen Zählern und Gezählten nicht auszuschließen ist, hat der Gesetzgeber gesehen. Anders als das Volkszählungsgesetz 1983 gibt daher das Volkszählungsgesetz 1987 (§ 13 Abs. 2 und 4) den Auskunftspflichtigen die Möglichkeit, die von ihnen selbst ausgefüllten Erhebungsbogen unmittelbar bei der Erhebungsstelle abzugeben oder dorthin zu schicken. Alle Bürger, die an der Diskretion ihres Zählers zweifelten, habe ich deshalb auf diese Möglichkeit hingewiesen.

3.5.2.2
Kollision mit der beruflichen Tätigkeit

Zu den Personen, bei denen aufgrund ihrer beruflichen Tätigkeit die Gefahr besteht, daß Erkenntnisse aus der Zählertätigkeit zu Lasten des Auskunftspflichtigen genutzt werden und die deshalb nicht als Zähler tätig werden dürfen (§ 10 Abs. 5 Satz 2 Volkszählungsgesetz 1987), zählt der Gemeinsame Runderlaß der Landesregierung zur Durchführung der Volkszählung vom 2. September 1986 (StAnz. 1986, S. 1774) die Bediensteten

- der Steuerverwaltung,
- der Polizei,
- des Landesamts für Verfassungsschutz
- sowie Staats- und Amtsanwälte.

Darüber hinaus sollen als Zähler grundsätzlich keine Mitarbeiter aus den Einwohnermeldeämtern eingesetzt werden, „sofern dies die personelle Ausstattung des Trägers der Erhebungsstelle zuläßt". Dieser Vorbehalt ist mit dem gesetzlichen Gebot der personellen Abschottung der Erhebungsstellen nicht vereinbar. Interessenkollisionen gibt es freilich nicht nur in den Fällen, die der Erlaß aufzählt. Ein Interessenkonflikt liegt beispielsweise auch dann vor, wenn ein Sozialarbeiter in seinem örtlichen Zuständigkeitsbereich zählt. Es ist jeweils der Einzelfall zu bewerten.

Bei klaren oder wahrscheinlichen Verstößen, die mir schriftlich oder telefonisch mitgeteilt wurden, habe ich in jedem Fall umgehend das Statistische Landesamt als zuständige oberste Erhebungsstelle unterrichtet und zum Einschreiten aufgefordert. Ob das Landesamt immer die erforderlichen Schritte unternommen hat, konnte ich nicht überprüfen. Manchmal war der Zählereinsatz auch bereits beendet, als mir die Beschwerde zuging. In gravierenden Einzelfällen habe ich mich selbst an die betroffene Erhebungsstelle gewandt.

Bei meinen Prüfbesuchen in kleineren Gemeinden habe ich den Erhebungsstellen immer empfohlen, die Zähler in wohnungsfernen Ortsteilen einzusetzen.

3.6
Die Reaktionen der Regierung und der Verwaltung

3.6.1
Hessisches Statistisches Landesamt

Mit dem Statistischen Landesamt bestand während des gesamten Berichtszeitraums ein intensiver Kontakt. Das Landesamt war für mich Ansprechpartner bei allen Problemen, die ich nicht selbst im Kontakt mit den Erhebungsstellen klären bzw. ausräumen konnte. Ich habe das Statistische Landesamt regelmäßig und umgehend über alle Verstöße unterrichtet, die ich bei Prüfbesuchen festgestellt hatte oder die mir Bürger schriftlich oder telefonisch mitgeteilt hatten. Wie bereits erwähnt, konnte ich schon aus Gründen der Kapazität meiner Dienststelle nicht in jedem Einzelfall weiterverfolgen, ob das Landesamt die Beseitigung der Mängel erreichen konnte. Manche Defizite, etwa bei der Zählerbestellung, waren schon aus Zeitgründen nicht mehr zu beheben.

Das Statistische Landesamt war regelmäßig bereit, Hinweisen auf Verstöße bei den örtlichen Erhebungsstellen nachzugehen und meine Vorschläge in Rundschreiben an die Erhebungsstellen aufzunehmen. Die Effizienz bei der

Beseitigung von Rechtsfehlern und organisatorischen Schwachstellen war jedoch erheblich beeinträchtigt durch die mangelnde personelle Ausstattung der zuständigen Fachreferate, die gleichzeitig Anfragen von Erhebungsstellen und Bürgern beantworten, Hinweisen des Datenschutzbeauftragten nachgehen und die internen Verwaltungsrichtlinien und -rundschreiben fertigen mußten. Angesichts der Dimension dieser Großzählung, der schwierigen Umsetzungsprobleme und auch der personellen Ausstattung anderer Statistikämter sehe ich hier ein schwer begründbares Defizit (zu den Problemen des Datenschutzes und der Datensicherung bei der Verarbeitung von Volkszählungsdaten im Hessischen Statistischen Landesamt und seiner Außenstelle vgl. Ziff. 3.4.5).

3.6.2
Staatskanzlei

Die Hessische Staatskanzlei als oberste Aufsichtsbehörde habe ich wiederholt über meine Erfahrungen und Bewertungen informiert. Bereits in einem Schreiben mit Datum des Stichtags der Volkszählung, dem 25. Mai 1987, hatte ich eindringlich auf die bis dahin bei den örtlichen Erhebungsstellen festgestellten Mängel aufmerksam gemacht. Zwei Monate später, mit Brief vom 27. Juli 1987, hatte ich meine Bedenken und Besorgnisse aufgrund der Prüfergebnisse erneuert und im einzelnen quantifiziert. Mir ging es darum, zu keinem Zeitpunkt einen Zweifel daran zu lassen, daß das Gesamtbild der Einhaltung des gesetzlich geforderten Datenschutzstandards in den Erhebungsstellen zu viele Schwachstellen und Verstöße aufwies.

Auch bei einzelnen Konflikten mit Erhebungsstellen habe ich immer wieder die Staatskanzlei eingeschaltet.

In seinem Antwortschreiben vom 26. August 1987 ging der Hessische Ministerpräsident detailliert auf meine Kritikpunkte ein, wobei unterschiedliche Rechtsauffassungen - etwa über die Frage der Interessenkollision bei den Mitarbeitern der Erhebungsstellen (vgl. Ziff. 3.2.2.5.1) - bestehen blieben. Er vertrat die Auffassung, die von mir angeführten Beispiele und Zahlen zu den Durchführungsmängeln dürften nicht zu einem negativen Gesamtbild zusammengefügt werden. Meine beiden Schreiben habe er den nachgeordneten Aufsichtsbehörden mit der Bitte übersandt, die Mängel zu beheben und sicherzustellen, daß sie künftig vermieden würden. Daß dies nicht ausreichend gelungen ist, belegen die Ergebnisse meines Prüfprogramms (vgl. Ziff. 3.4.2.2).

3.7
Prüfungsschwerpunkte 1988

3.7.1
Erhebungsphase

Auch 1988 werde ich mich in besonderem Maße mit der Volkszählung beschäftigen. Die Erhebungsstellen einiger Großstädte etwa in Frankfurt und Wiesbaden dürften erst im Frühjahr 1988 ihre Arbeit einstellen. Bis zur endgültigen Schließung wird voraussichtlich noch häufig Anfragen und Beschwerden von Bürgern vor Ort nachzugehen sein. Hinzukommt, daß in einigen wenigen ausgewählten Zählbezirken die in § 1 Abs. 4 VZG 1987 vorgesehene Wiederholungsbefragung zur Prüfung der Zuverlässigkeit der Ergebnisse ansteht. Die Erhebungsphase wird jedoch im kommenden Jahr auslaufen. Im Vordergrund steht dann zum einen die manuelle Verarbeitung in Korbach, d.h. die Vollzähligkeits- und Vollständigkeitskontrolle, die Signierung usw. etwa der Erhebungsbögen und Regionallisten. In diesem Abschnitt geht es in erster Linie darum, sicherzustellen, daß die Vorgaben des § 15 Abs. 1 und 2 VZG eingehalten werden. Danach sind die sogenannten Hilfsmerkmale (z.B. Namen) unverzüglich nach Durchführung der Eingangskontrollen in Korbach von den eigentlichen Erhebungsmerkmalen zu trennen und gesondert aufzubewahren.

Sämtliche Erhebungsunterlagen, also sowohl die verschiedenen vom Bürger ausgefüllten Fragebögen als auch die Organisationspapiere wie Regionallisten, Namenlisten usw. sind zum frühestmöglichen Zeitpunkt zu vernichten. Aus dieser Bestimmung entnehme ich ein „Beschleunigungsgebot" für die Bearbeitung. Anders ausgedrückt: Der vom Gesetz als spätestmöglicher Zeitpunkt für die Vernichtung angegebene Termin, nämlich zwei Wochen nach Feststellung der amtlichen Bevölkerungszahl, darf nur erreicht werden, wenn dies im Einzelfall wegen notwendiger Überprüfungen o.ä. zwingend geboten ist.

3.7.2
Automatisierte Verarbeitung

Zweiter Schwerpunkt ist die automatisierte Verarbeitung der Volkszählungsdaten im Hessischen Statistischen Landesamt und in dessen Auftrag bei der Hessischen Zentrale für Datenverarbeitung (HZD). Diese Verarbeitungsphase beginnt mit dem automatisierten Lesen der Erhebungsbogen und reicht über die Aufbereitung und Auswertung bis zur Übermittlung der Volkszählungsdaten an die im VZG vorgesehenen Empfänger. Eine Reihe von Überprüfungen habe ich in diesem Bereich bereits vorgenommen. So hat u.a. die HZD spezielle Datensicherungsvorkehrungen für die Beleglesung getroffen. Prüfen werde ich in diesem Durchführungsabschnitt vor allem, ob die Absätze 3 bis 5 des § 15 VZG auch peinlich genau eingehalten werden. Das Gesetz verlangt u.a., daß die die Reidentifizierung erleichternden laufenden Nummern und die Ordnungsnummern durch „Zufallsnummern", die keinen Rückgriff auf die Personalien zulassen, ersetzt und dann gelöscht werden. Straße und Hausnummer sind zu löschen, sobald die Zuordnung des Datensatzes zur sogenannten „Blockseite" erfolgt ist. Ein korrektes Zuordnungsprogramm für die kleinräumige Gliederung (Blockseite) ist hier entscheidend für eine verfassungsgemäße Abwick-

lung der Volkszählung. Bei Identität von Wohn- und Arbeitsstättenanschrift darf letztere nicht automatisiert gespeichert werden (vgl. oben Ziff. 3.2.2.2).

3.7.3
Kommunen

Für die Gemeinden gilt es, die organisatorischen Voraussetzungen zu schaffen, um Einzelangaben aus der Volkszählung vom Statistischen Landesamt zu erhalten. Ich werde überprüfen, ob dabei das Abschottungsgebot des § 14 VZG eingehalten wird und die Vorgaben des neuen Landesstatistikgesetzes (vgl. oben Ziff. 3.2.2.4) beachtet werden. Erste Überlegungen haben einzelne Statistikämter bereits angestellt; ich habe meine Mithilfe angeboten, um die Wahrung des Statistikgeheimnisses schon im Vorfeld organisatorischer Entscheidungen abzusichern.

Auf der kommunalen Ebene stellt sich ein weiteres Problem, nämlich der Versuchung zu widerstehen, rechtswidrigerweise doch - und wenn auch nur in vermeintlich gerechtfertigten Einzelfällen - Erkenntnisse aus der Arbeit in den Erhebungsstellen für Korrekturen im Melderegister oder Rückfragen der Meldeämter zu verwenden. Das befürchten vor allem Bürger in den Gemeinden, in denen das Erhebungsstellenpersonal aus den Meldeämtern stammt, was ich aus eben diesem Grund auch immer wieder kritisiert habe (vgl. Ziff. 3.2.2.5.1). Hinweisen auf eine zweckwidrige Nutzung von Volkszählungsdaten werde ich in jedem Fall nachgehen. Der „Melderegisterabgleich" ist ein strafbarer Bruch des Statistikgeheimnisses. Wie bisher werde ich auch regelmäßig die von den Meldeämtern bei den Kommunalen Gebietsrechenzentren in Auftrag gegebenen Änderungs- und Auswertungsläufe überprüfen.

3.7.4
Bußgeldverfahren

Ein Stichwort schließlich hat in der Volkszählungsdiskussion eine besondere Rolle gespielt: die „Verweigererdatei". Darunter ist vieles Falsche verstanden worden. Fest steht, daß alle Bußgeldverfahren nach § 23 Bundesstatistikgesetz zentral das Regierungspräsidium in Kassel durchführen wird, und zwar in dem landeseinheitlichen - etwa auch für Verkehrsverstöße eingesetzten - automatisierten Verfahren HESOWI. Insofern sind die Personalien aller Betroffenen, gegen die ein Ordnungswidrigkeitsverfahren wegen Nichtausfüllung der Erhebungsbögen eingeleitet wurde (zum Stand 17. Dezember 1987 lagen ca. 6.500 Anzeigen vor) an einer Stelle gespeichert.

Dies bedeutet jedoch keineswegs, daß alle diese Personen als „Verweigerer" einzustufen sind. Eine solche Charakterisierung kann erst dann in Betracht kommen, wenn eine Ordnungswidrigkeit wegen vorsätzlicher Nichtausfüllung rechtskräftig festgestellt ist.

Jedenfalls unterliegen die Personalien der von den Erhebungsstellen nach Kassel gemeldeten auskunftspflichtigen Einwohner nicht mehr dem Statistikgeheimnis; es handelt sich um „normale" Verwaltungsdaten, die nach dem Hessischen Datenschutzgesetz zu behandeln sind. Das Bundesverfassungsgericht hat in seinem jüngsten Kammerbeschluß klargestellt, daß die Mitteilung der für die Ahndung von Ordnungswidrigkeiten nach dem Volkszählungsgesetz unerläßlichen Angaben an die Bußgeldbehörden zulässig ist, diese dort aber strikt zweckgebunden zu verwenden sind. „Ausgeschlossen sein muß insbesondere eine weitergehende Verwendung der anläßlich der Erhebung anfallenden Informationen über das Auskunftsverhalten einer Person" (1. Kammer des Ersten Senats des BVerfG, Beschluß vom 18. Dezember 1987, 1 BvR 962/87, Ziff. II 4).

Über den Stand der Vorbereitung der automatisierten Abwicklung der Bußgeldverfahren habe ich mich vom Regierungspräsidium in Kassel laufend unterrichten lassen. 1988 werde ich die Einzelheiten der Durchführung, insbesondere die Beachtung der Zweckbindung, überprüfen.

4. Landesautomation

4.1
Allgemeine Entwicklung

Die derzeitige Entwicklung der Informationsverarbeitung in der Bundesrepublik weist eine Reihe charakteristischer Züge auf. Hier sind zum einen die Integrationsbestrebungen im Bereich der öffentlichen Netze zu nennen. Dabei soll die Fernmeldeinfrastruktur so weiterentwickelt werden, daß aus dem seit Jahren realisierten Integrierten Text- und Datennetz (IDN) und dem digitalisierten Fernsprechnetz ein universelles, diensteintegriertes, digitales Fernmeldenetz entsteht, das sog. ISDN (Integrated Services Digital Network). Bisher ist in der Regel für jeden Dienst (z.B. Fernsprechen, leitungsvermittelte und paketvermittelte Datenkommunikation, Fernkopieren (Telefax), Fernschreiben (Telex) und Bürofernschreiben (Teletex)) ein eigener Teilnehmeranschluß mit einer individuellen Rufnummer (und entsprechender Gebühr) erforderlich. Eine wesentliche Neuerung des ISDN besteht darin, daß bis zu acht Endgeräte mit einer einheitlichen Rufnummer von einem sog. Basisanschluß versorgt werden können, wobei der gleichzeitige Betrieb von zwei Geräten sowie Dienstewechsel möglich sind. Die international genormte Teilnehmerschnittstelle bietet erstmalig das Konzept der „universellen Telekommunikationssteckdose", d.h., dem Benutzer/Anwender stehen im ISDN erstmalig einheitliche Steckdosen für die verschiedenen Telekommunikationsgeräte zur Verfügung.

Im Bereich der DV-Anwender läßt sich weiterhin eine deutliche Zunahme bei der Beschaffung von Arbeitsplatzcomputern, Schreibsystemen und Datenstationen feststellen. Auslöser ist nur noch in wenigen Fällen die Neuentwicklung großer zentraler DV-Verfahren. Häufiger findet man noch die Umstellung älterer zentraler Verfahren auf „Dialog-Verarbeitung" in dem Sinne, daß der Sachbearbeiter Datenänderungen und -abfragen vor Ort über seine Datenstation vornimmt, wodurch der Datenbestand und damit auch die Abfrageergebnisse wesentlich aktueller werden. Der eigentliche Auslöser für die Mehrzahl solcher Beschaffungen ist sicherlich einerseits die unverminderte Tendenz zur Dezentralisierung bzw. zur Entwicklung dezentraler DV-Verfahren bis hin zur „individuellen" DV - teils neben und teils an Stelle der bisherigen Verfahren - andererseits die steigenden Ansprüche an die Textverarbeitung im Rahmen der Büroautomation. Es gehört schon zu den Gemeinplätzen, daß die Bereiche Daten- und Textverarbeitung längst nicht mehr sauber zu trennen sind, sondern regelrecht „zusammenwachsen", nicht nur weil mit denselben Geräten meistens beides möglich ist, sondern auch, weil es inzwischen teilweise sehr komfortable Übergänge zwischen Text- und Datenverarbeitung gibt.

Unter dem Gesichtspunkt des Datenschutzes ist besonders interessant, daß es längst nicht mehr nur um die Verarbeitung von Daten und Texten geht, sondern daß die Text- und Daten- Kommunikation in das Zentrum des allgemeinen Interesses gerückt ist. Hierbei geht es nicht mehr nur um die „Kommunikation" eines Menschen mit einer Maschine, genauer: mit einer Anwendung bzw. mit einem Programm auf einer Maschine, sondern auch um die Kommunikation von Menschen untereinander unter Zuhilfenahme von Maschinen, die dann miteinander verbunden sein müssen. Zwei Menschen können ja auch nur dann miteinander telefonieren, wenn zwischen ihren Telefonen eine Fernsprechverbindung besteht. Dabei ist es gleichgültig, ob diese Verbindung über eine Sprechanlage im eigenen Haus, über das öffentliche Telefonnetz oder sogar leitungsfrei über Funk hergestellt wird. Auch im Bereich Text- und Datenkommunikation werden die verschiedensten Netze aufgebaut, um solche Kommunikationsverbindungen zu ermöglichen. Neben dem klassischen DV-Netz mit einem (Zentral-)Rechner (Host), der im sogenannten Multi-User-Betrieb von mehreren Anwendern gleichzeitig benutzt werden kann, findet man digitale Nebenstellenanlagen, lokale (LAN, Local Area Network) und nichtlokale Netze (WAN, Wide Area Network) mit den verschiedensten Architekturen und technischen Realisierungen, die Geräte zur Informationsverarbeitung untereinander verbinden. Und es gibt Netzübergänge (Gateways, Bridges), die verschiedene Netze koppeln und damit netzübergreifende Kommunikation ermöglichen. Dabei ist es heute auch nicht mehr unabdingbar, daß die Geräte im Netz vom gleichen Hersteller stammen. Denn es gibt Normen und Standards, die - wenn sie nur an der „Schnittstelle", dem Übergang zwischen zwei Geräten oder zwei Netzen eingehalten werden - die reibungslose technische Kommunikation ermöglichen, völlig unabhängig davon, wie die einzelnen Netze intern strukturiert sind und arbeiten. Damit, wenn so eine Kommunikationsverbindung technisch hergestellt ist, die beiden Partner sich auch von der „Sprache" her verstehen können - also nicht beispielsweise einer Thai und der andere Finnisch spricht - sind bzw. werden auch Normen und Standards für den Austausch von Nachrichten, von Dateien und von Dokumenten entwickelt. Damit ist dann auch die netzübergreifende inhaltliche Kommunikation möglich. Von offenen Systemen bzw. Netzen spricht man, wenn die Kommunikation dem Schichtenmodell für offene Systeme, OSI (Open Systems Interconnection) des internationalen Normungsgremiums ISO (International Standards Organization) entspricht. Das bedeutet, daß die Systeme über eine Schichtung der Software im Sinne von OSI verfügen und daß deren Kommunikationsprotokolle zu den von OSI geregelten Diensten gehören. Über diese Offenheit verfügen heute nur wenige realisierte Systeme. Für die transportorientierten unteren Schichten, die eine reibungslose technische Kommunikation ermöglichen, hat sich dieses Referenzmodell mit den entsprechenden Protokollen dagegen schon sehr weit durchgesetzt.

Für die Zukunft ist neben der weiteren Verbreitung offener Netze auch ein größerer Komfort für den Anwender zu erwarten, beispielsweise durch die Integration von Funktionen, die bisher auf verschiedene Geräte verteilt sind, in ein Gerät, den sog. multifunktionalen Arbeitsplatz.

Die beschriebene allgemeine Entwicklung macht selbstverständlich nicht vor den Türen der öffentlichen Verwaltung halt. Gerade im Bereich der Landesautomation in Hessen gibt es eine ganze Reihe verschiedener Ansätze, die teilweise weit über den Rahmen der bisherigen klassischen DV in den Großrechenzentren (z.B. der Hessischen Zentrale für Datenverarbeitung (HZD) und der Kommunalen Gebietsrechenzentren (KGRZ)) hinausgehen.

4.2
DV-Verbund

Auf allen Großrechnern des Hessischen DV-Verbundes wird zur Zeit das Betriebssystem MVS (1) eingesetzt. Bei der Entwicklung dieses Betriebssystems wurden keine Datenschutzkomponenten, wie z.B. unter dem Betriebssystem UNIX (2), in die Systemphilosophie integriert. Es wurden lediglich Schnittstellen geschaffen (Open- Exit), über die eine Benutzer- und Zugriffskontrolle mit Hilfe spezieller Schutzsoftware realisiert werden kann.

Diese von den Rechenzentren verwendete Schutzsoftware war nicht für das gesamte Betriebssystem einheitlich, sondern es wurden bereits auf der Ebene der Sub-Systeme (3) (z.B. TSO, CICS, JES, COMPLETE) verschiedene Benutzer- und Zugriffskontrollsysteme unterschiedlicher Software-Hersteller mit jeweils eigener Verwaltung (z.B. Benutzer-, Paßwortdatei) eingesetzt.

Unter MVS kann damit auf alles zugegriffen werden, was nicht besonders geschützt ist; es ist also alles erlaubt, was nicht explizit verboten ist. Die zugrundeliegende Philosophie nennt man „Erlaubnis mit Verbotsvorbehalt".

Zusätzlich wurden auf der Ebene der Anwendungssysteme, wie z.B. im Einwohner- und im Finanzwesen, weitere anwendungsbezogene Mechanismen, wie z.B. Benutzerprofile (4), implementiert, um sicherzustellen, daß jeder

Benutzer nur auf die Daten zugreifen kann, die er zur Erfüllung seiner Aufgaben benötigt. Abgesehen vom Verwaltungsaufwand hat dies mit steigender Anzahl der automatisierten Verfahren auch auf der Seite des Anwenders zu Problemen geführt. Dieser mußte sich ggf. mehrere Benutzerkennungen (USER-ID's) und Paßwörter merken.

Diese teilweise aufwendigen Komponenten gewährleisteten aber insgesamt immer noch keinen umfassenden Datenschutz.

Vor diesem Hintergrund hat der Hessische DV-Verbund begonnen, über neue Konzepte und den Einsatz neuer Produkte nachzudenken. Diese Überlegungen betrafen sowohl die Ebene des Betriebssystems - hier wird zur Zeit die Schutzsoftware ACF2 (Access Control Facility) neu eingeführt - als auch die Ebene der Anwendungssysteme, für die das Verfahren „Vorstellungsdatei" entwickelt wurde.

Ich habe mich mit den Entwicklungen auf beiden Ebenen sehr gründlich beschäftigt und hierzu auch ausführliche Gespräche mit der HZD und dem KGRZ Kassel geführt.

4.2.1
Die Datenschutzsoftware ACF2

Bisher wurde im DV-Verbund die Datenschutzsoftware SECURE eingesetzt. SECURE ist ein System zum gezielten Dateienschutz (Erlaubnis mit Verbotsvorbehalt). Es konnte lediglich die Anforderungen an ein Dateizugriffsschutzsystem imTeilnehmerbetrieb (5) unter TSO (Time Sharing Option) und mit einigen Einschränkungen auch im Stapel-Betrieb (Batch) abdecken. Eine umfassende Benutzer- und Zugriffskontrolle in dem Sinne, daß z.B. festgelegt werden kann, welcher Benutzer von welchem Terminal aus auf welche Programme, Funktionen und Dateien zugreifen kann, konnte mit SECURE nicht realisiert werden.

Um hier Lücken zu schließen und Verbesserungen zu erreichen, hat der DV-Verbund seit Anfang der achtziger Jahre andere Produkte im Hinblick auf ihr jeweiliges Konzept und ihren Leistungsumfang untersucht und miteinander verglichen.

Am Ende dieser Überlegungen stand die Entscheidung für die Schutzsoftware ACF2 (Access Control Facility), deren Einführung zur Zeit stattfindet.

4.2.1.1
Konzept

ACF2 unterstützt konsequent die Philosophie des „Verbots mit Erlaubnisvorbehalt". Das heißt, ohne daß eine besondere Aktivität des Rechenzentrums oder des Eigentümers erforderlich ist, sind zunächst alle Dateien so geschützt, daß nur der Eigentümer - also derjenige, der die Datei angelegt hat - auf sie zugreifen kann. Damit auch eine gemeinsame Nutzung von Datenbeständen und Programmen möglich ist, können sogenannte Zugriffsregeln definiert werden, die beschreiben, unter welchen Umständen andere auf die Datei zugreifen dürfen.

Beispiel:
Der Eigentümer einer Datei hat uneingeschränkten Zugriff auf alle unter seiner Benutzerkennung gespeicherten Dateien, alle Mitarbeiter der Dienststelle erhalten eine Leseberechtigung. Ergänzt werden können noch das Volume (Plattenname), auf dem sich die Datei befinden muß, der Programmname und die Programmbibliothek, mittels derer auf die Datei zugegriffen werden kann, sowie die Uhrzeit und die Tage, an denen der Zugriff gestattet ist.

Die Eingabe von Zugriffsregeln ist dem Systemverwalter und dem Eigentümer vorbehalten, kann aber auch auf den Systemverwalter beschränkt werden.

An diesem Beispiel wird bereits deutlich, daß für einen qualifizierten Einsatz von ACF2 die notwendigen Datenflüsse innerhalb des Rechenzentrums und bei den Anwendern (Kunden) sehr viel sorgfältiger analysiert und abgestimmt werden müssen, als dies unter SECURE nötig war. Jetzt wird nicht nur festgelegt, wer auf welche Daten schreibend oder lesend zugreifen darf; sondern es kann angegeben werden wann, mit welchem Programm und von welchem Gerät aus ein Dateizugriff durch einen bestimmten Benutzer oder eine Gruppe von Benutzern erfolgen darf.

Diese organisatorischen Vorarbeiten sind mit ein Grund dafür, daß sich die Einführung von ACF2 im DV-Verbund verzögert hat. Die damit verbundene größere Transparenz der Datenflüsse ist begrüßenswert.

4.2.1.2
Leistungsumfang

Die Definition von Berechtigungen ist benutzerbezogen und nach einem einheitlichen Schema aufgebaut. So kann für jeden Benutzer u.a. festgelegt werden,

- mit welchen Sub-Systemen er arbeiten,

- welche Eingabegeräte er benutzen,

- ob er Bänder montieren lassen,
- ob er nur zu bestimmten Zeiten oder an bestimmten Tagen das System nutzen,
- ob er Operator-Kommandos benutzen,
- ob er neue Benutzer zulassen darf.

Diese Benutzerprofile sind jeweils der Benutzerkennung zugeordnet. Sie können zentral im Rechenzentrum oder dezentral, z.B. auf Behörden- oder Abteilungsebene, verwaltet werden.

Jeder Benutzer meldet sich mit seiner Benutzerkennung und seinem Paßwort an (LOGON).

Das Paßwort wird bei der Eingabe und beim Wechsel nicht angezeigt. Es wird nur verschlüsselt (Einweg-Verschlüsselung) abgespeichert. Es kann eine Mindestlänge, eine Mindestgültigkeitsdauer und eine maximale Gültigkeitsdauer für Paßwörter festgelegt, bestimmte Paßwörter (z.B. Vornamen, „4711" etc.) können ausgeschlossen werden. Außerdem können Fehlversuche protokolliert und nach einer bestimmten Anzahl von Fehlversuchen kann die Benutzerkennung gesperrt werden.

Nach erfolgreichem LOGON kann das Datum des letzten Systemzugriffs mit Terminalnummer und Angabe, ob der Zugriff erfolgreich war, sowie das Ablaufdatum des Paßworts angezeigt werden.

Darüber hinaus bietet ACF2 eine ganze Reihe von Parametern, Optionen und Erweiterungen an, mit denen die Schutzmechanismen auf das Rechenzentrum zugeschnitten werden können.

Die wichtigsten Schutzmöglichkeiten sind:

- Job-Eingabe (TSO-SUBMIT, RJE-Station, Kartenleser, JES)
- Zugang zu den Sub-Systemen (z.B. TSO, CICS)
- Kontrolle der Terminal-Adressen
- Schutz von Platten und Bändern
- Schutz von Dateien durch Vergabe von Schutzebenen (Lesen, Schreiben, Zuordnen, Ausführen) und durch Kontrolle der Eröffnung von Dateien (SCRATCH, RENAME)
- Vergabe von Operator-Berechtigungen
- Zusammenarbeit mit Netzwerkkontrollprogrammen und TP- Monitoren.
  Im TSO kann der Befehlsumfang eingeschränkt werden (z.B. kein SUBMIT) und die Session nach Ablauf einer bestimmten Zeit, in der keine Eingabe erfolgt, beendet werden (LOGOFF). Im CICS können u.a. Dateien, Transaktionen und Programme geschützt werden.

Zu Kontrollzwecken ist eine Reihe von Protokollierungen und Auswertungen möglich. Diese betreffen u.a.

- illegale Systemzugriffe (mehrfache ungültige Paßworteingabe)
- Regelverletzungen bei versuchten Dateizugriffen
- Kontrolle der Systemzugriffe während der Wartungsarbeiten.

ACF2 bietet also eine Fülle von Schutzmöglichkeiten. Es unterstützt das Rechenzentrum aber auch bei der Einführung, indem es fünf Stufen anbietet, mit denen das System schrittweise wirksam werden kann. Diese Stufen lassen sich folgendermaßen beschreiben:

QUIET-Mode: Der Systemzugang wird anhand des Benutzerprofils geprüft (Benutzerkennung, Paßwort usw.). Dateizugriffe werden nicht kontrolliert.

LOG-Mode: Auch die Zugriffsregeln werden geprüft, Regelverletzungen werden zugelassen, aber festgehalten. Mit den anfallenden Protokollen kann die Festlegung der Zugriffsregeln unterstützt werden.

WARN-Mode: Wie LOG-Mode; der Benutzer wird gewarnt, daß in Zukunft dieser Zugriff scheitert, wenn die Zugriffsregel nicht modifiziert wird. Die Regelverletzung wird protokolliert, der Zugriff aber durchgeführt.

ABORT-Mode: Bei Regelverletzung wird der Zugriffsversuch abgebrochen und protokolliert. Dies ist die normale Betriebsweise für ACF2.

RULE-Mode: Ermöglicht die Kombination der übrigen vier Stufen. Für jede Datei kann festgelegt werden, ob sie im QUIET-, LOG-, WARN- oder ABORT-Mode geschützt werden soll. Damit kann z.B. der ABORT-Mode nach und nach auf den gesamten Datenbestand ausgedehnt werden.

4.2.1.3
Implementierung und Generierung

Der Einsatz von ACF2 allein ist noch keine Garantie für einen guten Datenschutz. Zunächst kommt es darauf an, daß das sehr variable System ACF2 durch Setzen der entsprechenden Parameter sinnvoll generiert wird; es macht z.B. wenig Sinn, ACF2 generell für den WARN-Mode zu generieren und nur besonders wichtige oder vertrauliche Dateien zu schützen. Unabdingbare Voraussetzung hierfür ist zunächst, daß der Systembetreuer über sehr detaillierte Kenntnisse nicht nur von ACF2, sondern auch der vorhandenen System- und Anwendungssoftware sowie der Organisation verfügt.

ACF2 ist jedoch nicht nur hinsichtlich der Schutzmöglichkeiten sehr flexibel, sondern kann auch in Teilbereichen (z.B. TSO- LOGON) an verschiedenen Stellen in das Betriebssystem und seine Sub-Systeme eingebunden werden. So ist es z.B. möglich, die Benutzerkontrolle durch ACF2 vor dem Aufbau der eigentlichen TSO- Session durchzuführen, ACF2 kann aber auch nach dem Aufbau der TSO-Session über einen sog. EXIT aufgerufen werden.

Unter dem Gesichtspunkt einer größtmöglichen Systemsicherheit halte ich es für geboten, die Benutzer- und Zugriffskontrollen zum frühestmöglichen Zeitpunkt durchzuführen. Auf das obige Beispiel bezogen bedeutet dies, daß die Benutzerkontrolle vor dem Aufbau der TSO-Session erfolgen sollte.

4.2.1.4
Dezentralisierung der Benutzerverwaltung

ACF2 bietet, wie bereits oben erwähnt, die Möglichkeit, die Verwaltung der Benutzerprofile zu dezentralisieren. Ziel einer Dezentralisierung ist es, durch die Verlagerung der Verwaltung auf die Behörden- oder Abteilungsebene ein qualifizierteres Benutzerprofil für den einzelnen Benutzer zu erhalten, da auf dieser Ebene die Anforderungen des einzelnen Benutzers besser bekannt sind als im entfernten Rechenzentrum und auch die mit der zentralen Verwaltung verbundenen Durchlaufzeiten entfallen.

Eine dezentralisierte Benutzerverwaltung ist aber nur unter bestimmten Voraussetzungen zulässig. Zuallererst darf sie die Verantwortung des Rechenzentrums nicht untergraben. Das Rechenzentrum muß beispielsweise die Abschottung der Anwender gegeneinander und die ordnungsgemäße Datenverarbeitung gewährleisten. Es muß also eine klare Trennlinie definiert und technisch realisiert werden zwischen der Verantwortung des Rechenzentrums für den Rechnerbetrieb und die Anwenderunterstützung einerseits und der Autonomie des dezentralen Systemverwalters und der Verantwortung des Anwenders für seine Daten andererseits.

Das heißt konkret, daß das Rechenzentrum nur dann dezentrale Systemverwalter zulassen darf, wenn sichergestellt ist, daß deren Berechtigung entsprechend eingeschränkt ist. Der Systemverwalter darf beispielsweise Zugriffsregeln definieren und erweitern für die Datenbestände seiner eigenen Dienststelle oder seines Amtes (im Sinne des funktionalen Stellenbegriffs); er darf Benutzerprofile neu definieren, ändern oder ansehen nur für Benutzer aus dem Bereich seiner eigenen Dienststelle und nur für die von der Dienststelle genutzten Anwendungen. Er darf aber keine Operator-Berechtigung und keine Berechtigung zur Zulassung von Benutzern vergeben.

Die Stärken einer dezentralen Benutzerverwaltung sind jedoch gleichzeitig ihre Schwächen. Eine undifferenzierte oder unqualifizierte dezentrale Verwaltung ist ein beträchtliches Sicherheitsrisiko. Deshalb bin ich der Auffassung, daß die Voraussetzung für die Übernahme der Funktion des dezentralen Systemverwalters eine entsprechende Schulung sein muß.

4.2.1.5
Grenzen von ACF2

4.2.1.5.1
Differenzierung der Dateizugriffe

Trotz der vielfältigen Möglichkeiten von ACF2 können mit dieser Software nicht alle Systemzugriffe kontrolliert werden. Um die Grenzen von ACF2 zu erkennen, muß man sich vor Augen halten, daß die Kontrolle durch ACF2 bereits während des Eröffnens einer Datei endet. Die eigentlichen Lese- und Schreibzugriffe auf die Datei werden von ACF2 nicht mehr erfaßt. Eine Differenzierung der Zugriffsberechtigung auf Datensatz-, Datenfeld- oder Feldinhaltsebene ist mit ACF2 nicht möglich. Dies ist von Bedeutung, wenn man die Dateiverwaltung von TP- Monitoren, unter denen die meisten Dialog-Anwendungen laufen, etwas näher betrachtet. Bei dem im DV-Verbund eingesetzten TP-Monitor CICS (Customer Information Control System der Fa. IBM, s.u. 4.2.2.1) werden bereits beim Starten des TP-Monitors alle Dateien für alle Anwendungen durch diesen eröffnet.

Sofern für jeden Anwender und jede Anwendung eine eigene Datei vorhanden wäre, könnte der Zugriff mit Hilfe der o.g. Zugriffsregeln gesteuert werden. Aus technischen Gründen werden aber statt dessen häufig, so z.B. bei den

Verfahren Einwohner-und Finanzwesen, die Daten vieler Städte und Gemeinden in derselben Datei bzw. Datenbank gehalten. Mit Hilfe eines Abfrageprogramms (z.B. Anzeigen von Kontoständen) könnte, sofern über ACF2 hinaus keine weiteren Vorkehrungen getroffen würden, die Gemeinde A auch auf die Daten der Gemeinde B zugreifen oder diese verändern.

Um dies zu verhindern, müssen bei einer solchen Datenbestandsorganisation entweder die Schutzmechanismen des Datenbanksystems oder des Anwendungsprogramms eingreifen und einen solchen Zugriff kontrollieren. Die für die neueste Version von ACF2 angekündigte Kontrollmöglichkeit auf Datensatzebene kann höchstwahrscheinlich den komplexen Benutzerprofilen der vorhandenen Großanwendungen nicht gerecht werden und kommt deshalb als Alternative zu den Sicherungssystemen auf der Ebene von Datenbanken und Anwendungsprogrammen nicht in Betracht.

4.2.1.5.2
Netze mit mehreren Hosts

Eine weitere Beschränkung von ACF2 liegt darin, daß nur ein Host geschützt werden kann. Eine Kontrolle komplexerer Netzwerke mit mehreren Hosts ist also nicht möglich. Dieser Umstand wird bei der Planung eines landesweiten Netzes berücksichtigt werdenmüssen, falls mehrere Hosts (z.B. die Rechner des DV-Verbundes und des Landeskriminalamtes) vernetzt werden sollen. Dann muß die Netzwerk-Ebene mittels zusätzlicher Software kontrolliert und geschützt werden (s.u. 4.4).

4.2.1.5.3
Druckdateien
Druckdateien können vom Host zum Anwender übertragen werden. Soweit diese Dateien vor Ort auf Papier ausgedruckt und dann gelöscht werden, ist dagegen nichts einzuwenden. Bei meinen Gesprächen mit der HZD wurde bestätigt, daß die Dateien - ob sie nun zusätzlich auf Papier ausgedruckt werden oder nicht - dann, wenn der Anwender über einen Bürocomputer verfügt, dort in maschinenlesbarer Form solange gespeichert bleiben, bis der Anwender sie löscht. Dies entspricht faktisch einem File-Transfer und wird aus datenschutzrechtlicher Sicht dann zum Problem, wenn die Kontrolle der Verarbeitung auf dem Zielrechner beim Anwender nicht ausreicht, um unzulässige Datenverarbeitung zu verhindern.

4.2.2
Das Verfahren Vorstellungsdatei

Wie bereits oben (s.o. 4.2) erwähnt, ist in den letzten Jahren auch auf der Ebene der Anwendungssysteme eine Vielfalt unterschiedlicher Benutzer- und Zugriffskontrollsysteme entstanden. Es liegt nahe, die Datenschutzkontrolle auf der Anwendungsebene für möglichst viele Anwendungssysteme zu vereinheitlichen oder sogar zu zentralisieren. Damit kann evtl. die Verwaltung der Benutzerprofile vereinfacht werden. Außerdem läßt sich im Falle der Zentralisierung der Komfort für den Benutzer dadurch erhöhen, daß er nur noch ein Paßwort für alle Anwendungen benötigt und ein schneller Wechsel zwischen den Anwendungen möglich wird.

Diese Anforderungen sollen durch das Verfahren Vorstellungsdatei abgedeckt werden. Der Name „Vorstellungsdatei" beruht auf dem Gedanken, daß sich der Benutzer unter Eingabe seines Paßwortes beim Anwendungssystem (z.B. Einwohnerwesen) „vorstellt". Das Verfahren Vorstellungsdatei wurde ursprünglich für das neue Verfahren Einwohnerwesen (EWO-NEU) von der Stadt München entwickelt und in diesem Zusammenhang dann 1983 vom KGRZ Kassel übernommen.

Die Benutzer- und Zugriffskontrolle kann bei mehreren anderen Verfahren, wie z.B. Finanzwesen und Friedhofswesen, ähnlich gelöst werden. Dies ist auf zwei Wegen möglich. Es wäre denkbar, in jedes dieser Anwendungsverfahren ein eigenes Verfahren Vorstellungsdatei zu integrieren. Die andere Möglichkeit ist die, dem Verfahren Vorstellungsdatei die verschiedenen Anwendungsverfahren unterzuordnen; dann läßt sich in der Vorstellungsdatei übergreifend für alle Anwendungsverfahren jedem Benutzer ein Paßwort zuordnen, an das seine jeweilige Berechtigung für die verschiedenen Anwendungen geknüpft ist. Dieser zweite Weg wurde vom KGRZ Kassel beschritten. Das Verfahren Vorstellungsdatei wurde aus dem Verfahren Einwohnerwesen herausgelöst und verfahrensübergreifend für verschiedene Anwendungsverfahren implementiert.

4.2.2.1
Begriffe

Eine Transaktion kann als eine Aufgabe beschrieben werden, die entweder ganz oder gar nicht ausgeführt wird.

Beispiel:

Bei einer Eheschließung muß die Meldebehörde die Meldedaten des Ehepaars ändern bzw. zusammenfassen. Nach der Eingabe der Änderungsdaten (z.B. neuer Wohnsitz, neuer Nachname eines Ehepartners) wird zunächst der Datensatz der Ehefrau und dann der des Ehemanns geändert. Im Normalfall ist damit diese Aufgabe erledigt, d.h. die Transaktion ist durchgeführt. Sollte das System aber anhand der bisher gespeicherten Daten feststellen, daß der Ehemann bereits verheiratet ist, wird die Transaktion abgebrochen. Die bis dahin vorgenommenen Änderungen

(auch im Datensatz der Ehefrau) müssen rückgängig gemacht, d.h. der alte Zustand muß wiederhergestellt werden.

Ein weiteres Beispiel für eine Transaktion ist: Buchung einer Reise mit Hinflug, Hotel und Rückflug. Zunächst muß das System prüfen, ob noch ein Platz für den Hinflug vorhanden ist. Dieser Platz muß dann vorsorglich reserviert werden, damit er nicht von einem anderen Reisebüro aus inzwischen vergeben wird. Sollte sich aber herausstellen, daß das gewünschte Hotel bereits belegt oder der Rückflug bereits ausgebucht ist, muß auch die Buchung für den Hinflug rückgängig gemacht werden.

Aus technischer Sicht ist eine Transaktion ein Programm, das ggf. auch Unterprogramme oder weitere Transaktionen aufrufen kann.

Der TP-Monitor CICS ist ein Spezialprogramm, das den Ablauf von Transaktionen steuert. Es koordiniert weiterhin die Zugriffe mehrerer Transaktionen auf die gleiche Datei (Record-Locking) und den Nachrichtenaustausch mit den Datenstationen sowie der übrigen Peripherie.

4.2.2.2
Leistungsumfang, Funktionsweise

Mit Hilfe der Vorstellungsdatei kann geprüft werden, ob ein Benutzer

- die von ihm aufgerufene Transaktion zur Veränderung oder Abfrage von Daten aufrufen und
- auf die von ihm geforderten Daten zugreifen darf.

Im Gegensatz zu ACF2 kann der Zugriff auf Daten über die Gemeindekennziffer auf der Datensatzebene beschränkt werden. Eine weitere Einschränkung unterhalb der Gemeindeebene (z.B. auf bestimmte Kontengruppen, Steuernummern oder Haushaltstitel) ist möglich.

Die Verwaltung der Benutzerprofile kann, ähnlich wie bei ACF2, auf der Basis der Gemeindekennziffer dezentralisiert werden.

Aus der Sicht des Anwendungsentwicklers kann das Verfahren Vorstellungsdatei als Werkzeug (Tool) bezeichnet werden. Wenn ein Rechenzentrum ein Anwendungsverfahren entwickeln will, das die Benutzer- und Zugriffskontrolle über die Vorstellungsdatei realisiert, erhält es vom KGRZ Kassel ein Paket von Programmen im sog. Quellcode (Assembler, COBOL), die noch an die besonderen Belange des Rechenzentrums und des zu entwickelnden Verfahrens angepaßt werden müssen. Zusätzlich müssen die Benutzerprofile für das neue Anwendungsverfahren definiert werden. Die Transaktion bzw. Unterprogramme des Anwendungsverfahrens müssen dann nur noch an den richtigen Stellen die fertigen Programme der Vorstellungsdatei zur Benutzer- und Zugriffskontrolle aufrufen.

Einschränkend muß an dieser Stelle allerdings gesagt werden, daß das Verfahren Vorstellungsdatei nur für Anwendungssysteme eingesetzt werden kann, die unter dem TP-Monitor CICS laufen. Eine Implementierung unter anderen TP-Monitoren wäre zwar theoretisch möglich, ist aber derzeit nicht geplant.

4.2.2.3
Probleme und Forderungen

4.2.2.3.1
Dateischutz

Die Dateien oder Datenbanken müssen nicht nur gegen unberechtigte Zugriffe der Anwender, sondern auch gegen unberechtigte Zugriffe innerhalb des Rechenzentrums geschützt werden. Soweit es sich nicht um Datenbanken handelt, kann hier ein ausreichender Schutz mit ACF2 realisiert werden. Bei Datenbanken, die selbst wiederum mehrere logische Dateien (Tabellen, Segmente) beinhalten können, muß auch ein entsprechender Schutz durch das Datenbankverwaltungssystem realisiert werden. Dies gilt ganz besonders für die Datenbank, die die Benutzerprofile und die unverschlüsselten Paßwörter (Berechtigungscodes) der Benutzer enthält.

4.2.2.3.2
Paßwörter

Da mit dem einmal eingegebenen Paßwort evtl. mehrere Verfahren nutzbar sind, sollte besonderer Wert darauf gelegt werden, daß das Paßwortverfahren dem „Stand der Technik entspricht". D.h. u.a., daß die Paßwörter regelmäßig mit automatisierter Unterstützung geändert werden müssen und daß sie nur verschlüsselt gespeichert werden.

Ferner sollte eine Zeitschranke (Time-Out) verwendet werden, um das Datenendgerät abzuschalten, wenn innerhalb einer bestimmten Zeitspanne keine Eingabe erfolgte. Darüber hinaus sollte die Überprüfung der Terminalnummer geklärt werden.

4.2.2.3.3
Dezentrale Benutzerverwaltung

Zur Dezentralisierung der Benutzerverwaltung gilt das unter 4.2.1.4 Gesagte entsprechend.

4.2.2.3.4
Systemverwalter und Datenschutzbeauftragter

Für die Pflege der Vorstellungsdatei einschließlich der Benutzerprofile muß in jedem Rechenzentrum ein Systemverwalter benannt werden. Weder der zentrale noch ein dezentraler Systemverwalter (im Verfahren Vorstellungsdatei „Oberberechtigter" genannt) darf betrieblicher Datenschutzbeauftragter sein. Denn beide können dadurch in einen Interessenskonflikt geraten, beispielsweise bei der Überprüfung der nach § 10 HDSG erforderlichen Maßnahmen.

4.2.2.3.5
Verfahrens- und Programmfreigabe

Vor der Freigabe von Anwendungsverfahren und -programmen muß besonders überprüft werden, ob die standardisierten Zugriffsmodule für das Verfahren Vorstellungsdatei korrekt konzipiert und realisiert und ob sie an allen erforderlichen Stellen richtig eingebunden wurden. Da Änderungen an den Zugriffsmodulen die Wirksamkeit des gesamten Verfahrens gefährden können, sollten sie so weit wie möglich unterbleiben und nur von einem besonders autorisierten Personenkreis durchgeführt werden.

4.2.2.3.6
Spezielle Transaktionen

Zum Anmelden beim Verfahren Vorstellungsdatei dient die Transaktion „MELD", die das Paßwort abfragt, zum Abmelden die Transaktion „MELD ENDE". Darüber hinaus stellt das KGRZ Kassel zwei weitere Transaktionen zur Verfügung: „MELD P" zur Abfrage, wer am aktuellen Bildschirm angemeldet ist, und „MELD T,TAC" zur Abfrage, ob ein bestimmter Transaktionscode (TAC) für den angemeldeten Benutzer zugelassen ist. Ich halte diese Transaktionen für problematisch. Denn wenn jemand den Bildschirm ohne Abschalten verläßt, kann jeder andere unbefugt personenbezogene Daten des Benutzers (Name, Geburtsdatum, genaue Anschaltzeit und Gemeindekennziffer) und dessen Berechtigung zur Nutzung von Transaktionen erfragen, ohne sich selbst am Rechner anzumelden. Da jeder Anwender über sein eigenes Benutzerprofil informiert sein und sich beim Verlassen des Arbeitsplatzes abmelden sollte, dürften diese Transaktionen auch vom Anwender selbst nicht benötigt werden. Ich empfehle deshalb, sie ersatzlos zu streichen.

4.2.2.3.7
Zusammenarbeit mit dem CICS-Schutzsystem

Auch der TP-Monitor CICS als Sub-System des Betriebssystems (s.o. 4.2) verfügt über ein eigenes System zur Überprüfung von Benutzungs- und Zugriffsberechtigungen. So können z.B. Transaktionen Klassen zugeordnet und geschützt werden, indem man für jeden Benutzer festlegt, welche Klassen er benutzen darf. Die Schwachstelle dieses Schutzsystems liegt, ähnlich wie bei ACF2, in der mangelhaften Abschottung der Anwender untereinander, wenn diese auf die gleiche Datei oder Datenbank zugreifen. Diese Schwachstelle kann durch den zusätzlichen Einsatz der Vorstellungsdatei beseitigt werden, da dort für jeden Benutzer die zulässigen Ordnungsbegriffe (z.B. Gemeinde, Kontonummer) gespeichert werden.

Gleichzeitig werden aber durch die Vorstellungsdatei neue potentielle Risiken erzeugt: im KGRZ Kassel und wahrscheinlich auch in anderen Rechenzentren können Transaktionen aufgerufen werden, ohne daß sich der Benutzer bei dem TP-Monitor angemeldet hat; denn der Benutzer muß sich erst dann bei CICS anmelden, wenn er Transaktionen benutzen will, die durch CICS selbst geschützt sind. Diese Vorgehensweise wird damit begründet, daß eine doppelte Kontrolle den Komfort für den Anwender beeinträchtigt und daß sich die nicht durch CICS geschützten Transaktionen z.B. mit Hilfe von Informationen aus der Vorstellungsdatei oder einem ähnlichen Verfahren selbst schützen.

Hier entsteht eine Sicherheitslücke, die nur durch eine besonders große Sorgfalt seitens der Anwendungsprogrammierung vermieden werden kann. Falls z.B. der Programmierer beim Programmieren der Transaktion vergißt, die Unterprogrammaufrufe für die Berechtigungsprüfung durch das Verfahren Vorstellungsdatei zu codieren, könnte diese Transaktion von jedem, der mit diesem CICS-Bereich (Region) arbeiten kann, aufgerufen werden. Das gleiche gilt, falls das Ergebnis der Berechtigungsprüfung falsch interpretiert wird, wenn z.B. die Transaktion nicht abgebrochen wird, obwohl der Benutzer nicht berechtigt ist.

Hier ein Beispiel: Die Transaktionen des „EWO-NEU" werden in Kassel nicht durch CICS geschützt. Die Durchführung einer Berechtigungsprüfung für jede Transaktion soll im KGRZ Kassel dadurch sichergestellt werden, daß derartige Programme ausschließlich mit einem Programmgenerator erstellt werden, der die entsprechenden Aufrufe bezüglich der Vorstellungsdatei automatisch einfügt.

Da auch von anderen Rechenzentren des DV-Verbundes Online- Verfahren (z.B. Finanzwesen) entwickelt werden, bei denen der Datenschutz durch den Einsatz der Vorstellungsdatei gewährleistet werden soll, muß auf die korrekte und vollständige Implementierung der Funktionsaufrufe bezüglich der Vorstellungsdatei besonderer Wert gelegt werden. In den Rechenzentren, in denen der o.g. Programmgenerator nicht eingesetzt wird, entsteht ein Sicherheitsrisiko bei der Anwendungsprogrammierung, das durch zusätzliche Maßnahmen auf der Sub-System- bzw. Betriebssystem-Ebene beschränkt werden sollte.

4.2.3
Fazit

Aus dem bisher zu ACF2 und zum Verfahren Vorstellungsdatei Gesagten ist deutlich geworden, daß sich der Bereich derDatenschutzsoftware im DV-Verbund im Umbruch befindet. Die Entwicklungen auf den verschiedenen Ebenen sind zeitlich parallel verlaufen: Das Verfahren Vorstellungsdatei wurde gleichzeitig mit der Auswahl und dem Beginn der Implementierung von ACF2 realisiert.

Es ist aber auch deutlich geworden, daß die jeweiligen Schutzsysteme keineswegs unabhängig voneinander sind (vgl. 4.2.2.3.7). Jedes System hat seine Stärken und Schwächen, manche Komponenten sind in mehreren Schutzsoftware-Systemen in ähnlicher Form enthalten.

Was im DV-Verbund fehlt, ist die Koordinierung des Einsatzes der Datenschutzkomponenten sämtlicher Software-Systeme im jeweiligen Rechenzentrum. Nur so ist aber eine Verbesserung des Rechnereinsatzes mit gleichzeitiger Verbesserung des Datenschutzes möglich. Es geht zum einen darum, gleichartige Prüfungen und Abfragen, die bisher an mehreren Stellen durchlaufen wurden, an der logisch und softwaretechnisch optimalen Stelle zu konzentrieren. Zum anderen sollen natürlich vorhandene Lücken geschlossen werden und keine neuen entstehen.

Dies ist nur möglich, wenn unter Berücksichtigung aller im Einsatz befindlichen Systeme und ihrer Datenschutzkomponenten sowie der Organisation des jeweiligen Rechenzentrums ein Konzept erstellt wird, das

- detailliert beschreibt, welche Datenschutzkontrolle an welcher Stelle stattfinden soll
- festlegt, wie die einzelnen Systeme generiert werden müssen
- gewährleistet, daß jeder Anwender in jedem Fall sämtliche erforderliche Kontrollen durchlaufen muß und Beschränkungen seiner Zugriffsberechtigungen nicht umgehen kann.

Ein solches Konzept kann selbstverständlich nicht von einer Person erstellt werden. Hier ist vielmehr die Zusammenarbeit der verschiedenen Spezialisten erforderlich. Da viele Anwendungsverfahren von einem Rechenzentrum federführend betreut werden, ist eine gewisse Kooperation zwischen den Rechenzentren des DV-Verbundes sinnvoll. Dies ändert aber nichts daran, daß jedes Rechenzentrum für die zügige Erstellung und Umsetzung eines solchen Gesamtkonzepts für seinen Bereich verantwortlich ist.

Meine Forderungen und Anregungen zu ACF2 sowie zum Verfahren Vorstellungsdatei stellen lediglich eine Stellungnahme zu den einzelnen Systemen dar. Sie können wegen der dargestellten, übergreifenden Zusammenhänge ohne Vorlage eines Gesamtkonzepts nicht vollständig sein. Ich werde die weitere Entwicklung in den Rechenzentren aufmerksam verfolgen und behalte mir eine abschließende Wertung der Gesamtsysteme vor.

4.3
Büroautomation

4.3.1
Inhalte und Ziele

„Büroautomation", d.h. die Automation von Büroarbeit mit Hilfe der Informations- und Kommunikationstechnik, beschränkt sich keineswegs nur auf den Schreibdienst, sondern betrifft alle Verwaltungstätigkeiten, unabhängig von ihrer hierarchischen Eingliederung. So ist der Austausch einer mechanischen Schreibmaschine gegen eine moderne Speicherschreibmaschine sicherlich eine Maßnahme der Büroautomation. Die innovativen Elemente der Büroautomation sind allerdings auf einer anderen Ebene zu finden, nämlich bei der Unterstützung der Sachbearbeitung durch Computerleistung, insbesondere in den Bereichen Datenverarbeitung, Textverarbeitung undTelekommunikation.

Der Begriff Telekommunikation umfaßt u.a. Nebenstellenanlagen, Postdienste, Sondernetze (z.B. der Polizei) und lokale Netze.

Datenverarbeitung im Kontext der Büroautomation beschränkt sich nicht auf die traditionelle Massendatenverarbeitung, sondern umfaßt die Bereiche Datenbankanwendungen, Tabellenkalkulation, Grafik - als Übergang zur Bildverarbeitung -, Zugriff auf Großrechner und die Datenkommunikation.

Ziel der Büroautomation aus organisatorischer Sicht ist in der Regel nicht eine weitere Differenzierung der Arbeitsteilung, sondern im Gegenteil die Integration von Arbeitsschritten, so daß die ganzheitliche Bearbeitung einer

Aufgabe durch eine Person möglich wird. Eine andere Vorstellung, nämlich das lange auch von den Herstellern propagierte papierlose bzw. papierarme Büro, ist mittlerweile entweder ganz aufgegeben oder inhaltlich eingeschränkt worden. Denn im Zuge der Entwicklung solcher Systeme hat sich gezeigt, daß die Probleme des Ablaufs und der Dokumentation des Geschäftsganges mittelfristig technisch nicht gelöst werden können. Beispielhaft sei hier nur die Rekonstruktion und Authentizität der Inhalte und der Urheber von Änderungen, Anmerkungen und Sichtvermerken an Dokumenten genannt. Nur in wenigen Dienstleistungssparten, wie z.B. bei Versicherungen, konnten elektronische Aktenverwaltungssysteme erfolgreich eingeführt werden.

In den Verwaltungen, vor allem im nicht-öffentlichen Bereich, verändert sich auch die hausinterne Kommunikation. So beginnen Elektronische Mitteilungssysteme (MHS, Message Handling System) einen Teil der Hauspost und der (fern-)mündlichen Kommunikation zu ersetzen. Derzeit werden Normen (z.B. die CCITT-Protokolle X.400 ff.) und Anwendungssysteme (z.B. DISOSS, Distributed Office Support System) für den Nachrichten- und Dokumentenaustausch- auch zwischen Systemen unterschiedlicher Hersteller - entwickelt. Der Einsatz solcher Systeme steckt aber noch in den Anfängen.

Die in Frage kommende Hardware reicht, abhängig von der Anzahl der Teilnehmer, dem Schwerpunkt der Anwendungen (Grafik erfordert z.B. eine hohe Rechnerleistung) und dem Kommunikationsbedarf, von Textsystemen über Arbeitsplatzrechner bis hin zum Host. Auch die Konfigurationsmöglichkeiten von Büroautomationssystemen sind fast unbeschränkt. Sie reichen von Einzelplatz- über Mehrplatzsysteme bis hin zu lokalen Netzen.

4.3.2
Text- und Datenverarbeitung

4.3.2.1
Entwicklung in der Text- und Datenverarbeitung

Visuelle Information wird in Form von Schrift oder Bild dargestellt. Unter dem Aspekt der technologischen Entwicklung ist es zweckmäßig, die schriftliche Information weiter in Text und Daten zu unterscheiden. Dabei bezeichnet der Begriff Text eine sich selbst erklärende, schriftliche Information. Von Daten spricht man, wenn die Struktur und die Bedeutung schriftlicher Information in einer Datenbeschreibung explizit beschrieben wird.

Die zu den Informationsformen Bild und Schrift gehörenden Informationstechnologien sind Bildverarbeitung (z.B. Grafik), Daten- und Textverarbeitung. Diese Technologien waren früher personell, organisatorisch und maschinell strikt getrennt. So fand z.B. Textverarbeitung im Schreibdienst an der Schreibmaschine statt, Datenverarbeitung durch Buchhalter oder im Rechenbüro mit einem mechanischen bzw. elektronischen Rechner und Bildverarbeitung durch den technischen Zeichner am Reißbrett. Mit dem Fortschritt der Büroautomation vollzog sich ein grundlegender Wandel. Die ganzheitliche Sachbearbeitung führte nicht nur zur Aufhebung der strikten Arbeitsteilung. Zur Entlastung der Sachbearbeiter wurden formalisierbare Tätigkeiten automatisiert und damit den kreativen, nicht formalisierbaren Tätigkeiten größere Aufmerksamkeit entgegengebracht. Die Integration der Tätigkeiten hat auch die maschinelle Unterstützung verändert: die Arbeits- und Funktionsaufteilung blieb auch für die automatisierten Bereiche und die zugehörigen Maschinen nicht erhalten. Deshalb kann z.B. das Text- von dem Datenverarbeitungssystem nicht mehr strikt getrennt werden.

Dies wird an einem einfachen Beispiel deutlich:

In einen Standardtext für eine Lehrgangseinladung sollen für jeden Lehrgangsteilnehmer dessen individuelle Daten eingesetzt werden, die aus einer Teilnehmerdatei beschafft werden müssen. Das Selektieren und Sortieren der benötigten Daten ist eine Datenverarbeitungsfunktion, das Erstellen des Standardtextes mit den freien Stellen für die Teilnehmerdaten, das Formatieren und Ausdrucken der Briefe sind Textverarbeitungsfunktionen. Die variablen Daten müssen so aufbereitet werden, daß sie in den Standardtext eingesetzt werden können, d.h., die Funktionen der Daten- und der Textverarbeitung müssen aufeinander abgestimmt werden.

Diese Integration läßt sich erreichen durch

- Erweiterung des Funktionsumfangs des Textautomaten dahingehend, daß er auch den Datenverarbeitungsteil übernehmen kann,

- Verlagerung der Textverarbeitungsfunktionen auf die Datenverarbeitungsanlage, indem man dort Textverarbeitungssoftware einsetzt,

- Kopplung der Datenverarbeitungsanlage, auf der die Teilnehmerdaten gespeichert sind, mit dem Textsystem. Das Textsysstem, das als Terminal an die Datenverarbeitungsanlage angeschlossen ist, veranlaßt das Selektieren und Sortieren auf dem Rechner und die Übertragung der Ergebnisdaten an das Textsystem und setzt sie dort in die Standardbriefe ein.

Diese drei Verfahrensweisen sind auch in der Praxis zu finden. Sie machen deutlich, daß viele Geräte bestenfalls noch einen Schwerpunkt auf der Text- oder der Datenverarbeitung haben, daß die vorhandenen (Teil-)Funktionen sich aber vermischen.

Dieser technologische Wandel hat selbstverständlich Auswirkungen auf den Datenschutz. Sie wurden auch bei der Novellierung des Hessischen Datenschutzgesetzes, die am 1. Januar 1987 in Kraft getreten ist, berücksichtigt.

Da immer wieder Mißverständnisse und Unklarheiten in der öffentlichen Verwaltung deutlich werden, insbesondere bei der Einordnung der Textverarbeitung in die Regelungen des Gesetzes, soll hierauf noch einmal eingegangen werden.

4.3.2.2
Texte und Bilder im HDSG

Personenbezogene Daten im Sinne des HDSG sind „Einzelangaben über persönliche und sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person" (§ 2 Abs. 1). Solche Einzelangaben können visuelle oder akustische Informationen sein. Sie umfassen also Informationen in Form von Sprache, Bildern (z.B. Fotos, Grafiken) sowie Texten und Daten im Sinne der zu Beginn des letzten Abschnitts genannten Definitionen.

Neben der Einbeziehung von Akten wurde der Begriff „Datei" neu definiert. Dabei wurde erstmals unterschieden in automatisierte und nicht automatisierte Dateien:

„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)" (§ 2 Abs. 5 HDSG).

Dieser neue Dateibegriff bezieht Texte, Daten und Bilder mit Einzelangaben über persönliche und sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person dann generell mit ein, wenn sie mit automatisierten Verfahren ausgewertet werden können. Die einschränkenden Forderungen des gleichartigen Aufbaus und der Möglichkeit, sie nach bestimmten Merkmalen ordnen und auswerten zu können, sind in diesem Fall aufgehoben.

Damit fallen z.B. Schreiben und Adreßverteiler, die auf Textautomaten oder mit Hilfe von Textverarbeitungsprogrammen erstellt wurden, unter den Dateibegriff nach Nr. 1. Für die eingesetzten Geräte sind dann die Maßnahmen nach § 10 Abs. 3 HDSG zu treffen und sie sind in das Geräteverzeichnis nach § 6 Abs. 3 HDSG aufzunehmen.

4.3.3
Büroautomation in der Hessischen Landesverwaltung

Der LAA hat am 17. April 1986 die Einrichtung eines Unterausschusses „Büroautomation" beschlossen.

Dieser Ausschuß „hat den Auftrag:

a) künftige Entwicklungen der Informationstechnik im Bereich der Bürotätigkeiten in der Landesverwaltung (z.B. Textverarbeitung, Datenverarbeitung, Zugriff auf Informationssysteme, Bürokommunikation) zu untersuchen und evtl. personelle, sachliche und finanzielle Konsequenzen aufzuzeigen,

b) die Erfahrungen mit laufenden Pilotversuchen (z.B. beim Innenministerium, beim Ministerium für Wirtschaft und Technik, beim Finanzministerium, beim Ministerium für Umwelt und Reaktorsicherheit, beim Kultusministerium) auszuwerten und

c) unter Berücksichtigung der voraussichtlichen künftigen Entwicklung einen Vorschlag für technische und organisatorische Lösungen auszuarbeiten."

Bei den Vorführungen und Diskussionen im Rahmen der Pilotversuche ist mir folgendes aufgefallen:

- Der Schwerpunkt des Einsatzes liegt bei der Textverarbeitung. Die Nutzung von Tabellenverarbeitung, Datenbanken und Grafik ist von der dv-technischen Vorbildung und Erfahrung der Anwender abhängig; eine verstärkte Nutzung dieser Funktionen ist für die Zukunft wahrscheinlich.

- Keines der beteiligten Ressorts hat die Absicht, ein papierloses Büro einzurichten.

- Die eingesetzte Hardware und die jeweilige Konfiguration ist alles andere als einheitlich. Die verschiedenen Hersteller und Konzeptionen spiegeln das breite Spektrum der Realisierung von Büroautomation wider. Bei Mehrplatzsystemen ist der Host in der Regel der sog. Mittleren Datentechnik zuzuordnen.

- Angestrebt werden multifunktionale Arbeitsplätze.

- Alle eingesetzten Betriebssysteme (MS-DOS wird nicht als Basis-Betriebssystem verwendet) verfügen über Möglichkeiten zur Benutzer- und Zugriffskontrolle. Sowohl aus Unwissenheit, z.B. weil die Schutzmöglichkeiten auf der Betriebssystemebene im Schulungsplan nicht ausreichend berücksichtigt wurden, als auch aus mangelndem Problembewußtsein heraus wurden die Schutzmechanismen teilweise nicht bzw. nicht wirksam eingesetzt.

- Möglichkeiten zur Aufzeichnung von System- und Benutzeraktivitäten sind entweder nicht vorhanden oder für die Zwecke des § 10 Abs. 3 HDSG nicht zu gebrauchen.

- Alle Systeme verfügen über Kommunikationsanschlüsse (z.B. Teletex, X.25). Alle Hersteller bieten die Möglichkeit, die Bürocomputer im Wege der Terminal-Emulation an Hostrechner anzuschließen und Dateien auszutauschen (File-Transfer).

Die Pilotversuche und zwei im Bereich der Landesverwaltung durchgeführte Prüfungen veranlassen mich zu einigen grundsätzlichen Anmerkungen zum Datenschutz beim Einsatz von Bürosystemen:

- Die Einordnung der automatisierten Textverarbeitung (s.o. 4.3.2.2) wird noch längst nicht überall angemessen berücksichtigt. Auch wenn die Geräte ausschließlich zur Textverarbeitung verwendet werden, sind sie in das Geräteverzeichnis aufzunehmen und die technischen und organisatorischen Maßnahmen gem. § 10 Abs. 3 HDSG zu treffen. Die Angemessenheit von Maßnahmen muß unter Berücksichtigung der jeweils realisierten Verfahren und Projekte beurteilt werden; bei Textverarbeitung also insbesondere am Aufgabenbereich und damit auch am Inhalt des Schriftverkehrs der jeweiligen Stelle. Mit jedem neu realisierten Verfahren können somit zusätzliche Datenschutzmaßnahmen erforderlich werden.

- Dateien mit personenbezogenen Daten, auch in der Form von reinen Adreßverteilern, sind zum Dateienregister beim Hessischen Datenschutzbeauftragten zu melden.

- Auch wenn „Pilotprojekte" oder „Tests" mit echten personenbezogenen Daten durchgeführt werden, müssen vor deren Beginn die Dateien zum Register gemeldet und die Maßnahmen nach § 10 Abs. 3 HDSG getroffen werden; die sonstigen Vorschriften des HDSG sind zu beachten. Dies gilt selbstverständlich auch dann, wenn die Projekte von beschränkter oder unbestimmter Dauer sind.

- Für den Umgang mit den Geräten, die Aufbewahrung von Disketten und Ausdrucken sowie den Datenträgeraustausch etc. müssen Dienstanweisungen erlassen werden (vgl. hierzu auch meinen 15. Tätigkeitsbericht, Ziff. 9).

- Wenn Disketten, Kassetten etc. als Datenträger verwendet werden, ist eine entsprechende Datenträgerverwaltung, u.a. mit Kennzeichnung und Registratur, aufzubauen. Die Datenträger sind den jeweiligen Arbeitsbereichen bzw. dem Datenträgeraustausch jeweils fest zuzuordnen.

- Die räumliche Sicherung für die Aufbewahrung von DV-Geräten, insbesondere solchen mit Festplatte, und von Datenträgern muß ausreichend sein.

- Wenn Datenträger (auch Geräte mit Festplatte oder sonstigen Speichern) an andere Benutzer innerhalb oder außerhalb der Dienststelle weitergegeben werden, ist dafür zu sorgen, daß die personenbezogenen Daten vorher physikalisch gelöscht werden.

- Carbonbänder werden häufig in Druckern und Schreibmaschinen verwendet und enthalten den Klartext der Ausdrucke in lesbarer Form. Deshalb muß ihre datenschutzgerechte Entsorgung geregelt werden.

- Die Schulung bzw. das Wissen der Anwender über die technischen Möglichkeiten, die die Geräte für den Datenschutz bieten, ist häufig unzureichend. Dies führt dazu, daß aus Unwissenheit die entsprechenden Komponenten nicht oder nicht ausreichend genutzt werden. Hier sollten unbedingt die entsprechenden Schulungen der Hersteller genutzt und die dafür notwendigen Mittel schon vor der Beschaffung eingeplant werden. Wenn die HZD als Vertragspartner Bürosysteme in der Landesverwaltung installiert, sollte sie die entsprechenden Grundfunktionen implementieren und erklären. Auch die Lehrpläne für die Schulungen in Textverarbeitung, die gemeinsam vom Landespersonalamt und der HZD veranstaltet und von einem externen Berater durchgeführt werden, sollten geändert werden. Denn es ist wichtig, daß alle Teilnehmer die Schutzmöglichkeiten der jeweiligen Systeme kennenlernen und den praktischen Umgang mit diesen Mechanismen intensiv und aktiv üben. Eine Beschränkung einer solchen Schulung auf die Systemverwalter halte ich nicht für ausreichend.

- Im übrigen ist es erforderlich, daß das Problembewußtsein für den Datenschutz bei jedem einzelnen Anwender weiterentwickelt wird. Diese Thematik sollte - außerhalb der Schulung - beispielsweise der behördliche Datenschutzbeauftragte im Rahmen seiner Aufgaben nach § 5 Abs. 2 HDSG, insbesondere seiner Mitwirkung bei der Überwachung der nach § 10 HDSG erforderlichen Maßnahmen, aufgreifen.

4.4
Landesweites Kommunikationsnetz

Die Diskussion über ein umfassendes, landesweites Kommunikationsnetz wurde ausgelöst durch die Frage nach den Konsequenzen, die aus dem Reaktorunfall in Tschernobyl zu ziehen sind.

Es hatte sich beispielsweise gezeigt, daß die gemeinsame Telefonanlage des Ministeriums für Landwirtschaft und Forsten, des Ministeriums für Umwelt und Reaktorsicherheit und des Sozialministeriums dem zusätzlichen Kommunikationsbedarf innerhalb der Behörden im Behördenzentrum und nach draußen nicht gewachsen war. Die erhöhte Belastung entstand nicht nur durch Gespräche zwischen den Landesbediensteten, sondern auch durch das kurzfristig eingerichtete Bürgertelefon. Letzteres wurde als Informationsquelle für den Umgang mit der radioaktiven Belastung von den Bürgern sehr rege genutzt. Dies hatte zur Folge, daß die Bediensteten oft längere Zeit auf eine freie Amtsleitung warten mußten und daß externe Anrufer nicht zum gewünschten Gesprächspartner durchkamen. Es versteht sich von selbst, daß aus solchen Ereignissen Folgerungen gezogen werden müssen, um derartige Engpässe in Zukunft zu vermeiden.

Die Landesregierung hat in einem Kabinettsbeschluß vom 2. September 1986 unter anderem festgelegt, daß die betroffenen Ministerien „für den Bereich ihrer fachlichen Zuständigkeit jeweils Erfahrungsberichte und Lösungsvorschläge zur Verbesserung der Vorsorgeplanung unterhalb des Katastrophenfalls" erarbeiten sollen. Auf der Grundlage dieser Berichte „prüft eine vom Minister des Innern koordinierte Arbeitsgruppe, inwieweit bei der Vorsorgeplanung unterhalb der Katastrophenschutzschwelle Erfahrungen anderer Ressorts durch die Fachressorts verwendet werden können, inwieweit bei der Erarbeitung und Durchführung von Lösungen kooperiert werden kann und inwieweit die Schaffung gemeinsamer Infrastruktureinrichtungen sinnvoll und möglich ist". Darüber hinaus hat der Landesautomationsausschuß (LAA) am 3. Dezember 1986 auf Antrag des Hessischen Innenministeriums die Einrichtung eines Unterausschusses „Kommunikationsnetz" beschlossen.

„Der Unterausschuß hat den Auftrag

1. a) den Bedarf und die Möglichkeiten zum Aufbau eines landesweiten elektronischen Kommunikationssystems für Texte, Daten und Bilder unter Einbeziehung der bisherigen Planungen der Ressorts zu untersuchen und einen Realisierungsvorschlag zu erarbeiten;

   b) zu prüfen, inwieweit die ständig besetzten Leitfunkstellen und Zentralen Leitstellen für den Brand- und Katastrophenschutz sowie Rettungsdienst einschließlich Krankentransport in die landesweite Informations- und Kommunikationsstruktur einbezogen werden können.

2. Der Unterausschuß besteht aus je einem Vertreter des Innenministeriums, des Ministeriums für Wirtschaft und Technik, des Ministeriums für Umwelt und Reaktorsicherheit, des Sozialministeriums und des Ministeriums für Landwirtschaft und Forsten. Je ein Vertreter des Hessischen Datenschutzbeauftragten, der Hessischen Zentrale für Datenverarbeitung und des Hauptpersonalrats beim Innenministerium sind beratende Mitglieder. Vorsitzender ist der Vertreter des Innenministeriums."

Das Innenministerium hat in seiner Beschlußvorlage Bezug genommen auf den zitierten Kabinettsbeschluß, und damit zum Reaktorunfall in Tschernobyl, und fordert: „Das Kommunikationsnetz soll in erster Linie bei flächendeckenden Gefahrenlagen oder Schadensereignissen eingesetzt werden, muß jedoch ansonsten auch für den täglichen Routinebetrieb der Verwaltung zur Verfügung stehen".

Zur Aufgabe des Unterausssschusses heißt es: „Der Unterausschuß sollte in der ersten Phase seiner Arbeit die qualitativen und quantitativen Anforderungen der einzelnen Verwaltungen an ein Kommunikationssystem feststellen, die Kriterien für ein gemeinsames Netz untersuchen und den Kostenrahmen abstecken." Gleichzeitig werden in der Begründung extrem hohe grundsätzliche Anforderungen inhaltlicher und technischer Art formuliert, die - wenn überhaupt - erst das Ergebnis einer umfassenden, differenzierten Analyse des Kommunikationsbedarfs und der Kommunikationsstruktur innerhalb und zwischen sämtlichen Landes- und Kommunalbehörden sein können.

4.4.1
Unterausschuß Kommunikationsnetz

Der Unterausschuß hat zunächst beschlossen, die vorhandenen Kommunikationseinrichtungen kurzfristig zu verbessern, um den dringenden Bedarf für die Übermittlung von Sprache, Texten und Bildern (Skizzen, Grafiken) sicherzustellen. Die Zahl der zu beschaffenden Endgeräte wurde anhand der Angaben der einzelnen Ressorts ermittelt und in eine Kabinettsvorlage eingearbeitet:

- 34 Telexgeräte
- 72 Teletexgeräte
- 214 Telefaxgeräte.

Mit der Erstellung dieses kurzfristigen Konzepts mit Beschaffungskosten von ca. 4,5 Mio. und jährlichen Grundgebühren von 240.000 DM erklärten zwei Ressortvertreter ihre Aufgaben im Unterausschuß für erledigt.

In den Diskussionen über das, was technisch möglich und wünschenswert wäre, habe ich immer wieder auf folgendes hingewiesen: Der Unterausschuß hat die Aufgabe, den Bedarf und die Möglichkeiten für ein landesweites Kommunikationsnetz festzustellen. Dieser Auftrag kann nur so verstanden werden, daß zunächst eine inhaltliche Bedarfs- und Kommunikationsanalyse - losgelöst von den technischen Möglichkeiten - durchgeführt werden muß und erst auf deren Grundlage Anforderungen an ein landesweites Netz erarbeitet werden können. Hilfreich hierfür kann beispielsweise eine Auswertung der Informationsdefizite sein, die sich nach Tschernobyl ergeben haben.

Eine Bedarfsanalyse wurde bisher nicht begonnen; es blieb bei Überlegungen, wie sie aussehen und unter welchen Randbedingungen sie überhaupt mit einem brauchbaren Ergebnis durchgeführt werden könne.

Der Vorsitzende des LAA hat zwischenzeitlich klargestellt, daß dieses System „nicht nur die Anforderungen hinsichtlich des Reaktorunfalls in Tschernobyl, sondern generell landesweit alle Kommunikationsbedürfnisse abdecken" soll. Damit war erstmals klar gesagt, daß es nicht um die Beseitigung der Schwachstellen nach Tschernobyl ging - hierfür gab es einerseits die o.g. kurzfristigen Beschaffungsvorschläge und im übrigen die interministerielle Arbeitsgruppe -, sondern weit darüber hinaus um ein generelles landesweites Netz.

4.4.2
Datenfernverarbeitungskonzept der HZD

Im Sommer hatte die HZD ein „Technisches Konzept für die zukünftige Gestaltung des Datenfernverarbeitungsnetzes der HZD" vorgelegt, das ebenfalls im Unterausschuß Kommunikationsnetz diskutiert wurde. In diesem Rahmen habe ich zum Datenschutz in diesem Netz ausführlich Stellung genommen.

4.4.2.1
Vorgeschichte

Es gab bereits in der Vergangenheit Ideen zur Vernetzung innerhalb des öffentlichen Bereichs des Landes Hessen. Erinnert sei hier an Pläne, die Rechenzentren des DV-Verbundes untereinander zu vernetzen, einmal mit, einmal ohne Einbeziehung des Rechenzentrums des Landeskriminalamtes (LKA). Begründet wurde dies mit der Notwendigkeit des schnellen Programmaustauschs zwischen den Verbundrechenzentren und mit dem schnellen, direkten Zugriff der Polizei auf Einwohnermeldedaten.

Auch in diesem Fall gab es eine Unterlage, in der der grobe technische Aufbau dieses Netzes beschrieben wurde. Dabei wurde davon ausgegangen, daß ein einziges großes Landesnetz schon von der erforderlichen Gesamtorganisation und der hierfür in den Rechenzentren notwendigen Abstimmung und Umstellung der Organisation her viel zu kompliziert und zu aufwendig ist. Vorgeschlagen wurde als technische Realisierung, daß alle beteiligten Rechenzentren ihre Netze zukünftig unter einer bestimmten Software (SNA, System Network Architecture, Hersteller IBM) betreiben. Der Zusammenschluß der einzelnen „autonomen" Netze ist unter dieser Voraussetzung ohne große technisch- organisatorische Änderungen mit der Software SNI (System Network Interconnection, ebenfalls von IBM) möglich. Ein detailliertes Datenschutzkonzept für eine solche Vernetzung wurde nicht vorgelegt.

Dieses Netz ist bisher nicht realisiert worden. Die Gründe hierfür mögen vielfältig sein. Maßgeblich war neben von mir geäußerten Bedenken aber sicherlich das Problem der Kosten; es gab die entsprechend großen Anwendungen nicht, mit denen die hohen Investitionskosten der beteiligten Rechenzentren hätten finanziert werden können.

4.4.2.2
Netz mit Paketvermittlung

In einem Netz mit Paketvermittlung (kurz: Paketvermittlungsnetz) werden Daten nicht - wie beispielsweise beim Telefonieren - über die eigens hergestellte direkte Verbindung übermittelt. Sondern sie werden als „Pakete" verschickt: Der Absender packt seine Daten in ein Paket, verpackt und beschriftet es nach bestimmten Regeln (gibt z.B. die Anschrift des Empfängers mit besonders groß geschriebener Postleitzahl an, macht deutlich, ob die Sendung aus mehreren Paketen besteht, und wenn ja, das wievielte Paket das eben beschriftete ist etc.). Das Paket wird durch das Netz zum Empfänger transportiert, der es öffnet, den Inhalt herausnimmt und später vielleicht selbst Pakete verschickt. Die Parallele zum Paketdienst der Deutschen Bundespost ist offensichtlich.

Jedes Paket einer Sendung könnte dabei sogar auf einem anderen Weg transportiert werden. Wenn Teilstrecken ausfallen, werden die Pakete nicht gestapelt, bis die Strecke wieder in Ordnung ist, sondern auf einer anderen Strecke, eventuell auch über einen längeren Weg, ans Ziel gebracht. Da im Netz die verschiedenen Wege bekannt sind und bei Bedarf sofort automatisch umgeleitet wird, spricht man von einer hohen Ausfallsicherheit des Netzes.

Für die Verpackung und Beschriftung der Pakete sind verschiedene Regelsysteme denkbar. Man könnte den Empfänger beispielsweise auch in die linke obere Ecke schreiben, in der Reihenfolge Postleitzahl und Ort, dann die Straße und schließlich den Namen. Die vereinbarten Regeln müssen aber von allen Teilnehmern eines Netzes eingehalten werden, damit Mißverständnisse vermieden werden und die Zustellung nicht verzögert wird.

Es gibt ein international standardisiertes Regelsystem für Paketvermittlung, die sog. X.25-Protokolle. Die Deutsche Bundespost stellt mit ihrem Datex-P-Netz ein solches X.25-Netz zur Verfügung.

4.4.2.3
Offene Fragen und Probleme zur Netztechnik

Die HZD will jetzt ein eigenes Paketvermittlungsnetz aufbauen und damit die Basis für ein landeseinheitliches Netz legen. Die im HZD-Konzept getroffene lapidare Feststellung „Die Datensicherheit entspricht der des Datex-P-Netzes" ist nicht nachvollziehbar, geschweige denn überprüfbar, weil die HZD hierzu keine weiteren Erläuterungen gibt.

So bietet das Datex-P-Netz der Bundespost eine Reihe von „besonderen Leistungen" wie beispielsweise

- Teilnehmerbetriebsklassen
- feste virtuelle Verbindungen
- Subadressen
- Abweisung ankommender Rufe
- Benutzerangaben im Verbindungsanforderungspaket

mit denen der Datenschutz unterstützt und verbessert werden kann.

Die HZD hat bisher keine Angaben darüber gemacht, ob sie entsprechende Leistungen in ihrem Netz zur Verfügung stellen und nutzen wird und welche sonstigen Maßnahmen zur Realisierung des Datenschutzes getroffen werden sollen.

Als Netzbetreiber wird die HZD eine zentrale Vermittlungseinrichtung - ein Rechner hierfür wurde bereits beschafft - und dezentrale Knoteneinrichtungen unterhalten. Es versteht sich von selbst, daß über ein solches Netz dann auch mehr Wissen und Zugriffsmöglichkeiten vorhanden sind und vorhanden sein müssen als über das von der Post betriebene Netz, so daß wegen der höheren Mißbrauchsgefahr zusätzliche Schutzmaßnahmen erforderlich sind. So muß beispielsweise geklärt werden, wo Knoten- und Vermittlungseinrichtungen aufgestellt und wie sie gesichert werden, wer Zugriff auf die Software und die Dateien auf diesen Rechnern hat und wie unzulässige Benutzung verhindert wird.

Darüber hinaus fehlen in dem Konzept Angaben darüber,

- welche Informationen der gerufene Partner (Rechner, Anwendungsprogramm oder anderer Benutzer an anderem Datenendgerät) über den rufenden Partner bekommt: nur die Bezeichnung des X.25-Anschlusses oder auch genaue, unverfälschbare Angaben über das rufende Endgerät und seinen Benutzer

- wie Teilnehmerkennungen aufgebaut, ob sie verschlüsselt und wie und wo sie gespeichert werden

- wo und wie Paßwörter gespeichert und überprüft werden und welches Änderungsverfahren vorgesehen ist

- welche Netzübergänge von und zu diesem Paketvermittlungsnetz bereitgestellt werden sollen, beispielsweise für Anwender, die keinen X.25-Anschluß besitzen, also ihre Daten nicht selbst entsprechend den X.25-Protokollen in Pakete verpacken können

- wie Netzübergänge - auch von und zu anderen Netzen, beispielsweise der KGRZ und öffentlichen Netzen - kontrolliert werden; welche Schwachstellen und Probleme hier für den Datenschutz entstehen und wie ihnen begegnet werden kann.

Von dieser Transport- und Vermittlungsfunktion des Netzes muß die Ebene der darauf verfügbaren Dienste oder Anwendungsarten genau unterschieden werden. Hier werden neben dem Dialogdienst der File-Transfer, der Dokumenten- und Nachrichtentransfer sowie die Telematikdienste (Btx, Teletex etc.) genannt. Auch auf dieser höheren logischen Ebene müssen Datenschutz und -sicherheit gewährleistet werden.

Für den „klassischen" Dialogdienst, also die Kommunikation eines Anwenders mit einem Rechner oder einem Anwendungsprogramm, gibt es in der Regel Datenschutzprogramme, mit denen bei geeigneter Generierung im Falle nur eines Hosts keine neuen grundsätzlichen Probleme zu erwarten sind (vgl. beispielsweise Ziff. 4.2.1, ACF2). Anders sieht es beim File-Transfer aus. Er wird spätestens dann problematisch, wenn auf dem Zielrechner keine lückenlose Kontrolle ordnungsgemäßer Datenverarbeitung mehr möglich ist. Dies ist beispielsweise bei Arbeitsplatz- und Bürocomputern (und Netzen oder Clustern von solchen) der Fall, wenn Benutzeraktivitäten nicht ausreichend kontrolliert und protokolliert werden können oder wenn Datenbestände ohne Protokollierung oder von Unbefugten auf Disketten kopiert und aus der Dienststelle entfernt werden können. Selbstverständlich gilt auch bei Dezentralisierung der Datenverarbeitung der Grundsatz, daß Veränderungen oder Neuerungen keinesfalls zu einer Verschlechterung des Datenschutzes führen dürfen.

Mit ihrem Netz, speziell mit dem Dienst „Dokumententransfer" und den Telematikdiensten will die HZD die Voraussetzung für die Kommunikation „jeder mit jedem" schaffen. Diese Ankündigung gibt Anlaß zur Sorge, zumal auch sie keinerlei Angaben zu verschiedenen Aspekten des Datenschutzes, wie z.B. der Kontrolle der Zulässigkeit der Datenverarbeitung, enthält.

Unklar ist auch die Beziehung zwischen dem älteren Konzept zur Vernetzung der Rechenzentren des DV-Verbundes und dem neu vorliegenden Konzept. Letzteres heißt zwar „Konzept für die zukünftige Gestaltung des DFV-Netzes der HZD", nennt aber unter „Kommunikationsanforderungen" sowohl die „Kommunikation mit anderen zentralen Einrichtungen in Hessen (z.B. KGRZ)" als auch die „Kommunikation mit externen Rechenzentren". Dieser Widerspruch zwischen Titel und Anforderung wird von der HZD nicht aufgelöst. Auf die Technik, mit der die Netze anderer Rechenzentren an dieses HZD-Netz angeschlossen werden sollen, wird nicht eingegangen. Damit ist zunächst offen, ob eine Integration technisch möglich und ob sie geplant ist. Gemeinsam ist beiden Konzepten, daß sie technische Vorschläge sind, sich also auf die Beschreibung von technisch Machbarem beschränken. Die dabei formulierten Anforderungen benennen verschiedene Schwerpunkte: einmal die Vernetzung der Rechenzentren des DV-Verbundes (evtl. mit dem Rechenzentrum des LKA), zum anderen die Kommunikationsanforderungen der Landesbehörden, die ja inzwischen längst über eigene DV-Systeme verfügen (s.o. Ziff. 4.3). Auch wenn dies nicht explizit technisch dargestellt wird, ist doch implizit klar, daß das neue Netzkonzept wesentlich umfassender ist und die Anforderungen an das alte ebenfalls mit abdecken soll.

Auf dem derzeitigen Stand des Konzepts der HZD und der Diskussion im Unterausschuß ist eine fundierte, abschließende Stellungnahme nicht möglich. Deshalb habe ich im Unterausschuß vorgeschlagen, die HZD zu beauftragen, ein detailliertes Datenschutzkonzept zu dem geplanten Datenfernverarbeitungsnetz vorzulegen. Diese Forderung wurde akzeptiert; ein entsprechender Beschluß wurde im LAA bereits gefaßt.

Auf der Basis einer solchen Darstellung, die auch zur Transparenz der Netzplanung beitragen wird, können dann Fragen der Technik und der Organisation des Netzes nicht nur, aber auch unter dem Aspekt der Datensicherheit weiter diskutiert und geklärt werden.

4.4.3
Forderungen

4.4.3.1
Untersuchung des Informationsflusses

Das technisch Machbare kann nicht allein die Maxime für staatliches Handeln sein. Sondern es müssen - gerade bei solchen folgenschweren Entscheidungen wie der über ein landesweites Kommunikationsnetz - die inhaltlichen Anforderungen klar, möglichst objektiv und nachvollziehbar formuliert werden. Konkret heißt das, daß zunächst eine inhaltliche Bedarfsanalyse vorgelegt werden muß. Die Informationsprobleme nach dem Reaktorunglück inTschernobyl machen zwar unzweifelhaft deutlich, daß Engpässe vorhanden waren und Verbesserungen nötig sind, reichen aber als globale Begründung für die Erweiterung zu einem umfassenden Konzept eines landesweiten Netzes, in dem prinzipiell jeder mit jedem kommunizieren kann, bei weitem nicht aus.

Ich vermisse Überlegungen der Landesregierung - nicht nur, aber auch unter dem Aspekt des Schutzes personenbezogener Daten - darüber, welche Informationsflüsse unzulässig, zulässig, notwendig oder möglich sein sollen, wie Kontrolle und Beschränkung der Kommunikation wirksam installiert werden können. Nur damit ist aber die notwendige Transparenz für alle Bürgerinnen und Bürger erreichbar, wie sie das Bundesverfassungsgericht im Volkszählungsurteil verlangt hat. Auch das im HDSG formulierte Informationsgleichgewicht zwischen Legislative und Exekutive kann nur dann vor einer Gefährdung bewahrt werden, wenn für die Politikerinnen und Politiker die Informationsflüsse innerhalb der Verwaltung nachvollziehbar sind.

Es ist also eine differenzierte Kommunikationsanalyse erforderlich, die klare, definierte Datenströme mit ihren jeweils notwendigen Restriktionen beschreibt. Erst auf dieser Grundlage können, nachdem die Zulässigkeit der jeweiligen Informationsverarbeitung geklärt ist, technische Konzepte entwickelt und diskutiert werden. An einer solchen Kommunikationsanalyse müssen alle Ressorts, nicht nur die im Unterausschuß vertretenen, beteiligt werden.

Es ist selbstverständlich unzulässig, aus der Tatsache, daß die HZD ein solches Netzkonzept vorgelegt hat, zu folgern, daß ein landesweiter Bedarf an einem solchen Netz besteht. Denn die HZD macht hier als Unternehmen einen technischen Vorschlag und äußert sich zu seiner Wirtschaftlichkeit. Richtig wäre der umgekehrte Weg, daß, sobald der Bedarf untersucht und die inhaltlichenAnforderungen formuliert sind, von der Landesregierung geprüft wird, ob das geplante Netz den Anforderungen entspricht oder ob modifizierte oder andere technische Lösungen gefunden werden müssen.

4.4.3.2
Erstellung eines Gesamtkonzepts

Mit der Konzeption umfangreicher Informations-Infrastrukturen verschärfen sich die Datenschutzprobleme. Deshalb ist es besonders wichtig, Datenschutzfragen nicht erst in einer späten Phase der Entwicklung oder gar im Nachhinein zu berücksichtigen. Denn eine nachträgliche Implementierung ist meist nicht nur sehr aufwendig, sondern auch wenig wirksam. Dies ist auch der Grund dafür, daß ich mich bereits in dieser frühen Phase der Konzeption eines landesweiten Netzes in die Diskussion einschalte.

Wohlgemerkt, es geht dabei nicht um Technikfeindlichkeit und schon gar nicht um Verbote oder Verhinderung von Technik. Es geht mir vielmehr um die rechtzeitige Problematisierung mit dem Ziel, bereits auf der Konzept-Ebene

eine Integration zu erreichen von gesteigerter Bürgernähe und Arbeitsqualität einerseits sowie dem Schutz personenbezogener Daten der Bürgerinnen und Bürger und der Beschäftigten in der Verwaltung andererseits. Voraussetzung für das Gelingen einer solchen Integration ist die Transparenz und Kontrollierbarkeit sämtlicher Datenflüsse.

Deshalb ist es notwendig, daß die Landesregierung ein Gesamtkonzept entwickelt

- mit begründeten, klar definierten Informationsströmen
- mit einem detaillierten Netzkonzept
- mit einem detaillierten, hierauf abgestimmten Datenschutzkonzept, das die verschiedenen logischen Ebenen des Netzes berücksichtigt
- mit klaren Verantwortlichkeiten und Kontrollmöglichkeiten.

Aus technischer Sicht bedeutet dies unter anderem:

- Auf die Kontrolle des Verbindungsaufbaus und die Kontrolle der Benutzeraktivitäten muß besonderer Wert gelegt werden. Soweit wie irgend möglich sollte dabei das Prinzip des Verbots mit Erlaubnisvorbehalt eingehalten werden.
- Auch an die Fälschungs- und Mißbrauchssicherheit von Authentifikationsverfahren müssen höhere Anforderungen gestellt werden.
- Die Datensicherungsstandards müssen überprüft und ggf. angepaßt werden.
- Wenn mehrere Hosts mit eigenem Netz zu einem landesweiten Netz verbunden werden sollen, sind einige zusätzliche Anforderungen zu erfüllen:
  - Jedes Rechenzentrum muß den Datenfluß in seinem (Teil-)Netz vollständig kontrollieren können. Dazu gehört unter anderem auch eine zuverlässige Information/Kontrolle im Zielrechenzentrum darüber, welcher Benutzer von wo aus welche Anwendungen nutzt. Es kann nicht als ausreichend betrachtet werden, wenn diese Informationen nur nachträglich aus den Protokollen der verschiedenen Transit- oder Zielrechner zusammengestellt werden können; sie müssen zur Kontrolle der Benutzer am Zielrechner verwendet werden.
  - Es muß gewährleistet sein, daß kein Benutzer unberechtigt Anwendungen in den Transitnetzen nutzen kann.
  - Für den Fall, daß Netze oder Cluster von Arbeitsplatzcomputern an einen Host angeschlossen sind, bekommt die Kontrolle bzw. Verhinderung des File-Transfers und des Abgleichs mit lokalen Dateien durch die im Zweifel größeren lokalen Datenbestände möglicherweise eine neue inhaltliche Dimension. Für die Identifikation und Authentifikation von Benutzern kann der zwischengeschaltete Server (6) - der vom Rechenzentrum nicht kontrolliert werden kann - eine zusätzliche Schwachstelle werden.
  - Ich halte es für selbstverständlich, daß das zukünftige Netz wiederum ein geschlossenes Netz mit einem geschlossenen Benutzerkreis ist (vgl. dazu auch die Ausführungen der HZD in „Datensicherheit bei Datenfernverarbeitung, DS-DFV", Mai 1985). Das heißt, daß der Kreis berechtigter Personen festgelegt ist und daß jede berechtigte Person von bestimmten, dem Netz bekannten Endgeräten bestimmte Anwendungen auf einem bestimmten Rechner nutzen und ggf. mit bestimmten anderen Personen an bestimmten Endgeräten im Rahmen bestimmter Aufgaben kommunizieren darf. Je umfangreicher ein solches Netz wird, je mehr Rechner, Endgeräte und Anwendungen es umfaßt und je größer der Benutzerkreis wird, desto aufwendiger und schwieriger wird die Verwaltung des Netzes und die Kontrolle seiner Benutzung.
  - Über die Kontrollierbarkeit des zukünftigen Netzes muß die Landesregierung präzise Aussagen machen. Zum Vergleich sind dabei der derzeitige Stand der Landesautomation und ggf. auch alternative Konzepte zum geplanten Netz heranzuziehen.

Erläuterungen zu Ziff. 4

(1) MVS ist ein Betriebssystem der Firma IBM für Großrechner

(2) UNIX ist ein Betriebssystem der Firma Bell Laboratories. Es wird hauptsächlich auf Rechnern der sog. mittleren Datentechnik eingesetzt. Programme, die für den Einsatz unter UNIX entwickelt wurden, sind weitgehend hardwareunabhängig.

(3) Sub-Systeme sind Programme des Betriebssystems für besondere, abgegrenzte Aufgaben wie z.B. JOB-Eingabe oder Teilnehmerbetrieb.

(4) Das Benutzerprofil beschreibt die Berechtigung des Benutzers an dem Computer, insbesondere welche Programme er benutzen und auf welche Daten er zugreifen darf.

(5) Ein Teilnehmerbetriebssystem ist ein Steuerprogramm, das u.a. die Verteilung der Rechenzeit auf die einzelnen Anwender steuert.

(6) Ein Server ist ein Computer, der Dienstleistungen z.B. zum Kommunizieren, zum Speichern von Dateien oder zum Drucken zur Verfügung stellt, die von den übrigen Netzteilnehmern in Anspruch genommen werden können.

5. Kommunen

5.1
Umfragen

Bei Umfragen beachten die Gemeinden oft die datenschutzrechtlichen Anforderungen nicht oder nicht ausreichend. Die folgenden beiden Fälle (Ziff. 5.1.1 und 5.1.2) zeigen einige typische Mängel, die darauf beruhen, daß die Vorgaben des Hessischen Datenschutzgesetzes nicht eingehalten wurden. Seit dem Inkrafttreten des Hessischen Landesstatistikgesetzes am 23. Mai 1987 sind bei „kommunalen statistischen Umfragen" darüber hinaus die besonderen Bedingungen dieses Gesetzes zu beachten (vgl. hierzu Ziff. 5.1.3).

5.1.1
Umfrage zur Stadtentwicklung

Die Stadt Wiesbaden beauftragte ein kommerzielles Meinungsforschungsinstitut mit einer „Umfrage zur Stadtentwicklung". Das Institut rief 1.000 aus dem Telefonbuch nach dem Zufallsprinzip ausgewählte Einwohner der Stadt an und befragte sie über Wohnverhältnisse, Ausbildung, Beruf, Einkommen und Kontakte zu städtischen Ämtern (z.B. Sozialamt). Die Antworten wurden sofort ohne Namen, Anschriften oder Telefonnummern der Betroffenen automatisiert gespeichert.

Meine Überprüfung der Umfrage ergab gleich mehrere gravierende Mängel. Zum einen hatte die Stadt Wiesbaden fälschlich angenommen, nicht sie, sondern das Meinungsforschungsinstitut sei für die Datenverarbeitung verantwortlich. Tatsächlich handelte es sich jedoch um die gesetzlich besonders geregelte Auftragsdatenverarbeitung (§ 4 HDSG), d.h. die Stadt ließ in ihrem Auftrag Daten durch das Institut verarbeiten und war damit selbst für die Einhaltung der Datenschutzvorschriften bei der Befragung verantwortlich. Das folgte zwingend aus der von Stadt und Institut vertraglich vereinbarten Verteilung der Entscheidungskompetenzen. Die Stadt bestimmte im wesentlichen das Fragenprogramm, entschied über das Auswahlverfahren für die Stichprobe und konnte auch darüber hinaus das Erhebungsverfahren beeinflussen. Auswertungen wollte die Stadt hauptsächlich selbst vornehmen, das Institut sollte lediglich Häufigkeitsverteilungen der Antworten liefern.

Läßt eine öffentlich-rechtliche Stelle personenbezogene Daten „außer Haus" verarbeiten, muß sie bestimmte gesetzliche Bedingungen einhalten. Beauftragt sie eine privatrechtliche Einrichtung mit der Datenverarbeitung, muß sie vertraglich sicherstellen, daß diese die Bestimmungen des Hessischen Datenschutzgesetzes beachtet und sich der Kontrolle des Hessischen Datenschutzbeauftragten unterwirft. Damit soll verhindert werden, daß sich eine Behörde ihrer Verpflichtungen aus dem HDSG entzieht, indem sie eine privatrechtliche Einrichtung (für die das Gesetz nicht gilt) mit der Datenverarbeitung beauftragt. Beide Anforderungen waren nicht erfüllt. Die Stadt Wiesbaden hatte sich zudem nicht, wie gesetzlich vorgeschrieben, darüber vergewissert, ob bei dem beauftragten Institut ausreichende Datensicherheitsvorkehrungen vorhanden waren.

Eine zusätzliche Auflage enthält das neue Hessische Datenschutzgesetz, das die öffentliche Stelle außerdem verpflichtet, dem Hessischen Datenschutzbeauftragten die Beauftragung einer privaten Stelle mitzuteilen.

Zum anderen verstieß auch die Durchführung der Umfrage gegen Datenschutzvorschriften. Vor den Anrufen hätte von den Betroffenen die schriftliche Einwilligung in die Verarbeitung ihrer Angaben eingeholt werden müssen. Nur ausnahmsweise kann auf die Schriftform verzichtet werden (§ 7 Abs. 2 HDSG); eine Telefonumfrage ist jedoch grundsätzlich kein solcher Ausnahmefall. Das mag auf den ersten Blick etwas verwundern. Wenn man allerdings den Schutzzweck der Formvorschrift berücksichtigt wird unmittelbar verständlich, daß die Schriftform in der Regel bei Telefonumfragen unentbehrlich ist. Es geht darum, voreilige und unüberlegte Entscheidungen zu verhindern. Die Gefahr der Überrumpelung des Betroffenen ist gerade bei Telefonumfragen besonders groß. Hier ist außerdem das Risiko, daß es zu Mißverständnissen kommt, ungleich höher als etwa bei einer schriftlichen Datenerhebung. Das gilt erst recht dann, wenn das Erhebungsprogramm besonders umfangreich ist und die Daten z.T. sehr sensibel sind.

Da eine Einwilligung nur sinnvoll ist, wenn die Betroffenen wissen, worin sie einwilligen, bestehen für die datenverarbeitende Stelle eine Reihe von Unterrichtungspflichten. Das Hessische Datenschutzgesetz verlangt, daß die Betroffenen über die Bedeutung der Einwilligung, insbesondere über den Verwendungszweck der Daten und bei beabsichtigten Übermittlungen über den Empfänger der Daten unterrichtet und auf die Freiwilligkeit der Teilnahme

hingewiesen werden. Nach Auskunft der Stadt Wiesbaden wurde lediglich auf das Recht zur Verweigerung der Teilnahme hingewiesen.

Angesichts der Rechtsverstöße bei der Erhebung konnte die weitere Verarbeitung der Daten nur hingenommen und damit eine Löschung vermieden werden, wenn die Daten umgehend hinreichend anonymisiert würden. Wie viele andere datenverarbeitende Stellen, die Angaben ohne Namen und Anschriften der Betroffenen speichern, war allerdings auch die Stadt Wiesbaden zunächst der Ansicht, die Daten seien anonym und verkannte dabei, daß Daten dann bereits als personenbezogen gelten, wenn sie einer bestimmten Person zugeordnet werden können, was hier leicht möglich war. Aus den Angaben Zuzugsdatum, Alter der Kinder, Alter der Befragten, Stadtbezirk der Wohnung konnte mit Hilfe des Melderegisters in vielen Fällen ohne großen Aufwand auf eine bestimmte Person geschlossen werden. Auf mein Verlangen wurden deshalb die Einzeldatensätze folgendermaßen geändert: Anstelle des Stadtbezirks erfolgte eine Zuordnung nach Wohngebietstypen (z.B. Innenstadt, Innenstadtrand etc.), anstatt des genauen Alters der Kinder wurden drei Größenklassen erfaßt, für das Zuzugsdatum 5 Zeitklassen gebildet und statt des genauen Alters der Befragten die Alterklasse, bestehend aus 3 aufeinanderfolgenden Jahrgängen, gespeichert. Damit waren die Einzeldatensätze hinreichend anonymisiert, so daß einer Weiterverarbeitung datenschutzrechtlich nichts mehr im Wege stand.

Der Fall zeigt eines sehr deutlich: Datenschutzrechtliche Verstöße in der Phase der Datenerhebung sind mit einem erheblichen Risiko verbunden, denn unzulässig erhobene personenbezogene Daten müssen gelöscht werden (§ 19 Abs. 4 HDSG). Die Löschung kann auch durch Beseitigung des Personenbezugs erfolgen, die anonymisierten Daten können dann u.U. für das Untersuchungsziel noch ausreichen. Nicht immer ist jedoch eine Anonymisierung möglich, ohne daß die Einzeldaten wegen des damit zusammenhängenden Aussageverlustes wertlos werden für das Untersuchungsziel. Deshalb kann sich die datenverarbeitende Stelle keineswegs darauf verlassen, Fehler bei der Erhebung später ohne weiteres durch Anonymisierung der Daten „ausbügeln" zu können.

5.1.2
Umfrage zur Zerstörungswut an Schulen

Daß es teuer werden kann, wenn das Beratungsangebot des Hessischen Datenschutzbeauftragten nicht oder nicht rechtzeitig angenommen wird, mußte das Schulamt der Stadt Frankfurt erfahren. Das Stadtschulamt (Behörde des Schulträgers, nicht zu verwechseln mit dem Staatlichen Schulamt, der Aufsichtsbehörde) stellte allen Frankfurter Schulen insgesamt ca. 27.000 Fragebogen zur Verfügung, die die Schüler der Jahrgangsstufen 5 - 10 ausfüllen sollten.

In dem zehnseitigen Fragebogen wurde unter anderem gefragt, wie häufig - und welche - Gegenstände in der Schule beschädigt oder zerstört werden. Die Schüler sollten ihre Meinung dazu äußern, die nachteiligen Folgen schildern, angeben, wer nach ihrer Ansicht für die Schäden aufkomme, die Verursacher bestimmten Personengruppen zuordnen und mitteilen, wie sie es fänden, wenn es derartige Vorkommnisse in ihrer Schule nicht gäbe. Erbeten wurden Vorschläge, wie das Geld für die Beseitigung der Schäden anderweitig verwendet werden könne und wer etwas gegen die Beschädigungen und Zerstörungen unternehmen solle. Darüber hinaus sollten die Schüler beschreiben, welche Möglichkeiten sie für sich selbst sehen, Beschädigungen und Zerstörungen zu verhindern. Abschließend wurde noch gefragt nach Geschlecht, Alter, Klasse, Berufsgruppe des Haushaltsvorstands, Anzahl der Personen im Haushalt, Schule, Wohnort außerhalb Frankfurts nach Größenklasse und Namen des Schülers.

Die ausgefüllten Fragebogen sollten in den Schulsekretariaten abgegeben und von dort an das Stadtschulamt weitergeleitet werden. Ziel der Befragung war, Erkenntnisse über die Ursachen der Beschädigung, Verschmutzung und Zerstörung schulischer Einrichtungen und Ausstattung zu gewinnen und gleichzeitig von den Schülern Vorschläge zu erhalten, wie den Zerstörungen zu begegnen sei.

Die Schülerbefragung des Frankfurter Stadtschulamtes verstieß jedoch in mehrfacher Hinsicht gegen das Datenschutzrecht. Da auf dem Fragebogen Name, Klasse und Schule angegeben werden sollten, handelte es sich eindeutig um eine personenbezogene Datenerhebung. Gleiches gilt für die geplante Datenspeicherung. Zwar sollte der Name nur für ein mit der Umfrage verbundenes Preisausschreiben erhoben werden, aber auch ohne Namen der Betroffenen wären die zur Speicherung vorgesehenen Angaben noch personenbeziehbar gewesen. Aus den Daten Geschlecht, Alter, Klasse, Berufsgruppe des Haushaltsvorstands, Anzahl der Personen im Haushalt, Schule, Wohnort außerhalb Frankfurts nach Größenklasse läßt sich unschwer auf Einzelpersonen schließen.

Die Datenerhebung durfte deshalb nur mit ausdrücklicher schriftlicher Einwilligung der Betroffenen durchgeführt werden (§ 7 Hessisches Datenschutzgesetz). Ob hierzu die Einwilligung des Schülers oder der Schülerin genügt hätte oder angesichts der z.T. sensiblen Fragen die Einwilligung der Erziehungsberechtigten erforderlich gewesen wäre, kann hier dahingestellt bleiben, denn in den Erhebungsunterlagen wurden weder die Erziehungsberechtigten noch die Schüler um eine Einwilligungserklärung gebeten.

Darüber hinaus wurden die Unterrichtungspflichten nicht eingehalten: Den Betroffenen hätte der Verwendungszweck der Daten genauer dargelegt werden müssen als im Fragebogen geschehen. Es hätte außerdem mitgeteilt werden müssen, wer die Daten speichert, wie die Daten verarbeitet werden (z.B. automatisiert), wie lange sie gespeichert und ob und wenn ja, an wen sie übermittelt werden. Schließlich fehlte der gesetzlich zwingend

vorgeschriebene Hinweis auf die Freiwilligkeit der Teilnahme und darauf, daß bei einer Verweigerung keine Rechtsnachteile entstehen würden.

Unzureichend war zudem der Datensicherheitsstandard des Erhebungsverfahrens. Der ausgefüllte Fragebogen sollte von den Schülern offen im Schulsekretariat abgegeben und von dort in nicht näher beschriebener Form an das Stadtschulamt weitergeleitet werden. Damit wurde gegen § 10 Abs. 3 Ziff. 9 Hessisches Datenschutzgesetz verstoßen, wonach bei der Datenerhebung gewährleistet sein muß, daß Unbefugte keinen Einblick in ausgefüllte Erhebungsvordrucke nehmen können.

Verstoßen wurde außerdem gegen einen Erlaß des Hessischen Kultusministeriums vom 4. Mai 1977 (ABl. 1977, S. 256), erneut in Kraft gesetzt durch Erlaß vom 29. September 1987 (ABl. 1987, S. 756). Das dort für derartige Untersuchungen vorgeschriebene Genehmigungsverfahren wurde nicht durchgeführt.

Auf meine Intervention hin stoppte das Schulamt der Stadt Frankfurt die Umfrage. Das Stadtschulamt hat mir inzwischen bestätigt, das sämtliche Fragebogen eingezogen und die bereits ausgefüllten Bogen unausgewertet sofort vernichtet worden sind.

5.1.3
Neue Rechtslage für kommunale statistische Umfragen

5.1.3.1
Regelungsziel und Anwendungsbereich des Landesstatistikgesetzes

Das Hessische Landesstatistikgesetz (HessLStatG) vom 19. Mai 1987 (vgl. hierzu auch Ziff. 3.1.1, 3.4 und 13.2 dieses Berichts) stellt auch die Kommunalstatistik auf eine völlig neue Rechtsgrundlage. Eine spezielle Vorschrift behandelt die Zulässigkeitsvoraussetzungen „kommunaler statistischer Umfragen" (§ 10 Abs. 4). Darunter sind zunächst alle Erhebungen zu verstehen, die das gegenüber der sonstigen Verwaltung „abgeschottete" kommunale Statistikamt auf der Basis freiwilliger Teilnahme der Befragten durchführt.

Noch nicht abschließend geklärt sind die Fragen, ob auch die zahlreichen von Fachämtern zu Zwecken der Fachplanung realisierten Umfragen nach dem Landesstatistikgesetz zu behandeln sind, wie dann die Abschottungsbedingungen des § 12 Abs. 3 HessLStatG eingehalten werden können usw. Für eine Einbeziehung auch dieser Erhebungen in den Begriff der „kommunalen statistischen Umfragen" spricht vor allem, daß der durch die Befragung des Bürgers gegebene Eingriff in sein informationelles Selbstbestimmungsrecht völlig unabhängig davon ist, ob diese vom Statistikamt oder einem Fachamt seiner Gemeinde vorgenommen wird. Dementsprechend erscheint es folgerichtig, einen gleichen Datenschutzstandard im Hinblick auf die Wahrung des Statistikgeheimnisses und die strikte Trennung vom Verwaltungsvollzug sicherzustellen.

In diese Richtung ging auch die übereinstimmende Meinungsbildung bei einem ersten Gespräch, das zur Klärung dieses Problems im Dezember 1987 stattgefunden hat und an dem sich die Staatskanzlei als oberste Aufsichtsbörde für die Landesstatistik, der Hessische Städtetag, Kommunalstatistiker aus mehreren großen Städten sowie der Hessische Datenschutzbeauftragte beteiligt haben. Ich gehe davon aus, daß im neuen Jahr eine verbindliche Regelung bzw. Interpretation im Interesse der Rechtssicherheit für die Kommunen festgelegt wird.

Die Regelung des § 10 des HessLStatG hat zum Ziel, die Durchführung kleinerer Umfragen auf der Basis freiwilliger Beteiligung gegenüber den regulären Kommunalstatistiken zu erleichtern. Letztere erfordern nämlich eine kommunale Satzung, die Erhebungsprogramm und Durchführungsmodalitäten im einzelnen festlegt (vgl. § 12 Abs. 1 i.V.m. §§ 7 Abs. 2 und 13 HessLStatG).

5.1.3.2
Zulässigkeitsvoraussetzungen

Für statistische Umfragen der Kommunen und Gemeindeverbände gelten nach § 10 Abs. 4 HessLStatG folgende Bedingungen:

1. Der Gemeindevorstand oder - bei Verbänden - das entsprechende Entscheidungsorgan muß feststellen, daß die Umfrage für die Vorbereitung und Begründung politischer Entscheidungen oder Satzungen erforderlich ist.

2. Der Gemeindevorstand muß in einem förmlichen Beschluß die Umfrage anordnen (zu 1. und 2. vgl. § 10 Abs. 1 HessLStatG).

3. Die statistische Geheimhaltung muß - auch gegenüber anderen Ämtern der Kommune - gewährleistet sein (vgl. § 12 Abs. 5 HessLStatG). Insbesondere ist die Umfrage von einer Stelle innerhalb der Gemeinde- bzw. Verbandsverwaltung durchzuführen, die organisatorisch von den anderen Verwaltungsabteilungen getrennt und räumlich sowie personell abgeschottet ist; diese Statistikstelle darf keine auf den Bürger bezogene Verwaltungsaufgaben wahrnehmen (vgl. § 12 Abs. 3 HessLStatG).

4. Der die Umfrage anordnende Beschluß hat den Zweck der Umfrage genau zu benennen. Die Einzelheiten der Durchführung müssen zwar anders als bei den regulären Kommunalstatistiken (vgl. § 12 Abs. 1 Satz 2) nicht in

einer Satzung geregelt werden, sie sollten aber in jedem Fall in dem Beschluß enthalten sein. Nur dann sind für die betroffenen Bürger ebenso wie für den Datenschutzbeauftragten als Kontrollorgan Art und Umfang der Datenverwendung transparent.

5. Es dürfen nur maximal 3.000 Personen befragt werden (§ 10 Abs. 2 HessLStatG). Unter den „Befragten" im Sinne dieser Vorschrift sind nur die Personen zu verstehen, die an der Umfrage durch Ausfüllung von Erhebungsbögen oder Auskunftserteilung gegenüber Interviewern teilnehmen. Nicht in diese Zahl einzurechnen sind mithin Personen, die zunächst nur nach ihrer Bereitschaft gefragt werden, sich überhaupt an der Umfrage zu beteiligen, ohne daß ihnen bereits Erhebungsvordrucke ausgehändigt oder zugesandt werden.

5.2
Anrufung des Hessischen Datenschutzbeauftragten durch kommunale Bedienstete

Der Datenschutzbeauftragte der Stadt Frankfurt empfahl kürzlich in seinen Hinweisen zur Durchführung der Neufassung des Hessischen Datenschutzgesetzes den Ämtern und Betrieben „äußerste Zurückhaltung" gegenüber dem Hessischen Datenschutzbeauftragten. Nach seiner Ansicht können die Bediensteten nur dann unmittelbar, d.h. ohne den Dienstweg einzuhalten, den Hessichen Datenschutzbeauftragten anrufen, wenn es um ihre eigenen Daten gehe. In den übrigen Fällen hätten sie sich ausschließlich an die zuständige verwaltungsinterne Stelle zu wenden, die allein entscheide, ob der Hessische Datenschutzbeauftragte angerufen werde oder nicht. Datenschutzrechtliche Verstöße seien darüber hinaus dem Personal- und Organisationsamt sowie dem kommunalen Datenschutzbeauftragten zu melden.

Die Auffassung des Datenschutzbeauftragten der Stadt Frankfurt widerspricht dem Hessischen Datenschutzgesetz. In § 28 Abs. 2 HDSG wird den Beschäftigten öffentlicher Stellen ausdrücklich das Recht eingeräumt, sich ohne Einhaltung des Dienstweges an den Hessischen Datenschutzbeauftragten zu wenden. Dies gilt nicht nur, wenn es um eigene Daten des Bediensteten, sondern auch und gerade um die Verarbeitung von Daten anderer geht. Jede andere Interpretation würde der Intention, die der Gesetzgeber mit der Einrichtung der Institution des Hessischen Datenschutzbeauftragten verfolgt hat, zuwiderlaufen. Der Gesetzgeber hat bewußt davon abgesehen, den Datenschutzbeauftragten in die herkömmliche Verwaltungsstruktur einzubinden. Vielmehr ist der unabhängige Datenschutzbeauftragte vor allem als Einrichtung eines vorbeugenden Rechtsschutzes anzusehen. Das hat das Bundesverfassungsgericht im Volkszählungsurteil vom Dezember 1983 klargestellt (BVerfGE 65, 46). Diese Funktion wird jedoch illusorisch, wenn dem Datenschutzbeauftragten die Chance genommen wird, direkter Ansprechpartner für die Behördenmitarbeiter zu sein. Den unmittelbaren Zugang zum Datenschutzbeauftragten abzusichern, ist Aufgabe des neuen § 28 Abs. 2 HDSG. Im übrigen hat die bisherige Praxis deutlich bewiesen, daß es auch im Interesse der Kommunen liegt, den direkten und unbürokratischen Kontakt ihrer Bediensteten zu meiner Dienststelle bei allen auftretenden Datenschutzfragen nicht zu behindern.

Eine gegenteilige Handhabung würde darüber hinaus die gesetzliche Aufgabe des Datenschutzbeauftragten gefährden, das Parlament genau und erschöpfend über Anwendungsschwierigkeiten des Datenschutzes zu unterrichten. Zwar besteht neben dem Anrufungsrecht der Beschäftigten die Befugnis des Datenschutzbeauftragten, von den öffentlichen Stellen Auskünfte zu verlangen. Es ist jedoch ein großer Unterschied, ob mögliche Fragen und Schwierigkeiten auf Initiative des unmittelbar betroffenen Verwaltungsangehörigen aufgegriffen und besprochen werden oder unter dem förmlichen Hinweis auf die gesetzliche Auskunftspflicht mühsam geklärt werden müssen.

5.3
Anzeigepflicht der Stadtverordneten

Im letzten Jahr wollten verschiedene Stadtverordnete wissen, ob und in welchem Umfang sie verpflichtet seien, der Gemeinde ihre Mitgliedschaften in Verbänden mitzuteilen.

Die Hessische Gemeindeordnung verpflichtet die Stadtverordneten zur Anzeige von Mitgliedschaften in Verbänden (§ 26a). Dagegen bestehen keine Bedenken. Zweck der Vorschrift ist, mögliche Interessenkollisionen frühzeitig aufzudecken. Nur so kann sichergestellt werden, daß der Stadtverordnete gemäß § 25 der Hessischen Gemeindeordnung nicht über Angelegenheiten mitberät oder mitentscheidet, in denen er einem Interessenkonflikt ausgesetzt ist. Dadurch wiederum soll gewährleistet werden, daß die Gemeindeverwaltung unparteiisch und einwandfrei ihre Entscheidungen trifft.

Die Offenbarungspflicht ist nicht unbegrenzt, vielmehr ist die Anzeige zunächst nur gegenüber dem Vorsitzenden des Organs zu machen, dem der Betroffene angehört. Darüber hinaus erfährt nur noch der Finanzausschuß davon.

Die Anzeigepflicht beschränkt sich keineswegs auf Funktionärstätigkeiten in Verbänden. Auch „einfache Mitgliedschaften" (z.B. in einem Sport- oder Kaninchenzüchterverein) müssen angezeigt werden. Zwar ist bei solchen „einfachen Mitgliedschaften" oftmals eine Interessenkollision nicht naheliegend. Es kann jedoch nicht dem Anzeigepflichtigen überlassen bleiben, zu entscheiden, ob im Hinblick auf bestimme Mitgliedschaften eine Interessenkollision denkbar ist oder nicht. Die Stadtverordneten haben mit anderen Worten nicht das Recht, Angaben zu verweigern.

5.4
Automatisierte Abrufverfahren innerhalb der Kommunalverwaltung

Ob Kfz-Zulassungsstelle, Gemeindebücherei, Sozialamt, Stadtkasse oder Steueramt, sie alle stehen häufig in der Situation, mit Hilfe des Einwohnermelderegisters z.B. Anschriften überprüfen zu müssen. Es überrascht daher nicht, wenn diese Stellen in zunehmendem Maße einen Online-(Direkt-)Zugriff auf Meldedaten verlangen.

Das neue Hessische Datenschutzgesetz regelt in § 15 ausführlich die Bedingungen, unter denen Dritte in automatisierten Verfahren personenbezogene Daten abrufen können. Die Vorschrift ermächtigt die Landesregierung, durch Rechtsverordnung automatisierte Abrufverfahren einzuführen, wenn dies unter Berücksichtigung der schutzwürdigen Belange des Betroffenen und der Aufgabe der beteiligten Stellen angemessen ist. Vor der Einrichtung ist der Hessische Datenschutzbeauftragte zu hören. In der Verordnung sind Datenempfänger, Datenart und Zweck des Abrufs ebenso festzulegen, wie Maßnahmen zur Datensicherheit und zur Kontrolle. Eine Verordnung nach dieser Vorschrift ist allerdings noch nicht ergangen.

Mit der Regelung hat der Landesgesetzgeber auf die besonderen Gefahren automatisierter Abrufverfahren reagiert. Der Direktzugriff ist ohne Mitwirkung der Stelle, bei der angefragt wird, möglich. Das bedeutet, der anfragenden Stelle stehen die Daten gleichermaßen zur Verfügung. Unzulässige Abfragen können unter diesen Umständen allenfalls im Nachhinein durch Kontrollen festgestellt werden. Gerade deshalb läßt der Gesetzgeber für die Einrichtung automatisierter Abrufverfahren nicht eine verwaltungsinterne Entscheidung genügen, sondern verlangt eine Rechtsverordnung, die die erwähnten Anforderungen erfüllen muß.

Für den Abruf von Meldedaten ist § 15 HDSG jedoch nicht anwendbar. Das Hessische Meldegesetz (HMG) verlangt als Spezialvorschrift für jede regelmäßige Übermittlung von Informationen aus den Melderegistern eine besondere Rechtsvorschrift (§ 31 Abs. 4 HMG). In der daraufhin ergangenen Landesmeldedatenübermittlungsverordnung sucht man freilich vergeblich nach Bestimmungen für den innergemeindlichen Informationsaustausch. Zu Recht, denn weder § 31 Abs. 4 HMG noch § 15 HDSG gelten unmittelbar für die Fälle, in denen einer Stelle der Gemeinde ein Direktzugriff auf die personenbezogenen Daten einer anderen Stelle derselben Kommune gewährt wird. Der Gesetzgeber hat diesen Bereich ausgespart, denn die verfassungsrechtlich geschützte Organisationshoheit der Gemeinden verbietet es ihm oder dem Verordnungsgeber (Landesregierung), die einzelnen Stellen innerhalb der Gemeindeverwaltung festzulegen, die an einem solchen Abrufverfahren zu beteiligen wären. Da die Gefahren, denen die Vorschriften der §§ 31 Abs. 4 HMG und 15 HDSG entgegenwirken sollen, bei automatiserten Abrufverfahren innerhalb der Landesverwaltung gleich sind wie bei automatisierten Abrufverfahren innerhalb der Gemeinde, ist allerdings eine entsprechende Anwendung der Bestimmungen auf letztere erforderlich.

Das bedeutet: Zur Einführung eines automatisierten Abrufverfahrens ist eine Organisationsentscheidung der Kommune nötig. In Frage kommt bei Städten - dort besteht in erster Linie das Interesse an Direktzugriffsverfahren - entweder ein Magistratsbeschluß, ein Magistratsbeschluß ergänzt um eine Verfügung des Oberbürgermeisters oder eine Verfügung des Oberbürgermeisters. Ich halte grundsätzlich alle drei Möglichkeiten für rechtlich zulässig, eine Einrichtung ohne eine solche förmliche Entscheidung jedoch für nicht vereinbar mit den Grundsätzen des Datenschutzrechts. Denn es geht nicht nur um eine rein organisatorische Maßnahme, sondern auch um den Schutz personenbezogener Daten der betroffenen Bürger; mithin um eine grundrechtsrelevante Maßnahme. Die förmliche Entscheidung der Kommune muß sich an den vom Gesetzgeber für die staatliche Verordnung vorgeschriebenen Inhalten orientieren. Demnach sind in dem Beschluß und/oder der Verfügung Datenempfänger, Datenarten, der Zweck des Abrufs sowie die Maßnahmen zur Datensicherung und Kontrolle zu bezeichnen.

6. Gesundheit

6.1
Aids

In der Aids-Diskussion ist lange Zeit der Datenschutz allenfalls als marginales Problem zur Kenntnis genommen worden. Das hat sich im vergangenen Jahr grundlegend geändert. Mit der Ausbreitung der Krankheit ist auch die Öffentlichkeit zunehmend auf die datenschutzrechtlichen Probleme aufmerksam geworden. Die Folge war u.a. eine Vielzahl von Anfragen, die ich von Bürgern, Behörden und Medien insbesondere zu Aids-Tests, der Speicherung von Aids-Daten in polizeilichen Informationssystemen und zur Meldepflicht erhalten habe.

6.1.1
Aids-Tests

Aufgeschreckt und verunsichert durch Berichte in den Medien über heimliche Aids-Tests z.B. an Patienten, jungen Attachés im Rahmen der obligatorischen Tropentauglichkeitsuntersuchung, Beamtenanwärtern und Asylbewerbern wollten viele Bürger wissen, ob sie, ohne darüber informiert zu werden und ohne ihre Einwilligung, auf Aids getestet werden dürfen.

6.1.1.1
Aids-Tests im Krankenhaus

Aids-Tests können in Krankenhäusern aus verschiedenen Gründen veranlaßt werden. In den bekannt gewordenen Fällen, in denen die Tests ohne Wissen der Patienten vorgenommen wurden, geschah dies sowohl zu diagnostischen Zwecken als auch zum Schutz des medizinischen Personals.

Das Testen des Blutes eines Patienten auf Aids-Antikörper ist eine Datenerhebung. Der Test und damit die Datenerhebung erfolgt im Krankenhaus i.d.R. personenbezogen. Denkbar sind allerdings auch Aids-Tests in anonymisierter Form, etwa zu Forschungszwecken. Die Daten werden nicht nur erhoben (beschafft), sondern anschließend auch im Krankenhaus gespeichert, d.h. zur Weiterverwendung aufbewahrt. Da Krankenhäuser im Rahmen der Patientenbehandlung Wettbewersunternehmen sind, gelten, auch wenn es sich um öffentlich-rechtliche Einrichtungen handelt, für ihre Datenverarbeitung die Vorschriften des Bundesdatenschutzgesetzes (BDSG) für den privaten Bereich (§ 3 Abs. 7 Hessisches Datenschutzgesetz). Das Bundesdatenschutzgesetz wiederum gilt zwar - anders als das Hessische Datenschutzgesetz - mit Ausnahme einer Vorschrift (§ 9 Abs. 2) nicht für die Phase der Datenerhebung, bestimmt aber, unter welchen Voraussetzungen die Daten gespeichert werden dürfen. Danach ist die Speicherung von Patientendaten im Krankenhaus nur zulässig, wenn sie entweder im Rahmen der Zweckbestimmung des Behandlungsvertrages liegt oder zur Wahrung berechtigter Interessen des Krankenhauses erforderlich ist und keine schutzwürdigen Belange des Betroffenen beeinträchtigt werden (§ 23 BDSG). Ist keine dieser beiden Voraussetzungen erfüllt, bedarf es einer gesonderten ausdrücklichen Einwilligung des Betroffenen.

Zweck des Krankenhausaufnahmevertrages ist die Diagnose, Beratung, Heilung, Linderung oder Hilfe. Den genauen Zweck, ob also nur eine Diagnose und Beratung oder etwa auch eine Therapie erfolgen soll, legen die Parteien im Krankenhausaufnahmevertrag fest. Natürlich kann der Vertragszweck nach Abschluß des Aufnahmevertrages von den Parteien konkretisiert und geändert werden, was sogar meistens der Fall sein wird. Das Krankenhaus darf die personenbezogenen Daten speichern, die für die Verwirklichung des von den Parteien bestimmten Vertragszwecks erforderlich sind. Dazu ist keine besondere Einwilligungserklärung erforderlich.

Zu dem von den Parteien dem Krankenhausaufnahmevertrag zugrundegelegten Vertragszweck wird im allgemeinen nicht die Aids-Diagnose zählen. Wer sich zu einer Blinddarmoperation in ein Krankenhaus begibt, will regelmäßig nicht gleichzeitig diagnostiziert haben, ob er oder sie Aids-infiziert ist. Gleiches gilt beispielsweise auch bei einem Geburtshilfevertrag. Der Aids-Test ist für den Patienten keine medizinische Routinemaßnahme. Im Gegenteil: Ein positives Testergebnis bedeutet für den Patienten extreme psychische, wirtschaftliche und soziale Belastungen. Er muß nach den gegenwärtigen medizinischen Erkenntnissen mit hoher Wahrscheinlichkeit mit einer Erkrankung rechnen, die, da derzeit nicht heilbar, fast sicher zum Tode führt. Eine radikale Änderung der Lebensweise wird notwendig. Neben dem Arbeitsplatzverlust droht die Gefahr der sozialen Isolation. Der Patient muß deshalb grundsätzlich vorher über den Aids-Test und seine möglichen Folgen informiert werden und einwilligen.

Eine Ausnahme kann allenfalls dann gelten, wenn der Patient das Krankenhaus mit eindeutigen Aids-Symptomen oder der Selbstdiagnose „Aids" aufsucht; nicht jedoch dann, wenn der Arzt den Patienten einer Risikogruppe zuordnet. Während der Begriff der Risikogruppe zu Beginn der Verbreitung von Aids noch ralativ klare Konturen hatte, trifft dies heute kaum noch zu. In der medizinischen Diskussion besteht über die sogenannten „Kernrisikogruppen" der Homosexuellen mit wechselnden Intimpartnern und der intravenös Drogenabhängigen hinaus keineswegs Einigkeit darüber, welche Gruppen als „Risikogruppen" zu qualifizieren sind und welches die Kriterien für die Zugehörigkeit zu einer Risikogruppe sind. Angesichts dieser Sachlage muß der Patient nicht damit rechnen, daß ein Aids-Test erfolgen kann, wenn ihn der Arzt einer bestimmten Personengruppe zuordnet.

In jedem Fall ist es unerläßlich, konkrete Verfahrensweisen festzulegen, die die Transparenz im Krankenhausbereich sicherstellen. Die Unsicherheit der Patienten darüber, wann sie mit einem Aids-Antikörpertest rechnen müssen, ist nicht akzeptabel. Ich habe deshalb das Hessische Sozialministerium über meine Auffassung unterrichtet und einen Bericht darüber angefordert, wie in hessischen Krankenhäusern bei Aids-Tests verfahren wird. Von besonderer Bedeutung ist die Art und Weise, in der ggf. die besondere Einwilligung von den Patienten eingeholt wird. So ist z.B. die pauschale schriftliche Erklärung des Patienten bei Aufnahme in das Krankenhaus, daß er mit einem Aids-Antikörpertest einverstanden ist, „wenn diese Untersuchung aus ärztlicher Sicht angezeigt ist", keine rechtswirksame Einwilligung. Der Patient kann die Tragweite einer solchen Erklärung nicht übersehen, er weiß letztlich nicht, ob überhaupt ein Test durchgeführt wird und ggf. aus welchem Anlaß der Test erfolgt - etwa aus diagnostischen Gründen oder zum Schutz des Personals. Derartige Erklärungen sind daher eine rein formale Abänderung des Verfahrens, sie verfehlen jedoch das inhaltliche mit dem Einwilligungserfordernis verbundene Ziel, Transparenz und Entscheidungsfreiheit für den Patienten sicherzustellen.

6.1.1.2
Aids-Tests im Auswärtigen Dienst, bei der Bundeswehr, Amts- und Vertrauensärztlichen Untersuchungen und im Asylverfahren

Anders als im Krankenhausbereich gibt es in anderen Bereichen für die Durchführung von Aids-Tests bereits relativ klare behördliche Vorgaben, die sicherstellen sollen, daß keine Test hinter dem Rücken der Betroffenen durchgeführt werden.

So hat z.B. das Außenministerium in der Bundestagsdebatte über die im Rahmen von Tropentauglichkeitsuntersuchungen vorgenommenen heimlichen Aids-Tests erklärt, Aids-Tests würden derzeit nur noch auf ausdrücklichen und schriftlich bekundeten Wunsch der Betroffenen durchgeführt (Bundestags-Drucks. 11/781). Das Bundesministerium für Verteidigung hat in seiner Antwort auf die Kleine Anfrage betreffend Aids-Tests bei der Bundeswehr vom 7. Oktober 1987 (Bundestags-Drucks. 11/909) dargelegt, daß der Musterungsrat einen HIV-Test durchführen lassen kann, wenn er aufgrund der Musterungsuntersuchung Krankheitszeichen feststellt, die eine Aids-Erkrankung vermuten lassen, hierbei jedoch ausdrücklich auf die Notwendigkeit des Einverständnisses der Betroffenen hingewiesen. Im übrigen sollen generell Tests auf freiwilliger Basis angeboten werden.

Auch in Hessen ist diese Entwicklung festzustellen. Bereits im März 1987 hat das Hessische Sozialministerium in einem Erlaß betreffend Amts- und Vertrauensärztliche Untersuchungen festgelegt, daß die routinemäßige Durchführung des HIV-Tests grundsätzlich nicht erforderlich und nur dann zulässig ist, wenn auf Grund der besonderen Umstände des Einzelfalls ein Test für die amtsärztliche Beurteilung erforderlich ist. Das soll dann der Fall sein, wenn aufgrund der klinischen Untersuchung der Verdacht auf eine manifeste Erkrankung besteht. Sofern solche besonderen Umstände vorliegen, ist der Betroffene hierüber vorher aufzuklären. Im Rahmen der Untersuchung anläßlich der Einstellung in den öffentlichen Dienst darf der Test nur durchgeführt werden, wenn der Bewerber hierzu sein Einverständnis erklärt (Az.: III A 3 18 e 02.05, 18 a 04.11). Das Hessische Innenministerium hat allerdings inzwischen in seiner Antwort auf eine Kleine Anfrage betr. Aids-Zwangsuntersuchungen (Drucks. 12/512) hinsichtlich der künftigen Verfahrensweise auf die von der Bundesregierung zu diesem Problembereich eingesetzte Arbeitsgruppe verwiesen, an der auch die Länder und Gemeinden beteiligt sind.

Im Oktober 1987 mußte ich bei einer Überprüfung des Kreisgesundheitsamtes Main-Taunus feststellen, daß Asylbewerber ohne ihr Wissen auf Aids getestet worden waren. Auf meine Beanstandung hin hat mir das Hessische Sozialministerium im November 1987 mitgeteilt, derartige Tests sollten nur nach vorheriger Information und mit ausdrücklicher Einwilligung der Betroffenen vorgenommen werden. Das Sozialministerium hat in einem Erlaß nunmehr die konkrete Verfahrensweise festgelegt (Az.: III/III A 4 - 18 e 02.85). Dem Erlaß zufolge sind routinemäßige Aids-Tests bei Asylbewerbern nicht erforderlich. Der Test ist grundsätzlich freiwillig, soweit er nicht aufgrund der Bestimmungen des Bundesseuchengesetzes oder durch die Ausländerbehörde nach ausländerrechtlichen Bestimmungen angeordnet wird. Die Asylbewerber sind über die Freiwilligkeit der Untersuchung und über den Umfang, insbesondere auch von Laboruntersuchungen, aufzuklären. Eindeutig festgelegt ist damit, daß Aids-Tests in keinem Fall hinter dem Rücken der Asylbewerber durchgeführt werden dürfen.

Auf einen verbesserten Schutz des informationellen Selbstbestimmungsrechts zielt schließlich auch der Antrag der CDU-Landtagsfraktion vom September 1987 (Drucks. 12/570), in dem die Landesregierung aufgefordert wird, Richtlinien zu erlassen, die das Verhalten der Gesundheitsbehörden im Hinblick auf die Krankheit Aids regeln. Diese Richtlinien sollen dem Antrag zufolge sicherstellen, daß die Gesundheitsbehörden Aids-Tests nur nach vorheriger Information und mit ausdrücklicher Einwilligung der Betroffenen vornehmen und ein einheitliches Verwaltungshandeln in diesem Bereich gewahrt bleibt.

6.1.1.3
Aids-Tests in Haftanstalten

Im Vordergrund der Diskussion über die Verarbeitung von Aids-Daten in Justizvollzugsanstalten stand im vergangenen Jahr die Frage der Rechtsgrundlage für die Durchführung von Aids-Tests bei Gefangenen. Das Hessische Justizministerium geht einerseits nach eigener Aussage davon aus, daß die Tests mit Einwilligung der Gefangenen vorgenommen werden (Drucks. 11/5111). In seinem Erlaß vom 5. Dezember 1985 betreffend die Gesundheitsfürsorge in den Justizvollzugsanstalten (siehe hierzu 15. Tätigkeitsbericht, Ziff. 4.4.5) heißt es dagegen unter Ziff. 2.1, daß alle Gefangenen zur Teilnahme an der Aids-Untersuchung verpflichtet sind. Sollte ein Gefangener eine Untersuchung verweigern, ist er „nachdrücklich über die Rechtslage aufzuklären". Auf welche Vorschrift diese Rechtsauffassung gestützt wird, ist im Erlaß nicht angegeben und konnte mir bisher auch nicht überzeugend begründet werden.

Solche Widersprüchlichkeiten sind jedoch nicht akzeptabel. Der Aids-Test kann einschneidende Konsequenzen für die Betroffenen haben; deshalb müssen die rechtlichen Voraussetzungen für die Durchführung des Tests eindeutig geklärt und festgelegt sein. Das gilt auch und gerade für eine geschlossene Institution wie die Haftanstalten. Von einer rechtswirksamen Einwilligung der Gefangenen kann nur dann ausgegangen werden, wenn diese Einwilligung nicht lediglich rein formal eingeholt wird, sondern tatsächlich eine Entscheidungsfreiheit der Gefangenen besteht (siehe hierzu auch oben Ziff. 6.1.1.1). Wenn den Gefangenen aber mitgeteilt wird, daß sie rechtlich zur Teilnahme am Test verpflichtet sind, so kann nicht mehr von einer Entscheidungsfreiheit gesprochen werden.

Ich habe daher das Justizministerium im September 1987 noch einmal aufgefordert, diese Widersprüchlichkeiten auszuräumen. Die Antwort steht bislang noch aus.

6.1.2
Aids-Hinweise in polizeilichen Informationssystemen

6.1.2.1
Praxis

Polizeibeamte werden oft in körperliche Auseinandersetzungen verwickelt oder müssen bei Unfällen erste Hilfe leisten. Daß sie dabei mit Blut in Berührung kommen, ist häufig unvermeidbar. Ein Polizeibeamter, der einen Fixer festgenommen hat und durchsucht, kann sich möglicherweise an einer Aids-infizierten Injektionsnadel verletzen. Angesichts der medizinisch gesicherten Erkenntnis, wonach das Aids-Virus besonders durch Blutkontakt übertragen wird, überrascht es deshalb nicht, daß auch die Polizei ein starkes Interesse an personenbezogenen Aids-Daten hat.

Mitte des Jahres 1987 habe ich die Speicherung von Aids-Daten in den beiden polizeilichen Informationssystemen INPOL und HEPOLIS überprüft. Das gemeinsam von Bund und Ländern betriebene Informations- und Auskunftssystem für die gesamte Polizei der Bundesrepublik (INPOL) ist das wichtigste automatisierte Informationssystem. An ihm sind angeschlossen das Bundeskriminalamt, das den Computer zur Verfügung stellt, und die Polizeibehörden der Länder. HEPOLIS ist das mit INPOL verbundene zentrale Hessische Polizei-Informationssystem.

Bei der Prüfung konnten aus INPOL von Hessen aus denwahrscheinlich über eine Million Personendatensätzen ca. 700 abgerufen werden, in denen das Merkmal „Ansteckungsgefahr" gespeichert war. Zum Teil enthielten die Datensätze noch den Zusatz „Vorsicht Blutkontakt", „Blutkontakt vermeiden" oder „Aids". In den Fällen, in denen nur das Merkmal „Ansteckungsgefahr" gespeichert war, konnten damit neben Aids auch andere gefährliche ansteckende Krankheiten gemeint sein, wie etwa Hepatitis B oder Syphilis. Andererseits ist die Zahl der insgesamt mit dem Merkmal „Ansteckungsgefahr" und eventuell einem Zusatz in INPOL gespeicherten Personendatensätze vermutlich höher als 700. Denn Hessen kann nur auf die Daten zugreifen, die die Bundesländer oder das BKA in das System INPOL-Bund eingegeben haben, nicht jedoch auf die Daten, die ein Bundesland in das System INPOL-Land gespeichert hat und zu denen nur das jeweilige Land Zugang hat.

Zur Situation in Hessen hat sich das Hessische Innenministerium in einem Bericht an den Landtag (Drucks. 12/289) ausführlich geäußert. Danach hat die hessische Polizei in der Zeit vom Juni bis zum 8. Dezember 1986 bei Verdacht auf Aids-Infizierung in HEPOLIS den Hinweis „Vorsicht Blutkontakte", „Blutkontakt vermeiden" oder ähnliches registriert. Als am 3. Oktober 1986 die Innenministerkonferenz „aus Gründen der Fürsorge für Polizeibeamte" grundsätzlich die Notwendigkeit einer Speicherung des Datums „Aids-Infektion" bejahte und gleichzeitig eine Arbeitsgruppe beauftragte, unter Beteiligung der Datenschutzbeauftragten Kriterien für die Speicherung zu erarbeiten, untersagte das Hessische Innenministerium die Zusatzhinweise.

Daraufhin wurden am 8. Dezember 1986 in HEPOLIS bei 10 Personen, die nur bei hessischen Polizeidienststellen registriert waren, die jeweiligen Zusätze gelöscht. Bei weiteren 44 Personen, die sowohl im INPOL-Verbund als auch bei hessischen Polizeidienststellen registriert waren, war in 28 Fällen ein Hinweis in den hessischen Akten auf eine Aids-Infizierung vorhanden. In 27 dieser Fälle hat das Hessische Innenministerium die Löschung des Zusatzes veranlaßt. In dem einen Fall waren entsprechende Informationen über eine Infizierung auch in den Akten eines anderen Bundeslandes enthalten. Deshalb war der Zusatz als gemeinsamer Datensatz für Hessen nicht verfügbar, so daß Hessen allein die Löschung nicht veranlassen konnte. Bei den übrigen 16 Personendatensätzen konnte nicht festgestellt werden, daß der Zusatzhinweis aus Hessen stammte, deshalb blieb er unverändert.

Bei den Recherchen für diese Fälle wurde ein Grundproblem der INPOL-Datenbanken festgestellt: Verfügen mehrere Länder über kriminalpolizeiliche Informationen über eine Person und können somit den personenbezogenen Hinweis in INPOL eingegeben haben, ist nicht feststellbar, wer für die Eingabe dieses Hinweises verantwortlich ist. Mit anderen Worten: Derjenige, der für die Richtigkeit und Überprüfbarkeit des Hinweises verantwortlich ist, kann nicht eindeutig festgestellt werden. Dies ist unter datenschutzrechtlichen Gesichtspunkten nicht hinnehmbar. Ich habe deshalb das Hessische Innenministerium aufgefordert, sicherzustellen, daß das BKA als für die Programmierung verantwortliche Stelle die Dateienstruktur entsprechend verändert.

6.1.2.2
Erforderlichkeit

Das erhöhte Risiko der Polizeibeamten, mit Blut anderer Menschen in Berührung zu kommen, ist unverkennbar. Eine solch gravierende Maßnahme wie die Einspeicherung des Merkmals „Ansteckungsgefahr" mit oder ohne den weiteren Zusatz „Vorsicht, Blutkontakt vermeiden" bzw. „Aids" käme jedoch allenfalls dann in Betracht, wenn sie für die Polizei einen erheblichen Sicherheitsgewinn bringen würde. Andernfalls stehen die schutzwürdigen Belange des von der Speicherung Betroffenen im Vordergrund, für den die Verarbeitung dieser hochsensiblen Daten große Gefahren birgt. Ohne einen erheblichen Sicherheitsgewinn für den einzelnen Polizeibeamten ist die Speicherung unverhältnismäßig.

Ob personenbezogene Aids-Hinweise in polizeilichen Informationssystemen die Gefährdung der Polizeibeamten verringern können, ist zweifelhaft. So hält der Leiter der Abteilung Virologie beim Bundesgesundheitsamt und

Vorsitzender der Arbeitsgruppe Aids beim Bundesgesundheitsministerium, Professor Koch, es nicht für notwendig, daß die Polizei Aids-Infizierte registriert. Das Hessische Sozialministerium sieht für Polizeibeamte keine wesentlich höhere Gefährdung als für bestimmte andere Berufsgruppen, wie z.B. Rettungsdienste. Die Gefährdung sei mit Informationen über infizierte Personen nicht abwendbar.

Zweifel am Sinn einer Speicherung personenbezogener Aids-Hinweise in polizeilichen Informationssystemen sind vor allem deshalb angebracht, weil in Gefahrensituationen die Daten entweder nicht vorhanden sind, nicht abgerufen werden können oder die Gefahr aus anderen Umständen bereits erkennbar ist. So können in der Regel bei der Rettung von Unfallopfern, wo es um schnelles Handeln geht, nicht vorher Informationssysteme auf mögliche Aids-Infektionen der Betroffenen abgefragt werden; zudem ist es auch nicht sinnvoll, denn von den geschätzten ca. 100.000 Aids- Infizierten in der Bundesrepublik sind lediglich die Daten einiger weniger im polizeilichen Informationssystem gespeichert. An diesem Zahlenverhältnis kann die Polizei kaum etwas ändern. Von der Aids-Infektion wissen meist nur die medizinischen Kontaktpersonen des Betroffenen. Schließlich haben vielfach die Betroffenen selbst keinerlei Kenntnis von ihrer Infektion. Das bedeutet: Wenn bei der Ersten Hilfe die Gefahr besteht, mit Blut des Opfers in Berührung zu kommen, müssen sich die Polizeibeamten so verhalten, als ob sie einen Aids-Infizierten vor sich haben. Das gleiche gilt, wenn die Polizei etwa einen ihr als gewalttätig bekannten Straftäter oder Verdächtigen festnehmen will oder Maßnahmen im Drogenmilieu durchführt.

6.1.2.3
Bedingungen für die Speicherung

Das Hessische Innenministerium habe ich darauf hingewiesen, daß, wenn die Speicherung personenbezogener Aids-Hinweise in polizeilichen Informationssystemen notwendig sein sollte, diese nur unter folgenden Bedingungen vorgenommen werden dürfte:

In einer Vielzahl von Fällen erhält die Polizei nach eigener Auskunft den Hinweis vom Betroffenen selbst. Dieser dürfte sich allerdings meistens nicht darüber im klaren sein, welche Konsequenzen diese Angabe haben kann. Die Speicherung führt nicht nur dazu, daß er von den ermittelnden Beamten in besonderer Weise behandelt wird, z.B. indem er in eine Einzelzelle eingewiesen wird. Vielmehr ist es denkbar, daß die gespeicherten Daten im Zusammenhang mit Ermittlungen auch an Dritte gelangen und ein großer Personenkreis von dieser Information Kenntnis erhält. Die weitgehende psychische und soziale Isolierung des Betroffenen kann die Folge sein. Gerade aus diesem Grund muß der Betroffene in jedem Fall auf die Folge der Einspeicherung im polizeilichen Informationssystem und den Umfang der Weiterverwertung hingewiesen werden.

Erhält die Polizei die Information aus dem Verwandten- oder Bekanntenkreis des Betroffenen, darf auf eine medizinisch eindeutige Diagnose nicht verzichtet werden. Ohne sie ist eine Speicherung schon deshalb unzulässig, weil die Folgen für den Betroffenen unverhältnismäßig sind.

Der Verwendungszusammenhang der gespeicherten Daten muß eindeutig festgelegt werden. Die Polizei hat Kontakt mit einer Vielzahl von Behörden. Zu klären ist deshalb, ob die Daten z.B. an Justizvollzugsanstalten, Gerichte, Gesundheitsämter oder andere Stellen weitergegeben werden dürfen.

6.1.3
Aids-Meldung der Polizei an Gesundheitsamt

Die Bahnpolizei des Kasseler Hauptbahnhofs überprüfte den Fahrer eines falsch geparkten Fahrzeugs und stellte fest, daß das Fahrzeug nicht zugelassen war und der Fahrer keine Fahrerlaubnis hatte. In der Tasche des Fahrers fanden die Beamten eine Bescheinigung, die ihn als Aids-infiziert auswies. Die Bahnpolizei übergab den Fahrer der Schutzpolizei der Stadt Kassel. Diese übersandte dem örtlichen Gesundheitsamt Kopien des Polizeiberichts, aus dem zu entnehmen war, daß der Betreffende einige Stunden nach seiner Freilassung an einem Treffpunkt des Homosexuellen-Milieus angetroffen worden war. Die Polizei bat das Gesundheitsamt, den Betreffenden auf die Gefahren der Übertragbarkeit des Aids-Virus hinzuweisen und ihn über seine Pflichten als HIV-Träger aufzuklären.

Für die Datenübermittlung der Polizei an das Gesundheitsamt gab es keine Rechtsgrundlage. Das Hessische Gesetz über die öffentliche Sicherheit und Ordnung (HSOG) enthält lediglich eine Bestimmung über die Zusammenarbeit aller Behörden bei der Gefahrenabwehr. Konkrete Voraussetzungen über die Weitergabe personenbezogener Daten nennt das Gesetz jedoch nicht. Nach dem Hessischen Datenschutzgesetz (§§ 11, 14) wäre die Übermittlung nur zulässig, wenn das Gesundheitsamt die Daten zu seiner Aufgabenerfüllung benötigt.

Das Gesundheitsamt würde in einem solchen Fall jedoch lediglich eine Beratung anbieten. Maßnahmen der Gesundheitsüberwachung kommen nicht in Betracht. Ob der Betroffene das Beratungsangebot annimmt oder nicht, bleibt ihm überlassen. Darauf weist das Gesundheitsamt in den Medien und besonderen Broschüren ausdrücklich hin. Bislang beabsichtigen die Gesundheitsämter nicht, die einzelnen Betroffenen anzusprechen. Die Übermittlung war daher nicht zur Aufgabenerfüllung des Gesundheitsamtes erforderlich. Die Polizei hätte den Betroffenen direkt auf das Beratungsangebot hinweisen können. Lediglich mit seiner Zustimmung hätte sie das Gesundheitsamt informieren dürfen.

Wenn Polizeidienststellen erfahren, daß eine Person Aids-infiziert ist, dürfen sie diese Information grundsätzlich nicht ohne Wissen und Wollen des Betroffenen an das Gesundheitsamt weitergeben.

Ich habe sowohl das Hessische Innenministerium als auch das Hessische Sozialministerium zur Stellungnahme aufgefordert. Das Sozialministerium hat mir mitgeteilt, daß auch nach seiner Ansicht die Gesundheitsämter nach den derzeitig geltenden Bestimmungen zu ihrer Aufgabenerfüllung eine namentliche Meldung von HIV-Infizierten nicht benötigen. Eine Rechtsgrundlage für die Übermittlung der Daten könne es ebenfalls nicht erkennen. Auch das Innenministerium hat die Erforderlichkeit verneint, hält aber dennoch die Datenübermittlung nicht für eindeutig rechtswidrig - eine äußerst widersprüchliche Argumentation. Die Aussagen der beiden Ministerien zur Erforderlichkeit lassen nur einen Schluß zu: Die Datenübermittlung war unzulässig.

6.1.4
Meldepflicht

6.1.4.1
Personenbezogene Meldepflicht

In meinem 15. Tätigkeitsbericht (Ziff. 4.4.1) bin ich ausführlich auf die Diskussion um die personenbezogene Meldepflicht eingegangen. Ich habe die Auffassung vertreten, daß eine solche Meldepflicht ein schwerer Eingriff in die Rechte der von der Aids-Infektion Betroffenen ist, deren Eignung zur Bekämpfung der Krankheit bisher in keiner Weise überzeugend dargetan wurde. Dies entsprach im Ergebnis der damals vorherrschenden Ansicht in der gesundheitspolitischen Diskussion. Hieran hat sich 1987 nichts geändert. In ihrer am 27. März 1987 gefaßten Entschließung zur Bekämpfung von Aids (abgedruckt in AIFO 1987, 341) hat sich die Gesundheitsministerkonferenz u.a. nochmals zur namentlichen Meldepflicht geäußert. Die Gesundheitsminister und -Senatoren sind nach wie vor mehrheitlich der Ansicht, daß Test, Beratungs- und soziale Hilfsangebote wirksamer die Krankheit eindämmen können als eine namentliche Meldepflicht. Lediglich Bayern hat in einem abweichenden Votum gefordert, daß Notwendigkeit und Zweckmäßigkeit einer namentlichen Meldepflicht laufend überprüft werden sollten.

Im August 1987 hat mir das Hessische Sozialministerium den von Bayern im Bundesrat eingebrachten Antrag zur Änderung des Bundesseuchengesetzes (Bundesrats-Drucks. 294/87) zur Stellungnahme übersandt. In dem Antrag war u.a. eine Verpflichtung der Ärzte vorgesehen, Patienten, die HIV-infiziert sind oder bei denen der Verdacht besteht, daß sie HIV-infiziert sind, unter bestimmten Voraussetzungen namentlich dem zuständigen Gesundheitsamt zu melden. In meiner Stellungnahme habe ich dem Sozialministerium mitgeteilt, daß meine Einwände gegen eine personenbezogene Meldepflicht auch für eine nur in bestimmten Situationen vorgesehene Meldepflicht gelten. In der Zwischenzeit ist der Antrag von allen übrigen Bundesländern abgelehnt worden.

6.1.4.2
Anonyme Meldepflicht für HIV-Bestätigungstests

Eine andere Meldepflicht ist jedoch im vergangenen Jahr eingeführt worden. Im September 1987 hat das Bundesgesundheitsministerium auf der Ermächtigungsgrundlage des § 7 Bundesseuchengesetz eine Verordnung über eine anonyme Berichtspflicht für positive HIV-Bestätigungstests erlassen (Laborberichtsverordnung). Die Verordnung verpflichtet die Labors, positive Aids-Tests in anonymisierter Form an das Bundesgesundheitsamt zu melden. Da diese Verordnung ohne Zustimmung des Bundesrates erlassen wurde, ist die Geltungsdauer gemäß § 7 Bundesseuchengesetz auf drei Monate beschränkt. Am 1. Januar 1988 soll eine inhaltsgleiche Verordnung mit Zustimmung des Bundesrates erlassen werden.

Vor dem Erlaß der Verordnung habe ich mehrfach gegenüber dem Hessischen Sozialministerium zur Frage der anonymen Meldung positiver HIV-Bestätigungstests Stellung genommen. Das Sozialministerium hatte mir zunächst ein Formular der Deutschen Gesellschaft für Viruserkrankungen (DVV) in Berlin, die in enger Verbindung zum Bundesgesundheitsamt steht, zur Stellungnahme übersandt. Mit diesem Formular sollten alle Labors, die HIV-Bestätigungstests durchführen, auf freiwilliger Basis in anonymisierter Form die positiven Testergebnisse an die DVV übersenden. Die Meldungen sollten eine präzisere Einschätzung der epidemiologischen Lage ermöglichen.

Ich habe von Anfang an betont, daß ich großes Verständnis für das Bestreben habe, umfassendere epidemiologische Daten über Aids- Infektionen zu erhalten, und gegen anonymisierte Meldungen aus datenschutzrechtlicher Sicht keine Bedenken bestehen. Allerdings müssen die Rahmenbedingungen für die Verarbeitung der geplanten Meldungen vorher umfassend geklärt und festgelegt werden, damit die Anonymität der Betroffenen sichergestellt und die Gefahr einer Reidentifizierung möglichst ausgeschlossen ist. Diese Voraussetzungen waren bei dem Vorhaben der DVV nicht gegeben. Weder war hinreichend geklärt, daß das Bundesgesundheitsamt die rechtlich verantwortliche datenverarbeitende Stelle ist - die DVV ist ein privater Verein - noch wie die zu meldenden Daten weiterverarbeitet werden sollten. Bei einer derartig sensiblenDatensammlung können solche Unklarheiten auf keinen Fall akzeptiert werden. Das Hessische Sozialministerium hielt aufgrund meiner Stellungnahme die Formulare der DVV in den hessischen Medizinaluntersuchungsstellen und Medizinal-Untersuchungsämtern zurück.

Im Juli 1987 hat mir das Sozialministerium dann einen Entwurf einer Verordnung des Bundesgesundheitsministeriums zur Einführung einer Laborberichtspflicht zur erneuten Stellungnahme übersandt. Dieser Entwurf sah für alle Stellen, die HIV-Bestätigungstests durchführen, eine Verpflichtung vor, über ihre Testergebnisse monatlich zu

berichten. Gemeldet werden sollte an das Bundesgesundheitsamt. Im übrigen waren der Zweck der Meldungen - die Beurteilung der epidemiologischen Lage - und die Angaben sowie die Einzelheiten des Verfahrens konkret festgelegt. Maßgebliche Rahmenbedingungen der Verarbeitung der Meldungen waren damit geklärt. Fragen blieben jedoch noch hinsichtlich des Umfangs der zu meldenden Daten. Die Labors sollten u.a. auch Daten über den jeweiligen Anlaß der Untersuchung, den möglichen Infektionsweg und das konkrete Krankheitsbild melden - Daten, die die Labors für die Tests nicht benötigen und die ihnen der Arzt daher auch nicht übermitteln darf. Zwar war in dem Entwurf der Zusatz enthalten, daß diese Daten nur gemeldet werden sollten, soweit sie dem zum Bericht Verpflichteten bekannt sind. Damit war jedoch nicht geklärt, wie die Labors diese Angaben überhaupt erfahren können. Unklar war auch, wie die Berichte in den Krankenhäusern erstellt werden sollten, denn die Berichtspflicht darf nicht dazu führen, daß Informationen über Aids-Infizierte und -Kranke im Krankenhaus verbreitet werden. Das Sozialministerium hat diese Bedenken geteilt und das Bundesgesundheitsministerium zur Klärung der offenen Fragen aufgefordert.

Die in Kraft getretene Laborberichtsverordnung gewährleistet zwar, das das Bundesgesundheitsamt ausreichend anonymisierte Daten erhält. Die Berichte dürfen weder die Namen der Betroffenen noch Namensbestandteile oder einen alphanumerischen Schlüssel zur Kennzeichnung der Betroffenen enthalten. Name und Anschrift des Berichtenden dürfen nicht in das Aids-Infektionsregister aufgenommen werden und sind nach Auswertung der Berichte durch das BGA zu löschen. Das Risiko einer Identifizierung der Betroffenen ist daher soweit wie möglich reduziert worden. Gegen die Meldungen bestehen daher keine datenschutzrechtlichen Einwände. Die Laborberichtsverordnung hat allerdings nicht die von mir bereits am Entwurf kritisierten Unklarheiten beseitigt.

6.2
Aktenaufbewahrung im Krankenhaus

Ein Vater benötigte dringend Informationen aus einer alten Krankenhausakte seines Kindes. Die Informationen waren für die Behandlung des Kindes in einem anderen Krankenhaus erforderlich. Als der Vater sich an mich wandte, hatte er zuvor bereits mehrfach vergeblich das Krankenhaus um Akteneinsicht gebeten. Das Krankenhaus hatte weder die Krankenakte zur Verfügung gestellt noch eine klare Auskunft erteilt, wo sich die Krankenakte befindet und wann und auf welche Weise er die benötigten Informationen erhalten kann.

Nach einem erfolglosen Versuch, die Angelegenheit kurzfristig telefonisch zu klären, habe ich mich schriftlich an die Klinik gewandt. Meine Überprüfung hat keine Anhaltspunkte dafür ergeben, daß die Krankenakte rechtswidrig verwendet wurde. Schließlich erhielt der Vater die benötigten Informationen - aber erst mehrere Wochen nach der ersten Anfrage.

Ein solcher Fall darf sich nicht wiederholen. Jeder Arzt ist grundsätzlich verpflichtet, Aufzeichnungen über die Behandlung seines Patienten anzufertigen. Die Pflicht besteht auch im Interesse des Patienten. Selbstverständlich müssen diese Aufzeichnungen verfügbar sein, zum einen deshalb, damit der Arzt seiner Verpflichtung zur kollegialen Zusammenarbeit nachkommen kann, zum andern aber auch, damit der Patient sein ihm nach der Rechtsprechung des Bundesgerichtshofs zustehendes Einsichtsrecht ausüben kann. Hier stand die Krankenakte mehr als drei Wochen lang nicht zur Verfügung, obwohl diese Akte dringend für eine Behandlung benötigt wurde. Da mir die Klinik keine genaue Auskunft darüber geben konnte oder wollte, warum die Akte nicht verfügbar war, habe ich im Juli 1987 von ihr organisatorische Maßnahmen verlangt, die sicherstellen, daß ähnliche Verzögerungen künftig nicht mehr vorkommen. Obgleich ich das Krankenhaus aufgefordert habe, mich über die getroffenen Maßnahmen zu informieren, ist eine Antwort bis heute nicht erfolgt.

7. Sozialverwaltung

7.1
Unterrichtung der Gemeinde über Sozialhilfebescheide

Mehrere Landkreise schickten regelmäßig Kopien der Sozialhilfebescheide an die Wohnsitzgemeinde des Sozialhilfeempfängers. Begründet wurde dies in der Regel damit, daß die Wohnsitzgemeinden eher in der Lage seien, die Angaben der Antragsteller auf ihre Richtigkeit hin zu überprüfen und damit Mißbrauch zu verhindern.

So verständlich das Bestreben der Landkreise ist, Mißbräuchen bei der Sozialhilfe entgegenzuwirken; die regelmäßige Weitergabe von Kopien von Sozialhilfebescheiden an die Wohnsitzgemeinden ist jedoch kein zulässiges Mittel. Leistungsträger dürfen Sozialhilfedaten nur an andere Stellen offenbaren, wenn das Sozialgesetzbuch dazu eine ausdrückliche Befugnis einräumt (§§ 67 ff. SGB X). Eine solche ist gemäß § 69 Abs. 1 Nr. 1 SGB X vorhanden, wenn die Weiterleitung der Bescheide zur Aufgabenerfüllung nach dem Bundessozialhilfegesetz erforderlich ist.

Örtliche Träger der Sozialhilfe sind in Hessen die kreisfreien Städte und die Landkreise. Unter bestimmten Voraussetzungen können die Kreise diese Aufgaben ganz oder teilweise den Gemeinden übertragen. Im Rahmen der übertragenen Aufgaben können diese Gemeinden selbständig entscheiden, sie erstellen selbst die Bescheide. Eine allgemeine Überprüfung der Richtigkeit der Angaben von Antragstellern durch die Wohnsitzgemeinde, auch wenn diese den Antrag entgegennimmt und an den sachlich und örtlich zuständigen Träger zur Entscheidung weiterleitet,

sieht das Sozialhilferecht dagegen nicht vor. Im Einzelfall kann eine solche Überprüfung gerechtfertigt sein, aber auch dann ist es nicht erforderlich, der Gemeinde zu Kontrollzwecken den Bewilligungsbescheid mit allen Daten zu übermitteln. Ich habe sowohl die betroffenen Landkreise als auch den Hessischen Landkreistag darauf hingewiesen, daß Kopien von Sozialhilfebescheiden nicht an die Wohnsitzgemeinde weitergegeben werden dürfen.

7.2
Organisations- und Wirtschaftlichkeitsuntersuchungen im Sozialamt

Aufgrund eines Beschlusses der Stadtverordnetenversammlung beauftragte der Magistrat einen unabhängigen Prüfer mit einem Organisations- und Strukturgutachten über das städtische Sozialamt. Untersucht werden sollte neben der Zweckmäßigkeit der Sachgebietseinteilung die Personalstruktur einschließlich der Qualifikation der Mitarbeiter. Darüber hinaus sollten die Sozialhilfeakten materiell-rechtlich überprüft werden, um zu klären, ob entsprechend dem Grundsatz des „Nachrangs der Sozialhilfe" alle Kostenerstattungsansprüche gegen andere Sozialleistungsträger bzw. gegenüber Dritten geltend gemacht worden waren. Der Prüfer arbeitete eng mit demRechnungsprüfungsamt zusammen. Er konnte in den Räumen des Sozialamtes die Akten unbeschränkt einsehen. In seinem Abschlußbericht waren ausführlich Einzelfallprüfungen beschrieben, wobei jeweils Name, Geburtsdatum und Aktenzeichen genannt wurden. Der Anhang enthielt eine Aufstellung aller geprüften Akten mit Aktenzeichen und Namen. Den Bericht erhielten das Rechnungsprüfungsamt, der Stadtkämmerer sowie der Sozialdezernent.

7.2.1
Datenschutzrechtliche Anforderungen an Organisationsuntersuchungen

Bei Organisationsuntersuchungen wie auch bei materiell-rechtlichen Überprüfungen der Arbeit des Sozialamtes sind die Vorschriften des Sozialdatenschutzes zu beachten. Eine Weitergabe von Sozialdaten ist ohne Einwilligung der Betroffenen nur zulässig, soweit das Sozialgesetzbuch eine ausdrückliche Offenbarungsbefugnis gibt (§§ 68 bis 77 SGB X). Eine solche Befugnis besteht z.B. dann, wenn die Offenbarung zur Aufgabenerfüllung des Sozialamtes erforderlich ist (§ 69 Abs. 1 Nr. 1 SGB X). Organisationsuntersuchungen zu Zwecken der Behördenorganisation gehören nicht zu den Aufgaben, die das Sozialamt nach dem Sozialgesetzbuch hat. Zur gesetzlichen Aufgabenerfüllung kann allerdings im Einzelfall eine inhaltliche Überprüfung der Sozialhilfeakten erforderlich sein, z.B. wenn Anhaltspunkte für eine fehlerhafte Entscheidung oder Regreßansprüche bestehen. Einzelfallprüfungen waren jedoch nicht das Ziel der Untersuchung. Die fehlende Offenbarungsbefugnis konnte auch nicht dadurch kompensiert werden, daß mit dem Prüfer eine zeitweilige arbeitsrechtliche Eingliederung in die Stadtverwaltung vereinbart wurde.

Der Prüfer hätte daher nur anonymisierte Aktenteile, auszugsweise Kopien und ähnliches einsehen dürfen. Außerdem war auch die Weitergabe des Berichtes in dieser Form unzulässig, da auch für die Bekanntgabe der im Bericht enthaltenen Sozialdaten an das Rechnungsprüfungsamt und den Kämmerer keine Offenbarungsbefugnis bestand.

Bei solchen Organisationsuntersuchungen sind darüber hinaus auch die datenschutzrechtlichen Interessen der Beschäftigten im Sozialamt zu berücksichtigen. Gemäß § 34 Abs. 1 Hessisches Datenschutzgesetz ist die Verarbeitung von Beschäftigtendaten nur zulässig, soweit dies zur Durchführung des Dienstverhältnisses erforderlich ist. Ziel der Untersuchung war eine Analyse der Struktur und Organisation des Sozialamtes. Dazu ist es jedoch nicht erforderlich, bei den zu untersuchenden Vorgängen zu wissen, welche Mitarbeiter einen bestimmten Arbeitsschritt erledigt haben, sondern lediglich, in welcher Funktion oder zu welchem Zeitpunkt jeweils ein Arbeitsschritt von einem Mitarbeiter ausgeführt wurde. Auch deshalb war die unbeschränkte Einsicht in die Akten durch den Prüfer unzulässig.

Die Folge war, daß in den Berichtsexemplaren für das Rechnungsprüfungsamt und den Kämmerer der Personenbezug der Daten beseitigt werden mußte und das Gemeindeparlament folglich nur einen Bericht mit anonymen Daten einsehen konnte.

7.2.2
Mitwirkung des Rechnungsprüfungsamtes bei Analysen von Akten des Sozialamtes

In diesem Zusammenhang stellte sich auch die Frage, welche Einsichtsrechte das Rechnungsprüfungsamt, insbesondere bei Organisationsuntersuchungen oder im Rahmen von speziellen Prüfaufträgen hat. Für alle Bereiche der Gemeindeverwaltung und damit auch für die Sozialverwaltung gehört die ordnungsgemäße Haushaltsführung zu den gesetzlichen Aufgaben (§ 92 Abs. 2 Hessische Gemeindeordnung). Die HGO hat die Kontrolle der zweckmäßigen und wirtschaftlichen Haushaltsführung dem Rechnungsprüfungsamt übertragen (§ 131 Abs. 1 Nr. 6). Das Rechnungsprüfungsamt hat somit im Bereich der Sozialverwaltung die gesetzliche Aufgabe der Haushaltskontrolle und daher gemäß § 69 Abs. 1 Ziff. 1 SGB X Zugang zu allen Sozialdaten, die zur Erfüllung dieser Aufgabe erforderlich sind. Daraus folgt aber nicht, daß das Rechnungsprüfungsamt jederzeit für alle seine Tätigkeiten Einblick in Sozialakten nehmen kann. Auch wenn die Gemeindevertretung das Rechnungsprüfungsamt mit einer konkreten Prüfung beauftragt (§ 130 Abs. 2 HGO), hat es Zugang zu Sozialdaten nur, wenn die Prüfung als Erfüllung einer gesetzlichen Aufgabe im Sinne des Sozialgesetzbuches einzuordnen ist. Die Behördenorganisation zu überprüfen, gehört aber nicht zu den Aufgaben nach dem Sozialgesetzbuch. Die Berichte des Rechnungsprüfungsamtes dürfen zudem nur in dem Maße personenbezogen Daten enthalten, als dies für die Beurteilung des Berichts und die daraus abzuleitenden Maßnahmen erforderlich ist.

7.3
EG-Butter für Kälteopfer

Der EG-Ministerrat hatte im Winter 1986/87 beschlossen, daß aus den Überschußlagern der Europäischen Gemeinschaft Lebensmittel kostenlos durch karitative Organisationen an solche Personen verteilt werden sollten, die besonders von der strengen Kälte betroffen waren. Im Vorfeld der Aktion wollten verschiedene Sozialämter wissen, in welcher Form sie bei der Organisation der Verteilung mitwirken könnten, ohne gegen datenschutzrechtliche Bestimmungen zu verstoßen. Der Personenkreis, der die Lebensmittel erhalten sollte, war nicht klar bestimmt. Die verteilenden Organisationen brauchten deshalb zum einen Anhaltspunkte, wer zum Empfang der Waren berechtigt sein könnte und zum andern galt es, eine Möglichkeit zu finden, diesen Personenkreis möglichst umfassend über die geplante Aktion zu informieren.

Alle Angaben über Personen, die aufgrund sozialer Notlagen vom Sozialamt betreut werden, unterliegen dem Sozialgeheimnis. Das Sozialamt darf den Wohlfahrtsverbänden nur Adressen von Sozialhilfeempfängern mitteilen, wenn es dazu nach dem Sozialgesetzbuch (§§ 67 ff SGB X) befugt ist. Dies wäre hier nur dann der Fall gewesen, wenn die Unterstützung der Verteilaktion zur Aufgabenerfüllung des Sozialamtes erforderlich war. Die EG-Aktion war aber keine Leistung der Sozialhilfe, sondern eine Aufgabe der allgemeinen, dem Staat obliegenden Daseinsvorsorge und daher eine Offenbarungsbefugnis nicht gegeben.

Zusammen mit den Sozialämtern habe ich verschiedene Möglichkeiten entwickelt, die Wohlfahrtsverbände bei Ihrer Arbeit zu unterstützen:

- Das Sozialamt teilt den Sozialhilfeempfängern mit, wo sie die Waren abholen können und wer beim Transport behilflich ist. Dem Schreiben kann ein Abschnitt beigefügt sein, der zur Kontrolle bei der Ausgabestelle abgeliefert wird.

- Es wird durch die Presse bekannt gemacht, wo die Waren abzuholen sind. Gegebenenfalls ist eine Kontrolle der Sozialhilfebescheide durch die Ausgabestelle möglich, um Doppelabholung zu vermeiden. Die Ausgabestellen sollten nicht notieren, wer Waren erhalten hat; wenn doch, dürfen die Unterlagen nicht für andere Zwecke verwendet werden und sind nach Beendigung der Aktion zu vernichten. Die Mitarbeiter der Ausgabestellen sind auf die Vorschriften des Datenschutzes hinzuweisen.

Um Beeinträchtigungen der Empfänger zu vermeiden und den Aufwand gering zu halten, haben viele Organisationen auf eine Kontrolle der Bezugsberechtigung verzichtet. Im Verlauf der Verteilaktion wurden jedoch verschiedene Fälle bekannt, in denen Sozialämter offensichtlich doch Adressen weitergegeben hatten. Ich habe die betroffenen Stellen auf die Rechtswidrigkeit hingewiesen. In diesen Fällen wurde daraufhin sichergestellt, daß nach Abschluß der Aktion keine personenbezogenen Daten über die Empfänger mehr bei den freien Trägern verblieben sind. Für den Winter 1987/88 hat die EG-Kommission eine Wiederholung der Aktion angeregt. Ich gehe davon aus, daß nunmehr landesweit nach den o.g. Grundsätzen verfahren wird.

8. Personaldatenverarbeitung

Mit § 34 des neuen Hessischen Datenschutzgesetzes hat der Gesetzgeber die Verarbeitung von Personaldaten im hessischen öffentlichen Dienst erstmals weitreichend bereichsspezifisch geregelt. Die hessischen Behörden müssen nunmehr bei der Personaldatenverarbeitung eine ganze Reihe neuer Bedingungen beachten. Das betrifft z.B. die Weitergabe von Personaldaten an Privatpersonen (§ 34 Abs. 2), die Einführung und Veränderung automatisierter Verfahren zur Verarbeitung von Daten der Beschäftigten (§ 34 Abs. 5 und 8) oder die automatisierte Verarbeitung dienst- und arbeitsrechtlicher Beurteilungen sowie medizinischer und psychologischer Befunde (§ 34 Abs. 6).

8.1
Veröffentlichung von Personalnachrichten im hessischen Staatsanzeiger

Der gemeinsame Runderlaß der obersten Landesbehörden über die Veröffentlichung der Personalnachrichten im Staatsanzeiger (Erlaß vom 23. August 1982, StAnz. S. 1651, zuletzt geändert durch Erlaß vom 6. Februar 1986, StAnz. S. 383) verpflichtet die Personalabteilungen der Behörden und Dienststellen, Personalveränderungen bei den Landesbeamten im Staatsanzeiger zu veröffentlichen, soweit dies nicht in besonderen Amtsblättern zu geschehen hat. Mit Namen und Amtsbezeichnung des Betroffenen sind bekanntzugeben: Ernennungen (einschließlich Beförderungen), Berufungen in das Beamtenverhältnis auf Lebenszeit, Versetzungen von und zu anderen Dienstherren, Eintritt in den Ruhestand, Versetzungen in den Ruhestand, Entlassungen und Sterbefälle. Scheidet der Beamte aus dem Dienst aus, ist der Zeitpunkt anzugeben und kann auf die gesetzliche Grundlage hingewiesen werden.

Diese Veröffentlichungspraxis ist mit dem neuen Hessischen Datenschutzgesetz nur eingeschränkt vereinbar. Nach § 34 Abs. 2 HDSG dürfen Daten von Beschäftigten an Personen und Stellen außerhalb des öffentlichen Bereichs nur übermittelt werden, wenn der Empfänger ein rechtliches Interesse darlegt, der Dienstverkehr es erfordert oder der Betroffene eingewilligt hat. Damit die öffentliche Verwaltung für den Bürger transparent wird, ist es sicherlich auch grundsätzlich notwendig, Personalveränderungen im Staatsanzeiger zu veröffentlichen. Zur Transparenz trägt jedoch

nicht bei, wenn die Gründe veröffentlicht werden, aus denen ein Beamter aus dem Dienst scheidet. Ich habe deshalb das Innenministerium aufgefordert, auf die Veröffentlichung der Gründe für das Ausscheiden zu verzichten.

Der Antwort des Innenministeriums zufolge sollen jedoch zunächst lediglich die Angaben über die Gründe auf die drei Merkmale Ruhestand, Tod und sonstige Gründe reduziert werden. Dies ist keineswegs ausreichend, denn auch für die reduzierten Angaben gibt es keine Rechtsgrundlage. Darauf habe ich das Innenministerium hingewiesen.

8.2
Automatisierte Verarbeitung von Beschäftigtendaten

8.2.1
Präventive Kontrolle durch den Hessischen Datenschutzbeauftragten

Wegen der besonderen Schutzwürdigkeit der Beschäftigtendaten hat der Gesetzgeber für deren automatisierte Verarbeitung im neuen HDSG eine präventive Kontrolle durch den Hessischen Datenschutzbeauftragten angeordnet. Eine automatisierte Verarbeitung von Personaldaten darf erst eingeführt oder geändert werden, wenn dem Hessischen Datenschutzbeauftragten zuvor die im HDSG inhaltlich festgelegte Beschreibung der Dateien zur Stellungnahme vorgelegt worden ist (§ 35 Abs. 5 HDSG).

Viele Stellen wissen offensichtlich nicht oder nicht genau, in welchen Fällen dies zu geschehen hat. Automatisierte Personaldatenverarbeitung kann unterschiedlichste Inhalte haben und in vielfältiger Form erfolgen. Hierzu gehören nicht nur die sogenannten Personalinformationssysteme oder Personalabrechnungsverfahren. Einbezogen sind alle automatisierten Verfahren, die personenbezogene oder personenbeziehbare Daten von Beschäftigten verarbeiten. Dies sind unter anderem auch Personaldateien wie Urlaubs-, Krankheits- oder Abwesenheitsdateien, Gebührenabrechnungsverfahren für Telefongespräche, Zeiterfassungssysteme, Zugangskontrollsysteme, Verfahren für Organisationsuntersuchungen oder Verfahren für Stellenpläne. In allen Fällen müssen die Dateien vorgelegt werden.

Oft reichen die zur Verfügung gestellten Unterlagen für eine Prüfung nicht aus. In vielen Fällen fehlt bereits ein Konzept, welche Daten und welche Auswertungen zur Aufgabenerfüllung erforderlich sind, und welche notwendigen Datenschutz- und Datensicherungsmaßnahmen daraus folgen müssen. Das ist um so weniger verständlich, als die erforderlichen Angaben gesetzlich bestimmt sind (§ 6 Abs. 1 HDSG). Schwerpunkte sollten sein: Datenkatalog, Auswertungen, Zugriff auf Auswertungen und Behandlung von Ausdrucken, Schutz vor unberechtigten Zugriffen und Zugang zu den Geräten. Ausgangspunkt muß naturgemäß immer die beim jeweiligen Anwender geplante Verfahrensausgestaltung sein. Es genügt nicht, Werbeprospekte, Herstellerangebote oder etwa eine Verfahrensbeschreibung eines Kommunalen Gebietsrechenzentrums vorzulegen.

Die Beteiligung des Hessischen Datenschutzbeauftragten nach § 34 Abs. 5 HDSG ersetzt allerdings nicht - wie häufig angenommen - die Meldung der Dateien zum Dateienregister. Letztere muß vielmehr gesondert erfolgen.

8.2.2
Hessisches Personalinformationssystem - HEPIS

Unmittelbar betroffen durch die Novellierung des HDSG ist das vom Hessischen Landespersonalamt betreute Hessische Personalinformationssystem - HEPIS. Dieses besteht aus einem Programmpaket, mit dem aus den Besoldungs- und Vergütungsdaten der hessischen Landesbediensteten umfangreiches statistisches Material erstellt wird. Auf Anforderung der Ressorts werden auch bestimmte personenbezogene Sonderauswertungen geliefert. Das aus HEPIS gewonnene Zahlenmaterial dient in erster Linie der genaueren Kenntnis der Personalstruktur sowie der Personalbedarfsplanung. Das Landespersonalamt erfüllt damit seine Aufgaben gem. § 111 Hessisches Beamtengesetz „Untersuchungen über das Personalwesen anzustellen und der Landesregierung und der Landespersonalkommission zu berichten". Beschäftigungsdaten dürfen zu Zwecken der Personalplanung - darum handelt es sich hier - verarbeitet werden (§ 34 Abs. 8 HDSG). Mit dieser Vorschrift wollte der Gesetzgeber gerade auch für den Betrieb von HEPIS eine Rechtsgrundlage schaffen. Die Verarbeitung von Beschäftigtendaten zu Planungszwecken knüpft das Gesetz jedoch an besondere Voraussetzungen (§§ 34 Abs. 8, 32). Die Daten sollen von der übrigen Verwaltung personell und organisatorisch getrennt verarbeitet werden. Das hat zur Folge, daß aus dem Bestand der HEPIS-Dateien keine Auswertungen für Zwecke des Verwaltungsvollzuges gemacht werden dürfen. Hierzu gehören auf jeden Fall namensbezogene Auswertungen, wie sie zur Zeit z.B. zur Vorbereitung von Personalratswahlen oder als Geburtstags- und Jubiläumslisten erfolgen. Sobald die Planungsaufgabe dies erlaubt, müssen die personenbezogenen Daten so verändert werden, daß sie keine bestimmte Person mehr erkennen lassen. Die Probleme im Zusammenhang mit HEPIS sind noch keineswegs alle abschließend gelöst. Zu prüfen bleibt insbesondere noch, welche Daten der Beschäftigten für die durchzuführenden Untersuchungen erforderlich sind, und ggf. auch, zu welchem Zeitpunkt einzelne Daten zu verändern oder zu löschen sind. Hierzu habe ich das Landespersonalamt zur Stellungnahme aufgefordert, eine Antwort liegt noch nicht vor.

8.3
Automatisierte Textverarbeitung bei dienstrechtlichen Beurteilungen

Beurteilungen und Zeugnisse werden häufig mit Hilfe von Textverarbeitungsprogrammen/Textsystemen geschrieben. Das neue HDSG verbietet die automatisierte Verarbeitung von medizinischen Befunden sowie dienst- und

arbeitsrechtlichen Beurteilungen (§ 34 Abs. 6 HDSG). Auch das automatisierte Speichern von Texten ist zweifellos Verarbeitung im Sinne des HDSG. Ziel des Verbots war jedoch, eine Beeinträchtigung der Interessen der Bediensteten zu verhindern, die dadurch eintreten kann, daß die Daten aus ihrem Kontext herausgelöst und anderweitig verknüpft werden. Diese Gefahr besteht dagegen nicht, soweit Textverarbeitungsprogramme lediglich genutzt werden, um nicht bei jeder Änderung den Gesamttext neu schreiben zu müssen. Gegen die Verwendung automatisierter Textverarbeitungsprogramme bestehen dann keine Bedenken, wenn die einzelne dienstrechtliche Beurteilung jeweils nur so lange gespeichert bleibt, bis der verantwortliche Vorgesetzte den Text abgezeichnet hat. Nachdem die endgültige Fassung ausgedruckt ist, müssen alle Datenbestände, die während der Anfertigung entstanden sind, gelöscht werden.

9. Sicherheitsbehörden

9.1
Aufbewahrungsfristen für Kriminalakten der hessischen Polizei

9.1.1
„KpS-Richtlinien"

Hat die Polizei ein Ermittlungsverfahren abgeschlossen, benötigt sie i.d.R. die in der Akte über den Beschuldigten enthaltenen Informationen nicht mehr. Es fragt sich daher, was mit der Akte geschehen soll. Hinweise hierzu kann die Polizei den vom Hessischen Innenministerium erlassenen „Richtlinien für die Führung Kriminalpolizeilicher personenbezogener Sammlungen" (KpS- Richtlinien, StAnz. 1981, S. 881) entnehmen. Danach ist für jede Akte eine Aufbewahrungsdauer festzulegen, wobei abzuwägen ist zwischen dem öffentlichen Interesse, „zu Zwecken der Strafverfolgung, Strafvollstreckung oder Gefahrenabwehr auf polizeiliche Erkenntnisse zurückgreifen zu können" und dem grundrechtlich „geschützten Interesse des einzelnen, solchen Einwirkungen der öffentlichen Gewalt nicht ausgesetzt zu sein" (Nr. 5.1 der Richtlinien). Nach 10 Jahren sind die Unterlagen regelmäßig auszusondern, wenn in dieser Zeit keine weiteren Erkenntnisse über den Betroffenen in die KpS aufgenommen worden sind. Für Fälle von „geringerer Bedeutung", nach der Definition des Landeskriminalamtes gehören dazu bespielsweise leichte vorsätzliche Körperverletzung, Ladendiebstahl, Beleidigung oder Sachbeschädigung, sehen die KpS-Richtlinien eine grundsätzliche Aussonderungsfrist von 3 Jahren vor. Laufen die Fristen ab, werden die Angaben jedoch keineswegs automatisch gelöscht; genaugenommen handelt es sich vielmehr um „Wiedervorlage-Fristen", d.h. die Polizei hat zu prüfen, ob die Unterlagen weiterhin aufbewahrt werden müssen.

9.1.2
Aussonderungspraxis

9.1.2.1
LKA-Statistik

Zur Überprüfung der Aussonderungspraxis der hessischen Polizeidienststellen habe ich mir Anfang 1987 vom Landeskriminalamt eine Statistik darüber vorlegen lassen, wie häufig die einzelnen Dienststellen bei Datenspeicherungen im Hessischen Polizeiinformationssystem HEPOLIS eine Aussonderungsprüfung für 1995 verfügt haben. Das Stichjahr 1995 wurde gewählt, um möglichst nur 10jährige Fristen zu erfassen. Die Zahlen für die einzelnen Polizeidienststellen im Verhältnis zur Einwohnerzahl des Zuständigkeitsbereichs ergaben ein erstaunliches Bild: Während einige Polizeidienststellen jeden 91., 143. oder 154. Einwohner mit einer 10jährigen Speicherungsdauer registriert hatten, waren es bei anderen nur jeder 411., 477. oder gar nur 587. Einwohner. Die Zahlen korrelierten nicht mit der absoluten Einwohnerzahl und ließen auch keine regionalen Besonderheiten erkennen. Da auch sonst kein Grund für die unterschiedliche Verfahrensweise ersichtlich war, lag die Vermutung nahe, daß in den verschiedenen Polizeidienststellen gleiche Sachverhalte unterschiedlich bewertet worden waren.

9.1.2.2
Überprüfung einzelner Polizeidienststellen

Um den Grund für die unterschiedlichen Verfahrensweisen festzustellen, habe ich zwei Polizeidienststellen, die relativ selten und zwei, die verhältnismäßig oft eine 10jährige Speicherungsdauer verfügt hatten, überprüft. Zur Kontrolle wurde außerdem eine Dienststelle mit mittlerer Fallzahl überprüft.

Dabei stellte sich heraus, daß die beiden Polizeidienststellen mit vergleichsweise geringer Zahl 10jähriger Speicherungen ein eigenes Verfahren festgelegt hatten: Nur Fälle von Schwerkriminalität (Mord, Raub, Sexualverbrechen usw.) erhielten eine 10jährige Aussonderungsprüffrist. Die 3jährige Frist wurde nicht nur in den vom LKA beispielhaft definierten Fällen mit „geringerer Bedeutung" verfügt, sondern z.B. auch bei Einbruch und Betrug. Schließlich erfolgte bei „mittlerer Kriminalität" keine 10- sondern eine 5jährige Speicherung. Die Polizeidienststellen mit einer hohen Zahl 10jähriger Prüffristen verfuhren genau entgegengesetzt. Mit 3jähriger Frist speicherten sie nur die Fälle, die das LKA - allerdings nur beispielhaft - als Bagatellfälle eingestuft hat, alle übrigen, d.h. ca. 90 v. H., erhielten ohne besondere Abwägung eine Frist von 10 Jahren. Die Dienststelle mit mittlerer Fallzahl war Mitte 1986 von ihrem differenzierten System ebenfalls zu diesem Verfahren übergegangen.

Die Überprüfung von ca. 40 bis 50 Kriminalakten pro Dienststelle ergab außerdem, daß 4 Stellen die Fälle oft falsch eingeordnet hatten. So waren z.B. ein Ladendiebstahl und das Umetikettieren von Waren in einem Supermarkt - in beiden Fällen weniger als 10,00 DM Schaden - jeweils mit 10jährigen Aussonderungsfristen in HEPOLIS gespeichert worden. In den meisten Fällen haben die Dienststellen auf meine Beanstandung hin entweder die Daten gelöscht oder die Aufbewahrungsfrist verringert.

9.1.3
Änderung der KpS-Richtlinien

Auf meine Prüfergebnisse hat das LKA Mitte letzten Jahres reagiert und von allen Kriminaldienststellen verlangt, bei der Festlegung der Fristen seinen Katalog für Bagatelldelikte strikt anzuwenden und auf zusätzliche Abwägungen zu verzichten.

Sicherlich kann nicht hingenommen werden, daß die Polizeidienststellen gleiche Sachverhalte unterschiedlich behandeln. Die Vorgehensweise des LKA ist jedoch keine angemessene Lösung. Alle von mir überprüften Dienststellen haben die Fristenvorgaben der KpS-Richtlinien als zu unflexibel empfunden. Keine hat es für erforderlich gehalten, sämtliche nicht im LKA-Katalog als Bagatellfälle eingestuften Fälle 10 Jahre zu speichern. Die Prüfergebnisse lassen nur eine Konsequenz zu: Die KpS-Richtlinien müssen umgehend geändert werden.

Zugegeben, es ist nicht einfach, ein differenziertes System für Aussonderungsprüffristen zu entwickeln. Wenig hilfreich wäre z.B. ein Katalog mit fester Speicherungsdauer für jedes Delikt, denn bei den einzelnen Straftaten kann es sich um einen schweren, mittleren oder unbedeutenden Fall handeln. Überlegenswert wäre dagegen ein Deliktskatalog mit Rahmenfristen für besonders schwere Straftaten wie Mord, Raub usw. und einer höchstens 3jährigen Frist für Bagatelldelikte. Die detaillierte Festlegung des Fristensystems ist letztlich Sache der Kriminalisten.

In jedem Fall sollte aber für die Vielzahl der Fälle, die nicht der Schwerkriminalität zugeordnet werden können oder eindeutig als Fälle von geringerer Bedeutung einzustufen sind, eine Regelspeicherungsdauer von fünf Jahren festgelegt werden. Natürlich können bestimmte Faktoren eine längere Speicherungsdauer erforderlich erscheinen lassen, wie z.B. besondere kriminelle Energie, große Wiederholungsgefahr, ein hoher Schaden oder auch eine besondere Brutalität bei der Tatausführung. Andererseits können einzelne Faktoren dazu führen, eine kürzere Speicherungsdauer festzulegen, etwa bei Ersttätern oder einem geringen Schaden. Die Speicherungsdauer von fünf Jahren könnte in diesen Fällen möglicherweise auf drei Jahre reduziert werden.

Kürzere Aussonderungsfristen hätten auch Vorteile für die Polizei, denn das bedeutet, daß die Vernichtung der Unterlagen zu einem früheren Zeitpunkt geprüft wird. Dadurch werden überflüssige Aktenbestände frühzeitig ausgesondert und die Aktenverwaltung erleichtert.

9.2
Prüfung des polizeilichen Informationssystems APIS

Seit dem 2. Januar 1986 wird beim Bundeskriminalamt die „Arbeitsdatei PIOS - Innere Sicherheit" (APIS) geführt. Die Daten dieser Verbunddatei stammen von den Landeskriminalämtern und dem BKA; alle beteiligten Stellen können unmittelbar auf den gesamten Datenbestand zugreifen. Gespeichert werden ausschließlich Angaben aus dem Bereich des „polizeilichen Staatsschutzes". Die Informationen stehen nur den entsprechenden Fachabteilungen der Kriminalämter zur Verfügung. Besonderheit des Systems: Im Unterschied zu den traditionellen Aktennachweissystemen wie der Personendatei des Hessischen Polizeiinformationssystems HEPOLIS oder dem bundesweiten Kriminalaktennachweis (KAN) werden in APIS zu Ermittlungszwecken vor allem Daten aufgenommen, die noch nicht abschließend überprüft worden sind.

APIS habe ich bereits vor der Einführung kritisiert (vgl. 12. Tätigkeitsbericht, Ziff. 2.1.3.2 und 14. Tätigkeitsbericht, Ziff. 13.1.7). Wie berechtigt die Kritik ist, hat inzwischen auch eine Kontrolle der Speicherungspraxis bestätigt. Im vergangenen Jahr habe ich beim Landeskriminalamt die in einem bestimmten Zeitraum eingegebenen Datensätze sowie alle Informationen, die unter dem Stichwort „Volkszählung" bis zu einem bestimmten Tag eingespeichert worden waren, überprüft.

9.2.1
Speicherungsverfahren

Vor der langfristigen Speicherung in APIS werden die gemeldeten Daten in einem abgestuften Verfahren kontrolliert. Das Landeskriminalamt überprüft die Angaben, die es von den Dienststellen erhält und speichert sie im Regelfall mit einer 3monatigen „Aussonderungsprüffrist" in das System ein. Bestätigt die Dienststelle, die die Information an das LKA gegeben hat, innerhalb der Frist, daß die Daten überprüft worden sind und sich als zutreffend erwiesen haben, bleiben sie gespeichert. Kann die Dienststelle die Richtigkeit nicht innerhalb der 3 Monate bestätigen oder hält sie die Speicherung nicht mehr für erforderlich, werden die Daten gelöscht. Gleiches geschieht, wenn sie sich nicht äußert. Damit sind die längerfristig gespeicherten Angaben zwar noch nicht abschließend, aber doch mehrmals in zeitlichem Abstand überprüft worden, so daß immerhin ein höherer Grad an Zuverlässigkeit erreicht wird.

Abfragen aus dem Informationssystem werden grundsätzlich nicht protokolliert. Lediglich Eingaben, Veränderungen und Löschungen können deshalb noch nach einer gewissen Zeit einem Verantwortlichen zugeordnet werden. Die Erfahrungen mit dem System HEPOLIS haben ergeben, daß es durchaus sinnvoll ist, auch die Abfragen zu protokollieren. Nur auf diese Weise kann im Einzelfall festgestellt werden, ob und wenn ja von wem Informationen aus dem System abgerufen wurden. Da hierfür maschinentechnische Änderungen erforderlich sind, habe ich dem Hessischen Innenministerium vorgeschlagen, beim BKA als der für die technische Betreuung des Systems verantwortlichen Stelle eine entsprechende Änderung des Systems zu beantragen.

9.2.2
Gespeicherte Daten

Nicht zu beanstanden war die Speicherung der Daten über mögliche Opfer von Staatsschutzdelikten. Gleiches gilt für die schweren Fälle aus der Terrorismusbekämpfung. Die Datei enthält jedoch außerdem eine Vielzahl von Bagatellstraftaten; lediglich die Motivation der Täter war hier Ursache für die Speicherung. Wenn ein Schüler allgemeinpolitische Parolen auf die Schulwand sprüht oder jemand Wahlplakate beschädigt, gehört dies nicht in einer Datei wie APIS registriert. Allerdings läßt der Wortlaut von Ziff. 2.1.10 der Errichtungsanordnung für APIS genau das zu, denn danach können auch allgemeine Straftaten registriert werden, die wegen des Motivs des Täters, seiner Verbindung zu bestimmten Organisationen oder wegen des Objekts der Tat als „Staatsschutzdelikte" anzusehen sind.

Aber auch Delikte, die im Strafgesetzbuch als Staatsschutzdelikte bezeichnet werden, sollten nicht in jedem Fall in APIS gespeichert werden. So führte in einem Fall die Verwendung eines rechtsradikalen Symbols in der Öffentlichkeit ohne erkennbare Verbindung zu einer entsprechenden Organisation als „Verwenden von Kennzeichen verfassungswidriger Organisationen" (§ 86a StGB) zu einer Registrierung in APIS. In diesem Fall ging es nach meinen Informationen jedoch eher um die Geltungssucht eines einzelnen als um eine echte Gefährdung staatlicher Belange.

Die Prüfung der unter dem Stichwort „Volkszählung" gespeicherten Datensätze ergab das gleiche Resultat. Nach meinem Eindruck entwickelt sich das System APIS vornehmlich zu einem Register politisch motivierter Straftaten von geringer Bedeutung. Die bei der Einführung des Systems geäußerte Kritik, das für die Terrorismusbekämpfung entwickelte Informationssystem PIOS-TE würde durch APIS mit allgemeinen Staatsschutzdaten gekoppelt, die eine wesentlich einfachere, die Einführung eines solchen Systems nicht rechtfertigende Deliktsstruktur aufweisen, ist damit bestätigt. APIS ist ein vielschichtiges Erfassungs- und Auswertungssystem, in dem Informationszusammenhänge aus einer großen Anzahl komplex gespeicherter Informationen herausgefiltert werden sollen. Mit anderen Worten: Sinn eines solchen Spuren- bzw. Hinweisdokumentationssystems ist es, komplexe Tatstrukturen und Verknüpfungen von Tätern so zu speichern, daß über Auswertungsläufe Zusammenhänge aufgedeckt werden können. Aus datenschutzrechtlicher Sicht ist die im Regelfall unzulässige Speicherung personenbezogener Daten aus dem Tat- und Täterumfeld, insbesondere auch die Erfassung von noch nicht abschließend überprüften Informationen über eine Vielzahl von Personen auch aus dem Kontaktbereich von Verdächtigen, lediglich dann gerechtfertigt, wenn auf diesem Weg eine Aufklärung von schwerwiegenden Taten erreicht werden kann. Das trifft für eine große Zahl der gespeicherten Datensätze nicht zu. Es ist vielmehr zu befürchten, daß in Kürze APIS ebenso wie das alte Informationssystem PIOS wegen der Masse irrelevanter Informationen nicht mehr sinnvoll eingesetzt werden kann.

Es überzeugt auch nicht, die Bagatellfälle deshalb zu speichern, weil es sich möglicherweise in einem Einzelfall um den Beginn einer Täterkarriere im Staatsschutzbereich handeln kann. Die Delikte werden nach Abschluß der Ermittlungen in den traditionellen Polizeidateien - wie HEPOLIS - gespeichert. Diese Informationen können jederzeit abgerufen werden. Auch die regionalen und überregionalen Kriminalaktennachweissysteme sind geradezu auf Karrieretäter ausgerichtet. Demgegenüber enthielten die von mir überprüften Fälle in der Mehrzahl keine Tatstrukturen, die komplexe „modus operandi"-Untersuchungen nahelegten, um etwa Serientäter mit spezifischem Tatvorgehen oder einer hohen kriminellen Energie festzustellen. Es handelte sich zumeist auch nicht um Fälle, die eine unmittelbare Gefahr für besonders schützenswerte Rechtsgüter erkennen ließen.

Am 26. Januar 1988 hat sich der Unterausschuß Informationsverarbeitung und Datenschutz des Hessischen Landtags intensiv mit der Speicherung von Daten im Zusammenhang mit der Volkszählung 1987 in APIS beschäftigt. Zu dieser Sitzung habe ich die Ergebnisse meiner im Juni 1987 durchgeführten Prüfung (vgl. Ziff. 3.4.6) aktualisiert. Bis zum 22. Januar 1988 waren aus Hessen unter dem Stichwort „Volkszählung" in APIS zu 93 Sachverhalten 51 Personendatensätze gespeichert. Der Anteil der Bagatelldelikte lag wie Mitte des Jahres 1987 bei ca. 70 v.H. Der Hessische Innenminister kündigte in dieser Sitzung seinerseits eine Überprüfung aller Fälle an. Er stellte Löschungen in Aussicht, soweit die veränderte Sicherheitslage im Zusammenhang mit der Volkszählung eine solche Maßnahme erlaube.

Eine förmliche und umfassende Antwort auf meine Beanstandungen habe ich vom Hessischen Innenministerium bisher nicht erhalten.

9.3
Verfassungsschutz - Auskunft an Betroffene

9.3.1
Verbesserung durch das neue HDSG

Im Jahre 1987 erhielt ich außergewöhnlich häufig Anfragen von Bürgern, die zuvor vergeblich das Landesamt für Verfassungsschutz um Auskunft über die zu ihrer Person gespeicherten Daten gebeten hatten.

Die große Zahl der Eingaben beruht wohl auf zwei Gründen: Zum einen haben etliche Publikationen auf die gesetzlich verankerte Möglichkeit hingewiesen, Auskunftsansprüche an die Sicherheitsbehörden und insbesondere auch an die Verfassungsschutzämter zu richten. Zum anderen war wohl auch § 18 Abs. 5 des neuen Hessischen Datenschutzgesetzes ausschlaggebend, wonach der Betroffene, wenn ihm die Auskunft oder Einsicht verweigert wird „unter Mitteilung der wesentlichen Gründe darauf hinzuweisen (ist), daß er sich an den Hessischen Datenschutzbeauftragten wenden kann."

Bereits jetzt kann festgestellt werden, daß diese neue Bestimmung die ihr vom Gesetzgeber zugedachte Funktion erfüllt hat. In allen Fällen habe ich - soweit vorhanden - die beim Landesamt gespeicherten Informationen überprüft. In einzelnen Fällen wurden die Angaben gelöscht, da entweder das Verfassungsschutzamt selbst die Informationen für nicht mehr erforderlich hielt oder auf meine Anregung hin bereit war, auf weniger wichtige Angaben zu verzichten.

Das Hessische Datenschutzgesetz gibt in Fällen, in denen das öffentliche Interesse an der Geheimhaltung oder das Geheimhaltungsinteresse Dritter das Auskunftsinteresse des Betroffenen überwiegt, nur einen quasi mittelbaren Auskunftsanspruch. Wird dem Bürger die Auskunft verweigert, kann er den Hessischen Datenschutzbeauftragten einschalten, der zwar vom Landesamt für Verfassungsschutz die Auskunft verlangen kann, den Betroffenen allerdings nicht über den Inhalt informieren darf. Die Verfassungsschutzämter geben in der Regel keine unmittelbaren Auskünfte an den Betroffenen. Nach meiner Kenntnis hat sich das Landesamt für Verfassungsschutz bislang lediglich in einem Fall anders verhalten. Auf meinen Vorschlag teilte es einem hochbetagten Bürger, der sich verfolgt fühlte, mit, daß gegen ihn nicht ermittelt worden sei. Auch wenn der Betroffene nicht erfährt, ob das Verfassungsschutzamt Daten über ihn gespeichert hat oder nicht, so garantiert das neue Verfahren nach § 18 Abs. 5 HDSG doch immerhin eine Kontrolle, bei der in besonderem Maße seine Interessen berücksichtigt werden.

9.3.2
Rechtsprechung

Bei dem kleinen Fortschritt, den § 18 Abs. 5 HDSG für den Betroffenen gebracht hat, darf jedoch keinesfalls stehengeblieben werden.

Eine Reihe von Gerichten mußte sich in den letzten Jahren mit der Frage auseinandersetzen, ob die Verfassungsschutzämter dem Betroffenen im Einzelfall nicht doch Auskunft über die zu seiner Person gespeicherten Informationen geben müssen. Besonders das Oberverwaltungsgericht Bremen hat sich in seiner Entscheidung vom 24. Februar 1987 (NJW 1987, S. 2393) eingehend mit dem Problem beschäftigt und einige Lösungswege aufgezeigt.

Ausgehend von der bislang schon weitgehend akzeptierten Feststellung, daß die Entscheidung der Verfassungsschutzbehörden über den Auskunftsanspruch jeweils nach pflichtgemäßem Ermessen und unter Berücksichtigung der Datenschutzrechte des Betroffenen einerseits und der Geheimhaltungsinteressen des Verfassungsschutzes andererseits erfolgen muß, weist das Gericht den Weg für eine Lösung, die auch „unter Beachtung des Verhältnismäßigkeitsprinzips zu einem möglichst schonenden Ausgleich" für den Betroffenen führt. Das Gericht greift einen bereits seit Jahren existierenden Vorschlag der Datenschutzbeauftragten auf und differenziert nach den Aufgabengebieten der Verfassungsschutzämter. Strikt geheimzuhalten sind i.d.R. Informationen über „Bestrebungen, die durch Anwendung von Gewalt oder darauf gerichtete Vorbereitungshandlungen verfolgt werden" oder die sich auf eine geheimdienstliche Tätigkeit beziehen. Nur in diesen Fällen darf regelmäßig, d.h. aber auch hier nur nach pflichtgemäßem Ermessen, das öffentliche Interesse an der Geheimhaltung als höherrangig bewertet werden. Im Ausnahmefall ist selbst in diesem Zusammenhang Auskunft zu erteilen.

Anders beurteilt das Gericht Auskunftsansprüche, wenn die Daten im Rahmen der sog. Extremismusbeobachtung gespeichert worden sind. Hier ist die von den Verfassungsschutzbehörden immer wieder betonte Ausforschungsgefahr regelmäßig dann nicht zu befürchten, wenn die Angaben Tatbestände betreffen, die schon länger zurückliegen, abgeschlossen sind oder bereits allgemein zugänglichen oder amtlichen Quellen entnommen werden können. Es scheint geradezu widersinnig, wenn die Verfassungsschutzämter einerseits in ihren Jahresberichten mitteilen, daß bestimmte Organisationen observiert werden, andererseits den Mitgliedern dieser Organisationen aber gleichzeitig mit dem Argument „Ausforschungsgefahr" pauschal Auskünfte über ihre gespeicherten Daten verweigern. Bestimmte Parteien und Organisationen sind - was allgemein bekannt ist - Beobachtungsobjekte der Verfassungsschutzbehörden. Wenn Funktionäre oder Mitglieder dieser Organisationen sich in Publikationen äußern, so ist die Tatsache, daß die Verfassungsschutzämter diese Publikationen auswerten, nicht geheimhaltungsbedürftig. Entsprechend könnten die Betroffenen auch darauf hingewiesen werden, daß diese Informationen gespeichert werden. Das Oberverwaltungs-

gericht hat mit Recht darauf hingewiesen, daß eine großzügige Auskunftspraxis auch das Mißtrauen gegenüber den Nachrichtendiensten abbauen kann.

Das Gericht hat zudem anerkannt, daß „besondere Umstände" ein gesteigertes Auskunftsinteresse der Betroffenen begründen können. Als Beispiele nennt es „erschwerte Arbeitsplatzsuche, drohender Arbeitsplatzverlust, gesundheitliche Beeinträchtigungen oder die Herabsetzungen des Bildes des Betroffenen in der Öffentlichkeit." In diesen Fällen kann es eher angezeigt sein, die gespeicherten Informationen in entsprechenden Auszügen dem Betroffenen mitzuteilen.

Die Gerichtsentscheidungen sollten das Hessische Innenministerium und das Landesamt für Verfassungsschutz veranlassen, gemeinsam mit dem Hessischen Datenschutzbeauftragten nach Fallgruppen zu suchen, in denen Auskünfte ganz oder teilweise erteilt werden können. Das macht freilich eine entsprechende Regelung im Verfassungsschutzgesetz nicht entbehrlich, diese ist und bleibt dringend erforderlich.

10. Personalausweis

Seit 1. April 1987 gibt es den neuen maschinenlesbaren Personalausweis. Der Ausweis enthält neben den Angaben zur Person und einem Lichtbild auch eine Seriennummer, die von der Kommune zugeteilt wird. In einer Reihe von Fällen haben die Behörden ein und dieselbe Seriennummer an zwei Personen vergeben. Allein in Hessen wurden mir 240 solcher Fehler bekannt. Bundesweit sind rund 4.000 Seriennummern zweifach zugeteilt worden. Für die betroffenen Bürger kann dies gravierende Folgen haben. So können z.B. Maßnahmen, die gegen den Inhaber eines Personalausweises gerichtet sind, auch den „Doppelgänger", dessen Personalausweis die gleiche Personalausweisnummer hat, treffen. Kommt einer der Personalausweise abhanden, so entsteht die Gefahr, daß der Inhaber des Personalausweises mit der gleichen Seriennummer in den Verdacht des Diebstahls oder Ausweismißbrauchs gerät.

In einigen Kommunen, in denen es zu besonders zahlreichen Doppelvergaben kam, habe ich durch meine Mitarbeiter die Fehlerursachen untersuchen lassen. Zusammenfassend läßt sich zunächst feststellen, daß die Gründe für die zweifache Vergabe von Seriennummern vielfältig sind:

Die Zuteilung der Seriennummern ist zwar Sache der Kommunen; auf Anfrage stellt jedoch die Bundesdruckerei, die die Ausweise herstellt, den Gemeinden sogenannte Seriennummernlisten zur Verfügung. Auf diesen Listen stehen links untereinander die fortlaufenden Seriennummern. Neben den Nummern soll der Name des jeweiligen Antragstellers eingetragen werden, um auf diese Weise zu kennzeichnen, ob und an wen die Personalausweisnummer bereits vergeben wurde. Dabei kam es zu etlichen Fehlern. Teilweise wurden Seriennummernlisten des Testlaufs neben den regulären Listen verwandt oder man vergaß bei manueller Verarbeitung, die Seriennummern als vergeben zu kennzeichnen. Zu einer Vielzahl von Doppelvergaben kam es ferner bei der Umstellung vom manuellen zum automatisierten Verfahren. So versäumten es die Kommunen teilweise, den Kommunalen Gebietsrechenzentren mitzuteilen, welche Seriennummern bereits manuell vergeben worden waren. Dies hatte zur Folge, daß von den Rechenzentren die gleichen Seriennummern nochmals zugeteilt wurden. Zu Fehlern kam es auch, wenn die Ausweisanträge infolge technischer Schwierigkeiten zeitweise nicht automatisiert bearbeitet werden konnten. Wenn dann manuell verarbeitet werden mußte, wurde oftmals versäumt, auf der Seriennummernliste die Vergabe zu vermerken. Die beschriebenen Fehlerquellen können nicht allein durch einen Appell an die Kommunen behoben werden, die Anträge sorgfältig zu bearbeiten. Selbst bei einer automatisierten Verarbeitung sind, wie eben dargestellt, Fehler nicht gänzlich auszuschließen, da erfahrungsgemäß bei Systemausfällen auf eine manuelle Bearbeitung ausgewichen werden muß.

Entscheidend ist deshalb, daß durch Kontrollmechanismen bei der Bundesdruckerei Doppelvergaben rechtzeitig entdeckt und korrigiert werden können. Die dort vorhandenen Sicherungen sind jedoch unzureichend: Die Bundesdruckerei prüft zunächst nur bei Eingang einer Lieferung (ca. 30 - 60 Personalausweisanträge), ob eine Seriennummer innerhalb der Lieferung zweimal vergeben wurde. Ein Abgleich mit allen bisher zugeteilten Personalausweisnummern erfolgt frühestens nach 28 Tagen im Rahmen der Abrechnung der Bundesdruckerei mit den Kommunen. Dann sind die Ausweise jedoch bereits ausgefertigt und den Betroffenen ausgehändigt. Es bleibt in diesem Fall nur die Möglichkeit, einen der Personalausweise wieder einzuziehen. Zu diesem Zweck erstellt die Bundesdruckerei sogenannte „Warnlisten". Sie enthalten eine Aufstellung der doppelt vergebenen Personalausweisnummern. Zunächst werden die Warnlisten an die zuständigen Ministerien der Länder übermittelt und von hier aus dann über die Regierungspräsidenten und Landräte an die Kommunen weitergeleitet. Dadurch kommt es zu weiteren Zeitverzögerungen bei notwendigen Korrekturen. Ein Kontrollverfahren, das dazu führt, daß bereits ausgestellte Ausweise zurückgefordert werden müssen, ist weder im Sinne des Bürgers noch der Verwaltung. Es ist vielmehr eine präventive Kontrolle erforderlich. Dies kann in der Weise geschehen, daß die Bundesdruckerei vor Herstellung der Ausweise einen Abgleich mit allen bereits vergebenen Seriennummern vornimmt.

Ich habe deshalb das Hessische Innenministerium aufgefordert, darauf hinzuwirken, daß die Kontrollmechanismen bei der Bundesdruckerei verbessert werden.

11. Justiz

11.1
Meldungen der Staatsanwaltschaften und Gerichte an die Polizei über den Ausgang eines Strafverfahrens

Die Polizei gibt jedes Ermittlungsverfahren nach Abschluß an die Staatsanwaltschaft ab. Die abschließende Entscheidung über die Verfolgung der Straftat ist Sache der Staatsanwaltschaft bzw. des Gerichtes. Dort werden die Ergebnisse des polizeilichen Ermittlungsverfahrens oft ergänzt oder korrigiert. Nicht selten stellt sich - etwa aufgrund weiterer Zeugenvernehmungen oder sonstiger neuer Beweismittel - heraus, daß ein Verdächtiger die Straftat nicht oder unter anderen Umständen begangen hat. Außerdem kann die Staatsanwaltschaft ein Verfahren einstellen, wenn die Ermittlungsergebnisse keinen genügenden Anlaß für die Anklageerhebung bieten. Auch kann sie aus den verschiedensten Gründen - mit Zustimmung des zuständigen Gerichtes - von der Strafverfolgung absehen. Schließlich wird oft genug noch im gerichtlichen Verfahren aus den unterschiedlichsten Gründen ein Verfahren eingestellt oder der Verfahrensgegenstand verändert.

Natürlich kann die Polizei, die die Daten bei Abschluß ihrer Ermittlungen speichert (vgl. hierzu auch Ziff. 9.1), nicht wissen, wie ein Verfahren bei der Staatsanwaltschaft oder vor Gericht ausgeht oder ob Ermittlungsergebnisse sich aufgrundspäterer Erkenntnisse als unrichtig oder ergänzungsbedürftig erweisen. Die in den polizeilichen Informationssystemen gespeicherten Daten geben deshalb nur den Verfahrensstand zu diesem Zeitpunkt wieder. Die Beschuldigten haben selbstverständlich ein großes und berechtigtes Interesse daran, daß für sie günstige Veränderungen im Verfahren vor Staatsanwaltschaft oder Gerichten auch bei der Polizei registriert werden. Allgemeiner gesprochen: Der Zusammenhang zwischen polizeilichem und gerichtlichem Verfahren zwingt dazu, daß die Polizei in jedem Fall über das Ergebnis des weiteren Verfahrens unterrichtet wird.

Die Datenschutzbeauftragten des Bundes und der Länder haben deshalb in ihrer Konferenz am 4. und 5. Mai 1987 in einem Beschluß (vgl. Ziff. 14.3 dieses Berichts) eine ausdrückliche gesetzliche Regelung entweder in dem geplanten „Justizmitteilungsgesetz" oder in der Strafprozeßordnung verlangt. Noch sind die Mitteilungen an die Polizei lediglich in Nr. 11 der „Anordnungen über Mitteilungen in Strafsachen" (Mistra), einer Verwaltungsvereinbarung der Landesjustizverwaltungen und des Bundesministers der Justiz (in der ab 1. April 1985 geltenden Fassung), geregelt. Danach müssen Gerichte und Staatsanwaltschaften auf Antrag der Polizei Aktenzeichen und Ausgang des Verfahrens übermitteln.

Bei meiner Prüfung der Vergabe von Aussonderungsprüffristen im Hessischen Polizei Informationssystem (vgl. Ziff. 9.1) hatte ich Gelegenheit festzustellen, wie in der Praxis verfahren wird.

Zwei der überprüften Kriminalkommissariate stellen den Antrag, über den Ausgang des Verfahrens in jedem Fall und zwar bereits bei der Abgabe des Ermittlungsverfahrens an die Staatsanwaltschaft. Zirka 80 § der von meinen Mitarbeitern eingesehenen Kriminalakten enthielten eine Mitteilung über den Verfahrensausgang. Nach Eingang der Mitteilung überprüften die Kommissariate ihre gespeicherten Daten; hat die Staatsanwaltschaft das Verfahren eingestellt, wird außerdem die vorgesehene Speicherdauer überprüft und eventuell reduziert. Bei Verfahrenseinstellungen oder Freisprüchen, die die Unschuld des Betroffenen erkennen lassen, werden die gespeicherten Daten gelöscht. In unklaren Fällen wird die staatsanwaltschaftliche Akte oder das Gerichtsurteil angefordert.

In einem anderen Kriminalkommissariat enthielten die älteren Kriminalakten nur zum geringen Anteil Mitteilungen über den Ausgang des Verfahrens. Vorgänge, die 1986 abgeschlossen wurden, enthielten jedoch in zirka 80 von 100 Fällen entsprechende Mitteilungen. Einen formellen Antrag, über den Verfahrensausgang informiert zu werden, stellt das Kommissariat nicht. Die Staatsanwaltschaft sendet die Verfahrensmitteilungen vielmehr unaufgefordert zu. In den letzten Jahren ist die Mitteilungsquote stark angestiegen. Teilt die Staatsanwaltschaft mit, daß ein Verdächtiger wegen erwiesener Unschuld freigesprochen wurde, oder daß deshalb ein Verfahren eingestellt wurde, löscht das Kriminalkommissariat die gespeicherten Daten. Ansonsten wird nach Eingang einer Meldung über den Verfahrensausgang die vorgesehene Speicherdauer nicht überprüft, da dieses Kommissariat ohnehin die Erforderlichkeit der jeweiligen Datenspeicherung in einem Dreijahresrhythmus überprüft.

Ein weiteres Kriminalkommissariat stellt ebenfalls keinen formellen Antrag auf Meldung des Verfahrensausgangs. Die Staatsanwaltschaft übersendet nur in wenigen Fällen (nach grober Schätzung sind davon zirka 10 von 100 aller Vorgänge betroffen) - unaufgefordert eine entsprechende Mitteilung. Der Eingang der Mitteilung löst keine Überprüfung der Datenspeicherung aus. Die Nachricht wird lediglich zu den Akten genommen.

In einem anderen Fall teilt die Staatsanwaltschaft dem Polizeipräsidenten unaufgefordert in - soweit ersichtlich - allen Fällen mit, daß der Verdächtige verurteilt wurde oder ein Strafbefehl ergangen ist. Auch das Strafmaß wird in der Mitteilung genannt. Verfahrenseinstellungen werden nicht mitgeteilt. Die Mitteilung wird nur zu den Akten genommen, eine Überprüfung der Datenspeicherungen erfolgt nicht.

Als Ergebnis bleibt festzustellen: In den fünf Polizeidienststellen werden vier verschiedene Verfahren praktiziert. Dies macht erneut deutlich, daß die Problematik dringend gesetzlich geregelt werden muß. Die bisherigen Erfahrungen mit dem Gesetzgebungsverfahren für das Justizmitteilungsgesetz lehren zudem, daß diese gesetzliche Regelung nicht abgewartet werden sollte. Schon jetzt ist zuviel Zeit verstrichen. Da eine Reihe von Polizeidienststellen keine Anträge auf Rückmeldung nach Nr. 11 der Mistra stellen, muß das bisherige Verfahren überprüft werden. Es ist nicht

ersichtlich, weshalb ein besonderer Antrag gestellt werden muß. Vielmehr sollten Gerichte und Staatsanwaltschaften der Polizei auch ohne ausdrückliche Aufforderung in allen Fällen von sich aus den Ausgang des Verfahrens mitteilen. Da hier Rechte der Betroffenen berührt sind, müssen diese Informationen auch in jedem Fall bei der Polizei zu einer Überprüfung der vergebenen Aufbewahrungsfristen führen.

12. Milch-Garantiemengen-Verordnung

In meinem 15. Tätigkeitsbericht (Ziff. 1.4.1) hatte ich am Beispiel des Fragebogens, der zur Durchführung der Milch-Garantiemengen-Verordnung (MGVO) an die landwirtschaftlichen Haushalte ausgegeben worden war, das umfangreiche Informationsinteresse der Verwaltung bei der Gewährung von Subventionen demonstriert. Nach meinen damaligen Erkenntnissen bot die Verwendung des Fragebogens keinen Grund zur Beanstandung - das hat sich mittlerweile grundlegend geändert.

12.1
Inhalt und Zweck des Fragebogens

In dem Bogen wurde nicht nur nach den Wohnverhältnissen, dem Arbeitsablauf, der Freizeit oder der Aus- und Weiterbildung gefragt. Detailliert sollte unter anderem auch angegeben werden, ob die Mahlzeiten aus zwei (Suppe und Hauptgericht oder Hauptgericht und Dessert) oder drei Gängen besteht, wieviele Kalorien die einzelnen Haushaltsmitglieder (Name der Verpflegungspersonen) zu sich nehmen und was für Möbel, Geschirr, Blumenschmuck (aufgeteilt in „Schnitt- und Topfblumen, Wohngarten und Grabstätten"), Unterwäsche, Schlafanzüge, Socken, Zeitungen, Bücher und Kinobesuche ausgegeben wurde.

Mit dem Fragebogen sollte der genaue Haushaltsaufwand ermittelt werden. Hintergrund: Die Milchvermarktung milcherzeugender Betriebe ist mit der Milch-Garantiemengen-Verordnung vom 25. Mai 1984 auf ein bestimmtes Kontingent begrenzt worden. Darüber hinausgehende Mengen werden mit einer Abgabe belastet, die deren Erzeugung praktisch unwirtschaftlich macht, weil die Erlöse unter den Selbstkosten liegen. Weitere Referenzmengen können nur dann geltend gemacht werden, wenn ein Milcherzeuger Investitionen zur Erweiterung seines Betriebes getätigt hat und eine durch die Mengenregulierung herbeigeführte Existenznot des Betriebes entstanden ist. Ein Betrieb ist dann als existenzgefährdet anzusehen bzw. auf die Milcherzeugung angewiesen, wenn er trotz verbesserter Betriebsorganisation in den nächsten Jahren nicht in der Lage sein wird, ein jährliches Eigenkapital zu erwirtschaften, das mindestens eine planmäßige Schuldentilgung erlaubt und einen Ausgleich für Steigerungen des Preisniveaus gewährleistet. Die betroffenen Haushalte sollen in der Lage sein, aus den laufenden Einnahmen ihren Lebensunterhalt zu bestreiten und darüber hinaus zumindest das betriebsnotwendige Vermögen erhalten. Dazu müssen sie, ausgehend vom Gesamteinkommen abzüglich Haushaltsgeld und Schuldzinsen, eine positive Eigenkapitalbildung nachweisen. Die Eigenkapitalbildung vor und während der Quotenregelung ist das wichtigste zu prüfende Entscheidungskriterium für die Existenzfähigkeit des Betriebes und die Ermittlung des Haushaltsaufwandes zur Errechnung der Eigenkapitalbildung unerläßlich.

12.2
Überprüfung des Fragebogens im Jahr 1986

Der Fragebogen stieß jedoch auf heftige Kritik der Betroffenen. Im April 1986 bat mich ein Landtagsabgeordneter um eine datenschutzrechtliche Überprüfung. Das Ergebnis der Prüfung ließ zunächst auf einige Datenschutzmängel schließen. Im Juni 1986 teilte ich dem Landwirtschaftsministerium meine Bedenken mit und forderte es zur Stellungnahme auf. Ich wies darauf hin, daß vor allem nicht erkennbar sei, wieso im Rahmen der Milch-Garantiemengen-Verordnung eine derart detaillierte Befragung der Haushalte erforderlich sein sollte. Abgesehen davon verstoße der Fragebogen gegen § 11 Abs. 2 HDSG. (Da die Prüfung vor dem 1.1.1987 erfolgte, handelt es sich hier noch um das alte HDSG, die entsprechende Vorschrift findet sich nunmehr in § 12 Abs. 4). Danach muß dem Betroffenen die Rechtsgrundlage genannt werden, aufgrund der er zur Beantwortung der Fragen verpflichtet ist. Soweit eine solche Rechtsvorschrift nicht vorliegt, ist er auf die Freiwilligkeit seiner Angaben hinzuweisen und seine Einwilligung erforderlich.

Das Ministerium antwortete im August 1986, daß die Haushalte über die Bedeutung des Fragebogens aufgeklärt worden seien. Jeder Antragsteller habe mit dem Fragebogen ein Merkblatt ausgehändigt bekommen, in dem auf die Freiwilligkeit der Befragung hingewiesen werde und der Verbleib des Bogens bei den Betroffenen ausdrücklich festgelegt sei. Weiter teilte mir das Ministerium mit: „Der Hilfsbogen ist in keiner Weise zwingend erforderlich. Er dient dem Antragsteller als Arbeitshilfe und verbleibt bei ihm. Es werden keine Daten abgeschrieben, abgelichtet oder in sonstiger Weise gespeichert. Im Ermittlungsbogen ist lediglich der ermittelte Wert Haushaltsaufwand als Gesamtsumme einzutragen. Nur dieser Bogen wird zu den Akten genommen".

Unter diesen Umständen bestand für mich kein Anlaß zu einer datenschutzrechtlichen Beanstandung.

12.3
Prüfung im Jahr 1987

Im vergangenen Jahr mußte ich jedoch durch Prüfungen beim Landesamt für Ernährung, Landwirtschaft und Landentwicklung und bei einigen Landwirtschaftsämtern feststellen, daß die Auskunft des Ministeriums nur bedingt zutreffend, in wichtigen Einzelheiten vielmehr unrichtig und unvollständig war.

12.3.1
Anweisungen des Landesamtes für Ernährung, Landwirtschaft und Landentwicklung

Nach meinen Feststellungen ordnete die Mittelinstanz, das Landesamt für Landwirtschaft in Kassel, am 4. März 1986 gegenüber den Landwirtschaftsämtern (als den unteren Verwaltungsbehörden) an, den Landwirten den Kalkulationsbogen nach einer Erläuterung zum Ausfüllen zu übergeben und ihn einzeln wieder an die Landwirtschaftsämter zurückgeben zu lassen. Obwohl bereits am 12. März 1986 in einer Dienstbesprechung einige Leiter der Landwirtschaftsämter den Bogen scharf kritisiert hatten und obwohl die zuständige Abteilung des Landwirtschaftsministeriums ebenfalls Datenschutzbedenken zum Ausdruck gebracht hatte (Schreiben vom 13. März 1986) wurde die ursprüngliche Verfügung vom 4. März offenbar nur zögernd und stufenweise revidiert: Zunächst mit der Sammelverfügung vom 20. März 1986, die nunmehr erläuterte, dem Antrag sei nur das Blatt „Feststellung des Haushaltsaufwandes" beizufügen; der Kalkulationsbogen sei lediglich „als ein Leitfaden anzusehen".

Mit Sammelverfügung vom 22. April 1986, die den Kalkulationsbogen jetzt als „Hilfsbogen" bezeichnete, ordnete das Landesamt für Landwirtschaft an, „den Hilfsbogen im Amt nicht zu den Akten zu nehmen, sondern unverzüglich dem Antragsteller nach Übernahme der Daten auf den grünen Bogen ‚Feststellung des Haushaltsaufwandes' zurückzugeben". Der „grüne Bogen" bestand zu dieser Zeit aber noch aus 17 Einzelpunkten. Die Landwirtschaftsämter konnten sich daher für berechtigt halten, den Kalkulationsbogen (Hilfsbogen) erst nach Abschluß der Antragsbearbeitung dem Antragsteller zurückzugeben.

Einen Monat später, am 22. Mai 1986, ordnete das Landesamt in einer weiteren Sammelverfügung an: „Aufgrund eines erneuten Erlasses des Hessischen Ministers für Landwirtschaft und Forsten werden die Seiten 1 und 14 (= Deckblatt und grüner Bogen) noch einmal geändert bzw. ergänzt ..." Ab sofort durfte nur noch diese Form des Bogens verwendet werden; außerdem sollte jedem Antragsteller ein rotes Merkblatt ausgehändigt werden. Erst in diesem Merkblatt werden die Antragsteller über die Freiwilligkeit der Auskunftserteilung und den Verwendungszweck des Fragebogens informiert.

Die bisher letzte Verfügung des Landesamtes in der Sache erging mehr als ein Jahr später, am 7. September 1987. Darin heißt es nunmehr, daß nach Abschluß der Bearbeitung der Anträge nach der Milch-Garantiemengen-Verordnung der „Hilfsbogen zur Ermittlung des Haushaltsaufwandes nicht mehr zu verwenden" ist und alle Restexemplare auszusondern seien. Außerdem: „Es wird hiermit untersagt, den Hilfsbogen als Bestandteil von Anträgen auf Gewährung von Förderungsmitteln zu verwenden." Allerdings soll er weiterhin „für Zwecke der hauswirtschaftlichen Beratung, insbesondere im Zusammenhang mit der Haushaltsbuchführung" verwendet werden dürfen.

12.3.2
Verfahrensweise der Landwirtschaftsämter

Meine Prüfungen in 7 der 17 Landwirtschaftsämter hatten im wesentlichen folgendes Ergebnis:

Der Fragebogen wurde in allen geprüften Landwirtschaftsämtern zeitweilig zu den Akten genommen, allerdings unterschiedlich lange (8 Wochen bis 8 Monate) aufbewahrt. Die Aufbewahrungsdauer richtete sich offenbar nach der Zahl der Anträge, die zwischen unter 50 und bis zu 1000 schwankte, je nach Einzugsgebiet des Amtes. Die Zurückbehaltung der Kalkulationsbogen wurde mit der Notwendigkeit einer Plausibilitätskontrolle und der Beantwortung von Rückfragen entweder des Antragstellers oder des Landesamts für Landwirtschaft begründet.

Pro Amt gab es maximal zehn Fälle, in denen Landwirte sich geweigert hatten, den Kalkulationsbogen zu benutzen. Deren Anträge mit einem geschätzten Haushaltsaufwand wurden in allen Ämtern und im Landesamt ohne Beanstandung bearbeitet.

Spätestens in der ersten Jahreshälfte 1987 haben alle Landwirtschaftsämter den Kalkulationsbogen an die Antragsteller zurückgegeben. In einem einzigen Fall konnte ich noch einen Kalkulationsbogen in der Akte eines Landwirtschaftsamtes finden, der den Vermerk trug „an Antragsteller zurückgeben". Das Versäumnis wurde mit einem Wechsel des Sachbearbeiters begründet.

Es konnte nicht zweifelsfrei festgestellt werden, ob die Mehrheit der Landwirte bei Antragstellung über die Freiwilligkeit der Benutzung des Kalkulationsbogens informiert war, da eine große Zahl das entsprechende rote Merkblatt nicht oder nach Antragstellung erhalten hatte. Sicher ist jedoch, daß jedenfalls für ca. zwei Monate nach Beginn der Fragebogenaktion die Verfügung des Landesamtes bestand, den Kalkulationsbogen als Bestandteil des Antrags zu den Akten zu nehmen, daß also erst frühestens ab Mai 1986 für die Betroffenen eine Wahlmöglichkeit bestand, den Kalkulationsbogen zu benutzen (und zu Hause zu behalten) oder nicht.

Die Sicherung der Akten gegen Zugriffe Unbefugter war in 6 der 7 überprüften Landwirtschaftsämtern völlig unzureichend. Das ist um so weniger hinnehmbar, als die Akten der Landwirtschaftsämter zum Teil sehr sensitive Daten wie z.B. Angaben über Schulden, ärztliche Gutachten oder Testamente enthalten. Die Unterlagen lagerten in alten, nicht abschließbaren Holzschränken in mitunter öffentlich zugänglichen Räumen.

Bei der Prüfung im Landesamt für Ernährung, Landwirtschaft und Landentwicklung konnte nicht festgestellt werden, daß Kalkulationsbogen von den Landwirtschaftsämtern an das Landesamt weitergeleitet worden waren. In den überprüften Akten fand sich nur der zu dem einzelnen Antrag gehörende Teil, auf dem der Gesamtbetrag des Haushaltsaufwandes vermerkt war.

12.3.3
Bewertung

Es ist offensichtlich unrichtig, daß - wie das Landwirtschaftsministerium mir im August 1986 mitgeteilt hat - seit dem 20. März 1986 „jeder Antragsteller auf die Freiwilligkeit der Benutzung des Hilfsbogens hingewiesen" wurde: Zu dieser Zeit galt noch die Sammelverfügung des Landesamts für Landwirtschaft vom 4. März 1987, nach der die Landwirte den Kalkulationsbogen mit dem Antrag an die Landwirtschaftsämter zurückzugeben hatten. Im übrigen dürften viele Landwirte das erst seit dem 22. Mai 1986 vorhandene rote Merkblatt, in dem auf die Freiwilligkeit der Verwendung des Kalkulationsbogens hingewiesen wurde, nicht erhalten haben, da sie zu diesem Zeitpunkt den Antrag bereits gestellt hatten. Offensichtlich unrichtig ist auch die Auskunft des Ministeriums „es werden keine Daten abgeschrieben, abgelichtet und in sonstiger Art gespeichert". Richtig ist vielmehr ausweislich der Verfügung des Landesamts, der Aussagen der Bediensteten der Landwirtschaftsämter und meiner Stichproben in den Akten, daß - zumindest für einen Zeitraum von ca. zwei Monaten, in vielen Fällen jedoch erheblich länger - nicht nur die Angaben aus den Kalkulationsbogen, sondern diese selbst in den Landwirtschaftsämtern aufbewahrt und ausgewertet wurden.

Dies lag offenbar daran, daß es eine klare Anordnung des Landesamtes, daß der Kalkulationsbogen in keinem Falle in den Landwirtschaftsämtern verwendet werden dürfe, nie gegeben hat. Die Formulierungen in den Sammelverfügungen vom 20. März und vom 22. April 1986, wonach der Bogen nicht mehr „Bestandteil des Antrags" bzw. „nicht zu den Akten zu nehmen" war, schlossen - nach einhelliger Auffassung der Landwirtschaftsämter - eine vorübergehende Verwendung der Kalkulationsbögen in den Ämtern nicht aus.

Das Grundrecht auf informationelle Selbstbestimmung der Bürgers erfordert, daß ein Eingriff der Verwaltung in Form einer Datenerhebung und Speicherung entweder auf einer Rechtsvorschrift beruht oder auf der Freiwilligkeit des Betroffenen. Beide Voraussetzungen waren hier nicht oder nur unzureichend erfüllt: Weder eine EG-Verordnung noch die Milch-Garantiemengen-Verordnung erlauben für die Feststellung des Haushaltsaufwandes die Verwendung eines 14seitigen Fragebogens und die amtliche Speicherung der darin enthaltenen Angaben. Auch nach § 11 Abs. 1 des HDSG vom 31. Januar 1978 (GVBl. I S. 96) war das Speichern personenbezogener Daten nur zulässig, soweit es „zur rechtmäßigen Erfüllung der in der Zuständigkeit der speichernden Stelle liegenden Aufgaben erforderlich" war. Das war hier ganz offensichtlich nicht der Fall, da die Antragsbearbeitung auch mit einem weniger umfangreichen oder auch ganz ohne Fragebogen möglich war und geschehen ist. Eine Rechtsgrundlage für die Verwendung des Kalkulationsbogens bestand somit nicht.

Da vermutlich in den meisten Fällen nicht auf die Freiwilligkeit der Auskunftserteilung hingewiesen wurde und in keinem Fall die Einwilligung der Betroffenen eingeholt wurde, war die Datenerhebung und -speicherung somit rechtswidrig. Ich habe deshalb die Datenverarbeitung im Zusammenhang mit der Durchführung der Milch-Garantiemengen-Verordnung gegenüber dem Landwirtschaftsministerium beanstandet.

Bei Betrachtung des Informationsflusses vom Ministerium zum Landesamt und umgekehrt fällt zudem folgendes auf: Das Ministerium hat von der durch das Landesamt geplanten und vorbereiteten Fragebogenaktion offenbar erst einen Tag nach deren Beginn erfahren. Am 4. März 1986 erging die Sammelverfügung des Landesamtes an die Landwirtschaftsämter und am 5. März 1986 berichtete das Landesamt darüber dem Ministerium. Wenn es schon ungewöhnlich erscheint, daß in einer solch grundsätzlichen Angelegenheit die Mittelbehörde nicht vorher die zuständige oberste Behörde konsultiert, ist es mir vollends unverständlich, daß das Ministerium in seiner Antwort an das Landesamt vom 13. März 1986 zwar Datenschutzbedenken äußert, aber damit einverstanden ist, daß die Angelegenheit für eine „Erprobungsphase" zunächst einmal laufen kann; zumal ihm zu diesem Zeitpunkt schon bekannt sein mußte, daß die Amtsleiter der Landwirtschaftsämter das Projekt in der Dienstbesprechung vom Vortage heftig kritisiert hatten. Erst am 30. April 1986 erging die Anordnung an das Landesamt, „aus datenschutzrechtlichen Gründen unbedingt auf den o.a. Formularsatz bzw. Bogen folgende Zusätze bzw. Änderungen vorzunehmen", die dann vom Landesamt mit seiner Sammelverfügung vom 22. Mai 1986 (siehe Ziff. 12.3.1) auch ausgeführt wurden. Eine sogenannte „Erprobungsphase" hat allerdings weder stattgefunden, noch habe ich Erlasse oder Verfügungen gefunden, nach denen sie geplant gewesen wäre. Die Aktion lief auch von Anfang an in allen Bezirken und mit echten personenbezogenen Daten.

Im Hinblick darauf, daß für die öffentliche Verwaltung des Landes Hessen seit dem 7. Oktober 1970 ein Datenschutzgesetz besteht, ist es schwer verständlich, daß eine obere Verwaltungsbehörde wie das Landesamt für Landwirtschaft eine Fragebogenaktion mit einem weit in die Privatsphäre der Betroffenen gehenden vierzehnseitigen Kalkulationsbogen durchführt, ohne sich dabei Gedanken über den Datenschutz zu machen. Dies gilt um so mehr, als

zur gleichen Zeit, zu der die Fragebogenaktion durchgeführt wurde, bereits die Diskussion über die Volkszählung 1987 in vollem Gang und Datenschutz ein öffentliches Gesprächsthema war. Obwohl die Behörde, wie die verschiedenen Verfügungen zeigen, unsicher war, hat sie das nächstliegende, das in diesem Fall notwendig gewesen wäre, unterlassen, nämlich sich durch den Hessischen Datenschutzbeauftragten rechtzeitig beraten zu lassen.

13. Bilanz

13.1
Änderung des Straßenverkehrsgesetzes

Einführung des „Zentralen Verkehrsinformationssystems" (ZEVIS) (13. Tätigkeitsbericht, Ziff. 3.5.4, 14. Tätigkeitsbericht, Ziff. 13.2.5 und 15. Tätigkeitsbericht, Ziff. 6.3.2)

In den letzten drei Tätigkeitsberichten habe ich zu der Einführung des „Zentralen Verkehrsinformationssystems" (ZEVIS) beim Kraftfahrtbundesamt und der damit verbundenen Änderung des Straßenverkehrsgesetzes Stellung genommen.

Das im November 1986 vom Bundestag verabschiedete Gesetz enthält zwar vielfältige Zweckbindungsvorschriften für die Verwendung der Fahrzeug- und Halterdaten bei den örtlichen Kraftfahrzeugzulassungsstellen und dem Kraftfahrtbundesamt, stellt aber andererseits die Kraftfahrzeug- und Halterdaten weit über den bisherigen Rahmen hinaus vor allem den Sicherheitsbehörden zur Verfügung. Gerade für die Polizei eröffnet das neue Straßenverkehrsgesetz eine Vielzahl auch direkter Zugriffsmöglichkeiten auf die Dateien der örtlichen Zulassungsstellen und in Flensburg.

Ergänzend war nach § 47 des Straßenverkehrsgesetzes noch eine „Fahrzeugregisterverordnung" zu erlassen, was nach intensiver Diskussion zwischen den zuständigen Bundesressorts und den Datenschutzbeauftragten im letzten Jahr geschehen ist. In der Verordnung vom 20. Oktober 1987 (BGBl. I S. 2305) bilden die im dritten Abschnitt (§§ 12 - 14) vorgesehenen technischen Vorkehrungen zur nachträglichen Überprüfung, ob Direktabrufe beim Kraftfahrtbundesamt und den örtlichen Stellen durch die Polizei und einige andere Sicherheitsbehörden rechtmäßig erfolgten, das datenschutzrechtliche Kernstück.

Ruft eine Polizeidienststelle Daten aus dem zentralen Fahrzeugregister unter Verwendung von Fahrzeugdaten ab, muß in jedem fünfzigsten Fall der Beamte, der die Abfrage durchführt, bevor er eine Auskunft erhält, zusätzliche eigene Angaben eingeben (§ 14 Abs. 4 Fahrzeugregisterverordnung). In diesen Fällen hat er einen bestimmten Schlüssel einzugeben, der erkennen läßt, ob die Abfrage etwa zum Zwecke der „Fahndungs-, Grenzfahndungsaktion, Kontrollstelle", zur „Verfolgung von Straftaten oder Verkehrsordnungswidrigkeiten" oder z.B. auch aufgrund „sonstiger Anlässe" erfolgt. Bei bestimmten Schlüsseln sind ein Aktenzeichen oder eine Tagebuchnummer, „falls dies beim Abruf angegeben werden kann", sowie Daten einzugeben, die die Dienststelle und den Anfragenden Bediensteten erkennen lassen.

Damit soll nachträglich die Rechtmäßigkeit der Abfrage überprüft werden können. Aus diesem Grund sieht § 14 Abs. 6 auch ausdrücklich vor, daß diese Aufzeichnungen den Datenschutzbeauftragten des Bundes und der Länder übermittelt werden dürfen. Es ist jedoch äußerst zweifelhaft, ob dieses Verfahren seinen Zweck erfüllen kann. Bereits im Gesetzgebungsverfahren haben die Datenschutzbeauftragten darauf hingewiesen, daß es nicht genügt, nur bei zwei Prozent aller Abfragen so zu verfahren, denn in 98 v. H. der Fälle bleibt der Grund der Abfrage damit faktisch nicht überprüfbar. Ein weiteres kommt hinzu: Selbst bei dieser kleinen Auswahl wird der Bedienstete ausdrücklich darauf aufmerksam gemacht, daß seine Abfrage überprüft wird. Er kann sich dann entsprechend verhalten, will er tatsächlich mißbräuchlich Daten abfragen: Er bricht entweder die Abfrage ersatzlos ab oder erneuert sie kurz darauf, um damit eine der 98 v. H. nicht überprüfbaren Abfragen vorzunehmen. Damit steht fest: Das Verfahren ist eine Farce, eine echte Kontrolle ist nicht möglich.

Demgegenüber ist bei jedem Abruf eine entsprechende Zusatzspeicherung vorzunehmen, soweit er nicht unter Verwendung von Fahrzeugdaten sondern Halterdaten erfolgt. Gemeint ist damit die sogenannte P-Abfrage: Dabei werden Personendaten eingegeben (z.B. Name, Geburtsdatum) und entweder Fahrzeugdaten oder weitere Personendaten (z.B. die Anschrift) abgerufen. Bei dieser Abfrageart steht - wie bereits in früheren Tätigkeitsberichten ausführlich dargestellt - zu befürchten, daß der Fahrzeugbezug der Datenverwertung überhaupt nicht mehr gegeben ist und die abrufberechtigten Dienststellen das zentrale Fahrzeugregister beim Kraftfahrtbundesamt ähnlich einem Bundesmelderegister nutzen. Aus diesem Grund hat der Verordnungsgeber hier eine hundertprozentige Zusatzprotokollierung vorgeschrieben. Ob in diesen Fällen nachträgliche Kontrollmechanismen wirksam greifen können, bleibt abzuwarten. In jedem Fall wird es mühevolle Kleinarbeit sein, über die Abfrage, den weiteren Zugriff auf die in den Protokolldaten verzeichneten Akten und evtl. über eine Rücksprache mit dem betroffenen Bediensteten abzuklären, ob im Einzelfall die Abfrage zu Recht erfolgt ist. Zweifellos wird die zu erwartende große Zahl der Abfragen den Aussagewert kleiner Stichproben ebenso relativieren wie das erfahrungsgemäß geringe Erinnerungsvermögen einzelner Bediensteter bezogen auf einzelne Abfrageaktionen.

13.2
Landesstatistikgesetz

(9. Tätigkeitsbericht, Ziff. 2.3.2, 12. Tätigkeitsbericht, Ziff. 1.2.1 Nr. 2, 13. Tätigkeitsbericht, Ziff. 4.1.6, 14. Tätigkeitsbericht, Ziff. 5.3.1 und 13.1.4, 15. Tätigkeitsbericht, Ziff. 8.1)

Am 23. Mai 1987 ist das Gesetz über die Statistik im Land Hessen (Hessisches Landesstatistikgesetz - HessLStatG) in Kraft getreten (GVBl. I S. 67). Damit ist die von mir seit immerhin sieben Jahren erhobene Forderung nach Schaffung einer ausreichenden gesetzlichen Grundlage für die Landes- und Kommunalstatistik endlich erfüllt worden (Zum Ablauf des Gesetzgebungsverfahrens und Zusammenhang mit der Volkszählung 1987 vgl. Ziff. 3.2.2.4).

Das Gesetz regelt sowohl die allgemeinen materiell-rechtlichen Bedingungen (z.B. Statistikgeheimnis) als auch Organisation und Verfahren der Landes- und Kommunalstatistik sowie - ergänzend zum Bundesstatistikgesetz - die Durchführung von Bundes- und EG-Statistiken, die in der Regel den Ländern obliegt. Durch das Landesstatistikgesetz ist außerdem erstmals das Hessische Statistische Landesamt gesetzlich institutionalisiert worden.

Das Hessische Landesstatistikgesetz setzt neue Maßstäbe, in dem es sich löst von der zweifelsohne noch weitverbreiteten Vorstellung, die Funktionsfähigkeit der amtlichen Statistik sei nur gewährleistet, wenn grundsätzlich Auskunftspflicht bestehe. Landes- und Kommunalstatistiken müssen künftig grundsätzlich ohne Auskunftspflicht der zu Befragenden durchgeführt werden. Nur ausnahmsweise kann durch Rechtsvorschrift die Pflicht zur Auskunftserteilung angeordnet werden. Dazu müssen jedoch begründete Anhaltspunkte dafür bestehen, daß ausreichende Ergebnisse durch eine Befragung ohne Auskunftspflicht nicht erreicht werden können (§§ 12,13 HessLStatG).

Bedenken bestehen jedoch dagegen, daß das Gesetz den Gemeinden überhaupt gestattet, durch Satzung Kommunalstatistiken mit Auskunftspflicht anzuordnen. Das Bundesverfassungsgericht hat im Volkszählungsurteil dem Gesetzgeber auferlegt, für jede Einzelstatistik kontinuierlich und unter Berücksichtigung des jeweiligen Standes der Methodendiskussion die Methoden der Informationserhebung und -verarbeitung und damit auch die Geeignetheit und Erforderlichkeit der Auskunftspflicht zu prüfen. Diese Anforderung stellt nunmehr auch das Hessische Landesstatistikgesetz, da nach § 13 Abs. 1 die Auskunftpflicht nur angeordnet werden darf, wenn Anhaltspunkte dafür bestehen, daß ohne Auskunftpflicht keine ausreichenden Ergebnisse ermittelt werden können. Die meisten Gemeinden werden jedoch kaum in der Lage sein, dies festzustellen. Die Gemeindevertretung müßte unter Berücksichtigung des Standes der Methodendiskussion für die jeweilige eigene Datenerhebung die Notwendigkeit der Auskunftspflicht prüfen. Das setzt jedoch eine gründliche Kenntnis der Methoden der Statistik und der empirischen Sozialforschung voraus, die in der Regel auf kommunaler Ebene nicht vorhanden sein dürfte.

Darüber hinaus erscheint es mir verfassungsrechtlich äußerst fraglich, ob durch gemeindliche Satzung eine kommunale Statistik mit Auskunftspflicht angeordnet werden kann. Gemessen an der Rechtsprechung des Bundesverfassungsgerichts dürfte ein derart schwerwiegender Eingriff in das verfassungsrechtlich garantierte Recht auf informationelle Selbstbestimmung wohl nur aufgrundeines förmlichen Gesetzes zulässig sein (BVerfGE 65,1 (44); 22,180 (219)). Gesetze im formellen Sinne sind jedoch nur Parlamentsgesetze der staatlichen Gesetzgebungsorgane und nicht Satzungen einer nichtstaatlichen Selbstverwaltungskörperschaft (BVerfGE 33,156 ff).

Meine im Gesetzgebungsverfahren gegen die Übermittlungsvorschriften des Gesetzentwurfs geäußerten Bedenken sind nur zum Teil ausgeräumt worden. Der Entwurf sah in § 16 Abs. 5 für das Hessische Statistische Landesamt die pauschale Befugnis vor, statistische Einzelangaben an die Gemeinden sowie Gemeinde- und Zweckverbände für deren eigene statistische Aufbereitung zu übermitteln (Drucks. 12/33). Daß eine solche Regelung mit einem erheblichen verfassungsrechtlichen Risiko belastet ist, hat auch der Landtag erkannt.

Es ist zwar weder verfassungsrechtlich noch datenschutzrechtlich grundsätzlich ausgeschlossen, daß das Statistische Landesamt Einzelangaben an die Gemeinden zu statistischen Zwecken übermittelt (BVerfGE 65,61). Als Rechtsgrundlage genügt allerdings nicht eine pauschale Befugnisnorm. Zur Gewährleistung des Statistikgeheimnisses ist nicht nur die strikte Trennung von Statistik und Verwaltungsvollzug erforderlich, sondern auch, daß grundsätzlich nur das Statistische Landesamt Zugang zu nichtanonymisierten Einzelangaben aus seinen statistischen Erhebungen hat. Eine Übermittlung statistischer Einzelangaben an Gemeinden kommt daher nur ausnahmsweise in Frage und erfordert eine spezialgesetzliche Regelung in der die Einzelstatistik anordnenden Rechtsvorschrift. Folgerichtig darf deshalb nach § 16 Abs. 5 HessLStatG das Hessische Statistische Landesamt nunmehr nur dann Einzelangaben übermitteln, wenn das Einzelstatistikgesetz dies zuläßt, wobei in dem Gesetz Art und Umfang der Angaben bestimmt sein müssen.

Anders verfährt dagegen § 16 Abs. 6 HessLStatG. Dem Hessischen Statistischen Landesamt wird pauschal erlaubt, statistische (nichtanonymisierte) Einzelangaben an die für Landesplanung zuständige oberste Landesbehörde zu übermitteln. Weshalb die Voraussetzungen für die Datenübermittlung zu statistischen Zwecken hier nicht gelten sollen, dürfte wohl kaum erklärbar sein, zumal bei der Übermittlung zu Planungszwecken der Grundsatz durchbrochen wird, daß zu statistischen Zwecken erhobene Daten grundsätzlich nur für diese Zwecke verwendet werden dürfen.

Der Bundesgesetzgeber war hier konsequenter. Zum einen verlangt er eine besondere gesetzliche Regelung. Darüber hinaus dürfen das Statistische Bundesamt und die Statistischen Landesämter den obersten Bundes- und Landesbe-

hörden für Planungszwecke nur Tabellen mit statistischen Ergebnissen übermitteln und zwar auch dann, wenn die Tabellenfelder nur einen einzigen Fall ausweisen (§ 16 Abs. 4 Bundesstatistikgesetz). Diese Informationen reichen für die Landesplanung völlig aus.

13.3
Studentendaten

(13. Tätigkeitsbericht, Ziff. 2.4.2, 14. Tätigkeitsbericht, Ziff. 13.2.1, 15. Tätigkeitsbericht, Ziff. 11.1.5)

Das gesetzliche Regelungsdefizit bei der Verarbeitung von Studentendaten zu Verwaltungszwecken konnte im vergangenen Jahr noch nicht beseitigt werden. Es gilt deshalb nochmals, an die anläßlich der Beratung meines 14. Tätigkeitsberichts einstimmig geäußerte Auffassung des Landtags zu erinnern, „daß im Hochschulbereich Rechtsvorschriften über die konkrete Regelung der Erhebung und Verarbeitung von personenbezogenen Daten zu Verwaltungszwecken geschaffen werden sollten" (Beschluß Nr. 7 zu meinem 14. Tätigkeitsbericht, Drucks. 11/6231 i.V.m. Protokoll der 84. Plenarsitzung vom 19. Juni 1986, S. 4979).

Ende 1986 hatte das Hessische Ministerium für Wissenschaft undKunst einen ersten Entwurf einer „Verordnung über das Verfahren der Immatrikulation, Rückmeldung, Beurlaubung und Exmatrikulation für Studenten an den Hochschulen des Landes Hessen" vorgelegt, über den auch ein erstes Gespräch mit dem Hessischen Datenschutzbeauftragten geführt worden ist. Mitte Dezember 1987 hat mir das Ministerium einen neuen Verordnungsentwurf zugesandt, zu dem ich allerdings aus zeitlichen Gründen noch keine Stellung nehmen konnte.

Fraglich ist, ob für die Rechtsverordnung eine ausreichende Ermächtigungsgrundlage vorhanden ist. Die Verordnung soll aufgrund der §§ 36 Abs. 8 und 88 Hessisches Hochschulgesetz (HHG) erlassen werden. Nach § 36 Abs. 8 HHG regelt das Hessische Ministerium für Wissenschaft und Kunst durch Rechtsverordnung das Verfahren der Immatrikulation, Rückmeldung, Beurlaubung und Exmatrikulation. § 88 bestimmt, daß der Hessische Minister für Wissenschaft und Kunst die zur Ausführung des Hessischen Hochschulgesetzes erforderlichen Rechtsverordnungen und Verwaltungsvorschriften erläßt. Beide Normen enthalten - entgegen der Ansicht des Hessischen Justizministeriums (Stellungnahme vom 24. September 1987) - keine hinreichend bestimmte Ermächtigung für die Regelung der Verarbeitung von Studentendaten zu Verwaltungszwecken. Zwar stellt die Hessische Verfassung (Art. 107 und 118) nicht die Anforderungen des Art. 80 Abs. 1 Satz 2 Grundgesetz, dennoch gebietet das Rechtsstaats- und Demokratieprinzip, daß auch in der Landesgesetzgebung die Ermächtigung hinreichend bestimmt ist (BVerfGE 58,277), d.h. auch hier müssen Inhalt, Zweck und Ausmaß der erteilten Ermächtigung im Gesetz festgelegt werden.

Eine günstige Gelegenheit zur Schaffung einer ausreichenden Ermächtigungsnorm bot die durch das Hochschulrahmengesetz notwendig gewordene Novellierung des Hessischen Hochschulgesetzes vom 6. Juni 1978. In der Anhörung des Landtagsausschusses für Wissenschaft und Kunst am 9. September 1987 zum Gesetzentwurf der Fraktionen der CDU und der F.D.P. für eine Anpassung hochschulrechtlicher Vorschriften an das Dritte Gesetz zur Änderung des Hochschulrahmengesetzes - Drucks. 12/158 - habe ich deshalb vorgeschlagen, folgende Regelung in das Hessische Hochschulgesetz aufzunehmen:

„Die Studienbewerber, Studenten und Prüfungskandidaten sind verpflichtet, für Verwaltungszwecke der Hochschulen personenbezogene Daten zum Hochschulzugang, zum Studium, zum Studienverlauf und zu den Prüfungen anzugeben. Das Ministerium für Wissenschaft und Kunst bestimmt durch Rechtsverordnung die anzugebenden Daten und die Zwecke, für die sie verarbeitet oder sonst genutzt werden dürfen."

Die SPD-Fraktion hat daraufhin beantragt, § 36 Abs. 8 HHG wie folgt zu ändern:

„(8) Das Hessische Ministerium für Wissenschaft und Kunst regelt durch Rechtsverordnung, welche Angaben die Studienbewerberin bzw. der Studienbewerber, die Studentinnen und Studenten, die Gasthörerinnen und Gasthörer für die Immatrikulation, Rückmeldung, Beurlaubung, Exmatrikulation und die Zulassung als Gasthörerin oder als Gasthörer erforderlich sind sowie das Verfahren einschließlich der Fristen. Dabei ist im einzelnen festzulegen, welche Angaben zur Person, zur Hochschulzugangsberechtigung und -zulassung, zum Studienverlauf, zu den Prüfungen und für die Zulassung als Gasthörerin bzw. als Gasthörer erforderlich sind." (Der Antrag enthält genau diesen Wortlaut; wahrscheinlich sollte es jedoch heißen: „... welche Angaben der Studienbewerberin bzw. des Studienbewerbers, der Studentinnen und Studenten, der Gasthörerinnen und Gasthörer ... erforderlich sind ...")

Der Landtag hat jedoch mehrheitlich beide Vorschläge unberücksichtigt gelassen. Das ist um so unverständlicher, als beispielsweise der baden-württembergische Gesetzgeber erst kürzlich eine meinem Vorschlag entsprechende Verordnungsermächtigung in das Universitätsgesetz, Gesetz über die Pädagogischen Hochschulen, Kunsthochschulgesetz und Fachhochschulgesetz aufgenommen hat (vgl. Gesetz zur Änderung der Hochschulgesetze vom 5. Oktober 1987, GBl. S. 397, Art. 1, Nr. 50, Art. 2, Nr. 35, Art. 3, Nr. 35 und Art. 4, Nr. 35).

Wiesbaden, den 26. Februar 1988

gez. Prof. Dr. Simitis

14. Materialien

14.1
Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 5. Mai 1987 zur Neukonzeption des Ausländerzentralregisters

I.
Unter Federführung des Bundesministers des Innern wird zur Zeit das bestehende Ausländerzentralregister (AZR) beim Bundesverwaltungsamt mit dem Ziel einer Effizienzsteigerung überarbeitet.

Grundsätzlich ist die beabsichtigte Schaffung einer verfassungsrechtlich notwendigen gesetzlichen Regelung sowohl für die Datenverarbeitung beim Bundesverwaltungsamt als auch für die Kommunikation der Teilnehmer mit dem Ausländerzentralregister zu begrüßen. Schon jetzt stehen den Benutzern weit über 100 Millionen Daten von ca. 10 Millionen Ausländern zur Verfügung. Geplant ist, die Verwendbarkeit des Datenbestandes durch den potentiellen Teilnehmerkreis des AZR zu erhöhen.

Dient das AZR bis jetzt vorwiegend der Aufenthaltsermittlung von Ausländern und der Vorbereitung ausländerrechtlicher Entscheidungen, so sieht die geplante Regelung eine „stärkere Einbindung in das System zum Schutz der inneren Sicherheit" sowie eine verbesserte Nutzung zu statistischen Zwecken vor. So ist die Einstellung des polizeilichen INPOL-Fahndungsbestandes in das AZR geplant.

Das Recht auf informationelle Selbstbestimmung steht auch den in der Bundesrepublik Deutschland und Berlin lebenden Angehörigen anderer Staaten zu. Eine Neuregelung muß daher vermeiden, daß besondere Vorschriften für diese Personengruppe zu einer allgemeinen Diskriminierung der Betroffenen als potentielle Rechtsbrecher führen.

II.
Von entscheidender Bedeutung für die datenschutzrechtliche Bewertung des Registers sind die Funktionen, die es erfüllen soll. Außer Frage steht seine Verwendung als Indexregister zum Zweck der Feststellung, ob eine - und wenn ja, welche - Ausländerbehörde Unterlagen über einen bestimmten Ausländer besitzt.

Damit soll das AZR den Zugang zu den eigentlichen Ausländer- und Meldedaten erleichtern; es kann und darf den Rückgriff auf die bei den örtlichen Behörden gesammelten Informationen nicht ersetzen. Allenfalls bei Eilentscheidungen sollten die im Register gespeicherten Daten unmittelbar für Maßnahmen der Verwaltung herangezogen werden. Keinesfalls darf das AZR zu einem bundesweiten zentralen Melderegister für Ausländer werden.

Für nicht-öffentliche Stellen und Privatpersonen darf der Zugang zu den Daten des AZR nur in eng begrenzten Ausnahmefällen gewährt werden, die gesetzlich festzulegen sind.

III.
Das Urteil des Bundesverfassungsgerichts zur Volkszählung 1983 ist wesentlicher Anlaß für die gesetzliche Neuregelung. Aus Gründen der Normenklarheit, der Bestimmtheit und der Zweckbindung muß die Regelung das Ausmaß der vorgesehenen Datennutzung abschließend festlegen.

Das Register dient nicht dem Vollzug von Verwaltungsentscheidungen durch die Registerbehörde selbst. Wenn seine Hauptfunktion die Unterstützung der Tätigkeit der Ausländerbehörden und der Polizei ist - soweit diese Stellen ausländer- und allgemein-vollzugspolizeiliche Aufgaben erfüllen - , so muß der Gesetzgeber diesen Verwendungszusammenhang darstellen. Es ist zu begrüßen, daß nicht nur die Verwendung der Daten im Register selbst, sondern auch ihre Anlieferung und Weitergabe an andere Dienststellen gesetzlich geregelt werden sollen. Nur wenn die Datenverarbeitung klar und eindeutig festgelegt ist, kann der Betroffene den Eingriff in sein Recht auf informationelle Selbstbestimmung einschätzen. Allein ein Registergesetz genügt diesen Anforderungen nicht. Eine zeitlich parallele Novellierung des Ausländerrechts ist deshalb unabdingbar. Gleichzeitig muß auch der Datenaustausch zu Fahndungszwecken und zur Erfüllung anderer polizeilicher Aufgaben in der Strafprozeßordnung und in den Polizeigesetzen geregelt werden.

IV.
Für den in das AZR aufzunehmenden Datensatz sind die vom Register zu erfüllenden Funktionen maßgeblich.

Entsprechend der Indexfunktion gehören in das AZR solche Daten über einen Ausländer, die das Auffinden bestimmter, zu einer Person angelegter Unterlagen zur Vorbereitung vor allem ausländerrechtlicher Entscheidungen ermöglichen.

Darüber hinaus ist geplant, den Benutzern unmittelbar Daten zur Verfügung zu stellen, um verschiedene Informationsansprüche zu erfüllen. Dadurch sollen zum Teil die Empfänger die Möglichkeit erhalten, auf die Beiziehung von Akten vor Entscheidungen zu verzichten.

Besonders problematisch ist die Speicherung und Verwendung des Datums „Einreisebedenken". Unter diesem Datum werden belastende Vorgänge im Umfeld des Ausländers erfaßt, die noch keine ausländerrechtlichen Maßnahmen ausgelöst haben. Damit erhält der Datensatz eine neue Qualität: Gespeichert werden nicht mehr

Informationen über in einem formalisierten und rechtsstaatlichen Verfahren ergangene Maßnahmen der Ausländerbehörde, sondern auch präzise Angaben über ein vermutetes (Fehl-) Verhalten des Ausländers selbst.

Der Mangel an Genauigkeit dieses Datums bedingt es, daß z.B. ein bei einer Grenzpolizeibehörde beantragter Ausnahmesichtvermerk nicht ohne Hinzuziehung der zugrunde liegenden Akte versagt werden kann. Die Voraussetzungen der Entstehung dieses Datums sowie seiner Verwendung bedürfen wegen des verfassungsrechtlichen Gebots der Normenklarheit einer Präzisierung. Dabei wird nicht verkannt, daß sich diese Regelung in denjenigen Fällen positiv auswirken wird, in denen in diesem Datenfeld keine Eintragung vorliegt, und dies dürfte die große Mehrheit sein. Wenn nämlich das Datum „Einreisebedenken" nicht belegt ist, besteht die Möglichkeit, etwa über einen Ausnahmesichtvermerk in einem beschleunigten Verfahren zu entscheiden, ohne daß auf die Ausgangsunterlagen zurückgegriffen werden muß.

Die geplante Aufnahme von Daten aus dem INPOL-Fahndungsbestand macht die Funktionserweiterung in den Polizeibereich hinein deutlich. Die Notwendigkeit der Aufzeichnung von Fahndungsnotierungen im AZR ist bisher angesichts möglicher Alternativen - z.B. eines regelmäßigen Datenabgleichs - nicht ausreichend dargelegt.

Die Speicherung von Suchvermerken kann hingenommen werden, wenn sie nur für die Verfolgung im Gesetz selbst festgelegter Zwecke erfolgt und - wie im Bericht des Bundesministers des Innern vorgesehen - zeitlich begrenzt zugelassen wird.

Bei den Daten, die ausschließlich für statistische und Planungszwecke erhoben werden sollen, ist sicherzustellen, daß ihre Verwendung getrennt von derjenigen anderer Daten des Ausländers erfolgt und die Angaben derart anonymisiert werden, daß die Verbindung zu den personenbezogenen Daten nicht mehr hergestellt werden kann.

V.
Die Kommunikation zwischen AZR und den verschiedenen Behörden oder Privatpersonen ist gesetzlich so zu regeln, daß sie den Anforderungen des Bundesverfassungsgerichts an den bereichsspezifischen Datenschutz gerecht wird.

Eine gesetzliche Regelung ausschließlich des Teilnehmerkreises und des Datenumfangs wäre nicht ausreichend, solange nicht präzise festgelegt wird, für welche konkreten Zwecke die Behörden Daten abrufen dürfen, bzw. das AZR an sie übermitteln darf. Nur eine verwendungsorientierte Regelung macht den potentiellen Verwendungszusammenhang transparent und würde den Anforderungen des Bundesverfassungsgerichts genügen.

Eine Festlegung, daß den Benutzern nur solche Daten übermittelt werden, die sie zur Aufgabenerfüllung benötigen, würde nicht ausreichen; es bedarf gerade der Festlegung derjenigen Aufgaben, zu deren Erfüllung Datenübermittlungen vorgenommen werden sollen. Auch eine Differenzierung nach Abfragearten, die jeweils verschiedene, stufenweise gestaffelte Datenmengen umfassen, wäre ungenügend, solange nicht feststeht, für welche Aufgaben welche Behörden die festgelegten Datenmengen abrufen können.

Der Online-Zugriff auf die im AZR gespeicherten Daten stellt eine besonders intensive Form des Zugriffs auf personenbezogene Informationen dar. Er bedarf daher der besonderen Rechtfertigung, die in der Aufgabenstellung der beteiligten Behörden begründet sein muß.

14.2
Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 5. Mai 1987 zum Entwurf einer Fahrzeugregisterverordnung

Zu der von der Bundesregierung dem Bundesrat zugeleiteten Fahrzeugregisterverordnung hat der Innenausschuß des Bundesrates am 29. April 1987 Änderungen vorgeschlagen, die datenschutzrechtlich nicht akzeptiert werden können.

Danach sollen u.a.

- der Umfang der Auswahlprotokollierung zur Feststellung des konkreten Anlasses der Abrufe und der für die Abrufe verantwortlichen Personen von 5 v.H. auf ein Promille der Fälle reduziert werden.

  Für die künftige Praxis bedeutete dies, daß eine systematische Überprüfung des Abfrageverhaltens der abrufberechtigten Dienststellen nicht mehr möglich wäre. Denn nach dem erwarteten Umfang der ZEVIS-Nutzung und der vorgesehenen Zahl der abrufberechtigten Dienststellen würde bei der beabsichtigten Reduzierung durchschnittlich alle zwei Monate nur eine Protokollierung pro Dienststelle erfolgen. Außerdem brauchte bei einer solchen Protokollierungspraxis eine abrufende Person mit der Protokollierung gerade ihres Abrufes ernstlich nicht mehr zu rechnen.

- für den großen Bereich der Straftaten und Verkehrsordnungswidrigkeiten eine konkrete Angabe des Anlasses der Abrufe entfallen, wodurch deren Nachprüfbarkeit nicht mehr gewährleistet wird.

Sinn und Zweck des § 36 Abs. 7 des Straßenverkehrsgesetzes ist die Vermeidung oder Unterbindung von Mißbrauch und falscher Rechtsanwendung durch wirksame Kontrolle der Abrufe seitens der Fachaufsicht und der Datenschutz-

beauftragten. Die vom Innenausschuß des Bundesrates vorgeschlagenen Änderungen der von der Bundesregierung vorgelegten Fahrzeugregisterverordnung wären daher mit dem Straßenverkehrsgesetz nicht vereinbar. Sie ließen eine wirksame Kontrolle des erstmals durch den Gesetzgeber geregelten automatisierten Abrufverfahrens nicht zu. Damit würde auch die vom Bundesverfassungsgericht im Volkszählungsurteil aufgestellte Forderung nach einer effektiven Datenschutzkontrolle durch unabhängige Datenschutzbeauftragte mißachtet.

Die Datenschutzbeauftragten weisen daher nachdrücklich darauf hin, daß die zu erlassende Fahrzeugregisterverordnung keinen rechtlichen Bestand haben könnte, falls die beabsichtigten Änderungen übernommen würden.

14.3
Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 5. Mai 1987 über Rückmeldung von der Justiz an die Polizei

I.
Die Datenschutzbeauftragten des Bundes und der Länder und die Datenschutzkommission Rheinland-Pfalz haben sich während ihrer Konferenz am 4./5. Mai 1987 mit dem Problem der Information der Polizei durch Staatsanwaltschaften und Gerichte über den Ausgang von Strafverfahren befaßt:

Die von der Polizei geführten Datensammlungen beruhen zu einem großen Teil auf Erkenntnissen, die im Rahmen der polizeilichen Tätigkeit in Strafverfahren anfallen. Diese Erkenntnisse sind vorläufiger Natur. Die tatsächlichen Feststellungen werden im weiteren Verlauf des Verfahrens oft ergänzt oder korrigiert; Staatsanwaltschaft und Gericht können zu einer anderen Bewertung von Strafbarkeit und Verschulden kommen. Polizeiliche Datensammlungen können mehr als sonstige behördliche Datensammlungen das verfassungsrechtlich geschützte Persönlichkeitsrecht der betroffenen Bürger beeinträchtigen; dies gilt vor allem dann, wenn aus kriminalpolizeilichen Sammlungen Erkenntnisse an andere Stellen weitergegeben werden.

Bei Datensammlungen der Polizei muß daher in besonderem Maße darauf geachtet werden, daß nur richtige, im Einzelfall tatsächlich erforderliche Daten für den jeweils zulässigen Zeitraum gespeichert werden. Um dies sicherzustellen, sieht eine Bestimmung der „Mitteilungen in Strafsachen" vor, daß die Staatsanwaltschaft die Polizei über den Ausgang der Strafverfahren unterrichtet. Tatsächlich jedoch erfährt die Polizei in vielen Fällen den Ausgang der Strafverfahren nicht oder nicht vollständig, was zur Folge hat, daß ihre Datensammlungen teilweise unrichtig sind und daß Daten nicht gelöscht werden, obwohl die Gründe, die zur Speicherung geführt haben, nicht mehr zutreffen. Dieser Zustand ist für den betroffenen Bürger besonders nach einem für ihn günstigen Verfahrensausgang nicht hinnehmbar. Die Unterrichtung über den Ausgang des Verfahrens ist unabdingbare Voraussetzung dafür, daß die Polizei ihre datenschutzrechtliche Pflicht zur Löschung oder Berichtigung erfüllen kann.

II.
In jedem Einzelfall hat deshalb eine Unterrichtung der Polizei zu erfolgen, die sicherstellt, daß sie die zur Aktualisierung ihrer Datensammlungen unerläßlichen Informationen erhält. Hierbei sind insbesondere folgende Grundsätze zu beachten:

- Bei Verurteilungen sind Straftatbestand und Strafmaß mitzuteilen.

- Wird der Betroffene freigesprochen, genügt in der Regel die Mitteilung des Urteilstenors. Wurde der Tatverdacht nicht ausgeräumt, benötigt die Polizei ergänzende Informationen, um feststellen zu können, ob zur Erfüllung polizeilicher Aufgaben weiterhin Daten über den Betroffenen zu speichern sind.

- Wird ein Strafverfahren eingestellt, sind die Rechtsgrundlagen für diese Entscheidung, ein etwa bestehendes Verfahrenshindernis oder die Einstellung mangels hinreichenden Tatverdachts mitzuteilen. Wurde der Tatverdacht nicht ausgeräumt, benötigt die Polizei ebenfalls ergänzende Informationen, um feststellen zu können, ob zur Erfüllung polizeilicher Aufgaben weiterhin Daten über den Betroffenen zu speichern sind.

Ist eine Unterrichtung in angemessener Zeit nicht erfolgt, muß sich die Polizei nach dem Ausgang des Verfahrens erkundigen.

III.
Das Recht auf informationelle Selbstbestimmung verlangt eine korrekte Datenspeicherung bei der Polizei ohne Ausnahme. Die Konferenz begrüßt deshalb Bemühungen einiger Justiz- und Innenverwaltungen, durch regelmäßige Übermittlungen von der Staatsanwaltschaft an die Polizei die Voraussetzungen für eine Aktualisierung der polizeilichen Datensammlungen zu schaffen, und drängt auf eine Beschleunigung.

Die Konferenz hält eine ausdrückliche gesetzliche Regelung entweder in dem geplanten Justizmitteilungsgesetz oder in der Strafprozeßordnung für erforderlich. Ungeachtet dessen ist auch in der Übergangszeit bis zu einer solchen gesetzlichen Regelung eine Unterrichtung der Polizei unerläßlich, wenn sie bei der Nutzung ihrer Datensammlungen nicht Gefahr laufen soll, das informationelle Selbstbestimmungsrecht der Betroffenen zu verletzen.

14.4
Beschluß der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 7. Dezember 1987 zur Speicherung personenbezogener Aids-Daten in polizeilichen Informationssystemen

In zwei gemeinsamen Sitzungen von Arbeitsgruppen der ständigen Konferenz der Innenminister und -senatoren sowie der Datenschutzbeauftragten des Bundes und der Länder wurde das Problem der Speicherung von personenbezogenen Aids-Hinweisen in polizeilichen Informationssystemen erörtert. Nach eingehender Beratung der Ergebnisse dieser Gespräche faßten die Datenschutzbeauftragten des Bundes und der Länder sowie die Datenschutzkommission des Landes Rheinland-Pfalz bei Gegenstimme des Bayerischen Landesbeauftragten für den Datenschutz folgenden Beschluß:

I.
Die Speicherung von HIV-Hinweisen soll die Eigensicherung von Polizeibeamten und evtl. auch den Schutz von Personen in Polizeigewahrsam gewährleisten, die mit HIV-Infizierten in Kontakt kommen. Die Datenschutzbeauftragten verkennen nicht, daß Polizeibeamte bei der Berufsausübung spezifischen Gefahren ausgesetzt sind und die notwendigen Maßnahmen ergriffen werden müssen. Insbesondere ein direkter Blutkontakt oder eine Verletzung mit infizierten Injektionskanülen bei Kontakten mit Drogenabhängigen stellen eine solche spezifische Gefährdung dar. Dem Anspruch der Polizeibeamten auf einen weitestgehenden Schutz vor einer Infektion, die zu einer tödlichen Erkrankung führen kann, steht der Anspruch der infizierten Person gegenüber, daß Datenspeicherungen nur dann vorgenommen werden, wenn diese geeignet sind, die Gefährdung wirksam zu verringern und sie dadurch nicht unverhältnismäßig belastet werden. Hierbei ist auch zu berücksichtigen, daß eine automatisierte Speicherung von medizinischen Daten eine schwerwiegende Beeinträchtigung für die Betroffenen darstellt. Ebenso sind auch die gravierenden sozialen Folgen für diesen Personenkreis zu bedenken, wenn die gespeicherten Daten an Dritte gelangen.

II.
Sowohl medizinische Experten als auch Fachleute aus dem Sicherheitsbereich und dem Gesundheitsbereich haben wiederholt Zweifel daran geäußert, daß durch die Speicherung von Informationen über HIV-Infizierte in polizeilichen Informationssystemen die Gefährdung von Polizeibeamten abgewendet werden kann. Hierfür werden folgende Gründe vorgebracht:

In vielen Situationen wie z.B. bei der Hilfeleistung für verletzte Unfallopfer, der Festnahme unbekannter Personen oder auch der plötzlichen Konfrontation mit Straftätern oder Störern sei eine vorherige Überprüfung vorhandener Dateibestände ohnehin nicht möglich. Hinzu komme, daß der Polizei immer nur ein sehr geringer Teil der Infizierten bekannt sein werde, so daß die Polizei in jedem Fall und auch ohne besondere Hinweise Schutzmaßnahmen treffen müsse.

Angesichts dieser Zeifel, die von den Datenschutzbeauftragten geteilt werden, kann die Speicherung - wenn überhaupt - nur unter sehr eingeschränkten Voraussetzungen hingenommen werden. Möglich erscheint dies allenfalls für Situationen, in denen es mit hoher Wahrscheinlichkeit zu gewaltsamen Auseinandersetzungen mit infizierten Personen kommt. Keinesfalls darf eine „Aids-Datei" entstehen. Im übrigen wäre dabei mindestens folgendes zu beachten:

1. Die Speicherung von HIV-Hinweisen im Datenfeld der „personengebundenen Hinweise" im bundesweiten Inpol-System und in vergleichbaren Landessystemen muß eingestellt werden, da diese Hinweise bei sämtlichen Abfragen erscheinen.

2. HIV-Hinweise dürfen allenfalls in solche Dateien aufgenommen werden, in denen sie als Grundlage für die Eigensicherung bei polizeilichem Einschreiten tatsächlich in Betracht kommen.

3. Die Speicherung von HIV-Hinweisen aufgrund von Verdächtigungen und ungeprüften Informationen verbietet sich in jedem Fall. Kommt die Information vom Betroffenen selbst, muß dieser über die Tatsache und die Bedeutung der Speicherung aufgeklärt werden. Im übrigen kommt nur die Speicherung von ärztlich gesicherten Informationen in Betracht, die die Polizei rechtmäßig erlangt hat.

4. Auf die gespeicherten Daten darf nur ein besonders dazu befugter Benutzerkreis zugreifen, und dies nur zu Zwecken der Eigensicherung. Die Weitergabe an andere Stellen ist nur in besonders festzulegenden Fällen zulässig.

5. Es muß in jedem Fall erkennbar sein, wer wann den HIV-Hinweis in das System eingespeichert hat und hierfür verantwortlich ist, da nur so die Speicherungspraxis überprüft werden kann und notwendige Berichtigungen ermöglicht werden.

Sachwortverzeichnis zum 16. Tätigkeitsbericht