11. Wahlperiode

Drucksache **11/3215**

HESSISCHER LANDTAG

14. 02. 85

Dreizehnter Tätigkeitsbericht des Hessischen Datenschutzbeauftragten

Mit Schreiben vom 13. Februar 1985 legt der Datenschutzbeauftragte gemäß § 29 des Hessischen Datenschutzgesetzes vom 31. Januar 1978 dem Landtag folgenden Tätigkeitsbericht vor:

Eingegangen am 14. Februar 1985 · Ausgegeben am 12. März 1985

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

M/3215

INHALTSVERZEICHNIS

Kernpunkte des 13. Tätigkeitsberichts

1. Ein bundesweiter "Warndienst" vor angeblichen Sozialhilfe-Betrügern verletzt das Sozialgeheimnis (2.1.1).

2. Die Speicherung aller Freitodversuche durch die Polizei ist unzulässig (2.2.1).

3. Vor Ablehnung der Einstellung aufgrund einer Sicherheitsüberprüfung durch den Verfassungsschutz muß der Betroffene angehört werden (2.2.3).

4. Daten dürfen vor Erteilung einer beantragten Auskunft nicht gelöscht werden (2.2.5).

5. Die Gebührenpflicht für Auskünfte muß auch für Arbeitnehmerdaten und in der Sozialverwaltung abgeschafft werden (2.5).

6. Die deckungsgleiche Übernahme der Datenschutzregelungen im Staatsvertrag über den Bildschirmtext in Rechtsvorschriften des Bundes ist unverzichtbar (3.1.1).

7. Neue Postdienste wie das Fernwirksystem TEMEX dürfen ohne landesrechtliche Nutzungsregelungen nicht eingeführt werden (3.1.2).

8. Der neue Entwurf zum Volkszählungsgesetz erfüllt nicht die Anforderungen des Bundesverfassungsgerichts, wenn an der mündlichen Auskunftspflicht gegenüber dem Zähler festgehalten und der Inhalt des Fragebogens nicht gesetzlich geregelt wird (3.2.2).

9. Der Schutz von Arbeitnehmerdaten ist unzureichend. Eine kollektivrechtliche Regelung allein genügt nicht. Der Gesetzgeber muß auch und gerade die individuellen Rechte der Arbeitnehmer im Hinblick auf die Verarbeitung ihrer Daten präzisieren (3.3).

10. "Modellversuche zur Leistungs- und Kostentransparenz" in der Sozialversicherung bedürfen, wenn sie mit der Verarbeitung einer Vielzahl persönlicher Daten verbunden sind, präziser gesetzlicher Regelungen (3.4).

11. Bei der überfälligen gesetzlichen Regelung der polizeilichen Datenverarbeitung sind insbesondere Bedingungen für die Datenerhebung, den Einsatz von Video-Geräten und die Beobachtung von Versammlungen festzulegen (3.5.1).

12. Für den maschinenlesbaren Personalausweis besteht nach wie vor kein begründeter Bedarf (3.5.2).

13. Das Zentrale Verkehrsinformationssystem (ZEVIS) des Kraftfahrtbundesamtes darf nicht für bundesweite polizeiliche Personen-Anfragen im Direktabrufverfahren genutzt werden (3.5.3).

14. Der Bürger sollte unter Berücksichtigung bestimmter verfahrenstechnischer Bedingungen regelmäßig in Form eines "Daten-Kontoauszugs" über die zu seiner Person gespeicherten Daten informiert werden (3.6).

1. Zur Situation

1.1
Datenschutzdefizite

Die ständige kritische Begleitung durch das Parlament ist ohne Zweifel eines der wichtigsten Merkmale des Datenschutzes in Hessen. Der Landtag hat den Datenschutz von Anfang an in die parlamentarische Diskussion einbezogen und in ihr einen entscheidenden Ansatz gesehen, um der Entwicklung des Datenschutzes neue Impulse zu vermitteln. Nie zuvor hat der Landtag freilich seine Erwartungen so konkret und detailliert geäußert wie in seinem Beschluß zum 12. Tätigkeitsbericht und zu der damit zusammenhängenden Stellungnahme der Landesregierung. Anlaß genug, um 15 Jahre nach der Verabschiedung des ersten und 7 nach der des zweiten Hessischen Datenschutzgesetzes nach den Defiziten des Datenschutzes zu fragen.

Keineswegs geht es darum, auch nur einen Augenblick lang den entscheidenden Beitrag zu bestreiten, den gerade Hessen zum Datenschutz geleistet hat. Hier ist er entstanden und hier ist es über die Jahre hinweg immer wieder gelungen, sich den Herausforderungen einer sich ständig verändernden Informationstechnik zu stellen und sie in neue, auf einen besseren Datenschutz bedachte Regelungen umzumünzen. Kaum verwunderlich deshalb, wenn auch dieser Tätigkeitsbericht hinreichend Beispiele für das Bemühen des Landes enthält, den Datenschutz nicht zur bedeutungslosen Routine erstarren zu lassen, sondern als fortwährende, zu neuen Anstrengungen verpflichtende Aufgabe zu begreifen.

Allzu groß ist freilich die Versuchung, die historische Rolle des Landes bei der Entwicklung des Datenschutzes zu benutzen, um vorschnell festzustellen, wo noch Überlegungen zum Datenschutz notwendig seien, erschöpften sie sich in Reflexionen über kleinere Details, wirkliche Probleme gäbe es dagegen nur anderswo. Ein Grund mehr, um die Realität des Datenschutzes, damit aber auch und gerade seine Defizite in Erinnerung zu rufen. Sie lassen sich auf drei, im Tätigkeitsbericht ausführlich angesprochenen Ebenen lokalisieren: der bedenklich lückenhaften Datensicherheit, dem auch nach so vielen Jahren der gesetzlichen Garantie des Datenschutzes erstaunlichen Beharrungsvermögen der Verwaltung in überholten Strukturen und dem nach wie vor mangelnden Konzept einer langfristigen Auseinandersetzung mit den gesellschaftlichen und politischen Folgen einer sich rapide wandelnden Informationstechnologie.

1.2
Datensicherheit

1.2.1
Vorfälle

Zunächst zur Datensicherheit: Der Tätigkeitsbericht geht ausdrücklich auf eine Reihe von Fällen ein. Listen mit hochempfindlichen Daten wurden in Mülltonnen gefunden (2.3.1), eindeutig gesperrte Angaben in Adreßbüchern (2.3.3) und Bänder mit Informationen, die längst hätten gelöscht werden müssen, gelangten in die Hände Außenstehender (2.3.2). Vordergründig durchweg recht peinliche Vorfälle, die aber, so möchte man meinen, nicht sonderlich aufregend sind. Schließlich hat es Ähnliches schon früher gegeben. In Schränken vergessene Akten oder auf offener Straße herumflatternde Auszüge haben bereits Material für manchen Tätigkeitsbericht geliefert. Auf den ersten Blick spricht zudem viel dafür, in jedem dieser Fälle letztlich nicht mehr zu sehen als den Ausdruck bedauerlichen, doch unvermeidlichen menschlichen Versagens. Drei Gründe zwingen freilich dazu, gerade diesen Vorfällen weit mehr Aufmerksamkeit als bisher zu schenken.

Eines fällt sofort auf. Im Unterschied zu manch anderer, länger zurückliegenden, aber durchaus vergleichbaren Situation waren beispielsweise sowohl in Frankfurt als auch in Gießen (vgl. 2.3.1) die notwendigen organisatorischen Voraussetzungen, die gerade eine Vernichtung der Daten sicherstellen sollten, getroffen worden. Die Stadtverwaltung verfügte sehr wohl über die notwendige technische Ausstattung, um die Unterlagen zu zerreißen, das Finanzamt war schon früher vom zuständigen Minister an seine Datensicherungspflichten erinnert worden. Der Mangel ist also anderswo zu suchen, genauer: in der offensichtlich nach wie vor bestehenden Unfähigkeit, die Bedeutung der Verarbeitung personenbezogener Daten und die mit ihr einhergehenden Gefahren richtig einzuschätzen. Es ist eben nicht gleichgültig, auf welche Angaben bei der behördlichen Tätigkeit zurückgegriffen wird. Der Gesetzgeber hat klare Trennungslinien gezogen und mit den Datenschutzvorschriften verbindliche Prioritäten formuliert. Just diesem Unterschied kann nicht allein durch den immer wiederkehrenden Hinweis auf Erlasse und Richtlinien Rechnung getragen werden. Allzu offenkundig ist die Gefahr, die Verantwortung für den Datenschutz nur als eine rein formale Aufgabe zu verstehen, statt in der täglichen Verwaltungspraxis das Bewußtsein für die Besonderheiten der Verarbeitung personenbezogener Daten zu schärfen. Der Datenschutz fordert mehr als einen bloßen Austausch von Vorschriften, er verlangt eine andere Mentalität im Umgang mit personenbezogenen Daten, eine Verwaltung also, die von sich aus jederzeit und aktiv auf Verarbeitungsbedingungen hinwirkt, die den vom Gesetzgeber gewollten restriktiven Zugriff auf personenbezogene Daten sicherstellen.

1.2.2
Verantwortlichkeit

Überdies: Die rein formale Betrachtung der Datenschutzprobleme führt, wie sich wiederum am Tätigkeitsbericht ablesen läßt, alsbald zu verstärkten Anstrengungen, sich der Verantwortung für die Verarbeitung möglichst zu entledigen, indem sie entgegen den Intentionen der gesetzlichen Regelung den Rechenzentren zugeschoben wird. Bezeichnend dafür ist die Auseinandersetzung um das Wiesbadener Adreßbuch (vgl. 2.3.3). Das Gesetz läßt Zweifel gar nicht erst aufkommen. Die Kommunalen Gebietsrechenzentren verarbeiten die Daten für ihre jeweiligen Auftraggeber. Diesen und niemandem sonst obliegt es daher, sich zu vergewissern, ob die verarbeiteten Angaben unter Bedingungen an Dritte weitergelangen, die den gesetzlichen Erwartungen entsprechen. Anders ausgedrückt: Wo die Gemeinde die Daten verarbeiten läßt, innerhalb ihres eigenen Bereiches mit ihren Mitteln und ihren Bediensteten oder bei einem Dritten, der in ihrem Auftrag und für sie handelt, ist völlig gleichgültig. Das Gesetz interessiert sich ausschließlich für einen maximalen Schutz des Betroffenen. Die Gemeinde ist insofern frei, den von ihr für richtig gehaltenen organisatorischen Weg zu gehen, sie muß aber in jedem Fall das gesetzlich geforderte Maß an Sicherheit des Betroffenen erfüllen. Kein Wunder, wenn sich deshalb Innenminister und Datenschutzbeauftragter insoweit einig waren. Verwunderlich, aber nicht überraschend ist allenfalls der Widerstand der betroffenen Stadt. Für sie, aber auch für jeden anderen Teil der öffentlichen Verwaltung, bietet die Verselbständigung der Verarbeitung in Gestalt der Kommunalen Gebietsrechenzentren zugleich die Chance, sich einer Risikoquelle zu entledigen. Die Organisation der Verarbeitung wird zum Anlaß genommen, um zugleich die Verantwortungsbereiche neu zu definieren.

Wie kurzsichtig und widersprüchlich solche Reaktionen freilich sind, zeigt sich auch daran, daß sich die gleiche Verwaltung, die auf ihre mangelnde Kompetenz für die Verarbeitungsvorgänge und damit auf ihre fehlende Verantwortung hinweist, in steigendem Maße für eine dezentralisierte Verarbeitung interessiert und in immer größerem Umfang just die apparative Ausstattung anstrebt, die den Verarbeitungsprozeß mehr und mehr an den einzelnen Arbeitsplatz zurückführt. Eine solche Entwicklung kann und darf nur unter der Voraussetzung entsprechender, die Datensicherheit garantierender Vorkehrungen zulässig sein. Genau hier liegt aber der Sinn einer erneuten intensiven Auseinandersetzung mit den im Tätigkeitsbericht erwähnten Vorkommnissen. Mit den Veränderungen der automatischen Verarbeitung bekommt auch die Datensicherheit eine ganz andere Bedeutung. So gesehen, sind die bisherigen kritischen Fälle Alarmzeichen, die es rechtzeitig aufzugreifen gilt, will man Konsequenzen vermeiden, die von ihrer Bedeutung her keinen Vergleich mit vergessenen Akten oder unzerstört in die Mülltonne geworfenen Unterlagen dulden.

1.2.3
Verletzlichkeit neuer Systeme - Verletzlichkeit der Gesellschaft

Symptomatisch dafür sind die erst jüngst diskutierten Sicherheitsmängel beim Bildschirmtext (vgl. 3.1.1). Ihre Tragweite läßt sich letztlich nur verstehen, wenn zugleich die gegenüber der ersten Zeit der Datenverarbeitung radikal veränderten Umweltbedingungen bedacht werden. Die automatische Verarbeitung war über viele Jahre ein praktisch nur wenigen Spezialisten zugänglicher Vorgang. Ihre Abschottung in besonderen Rechenzentren verschärfte zudem ihre Exklusivität. Beides gilt nicht mehr. Spätestens an der Diskussion über den Computer in der Schule ist sichtbar geworden, daß die Kenntnis der Datenverarbeitung und die Fähigkeit zum Umgang mit der technischen Apparatur mehr und mehr zu den notwendigen, allgemeinen Wissensvoraussetzungen gezählt werden. In dem Maße aber, in dem sich diese Vorstellungen durchsetzen, wächst notwendigerweise auch die Vertrautheit mit dem Computer, wird er zu einem Instrument, das zu beherrschen kein Privileg, verbunden mit einem Spezialisten vorbehaltenen Wissen, mehr ist. Begünstigt wird diese Entwicklung durch eine Produktionstechnik, die an die Stelle der gleichsam klassischen, schwerfälligen Rechner den jedermann zugänglichen Personal-Computer setzt. Die Kehrseite ist eine steigende Verletzlichkeit der Gesellschaft. Die Informationssysteme werden immer anfälliger für unbefugte Eingriffe. Anders ausgedrückt: Das sich verbreitende sowie verfestigende Wissen über die Informationstechnik destabilisiert zugleich die vorhandenen und neu eingeführten Informationssysteme.

Längst ist die automatische Verarbeitung zum unentbehrlichen Administrationsinstrument geworden. Längst ist es aber auch und gerade deshalb selbstverständlich, die personenbezogenen Daten zu speichern, von den alltäglichen Angaben, wie etwa Name und Anschrift, bis hin zu den sensibelsten, wie beispielsweise Gesundheitsdaten. Zum ersten Mal aber sieht sich die immer weiter ausgebaute automatische Verarbeitung einer ständig zunehmenden Zahl von einzelnen gegenüber, die durchaus in der Lage sind, deren Gesetzlichkeiten nachzuvollziehen und in das System einzudringen. Wie unbeachtet diese Entwicklung geblieben ist, zeigt sich nicht zuletzt an den üblichen, in den verschiedenen gesetzlichen Regelungen aufgezählten Sicherheitsvorschriften. Da ist von allen möglichen Verpflichtungen, etwa den Zugang zum Rechenzentrum zu kontrollieren, die Rede, aber der Zugang zum System, so wie ihn eine veränderte Technik, gepaart mit einem sich verbreitenden Wissen, möglich macht, bleibt genaugenommen außer Betracht. Ja noch mehr: Der Aufwand, mit dem neue Informationstechniken propagiert und

popularisiert werden, steht in keinem Verhältnis zum Aufwand für die Datensicherheit. Die Erfahrungen mit dem Bildschirmtext sind symptomatisch dafür. Man kann sie nicht mit dem Hinweis beiseiteschieben, es handle sich um nicht wiederholbare, durch irgendwelche Sonderbedingungen begünstigte Ausnahmefälle. Sie sind in Wirklichkeit typisch für die Anfälligkeit eines auf seine Sicherheit hin nicht durchdachten Systems. Wer bereit ist, einen Augenblick lang über die Grenzen der Bundesrepublik hinauszusehen, stellt zudem alsbald fest, wie sich die Erfahrungen wiederholen. So wenig es aber an Studien über den Nutzen und die Unentbehrlichkeit neuer Informationstechniken fehlt, so sehr mangelt es an Reflexionen über die Verletzlichkeit der Gesellschaft, die durch eben diese Systeme maximiert wird. Die eher zurückhaltenden Ansätze in den skandinavischen Ländern sind weitgehend unbeachtet geblieben.

1.2.4
Datensicherheit - Aufgabe des Anwenders

Man kann sich auch nicht mit dem Argument herausreden, die gesetzlichen Regelungen hätten schließlich besondere Kontrollinstitutionen, die Datenschutzbeauftragten, vorgesehen, deren Bedeutung zudem vom Bundesverfassungsgericht nachdrücklich hervorgehoben worden sei. Ohne Zweifel fällt den Datenschutzinstanzen eine weitgehend präventive Kontrollfunktion zu. Nur dürfen ihre Möglichkeiten nicht überschätzt werden. Kein seine Aufgabe noch so gewissenhaft erfüllender Datenschutzbeauftragter ist allein, ohne kooperative Informationshilfe durch die Verwaltung, in der Lage, Sicherungskonzepte zu entwickeln, die in die Informationstechnik aufgenommen werden müßten, um den Zugriff Außenstehender und die Zweckentfremdung der Verarbeitung zu verhindern. Wiederum gilt es auf die Erfahrungen mit dem Bildschirmtext zu verweisen. Penetrant, aber umsonst haben die Datenschutzbeauftragten nach Informationen gefragt, um sich dann bei ihren Überlegungen auf eigene Spekulationen auf dem Hintergrund eines spärlichen, mehr oder weniger zufälligen Informationsmaterials stützen zu müssen. Zudem und letztlich weitaus wichtiger: Den Datenschutzbeauftragten fehlt es an der notwendigen technischen Kapazität und Kompetenz, um gleichsam begleitend zu der rapiden Entwicklung der Informationstechnik Sicherheitsvorkehrungen bereitzustellen. Dies kann auch nicht ihre Aufgabe sein. Vielmehr ist es die ureigenste Verpflichtung desjenigen, der neue technische Verarbeitungsmöglichkeiten produziert, zugleich auch die den Datenschutz garantierenden Sicherheitsbedingungen zu realisieren.

Kurzum, die Datenschutzbeauftragten dürfen nicht zu einem Alibi für die mangelnde Auseinandersetzung mit einer der veränderten Informationstechnik entsprechenden Datensicherheit stilisiert werden. Ihre Existenz entpflichtet nicht von der Aufgabe, verbesserte Verarbeitungsmodalitäten mit adäquaten Sicherheitsvorkehrungen zu koppeln. Eben deshalb geht es nicht an, sich lediglich darüber Gedanken zu machen, wie auch die öffentliche Verwaltung möglichst bald und umfassend auf die Vorteile der neuen Informationstechniken zurückgreifen könnte. Jedem Schritt auf diese Techniken hin muß eine überzeugende Antwort auf die Frage nach einer technisch ebenso einwandfreien Abwehr von Eingriffen in die Datenbestände vorausgehen. Solange es an einer solchen Antwort fehlt, potenziert die Entwicklung der Datenverarbeitung die Verletzlichkeit der Gesellschaft.

Spätestens mit dem Personal-Computer und dem Bildschirmtext rückt daher die Datensicherheit in den Mittelpunkt der Datenschutzüberlegungen. So unentbehrlich nach wie vor normative Anstrengungen zur Steuerung und Kontrolle der Verarbeitung sind, so deutlich gewinnt der Datenschutz daneben eine technische Dimension. Erst wenn er auch und gerade als technisch-konstruktive Anforderung verstanden und praktiziert wird, kann die gesetzliche Regelung eine realistische Absicherung bieten. Damit einher muß allerdings eine Auseinandersetzung mit der Sicherheit der bestehenden Informationssysteme gehen. Sie sind, um es noch einmal zu sagen, auf einem ganz anderen Hintergrund entstanden und deshalb zu keinem Zeitpunkt bisher vergleichbaren Belastungen ausgesetzt gewesen. Insofern kommt es jetzt vor allem darauf an, sie in Kenntnis der veränderten Umweltbedingungen gezielt auf ihre Sicherheit zu prüfen.

1.3
Widerstände der Verwaltung

Das Hessische Datenschutzgesetz hat von Anfang an bewußt davon abgesehen, dem Datenschutzbeauftragten Sanktionsmöglichkeiten einzuräumen. Es vertraut statt dessen auf die Verbindung konsequenter Kontrolle und intensiver öffentlicher, vor allem parlamentarischer Diskussion. Sie ist letztlich das eigentliche und entscheidende Korrektiv. Funktionieren kann es freilich nur, wenn die über die Kontrolle des Datenschutzbeauftragten und die parlamentarische Auseinandersetzung vermittelten Anregungen von der Verwaltung aufgenommen und in datenschutzkonforme Maßnahmen umgesetzt werden.

1.3.1
Einzelfälle

Ohne Zweifel haben sich die Vorstellungen des Gesetzgebers in einer Vielzahl von Fällen als richtig erwiesen. Ebensowenig läßt sich bestreiten, daß kein anderes Regelungssystem ein vergleichbares und gerade im Hinblick auf die fortschreitende Veränderung der Verarbeitungsbedingungen unentbehrliches Maß an Flexibilität bieten kann. Im vom Erfahrungsaustausch geprägten Dialog zwischen Verwaltung und Datenschutzbeauftragten kann sich weit besser als über irgendwelche Sanktionsmechanismen die notwendige Anpassung der Verwaltung an die vom Datenschutz geprägten Verarbeitungsbedingungen vollziehen. Die prinzipielle Richtigkeit dieser Regelung darf allerdings nicht dazu verleiten, Widerstände in der Verwaltung zu übersehen oder zu verharmlosen. Bezeichnend dafür sind die im Tätigkeitsbericht referierten Schwierigkeiten bei der Verwirklichung der für das Hochschulrechenzentrum in Gießen erforderlichen Sicherungsmaßnahmen (vgl. 4.3.1). Die Beanstandung, ausgelöst durch die festgestellte unzureichende Datensicherheit, liegt mittlerweile fast drei Jahre zurück. Der Landtag hatte sich im Anschluß an den 10. Tätigkeitsbericht unmittelbar eingeschaltet, der Kultusminister die erforderlichen Mittel vorgesehen. Geschehen ist nichts. Wenn bei einer so eindeutigen Ausgangslage notwendige Vorkehrungen bei einer Verarbeitung höchst sensibler Daten unterbleiben, dann steht es schlecht um die Glaubwürdigkeit der öffentlichen Verwaltung bei ihren Beteuerungen, den Datenschutz ernst zu nehmen und sich bei ihren Entscheidungen auch danach zu richten.

Ohnehin hat sich spätestens bei der Diskussion über die Auswirkungen der Entscheidung des Bundesverfassungsgerichts zum Volkszählungsgesetz erwiesen, wie schwer es der öffentlichen Verwaltung immer wieder fällt, den Datenschutz als Handlungsmaxime und nicht als lästige Barriere bei der Verwirklichung der eigenen Vorstellungen zu begreifen. Sicher, die Landesregierung hat, wie sich beispielsweise am im September 1984 veranstalteten Symposium zeigt, schnell auf die Notwendigkeit reagiert, die vorhandenen Regelungen auf ihre Übereinstimmung mit den Datenschutzanforderungen zu überprüfen. Genauso signifikant sind die Bundesratsinitiativen der Landesregierung bei der Erörterung des geplanten neuen Volkszählungsgesetzes, um nur noch dieses Beispiel zu nennen. Der eigentliche Test ist nicht die abstrakte Diskussion über die Korrektur und Entwicklung des Datenschutzes, sondern die gesetzliche Neuregelung. Zur Debatte steht mehr als nur die Revision bestehender oder die Einführung neuer Regelungen, sei es auf der Ebene des Datenschutzgesetzes selbst, sei es im Hinblick auf spezifische Verarbeitungszusammenhänge, wie etwa bei den Sicherheitsbehörden. Zur Debatte steht zugleich die Fähigkeit der öffentlichen Verwaltung, konkret und ständig die eigenen Verarbeitungserwartungen zu überprüfen und sich dabei auch zu fragen, wie der Bestand an personenbezogenen Daten reduziert und ein weiterer Zugriff vermieden werden kann.

Die Schwierigkeiten sind offensichtlich beträchtlich. Hinweise im Tätigkeitsbericht auf eine gründliche Durchforstung bestehender Dateien mit dem Ergebnis einer Verminderung des Datenbestandes besitzen Seltenheitswert. Mit der größte Berichtsteil ist nach wie vor der Auseinandersetzung mit den Plänen für die Einführung neuer Informationssysteme und Dateien gewidmet. Immerhin, der diesjährige Bericht fügt sich nicht ganz in dieses Schema. So gab etwa die Polizei ihre Datei der Freitodversuche auf (vgl. 2.2.1). Nur: Der Verzicht hätte ohne die vorherige Diskussion, die Kritik des Datenschutzbeauftragten und die unmittelbare Intervention des Innenministers schwerlich stattgefunden. Zudem: Das beim Datenschutzbeauftragten geführte Register verzeichnet mittlerweile eine ganze Reihe polizeilicher Dateien, bei denen die Frage ihrer Existenzberechtigung sehr sorgfältig geprüft werden muß. So gesehen, kann und darf die Auseinandersetzung mit der Datei über Freitodversuche nur ein erster Schritt einer genauen Revision der Datenbestände sein.

Wie viel leichter es dagegen fällt, neue Dateien einzurichten, zeigt das Beispiel der Warnmeldungen vor "Unterstützungsschwindlern" (vgl.2.1.1). Hier gilt es, sich nicht damit zufriedenzugeben, daß die kritische Reaktion des Datenschutzbeauftragten zu einer schnellen Einstellung der Verarbeitung geführt hat. Die Kooperationsbereitschaft der öffentlichen Verwaltung mag zwar in dieser Situation außer Frage stehen. Was aber mindestens ebenso interessiert, sind die Vorstellungen, die zu einer solchen eindeutig unzulässigen Datei geführt haben. Für die Verwaltung war es fast selbstverständlich, die Datei einzurichten. Die Rechtfertigung folgte für sie aus der Aufgabe, eine korrekte Leistung sicherzustellen. Die Verarbeitung der Daten war, so gesehen, nicht mehr als ein technisches Hilfsmittel. Welche Konsequenzen sie sonst haben könnte, wie sich die Stigmatisierung als "Unterstützungsschwindler" auf dem Hintergrund höchst pauschaler Annahmen für den Betroffenen auswirkt, und vor allem, was unter diesen Umständen noch vom immer wieder bekräftigten und gesetzlich garantierten Sozialgeheimnis übrig bleibt, wurde gar nicht erst bedacht. Eben diese kritiklose Instrumentalisierung der Datenverarbeitung für eine ganz allgemein gefaßte und in dieser abstrakten Form durchaus einleuchtende Aufgabe macht den Kern der Schwierigkeiten bei der Verwirklichung des Datenschutzes aus.

Nichts anderes vollzieht sich dort, wo etwa generell auf die öffentliche Sicherheit, die Solidarität der Versicherten oder überhaupt auf die Funktionsfähigkeit der öffentlichen Verwaltung hingewiesen wird. Jede dieser Formeln reicht zunächst einmal aus, um nahezu alle Verarbeitungsintentionen abzudecken. Nicht von ungefähr ist der lange und mühsame Weg zu einer bereichsspezifischen Regelung der polizeilichen Datenverarbeitung noch immer nicht beendet. Mit allgemeinen Hinweisen auf die Notwendigkeit eines Schutzes der öffentlichen Sicherheit ist es spätestens seit der Entscheidung des Bundesverfassungsgerichts zum Volkszählungsgesetz nicht mehr getan, auch und gerade bei der vorbeugenden Verbrechensbekämpfung. Was nottut, sind präzise Aussagen zur Erhebung, Speicherung und Übermittlung personenbezogener Daten durch die Polizei. Sollen aber solche Regelungen eine reale Steuerungschance haben, müssen sie auch die Bedingungen festlegen, unter denen neue Dateien errichtet werden dürfen, und zugleich eine konstante Überprüfung der vorhandenen Datensammlungen vorsehen. Jeder Schritt in diese Richtung zwingt freilich zugleich zur Selbstbeschränkung. Nicht die offene, maximale Nutzung des Instruments der Datenverarbeitung ist der Sinn der vom Landtag geforderten Regelung, sondern die kritische Revision der bisherigen Praxis und die gezielte Einschränkung im Umgang mit der Verarbeitung personenbezogener Daten. Dies ist der Ausgangspunkt sowohl der im Tätigkeitsbericht enthaltenen Überlegungen als auch der in den Gesprächen mit dem Innenminister formulierten Position des Datenschutzbeauftragten; und davon wird auch bei den Beratungen der geplanten gesetzlichen Regelung auszugehen sein.

Vor einem Mißverständnis muß man sich freilich hüten: Die Tendenz, sich unter Berufung auf eine möglichst allgemein formulierte Aufgabe die Vorteile der Datenverarbeitung zunutze zu machen und sich damit die unbequeme und oft komplizierte Auseinandersetzung mit dem Datenschutz zu ersparen, ist keineswegs auf den öffentlichen Bereich beschränkt. Sie kehrt bei fast jedem wieder, der personenbezogene Daten, ganz gleich zu welchem Zweck und in welchem Kontext auch immer, verarbeiten möchte. Nahezu durchweg wird zunächst alle Anstrengung darauf verwendet, die Besonderheit der eigenen Aufgabe hervorzuheben, um dann aus eben dieser Eigenart das Privileg zu folgern, personenbezogene Daten möglichst ungebunden zu verarbeiten. So hat sich beispielsweise die Diskussion über den Zugriff auf personenbezogene Daten im Rahmen der wissenschaftlichen Forschung abgespielt und so verläuft sie wenigstens partiell im Zusammenhang mit dem auch in diesem Tätigkeitsbericht erwähnten Modellversuch der Krankenkassen (vgl. 3.4.1). Ähnlich wie zuvor "die" öffentliche Sicherheit und "die" wissenschaftliche Forschung ist es jetzt "die" soziale Solidarität, die es scheinbar rechtfertigt, all die Schranken, die man wie selbstverständlich für jeden anderen Sektor, für den Sicherheitsbereich also genauso wie für Personalinformationssysteme, voll und ganz bejaht, für das konkret anvisierte Ziel, die Verarbeitung von Patientendaten, in Frage zu stellen.

1.3.2
Strikte Zweckbindung: Kernforderung des Bundesverfassungsgerichts

Nur: Gesetzgeber und Bundesverfassungsgericht haben keinen Zweifel gelassen. Der Datenschutz ist keine sektorale, auf einige wenige Verarbeitungsfälle begrenzte Angelegenheit. Wer personenbezogene Daten verarbeitet, spielt vielmehr weiter keine Rolle. Die Verarbeitung als solche genügt, um die Verpflichtung, sich an die gesetzlich vorgesehenen Vorkehrungen strikt zu halten, auszulösen. Man mag über die Qualität dieser Vorkehrungen noch so sehr streiten, sie bleiben dennoch verbindliche Vorgaben, an denen niemand vorbei kann, ohne Rücksicht im übrigen darauf, wie hoch er seine eigene Aufgabe einschätzt. Kurzum, der Datenschutz ist keine beliebig einschränkbare oder modifizierbare Ausnahme, sondern Grundregel aller Datenverarbeitung. Wer immer deshalb meint, auf personenbezogene Daten zurückgreifen zu müssen, hat zunächst und vor allem die Erforderlichkeit der Daten für den konkret von ihm verfolgten Zweck, die gesetzliche Verarbeitungsgrundlage und die konkret getroffenen, den gesetzlichen Anforderungen entsprechenden Schutzmaßnahmen nachzuweisen.

Ganz in diesem Sinn hat der Datenschutzbeauftragte beispielsweise auf verbindliche, die Zweckbindung der Gesundheitsdaten garantierende Regeln bei einer Aufnahme solcher Angaben in Personalakten bestanden (vgl. 4.2.2), eine Forderung, der die Landesregierung nunmehr Rechnung tragen will. Aus dem gleichen Grund ist in den vergangenen Tätigkeitsberichten immer wieder auf die Notwendigkeit einer Sonderregelung für Arbeitnehmerdaten hingewiesen worden. Auch dies eine Erwartung, der in Hessen der Gesetzgeber jedenfalls partiell entsprochen hat, und die im Rahmen der öffentlichen Verwaltung zumindest zu einer vorläufigen Unterbrechung der Verarbeitungsvorbereitungen geführt hat (vgl. 3.3). Auf eben dieser Linie liegt aber genauso die sowohl im letzten Tätigkeitsbericht als auch auf dem Symposium der Landesregierung ausgesprochene Erwartung einer schnellen und konsequenten Reaktion auf die Entscheidung des Bundesverfassungsgerichts. Gewiß, für diese Entscheidung gilt genauso wie für jede andere, daß sich unscharfe Stellen immer finden lassen. Zudem, Äußerungen, die verschieden zu interpretieren sind, gibt es stets. Maßgeblich ist aber in Wirklichkeit allein die Einstellung, von der man bei der Lektüre ausgeht und die dann auch die Konsequenzen bestimmt, die man bereit ist, aus der Entscheidung zu ziehen. Wer aber genau den Weg befolgen will, den auch das Bundesverfassungsgericht eingeschlagen hat, allen Zweifeln und Widerständen zum Trotz also den Datenschutz als eine fundamentale, unverzicht-

bare Funktionsvoraussetzung einer demokratischen Gesellschaft anzusehen, der kann kein anderes Ziel haben als das Gericht selbst, eine ebenso folgerichtige wie überzeugende Verwirklichung des Datenschutzes sicherzustellen. Wer dagegen an der gegenwärtigen Praxis festhalten und möglichst auch Veränderungen vermeiden möchte, der beginnt mit Überlegungen zum beschränkten Anwendungsbereich der Entscheidung, fährt mit einer Aufzählung aller "unverständlichen" und "unklaren" Stellen fort und endet schließlich mit der beruhigenden Bemerkung, geändert habe sich wohl kaum etwas, und wo doch Änderungen möglicherweise notwendig seien, bedürften sie erst langer und sorgfältiger Reflexion. Und in der Tat, wer die vielen außerhalb Hessens mittlerweile vorgelegten Stellungnahmen liest, stellt immer wieder überrascht fest, daß offenkundig fast alle Phantasie und Energie dem Nachweis der Bedeutungslosigkeit der Entscheidung und nicht etwa der durch sie ausgelösten Handlungsverpflichtungen dient.

1.3.3
Prüfstand: HDSG-Novellierung

Ob und in welchem Umfang es auch innerhalb Hessens zu ähnlichen Bestrebungen kommt, ja sie sich unter Umständen durchsetzen, wird sich spätestens bei der Diskussion über die Novellierung des Datenschutzgesetzes und die geplanten bereichsspezifischen Regelungen erweisen. Wie gern Verwaltungen an tradierten Vorstellungen festhalten, zeigt das im Tätigkeitsbericht erwähnte Beispiel der Gebührenpflicht für Auskünfte (vgl. 2.5). Sie ist in Wirklichkeit nichts anderes als ein Mittel, um das Auskunftsrecht zu unterlaufen. Eben deshalb hatte sich der hessische Gesetzgeber als erster eindeutig gegen eine Gebührenpflicht ausgesprochen. Umso erstaunlicher ist für die Betroffenen, wenn ihnen Jahre nach der unmißverständlichen Entscheidung des Landtags in einem für sie wichtigen Bereich immer noch eine Auskunftsgebühr abgefordert wird.

Vielleicht läßt sich im Fall mit den Sozialdaten (2.5.2) eine formale juristische Rückzugsposition aufbauen. Doch ebensogut ist es rechtlich möglich, von der Gebühr abzusehen. Ein Beispiel dafür zeigt der Abschnitt über die Arbeitnehmerauskunft (2.5.1). Wiederum kommt es deshalb einzig und allein auf das Verständnis des Datenschutzes und die ihm zugemessene Bedeutung an. Solange es wirklich nur darum geht, ihm Geltung zu verschaffen, gilt es einzig über die Wege nachzusinnen, die der Landtagsentscheidung entsprechen.

Das Beispiel der Gebührenpflicht ist aber zugleich Warnzeichen. Es signalisiert die Widerstände, die sich jetzt schon, wenn auch zaghaft, gegen eine Novellierung abzuzeichnen beginnen. Die kritischen Punkte sind schon lange bekannt, von der Einbeziehung der Akten in den Anwendungsbereich des Datenschutzgesetzes, über den endgültigen Verzicht auf "interne" Dateien, die bessere Transparenz mit Hilfe eines dem Bürger regelmäßig zugehenden Auszugs der zu seiner Person verarbeiteten Daten, der unmißverständlichen Zweckbindung, bis hin zu Vorschriften, die jedenfalls eine ebenso kontinuierliche wie umfassende Information über die Verarbeitung im privaten Bereich sichern wie bei der öffentlichen Verwaltung. Eine erste Gelegenheit festzustellen, ob und wie sich die Reaktionen von den Versuchen unterscheiden, die Entscheidung des Bundesverfassungsgerichts auf einen letztlich unverbindlichen Appell an den Gesetzgeber zu reduzieren, bietet der Tätigkeitsbericht mit den Vorschlägen zur besseren Information des Bürgers über die Verarbeitung seiner Daten. Sie knüpfen an den Beschluß des Landtags an und versuchen, Ansatzpunkte für eine kontinuierliche Unterrichtung aufzuzeigen, zugleich aber den Gefahren auszuweichen, die mit jedem Versuch einer möglichst umfassenden, zentralisierten Information verbunden sind.

Schon ein Blick in den entsprechenden Abschnitt des Tätigkeitsberichts (3.6) zeigt, wie groß die Schwierigkeiten sind, die es zu überwinden gilt. Doch so wenig sie übersehen werden dürfen, so sehr kommt es darauf an, sie nicht zu einer Ausrede für eine weitere Untätigkeit kunstvoll zu stilisieren. Die Überzeugungskraft und Glaubwürdigkeit des Datenschutzes hängt entscheidend von der Fähigkeit des Betroffenen ab, die Verarbeitung seiner Daten jederzeit nachvollziehen und überprüfen zu können. Genau deshalb haben sich alle Datenschutzgesetze für ein Auskunftsrecht entschieden. Nur: Das Auskunftsrecht bleibt solange letztlich nutzlos, wie der Betroffene nicht über die notwendige Information verfügt, die ihn zum Nachdenken anregt und zum Handeln veranlaßt. Ein Gesetzgeber, der dies außer acht läßt, begründet kein Auskunftsrecht, er findet sich vielmehr mit einer Fiktion ab.

1.4
Weiterentwicklung des Datenschutzes: Schwerpunkt Informationstechnologie

Schon das erste Hessische Datenschutzgesetz hatte die Grundvoraussetzung einer wirksamen Datenschutzregelung deutlich formuliert: Jede ihrer Vorschriften stets als Teil eines auf die kontinuierliche Auseinandersetzung mit den Folgen einer sich ständig verändernden Informationstechnologie abzielenden Gesamtkonzepts zu sehen und auszugestalten. In der Folgezeit engte manche, durch die mißverständlichen Formulierungen des Bundesdatenschutzgesetzes begünstigte Interpretation das Blickfeld ein, löste den Datenschutz aus der Reflexion über die Entwicklung der Informationstechnologie und ihre Folgen heraus und reduzierte ihn auf die Ahndung wie immer

verstandener "Mißbräuche". Das Bundesverfassungsgericht rückte das Bild erneut zurecht. Was freilich scheinbar eine rein abstrakte Diskussion war, erhält spätestens mit der Einführung des Bildschirmtextes eine überaus konkrete Dimension. Konsequenterweise hat der Landtag schon zweimal, bei der Beratung des Bildschirmtext-Staatsvertrages und bei der Erörterung des letzten Tätigkeitsberichts, auf die Notwendigkeit hingewiesen, Datenschutzvorstellungen im Rahmen eines auf die Informationstechnologie abgestellten Gesamtkonzepts zu formulieren.

Nach wie vor fehlt es allerdings daran. Mit einer der wichtigsten Gründe dafür ist der bisher ebenso vordergründige wie einseitige Diskussionsverlauf in der Bundesrepublik. Ähnlich wie in den Vereinigten Staaten und anders als etwa in Großbritannien und Frankreich konzentrierte sich alle Aufmerksamkeit auf das Medium und nicht auf die Informationstechnologie. Kaum verwunderlich, wenn unter diesen Umständen die Veränderungen der Informationstechnologie fast ausschließlich als Veränderungen von Rundfunk und Fernsehen wahrgenommen wurden und die Argumentation sich nur auf Überlegungen zur Medienstruktur und Medienentwicklung stützte. In Wirklichkeit ist aber damit nur ein, wenngleich unstreitig wichtiger Aspekt, der veränderten Informationstechnologie angesprochen. Nicht von ungefähr haben die letzten Tätigkeitsberichte auf die durch den Bildschirmtext ermöglichten interaktiven Systeme, von der Bestellung aus Versandhauskatalogen über die Buchung von Reisen bis hin zu der Erledigung von Bankgeschäften und der Verlagerung der Arbeit zurück in den Wohnbereich hingewiesen. Auch die in diesem Tätigkeitsbericht erneut hervorgehobenen Auswirkungen von Fernwirksystemen (3.1.2) lassen erkennen, wie sehr eine auf die Medienstruktur fixierte Diskussion an den Problemen vorbeiführt. Mit der Entwicklung der Informationstechnologie verändern sich die bisher bestehenden Kommunikations- und Arbeitsbedingungen von Grund auf. Weder kann davon die Rede sein, daß, nach ihrer Einführung, Arbeitsleistungen nach wie vor ausschließlich in den tradierten, für selbstverständlich hingenommenen Formen erbracht werden, noch lassen sich die überkommenen und für nicht minder selbstverständlich gehaltenen Vorstellungen über Alltagsgeschäfte aufrechterhalten. Hier gilt es deshalb anzusetzen und von hier aus zu fragen, welche Auswirkungen die Informationstechnologie haben kann und wie sich eine auch und gerade an den Zielen der Datenschutzgesetzgebung ausgerichtete Reaktion des Gesetzgebers gestalten muß.

Nur: Bemerkungen über unstreitig vorhandene Mängel helfen ebensowenig weiter wie summarische Aussagen über mögliche Konsequenzen. Wer darauf beharrt, verdrängt nicht nur die Erfahrungen mit der technischen Entwicklung, er übergeht, bewußt oder unbewußt, um der eigenen Vorurteile willen Studien, wie sie beispielsweise von der Gleichberechtigungskommission in Großbritannien vorgelegt worden sind. Wohlgemerkt, keineswegs geht es darum, irgendwelche, wo immer geäußerte Meinungen schlicht zu übernehmen. Zur Debatte steht allein die Notwendigkeit, sich einerseits von der einseitigen Mediendiskussion zu lösen und andererseits konkret und präzise auf die Informationstechnologie einzugehen, mögliche Konflikte offenzulegen, sie auf ihre Auswirkungen hin zu analysieren und erst dann den Versuch zu unternehmen, den erforderlichen normativen Handlungsrahmen festzulegen. Hessen hat Ende der sechziger Jahre, spät, aber doch noch vor jedem anderen Land, nach den sozialen und politischen Folgen der automatischen Datenverarbeitung gefragt und mit einer eigens darauf abgestellten gesetzlichen Regelung reagiert. Fünfzehn Jahre danach hat es die Chance, den damals begonnenen Weg fortzusetzen, einmal mehr also die politische und soziale Dimension der Informationstechnologie präzise zu orten und in ein auch und gerade einen ebenso überzeugenden wie wirksamen Datenschutz garantierendes Regelungskonzept umzusetzen. Bestandteil dieses Konzepts müssen auch und gerade Antworten auf die vom Landtag gestellten Grundsatzfragen - nach der Zukunft des Informationsgleichgewichts, nach Öffnung des Informationszugangs ("freedom of information") - sein. Noch ist es nicht zu spät.

2. Erfahrungen

2.1
Sozialverwaltung

2.1.1
Diskriminierung von Sozialhilfeempfängern durch "Warnmeldungen"

2.1.1.1
Weitgespanntes Meldenetz

Die Gefahr, ohne genaue Prüfung verdächtigt zu werden, in eine bundesweite Zentraldatei zu geraten und durch Streuung negativer Zuschreibungen diskriminiert zu werden, ist keineswegs auf den Bereich der Datenspeicherung durch die Sicherheitsbehörden beschränkt. Ein besonders drastisches Beispiel dafür, daß auch eine überzogene Kontrolle durch Behörden der Sozialverwaltung die gleichen Konsequenzen haben kann, ist der - inzwischen eingestellte - Warndienst vor sogenannten "Unterstützungsschwindlern".

Aufgrund von Beschwerden und Hinweisen konnte ich feststellen, daß der Landeswohlfahrtsverband Hessen (Landessozialamt) als zentrale Sammel- und Verteilstelle für sog. "Warnmeldungen" fungierte, die von Sozial- und Gesundheitsämtern einer Reihe von Bundesländern angeliefert wurden. Diese Mitteilungen wurden beim LWV aufgezeichnet und in Listenform an einen breiten Verteilerkreis weitergegeben. Auf diesen Listen befanden sich neben den Personalien und der meldenden Stelle als Grund der Information Begriffe wie "Unterstützungsschwindler", "Krankenhausschwindler", "versuchter Sozialhilfebetrug" usw. Adressaten dieser Angaben waren sämtliche überörtlichen Träger der Sozialhilfe in der Bundesrepublik. In Hessen gingen die einschlägigen Schreiben u.a. an den Sozialminister, die Regierungspräsidenten, sämtliche kreisfreien Städte und Landkreise sowie zahlreiche private Einrichtungen vom Nichtseßhaftenheim bis zur Männer-Wohnunterkunft der Heilsarmee. Bei einigen der angegebenen Namen waren sogar polizeiliche Suchhinweise mit abgedruckt bzw. Aufforderungen zur Benachrichtigung der zuständigen Polizeidienststelle.

2.1.1.2
Verstoß gegen das Sozialgeheimnis

Ich habe den Landeswohlfahrtsverband umgehend darauf hingewiesen, daß ein solcher bundesweiter Warndienst den Bestimmungen über das Sozialgeheimnis eklatant widerspricht. Dies gilt sowohl für die Meldungen der einzelnen Sozialämter an den LWV als auch für die Weiterleitung von diesem an die örtlichen Sozialbehörden. Zwar mag es im Einzelfall sachgerecht sein, gezielt eine andere Dienststelle vor einer Person mit betrügerischen Absichten zu warnen, wenn mit einer gewissen Wahrscheinlichkeit davon ausgegangen werden kann, daß sich der Betroffene an diese Stelle wendet. Nur eine solche Offenbarung in einer konkreten Verdachtssituation könnte als "erforderlich" zur Aufgabenerfüllung der Sozialhilfeträger bezeichnet und durch § 69 Abs. 1 Nr. 1 SGB X gerechtfertigt werden.

Eine bundesweite Verbreitung von abfälligen Bewertungen und Charakterisierungen, von denen die Betroffenen nichts wissen und gegen die sie sich dementsprechend auch nicht zur Wehr setzen können, deren Begriffsinhalt pauschal und nirgends präzise definiert ist und die den Empfängerstellen ohne Wissen um die Hintergründe zur Kenntnis gelangen, bedeutet dagegen einen unverhältnismäßigen Eingriff in die Persönlichkeitsrechte der Betroffenen. Dies gilt erst recht, wenn derartige Informationen nicht aktuell sind, sondern - wie im vorliegenden Fall - bis zu drei Jahre alte Behördenmeldungen offenbart werden.

"Erforderliche" und damit zulässige Datenoffenbarungen im Sinne der Bestimmungen über das Sozialgeheimnis und den Sozialdatenschutz können auch nur solche Übermittlungen sein, die zur Erreichung ihres Zwecks überhaupt geeignet sind. An der Eignung dieser Warnmeldungen, unberechtigten Sozialhilfebezug zu verhindern, bestehen aber erhebliche Zweifel. Zum einen beteiligten sich die Sozialbehörden einer Reihe von Bundesländern seit langem nicht mehr an diesem Warndienst, zum Teil aus Datenschutzbedenken, zum Teil aber auch deshalb, weil sie sich mit anderen Mitteln (z.B. durch ratenweise oder gar tägliche Auszahlung von Geldleistungen) gegen Unterstützungsmißbrauch absichern. Die Bundesarbeitsgemeinschaft der überörtlichen Träger der Sozialhilfe hatte sogar bereits im Jahre 1978 ihren Mitgliedern empfohlen, zukünftig auf Warnmitteilungen zu verzichten. Zum anderen kann ein Rechtsanspruch auf Sozialhilfe auch dann gegeben sein, wenn früher einmal unberechtigt diese Sozialleistung in Anspruch genommen wurde.

Die Aufforderung zur Meldung eines Hilfeempfängers an die Kriminalpolizei wegen des Verdachts einer Körperverletzung konnte zusätzlich zu einem Verstoß gegen § 73 SGB X führen, der die Datenoffenbarung an die Strafverfolgungsbehörden bei allen Delikten, die nicht mit der Gewährung von Sozialhilfe zusammenhängen, von einer vorherigen richterlichen Anordnung abhängig macht.

2.1.1.3
Reaktion: Einstellung und Löschung

Der Landeswohlfahrtsverband hat auf meine Intervention hin diesen Warndienst mit sofortiger Wirkung eingestellt und die Vernichtung der diesbezüglichen Aktenunterlagen angekündigt. Mit Rundschreiben vom 3. Oktober hat er alle bisherigen Empfänger davon unterrichtet und sie gebeten, keine "Warnmeldungen" mehr zu übersenden. Diese rasche Reaktion und die damit dokumentierte Bereitschaft, jahrzehntelange Verwaltungspraktiken und Informationsflüsse zu stoppen, wenn begründete datenschutzrechtliche Einwände auftauchen, ist keineswegs bei allen Behörden selbstverständlich. Bei aller Kritik an datenschutzwidrigen Zuständen wie dem Betrieb eines solchen "Warnsystems" verdient ein solches Behördenverhalten Anerkennung.

2.1.2
Irrweg der BAföG-Kontrolle: die zentrale Förderungsnummer

Ein weiteres Beispiel für überzogene Maßnahmen sozialer Kontrolle sind Bestrebungen, für alle hessischen BAföG-Bezieher eine zentrale Förderungsnummer einzuführen. Schon im 11. Tätigkeitsbericht (5.5) hatte ich das -später nicht realisierte -Projekt eines umfassenden Datenaustauschs über die Ländergrenzen hinweg zur Überwachung mißbräuchlichen Leistungsbezugs nach dem Bundesausbildungsförderungsgesetz (BAföG) als unverhältnismäßige "Rasterkontrolle" kritisiert. Der jetzige Beispielsfall erhärtet meinen damaligen Standpunkt: Das Staatliche Rechnungsprüfungsamt Kassel stellte bei einer am 28. Februar 1984 durchgeführten Vorprüfung der Leistungen nach dem BAföG zwei Fälle betrügerischer Mehrfachförderung fest. In seinem Bericht an den Hessischen Rechnungshof hielt dieses Amt eine bundesweite Kontrollregelung für dringend erforderlich, um das mehrfache Beantragen von Förderungsleistungen auszuschließen. Der Hessische Rechnungshof forderte daraufhin, daß wenigstens in Hessen eine zentrale maschinelle Förderungsnummer für die Verarbeitung der Daten von BAföG-Empfängern eingeführt werden müsse.

In einer Stellungnahme gegenüber dem Hessischen Minister für Wissenschaft und Kunst habe ich erhebliche Bedenken gegen die Anregung des Rechnungshofs geäußert, weil dessen Initiative weder geeignet noch erforderlich erschien, unzulässige Doppelzahlungen zu verhindern.

Seit dem Inkrafttreten des Bundesausbildungsförderungsgesetzes am 1. September 1971 haben im Durchschnitt 200.000 bis 250.000 Schüler und Studenten in Hessen monatlich Leistungen nach diesem Gesetz erhalten. Im November 1984 verzeichnete das Land Hessen 214.901 Bestandsfälle. In dem gesamten Zeitraum seit 1971 sind jedoch für ganz Hessen insgesamt nur die genannten beiden Fälle bekanntgeworden, in denen mehrfache Ausbildungsförderung erschlichen wurde.

In Anbetracht dieser Zahlenrelationen ist die Forderung nach einer landesweiten oder gar bundesweiten Förderungsnummer unverhältnismäßig, die Speicherung einer solchen Ziffer mithin mangels Erforderlichkeit nicht zulässig. Die Gründe: Sieht man einmal von den erheblichen Kosten ab, die dem Land Hessen durch eine solche Maßnahme entstehen würden, könnte die Vergabe eines solchen Personenkennzeichens die Mehrfachförderung nur dann verhindern, wenn der Betrug unter Verwendung des gleichen Namens begangen wird. Wenn andererseits Namen, Adressen und Geburtsdaten bekannt sind, dann ist auch eine numerische Identifikation durch eine Ordnungsziffer nach dem aktuellen Stand der Datenverarbeitung überflüssig. So gleicht das Bundesverwaltungsamt als zentrale Inkassostelle für die Rückzahlung der aufgrund des BAföG gewährten Ausbildungsdarlehen bereits seit einiger Zeit die von den Ländern gemeldeten Bestandsfälle zur Ermittlung von Mehrfachförderungen ab. Spätestens nach einem Jahr Förderungsdauer wird die vom Hessischen Rechnungshof geforderte Kontrolle durch internen Abgleich der Daten aller Leistungsempfänger beim Bundesverwaltungsamt durchgeführt. Auch dieser bereits seit einigen Jahren praktizierte Abgleich hat für das Land Hessen keine Hinweise auf andere als die auch dem Hessischen Rechnungshof bekannten Fälle betrügerischer Mehrfachförderung ergeben.

Im Ergebnis habe ich daher der Hessischen Landesregierung empfohlen, der Bemerkung des Hessischen Rechnungshofs nicht zu folgen und auf die Einführung einer zentralen Förderungsnummer zu verzichten. Sie ist nicht erforderlich, da ihr Zweck durch den Datenvergleich beim Bundesverwaltungsamt substituiert und in der Sache auch erreicht worden ist. Sie ist darüber hinaus nicht geeignet, solche Fälle von ungerechtfertigten Zahlungen zu verhindern, die unter Vortäuschung falscher Namen erschlichen werden. Vor allem aber: Der Verzicht auf eine einheitliche, zentral vergebene und verarbeitete Förderungsnummer vermeidet Probleme wegen der Funktion einer solchen Ziffer als mögliches Substrat eines verfassungswidrigen Personenkennzeichens für den Sektor der Ausbildungsförderung.

2.1.3
Ärztedaten als Mittel gesundheitspolitischer Auseinandersetzungen

2.1.3.1
Mitteilung und Weiterverbreitung von Abrechnungszahlen

Die Voraussetzungen und die Durchführungspraxis legaler Schwangerschaftsabbrüche bzw. die Tatsache und Häufigkeit unzulässiger Abtreibungen bilden seit langem immer wieder den Gegenstand gesundheitspolitischer Auseinandersetzungen. Bei allem legitimen Meinungsstreit um den § 218 des Strafgesetzbuchs dürfen jedoch, auch und gerade wenn er zwischen Ärzten ausgetragen wird, die Grenzen nicht überschritten werden, die das Datenschutzrecht und das Sozialgeheimnis der namentlichen Nennung von Betroffenen ziehen. Dies festzustellen hatte ich im Fall zweier Wiesbadener Ärzte Anlaß, deren bei der Kassenärztlichen Vereinigung Hessen abgerechnete Fälle von Schwangerschaftsabbrüchen unzulässigerweise einem breiten Verteilerkreis zur Kenntnis gebracht wurden.

Der Vorgang im einzelnen: Ein Mitglied des Präsidiums der Landesärztekammer Hessen erfuhr auf einer Sitzung dieses Gremiums von einer Diskrepanz zwischen den aufgrund statistischer Bestimmungen zu meldenden Zahlen von Schwangerschaftsabbrüchen und den bei der Kassenärztlichen Vereinigung abgerechneten Fällen. Ohne Auftrag der Landesärztekammer wandte sich dieses Vorstandsmitglied, Dr. X, telefonisch an die zuständige Bezirksstelle der KV und ließ sich von deren Geschäftsführer auf namentlich genannte einzelne Ärzte bezogene Abrechnungszahlen nennen. Dr. X teilte diese Zahlen unter Angabe der Namen der Ärzte sowohl der Bundesärztekammer als auch einer sog. "Europäischen Ärzteaktion", die sich u.a. gegen die Anwendung des § 218 StGB wendet, mit. Die Bundesärztekammer wiederum versandte das Schreiben von Dr. X an einen breiten Verteilerkreis, der vom Bundeskanzleramt über die Katholische Bischofskonferenz bis hin zu zahlreichen Ärzteverbänden reichte. Dr. X ging es nach seinen Behauptungen darum, im Zusammenhang mit einer Expertenanhörung der interministeriellen Arbeitsgruppe "Schutz des ungeborenen Lebens" auf Bundesebene konkrete Zahlen zum Beleg der Dunkelziffer bei Abtreibungen zu liefern.

2.1.3.2
Unzulässigkeit der Datenoffenbarungen

Datenschutzrechtlich waren zwei Übermittlungsvorgänge auseinanderzuhalten und zu bewerten. Zum einen die Mitteilung der arztbezogenen Abrechnungszahlen durch die zuständige KV- Bezirksstelle an Dr. X. Der Vorstand der Kassenärztlichen Vereinigung Hessen hat sich ausdrücklich meiner Auffassung angeschlossen, daß diese Offenbarung unzulässig war. Die von der KV verarbeiteten Abrechnungsdaten sind Sozialdaten bzw. ihnen gleichgestellte (vgl. § 35 Abs. 4 SGB I) Betriebs-und Geschäftsgeheimnisse. Sie unterliegen dem Sozialgeheimnis bzw. dem Sozialdatenschutz (§ 35 SGB I, §§ 67 ff. SGB X) und dürfen nur unter den gesetzlichen Offenbarungsvoraussetzungen weitergegeben werden. Für die Kenntnisgabe an Dr. X in seiner Eigenschaft als Privatperson - ein Nachfrageauftrag der Landesärztekammer lag wie ausgeführt nicht vor - gab es keine gesetzliche Rechtfertigung. In diesem Zusammenhang habe ich vorsorglich darauf aufmerksam gemacht, daß die Schranken der Datenschutzgesetze und des Sozialgeheimnisses selbst dann zu beachten sind, wenn ein Arzt gleichzeitig Gremienmitglied sowohl der Ärztekammer als auch der KV ist. Auch in diesem Fall darf dienstliches Wissen aus dem einen Gremium in dem anderen Organ nur dann personenbezogen bekanntgegeben werden, wenn dies im konkreten Fall zur Aufgabenerfüllung der ärztlichen Berufsorgane erforderlich ist. Grund: Auch in dieser Situation liegt datenschutzrechtlich eine Übermittlung bzw. Offenbarung vor.

Der Vorstand der KV Hessen hat den Vorfall zum Anlaß genommen, die Geschäftsführungen aller Dienststellen sowie seine Mitglieder um strikte Einhaltung des Datenschutzes zu ersuchen.

Auch die namensbezogene Information der Bundesärztekammer und der "Europäischen Ärzteaktion" durch Dr. X war rechtswidrig. Die Weitergabe von Daten, die unter Verstoß gegen das Sozialgeheimnis erhalten worden sind, ist unzulässig. Selbst bei zulässigerweise offenbarten Sozialdaten muß sich der Empfänger an die Bestimmungen der §§ 67 ff. SGB X halten; das Sozialgeheimnis wird - anders ausgedrückt - auf den Empfänger "verlängert" (§ 78 SGB X). Diesem meinem Rechtsstandpunkt hat sich der Vorstand der Landesärztekammer angeschlossen.

2.1.3.3
Unkenntnis keine Rechtfertigung

Allerdings hat er das berufsrechtliche Verfahren, das Dr. X gegen sich selbst beantragt hatte, eingestellt. Als Begründung wurde angeführt, Dr. X seien die Vorschriften über das Sozialgeheimnis und den Sozialdatenschutz nicht bekannt gewesen. Daher habe ihm die Unrechtseinsicht gefehlt. Dieser "Verbotsirrtum" sei auch unvermeidbar gewesen, da diese Vorschriften "keine dem Berufskreis des Arztes spezifisch zuzurechnenden Normen" seien, wie dies bei den Bestimmungen der Ärztlichen Berufsordnung, des Betäubungsmittelgesetzes o.ä. der Fall sei.

Zwar gehört es nicht zu meinen Aufgaben, das standesrechtliche Verfahren im Einzelfall oder die Motive des betroffenen Arztes zu werten; die angeführte Begründung allerdings halte ich - sollte sie von der Ärztekammer über diesen Einzelfall hinaus als allgemein gültige Argumentation verstanden werden - für nicht akzeptabel. Vier Jahre nach Inkrafttreten der Vorschriften über das Sozialgeheimnis und den Sozialdatenschutz, die ja nicht zuletzt auch die Daten der Ärzteschaft bei den Sozialleistungsträgern und den Kassenärztlichen Vereinigungen schützen, ist eine Berufung auf die Unkenntnis der Geheimhaltungsbedürftigkeit dieser Datenbestände nicht mehr annehmbar. Nach meiner Auffassung, die ich der Landesärztekammer mitgeteilt habe, ist es nicht zuletzt ihre Aufgabe, ggf. vorhandene Informationsdefizite über den medizinischen und den Sozialdatenschutz so abzubauen, daß jedenfalls künftig eine Rechtfertigung unzulässiger Datenübermittlungen mit Hinweis auf die fehlende subjektive Kenntnis der einschlägigen Bestimmungen nicht mehr erfolgen kann.

Auch die Argumentation in der Beschlußbegründung, den beiden Wiesbadener Ärzten sei durch die Namensnennung bei der Mitteilung ihrer Abrechnungszahlen kein Nachteil entstanden, weil ihre Person "ohne weiteres feststellbar war" - sie betreiben die einzige für Schwangerschaftsabbrüche zugelassene Praxis -, geht fehl. Wie aufgezeigt, wurden ihre Namen durch Schreiben der Bundesärztekammer bundesweit gestreut. Vor allem aber: Zum einen rechtfertigt die mögliche Kenntnis des Empfängers keineswegs die Übermittlung personenbezogener Informationen ohne Einhaltung der Offenbarungs- und Übermittlungsvorschriften. Zum anderen zeigt gerade dieser Fall, daß niemand es in der Hand hat, ob und in welchem Umfang ein Datenempfänger, dem vielleicht Informationen in der lautersten Absicht zugeleitet wurden, diese Mitteilungen anschließend weiterverbreitet und damit rufschädigende Konsequenzen auslösen kann. Auch und gerade diese potentiellen Auswirkungen auf die schutzwürdigen Belange der Betroffenen gilt es aber bereits vor der namensbezogenen Datenübermittlung zu bedenken.

2.2
Sicherheitsbehörden

2.2.1
Freitodversuche im Polizeicomputer

Die Polizei speichert im zentralen Hessischen Polizeiinformationssystem (HEPOLIS) die Daten derjenigen Bürger, die in den Verdacht einer strafbaren Handlung geraten sind. Bis vor kurzem waren in HEPOLIS darüber hinaus auch Angaben über alle Personen registriert, die versucht haben, sich das Leben zu nehmen, sofern die Polizei im Zusammenhang mit dem Freitodversuch tätig geworden war. Meine Überprüfung im Frühjahr 1984 ergab zu diesem Zeitpunkt 5.114 Fälle. Diese Daten waren - wie alle in HEPOLIS erfaßten Daten - landesweit von jeder Polizeidienststelle direkt abrufbar.

Die Polizei hat zur Erforderlichkeit einer Speicherung dieses Personenkreises vor allem angeführt, sie benötige die Daten für den Fall, daß der Betroffene später einmal

- erneut einen Freitodversuch unternehme,
- aus anderem Anlaß festgenommen werde, weil dann spezielle Maßnahmen zum Schutz vor einer Selbsttötung in der Zelle erforderlich seien,
- vermißt oder tot aufgefunden werde.

Dem Hessischen Minister des Innern habe ich dargelegt, daß mich diese Begründungen nicht überzeugen und ich eine Löschung der Daten für geboten halte.

So kann keineswegs angenommen werden, daß jeder, der einmal einen Freitodversuch begeht, später in eine dieser erwähnten Situationen gerät. Vielmehr muß im Gegenteil davon ausgegangen werden, daß dies nur bei einem sehr geringen Prozentsatz der Betroffenen der Fall sein wird. Die Datenspeicherung ist daher auf alle Fälle unverhältnismäßig. Die Polizei weist zwar in diesem Zusammenhang häufig darauf hin, daß sie nicht in der Lage ist, einzuschätzen, ob ein Betroffener möglicherweise noch einmal einen Suizid versuchen könnte. Aus diesem Grund sei eine generelle Registrierung in HEPOLIS unumgänglich. Für mich spricht die Schwierigkeit einer Prognose durch die Polizei jedoch im Gegenteil um so mehr dafür, von einer Speicherung insgesamt abzusehen.

Darüber hinaus erscheint es mir aber auch zweifelhaft, ob eine Speicherung in HEPOLIS überhaupt geeignet ist, der Polizei bei der Aufgabenerfüllung zu helfen, wenn eine der genannten vier Situationen im Einzelfall eintritt. Denn:

- Bei aktueller Lebensgefahr für den Betroffenen muß sehr schnell eingeschritten werden. Dies bedeutet, daß die Polizei regelmäßig ihre Entscheidung über die zu treffenden Maßnahmen fällen muß, bevor überhaupt eine HEPOLIS-Abfrage möglich ist.
- Wenn der Betroffene später vermißt bzw. tot aufgefunden werden sollte, sind die in HEPOLIS gespeicherten Daten in der Regel nicht geeignet, den Hintergrund des Vorfalls zuverlässig aufzuklären. Zur Aufklärung sind in erster Linie Informationen darüber notwendig, in welcher persönlichen Situation sich der Betroffene in letzter Zeit befand. Die Polizei muß daher in jedem Fall aktuelle Auskünfte über ihn von Verwandten, Freunden usw. einholen. Die Tatsache, daß er einmal vor längerer Zeit einen Freitodversuch unternommen hat, kann zur konkreten Aufklärung nicht beitragen. Umgekehrt muß ohnehin bei jeder Person, die vermißt bzw. tot aufgefunden wird, von der Polizei geprüft werden, ob die Möglichkeit eines Suizids in Betracht kommt.
- Entsprechendes gilt auch für die Maßnahmen zum Schutz des Betroffenen vor einer Selbsttötung in der Haftanstalt. Sie zu treffen, ist die Polizei ihren Dienstvorschriften zufolge (PDV 350; Vorschrift für den täglichen Dienst) ohnehin generell verpflichtet.

Vor allem aber: Die Speicherung der Daten der Betroffenen in einer Datei, die im übrigen ausschließlich für solche Personen bestimmt ist, die in Verdacht geraten sind, eine Straftat begangen zu haben, führt zu einer nicht hinnehmbaren Stigmatisierung. Es handelt sich um in keiner Weise vergleichbare Sachverhalte. Besonders bedenklich erscheint diese Registrierung auch im Hinblick auf das vielfach beeinträchtigte Selbstwertgefühl der Betroffenen.

Ich begrüße es, daß der Innenminister nunmehr eine Löschung aller in HEPOLIS gespeicherten einschlägigen Daten veranlaßt und für die Zukunft festgelegt hat, daß die Polizei Personen, die einen Freitodversuch unternommen haben, weder in manuellen noch in automatisierten Dateien erfaßt (vgl. auch die Antwort des Hessischen Ministers des Innern auf eine Kleine Anfrage, Drucks. 11/2186). Damit ist gewährleistet, daß diese Bürger nicht mehr landesweit registriert werden und die zentrale polizeiliche Datei HEPOLIS einer präziser abgegrenzten Zweckbestimmung unterliegt.

2.2.2
Ausschluß vom Schöffenamt aufgrund pauschaler Datenübermittlung

Datenschutzwidrige Praktiken habe ich auch im Zusammenhang mit der Verfahrensweise bei der Vorbereitung der Schöffenwahl festgestellt. Zunächst zur Rechtslage: Die Durchführung der Wahl ist im Gerichtsverfassungsgesetz (GVG) geregelt. In diesem Gesetz ist auch festgelegt, von welchen Bürgern das Amt eines Schöffen nicht ausgeübt werden darf (§ 32 GVG). Es handelt sich vor allem um

- Personen, die infolge Richterspruch die Fähigkeit zur Bekleidung öffentlicher Ämter nicht besitzen oder wegen einer vorsätzlichen Tat zu einer Freiheitsstrafe von mehr als sechs Monaten verurteilt sind;
- Personen, gegen die ein Ermittlungsverfahren wegen einer Tat schwebt, die den Verlust der Fähigkeit zur Bekleidung öffentlicher Ämter zur Folge haben kann.

Das Gesetz trifft keine Regelung darüber, zu welchem Zeitpunkt und auf welche Weise im Rahmen der Wahl geprüft werden soll, ob im Einzelfall einer dieser Ausschließungsgründe vorliegt. Die Vorschriften gelten entsprechend für die Ausschüsse für Kriegsdienstverweigerung (§ 9 Abs. 2 Kriegsdienstverweigerungs-Neuordnungsgesetz).

In dem von mir aufgrund einer Eingabe nachgeprüften Fall hatte die für die Vorbereitung der Wahl zuständige Stelle der Polizei die Vorschlagslisten übersandt zur Überprüfung, ob bei den aufgeführten Personen ein Ausschließungsgrund vorlag. Die Polizei stellte mit Hilfe einer Abfrage des Polizeiinformationssystems (HEPOLIS) fest, ob Erkenntnisse vorlagen. Soweit dies der Fall war, wurde ohne Prüfung des der Speicherung zugrunde liegenden Sachverhalts das jeweilige Aktenzeichen des staatsanwaltschaftlichen Ermittlungsverfahrens an die anfragende Stelle übermittelt. Im Fall des Bürgers, der sich an mich gewandt hatte, wurde der Hinweis auf ein Ermittlungsverfahren aus dem Jahre 1966 (!) mitgeteilt. Die entsprechende Akte war in der Zwischenzeit zwar von der Polizei ausgesondert worden, da keine Notwendigkeit mehr zu einer Aufbewahrung gesehen worden war. Es war aber versäumt worden, auch für die entsprechende Datenlöschung in HEPOLIS zu sorgen. Die anfragende Stelle strich dann - ebenfalls ohne Überprüfung des zugrundeliegenden Sachverhalts - den Betroffenen aufgrund der bloßen Mitteilung des Aktenzeichens von der Vorschlagsliste.

Dieser Vorfall zeigt erneut grundsätzliche Probleme der polizeilichen Datenspeicherung auf. Ihre Lösung ist besonders dringlich, weil im Zusammenhang mit der Schöffenwahl regelmäßig eine ganz erhebliche Anzahl von Personen überprüft wird.

Zunächst: Die Verwendung von Daten, die bereits vor langer Zeit in HEPOLIS hätten gelöscht werden müssen, belegt erneut, daß die Bereinigung der hessischen Kriminalaktensammlungen bis heute keineswegs in hinreichendem Umfang durchgeführt worden ist. Auf diese Tatsache habe ich in der Vergangenheit immer wieder hingewiesen. Solange dies nicht der Fall ist, muß umso mehr darauf geachtet werden, daß Daten vor ihrer Übermittlung an andere öffentliche Stellen auf ihre Aktualität überprüft werden. Es muß sichergestellt werden, daß inaktuelle und damit zu löschende Informationen nicht mehr an andere Behörden gelangen, denn diese Daten können auf keinen Fall für die Aufgabenerfüllung einer anderen Stelle erforderlich sein. Auch in meinem letzten Tätigkeitsbericht (12. Tätigkeitsbericht, Ziff. 4.5) habe ich von einem Fall der Übermittlung von überholten Angaben, und zwar an den Arbeitgeber des Betroffenen, berichtet und darauf hingewiesen, daß es verstärkter Anstrengungen bedarf, um die in den KpS-Richtlinien festgelegten Löschungsfristen auch tatsächlich einzuhalten. Solange während einer Übergangszeit die polizeilichen Datenbestände nicht vollständig bereinigt seien, müsse durch klare organisatorische Vorkehrungen und Dienstanweisungen sichergestellt werden, daß die Betroffenen hierdurch keine Nachteile erleiden. In der Stellungnahme der Landesregierung zum 12. Tätigkeitsbericht (Drucks. 11/1258, zu Ziff. 4.5.1) ist dieser Fall als eine Ausnahme bezeichnet worden; Maßnahmen zum Schutz der Betroffenen wurden nicht als erforderlich angesehen.

Daß ich schon wieder über einen vergleichbaren Fall berichten muß, widerlegt diese Auffassung und beweist die Richtigkeit meiner Forderung nach einer generellen Änderung der Speicherungs- und Übermittlungspraxis.

Zweites Problem: Die Polizei prüft nicht nach, ob im Einzelfall ihre Informationen für den Ausschluß vom Schöffenamt nach § 32 GVG relevant sind. Sie übermittelt pauschal ihre Daten über eingeleitete Ermittlungsverfahren, unabhängig davon, welcher Straftatbestand betroffen ist, ob das Ermittlungsverfahren bereits eingestellt ist oder noch schwebt bzw. ob das spätere Strafverfahren mit Freispruch oder Verurteilung endete. Damit erhält die anfragende Stelle zum einen viel mehr Informationen, als sie für die Überprüfung der Vorschlagsliste zulässigerweise verwenden darf. Zum anderen ist für Auskünfte über Verfahren, die zu einer Verurteilung geführt haben, ausschließlich das Bundeszentralregister die zuständige Stelle. Sicherlich gibt es praktische Schwierigkeiten angesichts der Tatsache, daß die Polizei in der Regel nicht über den Ausgang eines Ermittlungsverfahrens unterrichtet wird. Ich habe dies wiederholt kritisiert. Solche praktischen Durchführungsprobleme rechtfertigen aber keineswegs ein Abweichen von den eindeutigen gesetzlichen Voraussetzungen: Ist keine differenziertere Auskunftspraxis möglich, muß eine andere Form der Überprüfung der Vorschlagslisten gewählt werden.

Auf meine Kritik an der gegenwärtigen Verfahrensweise hat der Innenminister geantwortet, er habe die im konkreten Fall betroffene Polizeidienststelle angewiesen, bei künftigen Anfragen auf das Bundeszentralregister zu verweisen. Der Innenminister hat damit zwar meiner Auffassung über die ausschließliche Zuständigkeit dieses Registers für Mitteilungen über Verurteilungen zugestimmt. Dennoch genügt diese Antwort deshalb nicht, weil es um eine landesweit geübte Praxis geht und im übrigen auch nach der Regelung des Gerichtsverfassungsgesetzes unter Umständen ein Ausschluß vom Schöffenamt auf Grund eines schwebenden Ermittlungsverfahrens in Betracht kommt.

2.2.3
Sicherheitsüberprüfung durch den Verfassungsschutz: Mangelnde Transparenz für den Betroffenen

Ein konkreter Fall einer Sicherheitsüberprüfung durch den Verfassungsschutz hat die derzeitigen Mängel des Verfahrens besonders deutlich gemacht. Er betraf eine Studentin, die im Rahmen ihres Studiums ein Praktikum in einer Justizvollzugsanstalt absolvieren wollte. Im Zusammenhang mit ihrer Bewerbung wurde eine Sicherheitsüberprüfung durchgeführt. Es wurde ihr dann telefonisch mitgeteilt, daß eine Einstellung aufgrund der Ergebnisse der Überprüfung nicht möglich sei. Meine Nachprüfung des konkreten Sachverhalts ergab, daß die Studentin weder über das grundsätzliche Verfahren informiert noch später zu den Gründen der Ablehnung angehört worden war.

Die Sicherheitsüberprüfung ist im Verfassungsschutzgesetz des Bundes nur fragmentarisch geregelt. § 3 Abs. 2 sieht die "Mitwirkung" der Verfassungsschutzbehörden bei der Überprüfung bestimmter Personenkreise vor. Es handelt sich um

- "Personen, denen im öffentlichen Interesse geheimhaltungsbedürftige Tatsachen, Gegenstände oder Erkenntnisse anvertraut werden, die Zugang dazu erhalten sollen oder ihn sich verschaffen können," und
- "Personen, die an sicherheitsempfindlichen Stellen von lebens- und verteidigungswichtigen Einrichtungen beschäftigt sind oder beschäftigt werden sollen".

Konkrete Regelungen über die Verfahrensweise bei der Sicherheitsüberprüfung sind im Gesetz nicht enthalten, obwohl diese für die Betroffenen sehr schwerwiegende Konsequenzen - so z.B. die Ablehnung der Einstellung -haben kann. Das "Hessische Gesetz über die Errichtung eines Landesamtes für Verfassungsschutz" enthält keine Vorschriften über die Aufgaben und Befugnisse des Landesamtes, sondern nimmt lediglich auf das Verfassungsschutzgesetz des Bundes Bezug. Im übrigen ist die Verfahrensweise bei der Sicherheitsüberprüfung in Richtlinien aus dem Jahre 1962 festgelegt. Insbesondere Vorschriften über etwaige Datenspeicherungen sowie über Informations- und Anhörungsrechte der Betroffenen sind weder im Gesetz noch in den Richtlinien enthalten.

Ich halte es jedoch für dringend geboten, daß ein Mindestmaß an Transparenz für den Betroffenen hergestellt wird. Der Bürger muß wissen, was mit seinen Daten geschieht. So hat auch das Bundesverfassungsgericht im Urteil zum Volkszählungsgesetz mit Recht auf die Bedeutung der Aufklärungsrechte des Bürgers als verfahrensrechtliche Schutzvorkehrungen gegen die Gefahren der Datenverarbeitung hingewiesen. Zwar wird in der Praxis der Überprüfte in vielen Fällen informiert. Ich habe jedoch festgestellt, daß sehr uneinheitlich verfahren wird. Auch eine Anhörung halte ich grundsätzlich für notwendig, und zwar vor allem aus zwei Gründen: Zunächst ist zu bedenken, daß der Verfassungsschutz bereits im weiten Vorfeld polizeilicher Gefahren personenbezogene Informationen speichert, die zudem sehr langen Speicherungsfristen unterliegen. Hinzu kommen die möglichen einschneidenden Folgen für die Betroffenen. Sie müssen daher möglichst weitgehend Gelegenheit haben, Erkenntnisse des Verfassungsschutzes aus ihrer Sicht zu ergänzen oder zu korrigieren.

Schon 1982 hat mir der Hessische Minister der Justiz auf meine Bitte um umfassende Information über die gegenwärtige Praxis der Sicherheitsüberprüfung in Hessen mitgeteilt, daß eine Anhörung in jedem Fall vor einer Ablehnung erfolge. Auf meine Frage, warum in diesem konkreten Fall eine Anhörung nicht stattgefunden habe, wies der Justizminister darauf hin, die Betroffene habe am Telefon auf entsprechendes Befragen erklärt, daß sie eine schriftliche Mitteilung der Ablehnung nicht mehr für erforderlich halte. Das Verfahren sei damit ordnungsgemäß abgewickelt worden.

Demgegenüber stelle ich nachdrücklich fest: Mit einer derartigen Vorgehensweise, die den Bürger über seine Rechte im unklaren läßt, ist selbstverständlich dem Erfordernis der Durchführung einer Anhörung nicht Genüge getan.

Nichtsdestoweniger begrüße ich es, daß der Justizminister aufgrund meiner erneuten Anfrage in einem Runderlaß an alle Vollzugsanstalten auf die Anhörungsrechte von Einstellungsbewerbern hingewiesen hat.

Meine Prüfung hat ferner ergeben, daß der in den Richtlinien für die Sicherheitsüberprüfung vorgesehene Verfahrensablauf nicht eingehalten wurde. Insbesondere konnte ich ein unklares Nebeneinander von telefonischen und schriftlichen Mitteilungen feststellen.

Der Hessische Landtag hat anläßlich der Beratung meines 12. Tätigkeitsberichtes die Landesregierung gebeten, bis zum Frühjahr einen Entwurf für bereichsspezifische Datenschutzregelungen im Verfassungsschutzgesetz vorzulegen (vgl. Beschluß Nr. 3, Beschlußempfehlung des Innenausschusses Drucks. 11/1551). In diesen Zusammenhang gehört auch die Regelung einer klaren und rechtsstaatlichen Verfahrensweise bei der Sicherheitsüberprüfung.

2.2.4
Verdeckte Identifizierung mit Hilfe des Kfz-Kennzeichens

In einer Reihe von Anfragen wurde die Frage gestellt, unter welchen Voraussetzungen die Identifizierung von Bürgern durch die Polizei mit Hilfe des Kfz-Kennzeichens zulässig ist. Den folgenden Fall habe ich zum Anlaß genommen, das Problem noch einmal grundsätzlich aufzugreifen: Besucher einer Tagungsstätte, die von einem privaten Freizeitverein unterhalten wird, wurden polizeilich überprüft, und zwar aufgrund der bloßen Tatsache, daß dort an den Wochenenden Fahrzeuge aus dem gesamten Bundesgebiet abgestellt waren. Dies genügte der Polizei, die entsprechenden Kfz-Kennzeichen zu notieren, beim Kraftfahrtbundesamt die Namen der Halter zu erfragen und anschließend nachzuprüfen, ob sie im polizeilichen Informationssystem gespeichert waren. Da in den meisten Fällen Halter und Fahrer eines Autos übereinstimmen, hat die Polizei damit faktisch eine Identitätsfeststellung der Besucher der Tagungsstätte vorgenommen. Diese Identitätsfeststellung erfolgte jedoch nicht in der Form, die in den polizeigesetzlichen Bestimmungen (HSOG) vorgesehen ist, d.h. durch das Verlangen des Personalausweises direkt vom Betroffenen, sondern unbemerkt von den Überprüften mit Hilfe der Datenbestände einer anderen Behörde, des Kraftfahrtbundesamtes.

Nun ist zwar die Möglichkeit, Bürger mit Hilfe des Kfz-Kennzeichens zu identifizieren, keineswegs neu. Mit dem Aufbau von ZEVIS (Zentrales Verkehrsinformationssystem) beim Kraftfahrtbundesamt, mit der zum Teil bereits realisierten, zum Teil erst geplanten Direktanbindung aller Polizeidienststellen der Bundesrepublik an ZEVIS (s. hierzu Ziff. 3.5.4) und der fortschreitenden Entwicklung der technischen Infrastruktur der Polizei ergibt sich jedoch eine völlig neue Situation. Der Polizei wird die Möglichkeit eröffnet, in erheblichem Umfang, in Sekundenschnelle und von jeder örtlichen Dienststelle bzw. von jedem mobilen Abrufgerät aus die Identität jedes Bürgers zu ermitteln, der sein Kraftfahrzeug benutzt - in der Bundesrepublik gibt es etwa 30 Millionen Fahrzeugbesitzer. Daß solche Möglichkeiten auch genutzt werden, zeigen erste Untersuchungen über die Nutzung der vorhandenen on-line-Anschlüsse an ZEVIS: Die Anfragen der Polizei beim Kraftfahrtbundesamt haben sich verdreifacht. Wenn die Identität des Bürgers feststeht, können gegebenenfalls weitere Maßnahmen wie z.B. Datenspeicherungen vorgenommen werden.

Umso wichtiger ist eine Klärung der Frage, wann denn die Polizei zur Abfrage von ZEVIS berechtigt sein soll. Im HSOG sind die rechtlichen Voraussetzungen einer Identitätsfeststellung festgelegt. Dies gilt sowohl für den Anlaß - es muß eine konkrete Gefahr vorliegen - als auch für den Grundsatz, daß offen vorgegangen wird, d.h. die Polizei das Vorzeigen des Ausweises verlangt (vgl. § 45 HSOG). Diese Regelungen dürfen nicht dadurch leerlaufen, daß die Polizei in zunehmendem Maße die Möglichkeit von - für den Bürger verdeckten - Abfragen des ZEVIS nutzt.

Zwar mag es auf den ersten Blick so aussehen, als würde der Betroffene durch eine solche Maßnahme weniger beeinträchtigt: Er wird nicht von der Polizei angehalten bzw. zum Vorzeigen des Ausweises aufgefordert, vielmehr gar nicht von ihr behelligt. Doch diese Sichtweise ist kurzsichtig und geht an dem wirklichen Problem vorbei: Auch eine verdeckte Identifizierung greift in das informationelle Selbstbestimmungsrecht des Bürgers ein, allerdings entgeht ihm die Möglichkeit, die Rechtmäßigkeit der Maßnahme zu überprüfen und gegebenenfalls dagegen vorzugehen. Verdeckte Informationsbeschaffung nimmt auch der Öffentlichkeit die Möglichkeit der Diskussion und Kontrolle polizeilicher Tätigkeit. Der berichtete Fall zeigt, wie niedrig die Schwelle für eine Überprüfung von Bürgern in der Praxis sein kann. Nur größtmögliche rechtsstaatliche Transparenz auch der polizeilichen Arbeit gewährleistet, daß der Gefahr eines Übergangs in den Überwachungsstaat begegnet werden kann.

Dem Hessischen Innenminister habe ich diese Probleme noch einmal eindringlich dargelegt. Konsequenzen müssen sowohl bei den neuen Regelungen für die polizeiliche Datenverarbeitung in Hessen (dazu Ziff. 3.5.2) als auch durch eine Korrektur der Entwürfe zum Straßenverkehrsgesetz - was die polizeiliche Nutzung des ZEVIS angeht - gezogen werden (dazu Ziff. 3.5.4).

2.2.5
Datenlöschung vor Auskunftserteilung

Im Jahr 1981 hatten sich mehrere Frankfurter Rechtsanwälte an das Hessische Landeskriminalamt gewandt und um Auskunft über die zu ihrer Person gespeicherten Daten gebeten. Diese Auskunft war ihnen unter Berufung auf Sicherheitserwägungen verweigert worden. In diesem Jahr hat das Verwaltungsgericht Frankfurt das Landeskriminalamt verurteilt, den Betroffenen Auskunft zu erteilen (Entscheidungen vom 17. Juli 1984, Az.: IV 1 - E 3255/82, IV 1 - E 3998/82, IV 3 - E 5355/82). Kurz darauf erhielten die Kläger die Auskunft, daß Daten zu ihrer Person weder in HEPOLIS noch in sonstigen Dateien des Landeskriminalamts gespeichert seien. Die Betroffenen wandten sich daraufhin an mich mit der Bitte nachzuprüfen, ob die ihnen erteilte Auskunft korrekt sei. Meine Überprüfung ergab, daß zum Zeitpunkt der Prüfung in der Tat keine Daten gespeichert waren. Weiter stellte sich heraus, daß zwar zum Zeitpunkt des Auskunftsantrags im Jahre 1981 Daten vorhanden gewesen, diese Daten jedoch Ende Juli 1984 - also nach der Entscheidung des Verwaltungsgerichts - gelöscht worden waren, weil - so die Begründung des Landeskriminalamts - eine weitere Speicherung dieser Daten nicht mehr erforderlich erschien.

Ich habe dem Innenminister und den Betroffenen meine Auffassung mitgeteilt, daß die hier gewählte Vorgehensweise nicht im Einklang mit dem in § 18 HDSG gewährleisteten Auskunftsrecht des Bürgers steht. Einerseits ist es sicherlich im Interesse des jeweils betroffenen Bürgers, daß zu seiner Person gespeicherte Daten, die nicht mehr für die Aufgabenerfüllung der Behörde benötigt werden, sobald wie möglich gelöscht werden. Andererseits ist jedoch das Ziel des Auskunftsrechts zu bedenken: Der Bürger soll durch dieses Recht die Möglichkeit erhalten, sich jederzeit selbst vergewissern zu können, ob und ggf. welche Daten zu seiner Person gespeichert sind. Erst auf dem Hintergrund einer umfassenden und genauen Auskunft vermag er abzuschätzen, inwieweit er weitere Maßnahmen, wie beispielsweise eine Berichtigung oder Löschung der Daten oder auch einen Schadensersatz, verlangen kann. Dieses Ziel kann und darf nicht ohne Konsequenzen für die Reaktion der speichernden Stelle auf das Auskunftsersuchen des Betroffenen bleiben. In dem Augenblick, in dem der Betroffene sein Auskunftsrecht gegenüber der speichernden Stelle geltend macht, ist auch der Gegenstand der Auskunft festgelegt. Die speichernde Stelle muß dem Betroffenen genau den Bestand an Daten mitteilen, der zu diesem Zeitpunkt gespeichert ist. Das Auskunftsrecht darf nicht dadurch unterlaufen werden, daß die speichernde Stelle aus Anlaß des Auskunftsersuchens und vor Auskunftserteilung einzelne Angaben löscht oder berichtigt. Es ist gerade der Sinn der gesetzlichen Regelung, dem Betroffenen die Chance zu geben, volle Einsicht in den seine Person betreffenden Verarbeitungsprozeß zu gewinnen und nicht etwa der speichernden Stelle die Möglichkeit zu eröffnen, ihren eigenen Datenbestand auch im Hinblick auf das Auskunftsersuchen zu überprüfen. Nur unter dieser Bedingung läßt sich das Ziel der Datenschutzgesetzgebung, die Transparenz der Informationsverarbeitung herzustellen und Mißtrauen abzubauen, erreichen.

Jede andere Beurteilung der Konsequenzen des Auskunftsrechts würde dem Betroffenen die Möglichkeit nehmen, einen konkreten Sachverhalt aufzuklären. Er könnte die Rechtmäßigkeit der Datenverarbeitung nicht kontrollieren, denkbare Rechtsansprüche gegen die speichernde Stelle wären von vornherein vereitelt. Von diesem Ergebnis darf nur in einem einzigen Fall abgewichen werden, wenn es feste, generell bestimmte Fristen für die Bereinigung der Datenbestände gibt und diese in den Zeitraum zwischen Auskunftsersuchen und Auskunftserteilung fallen. Allerdings müßte der Betroffene in einem solchen Fall auf die regelmäßig stattfindenden Überprüfungen der Datenbestände hingewiesen werden.

Für die Zukunft hat der Hessische Innenminister nunmehr vorgesehen, daß in vergleichbaren Fällen, in denen Streitverfahren anhängig sind und die Daten der Kläger aus der Sicht der Polizei gelöscht werden könnten, zunächst keine Löschung erfolgt, sondern die Angaben lediglich gesperrt werden.

2.3
Datensicherung

2.3.1
Behördenakten im Müll

In der Öffentlichkeit und den Medien wurden zwei Vorfälle unzureichender "Entsorgung" von ausgesonderten Behördenunterlagen viel beachtet: Bei der Stadt Gießen wurden Schriftstücke aus städtischen Ämtern in einem öffentlich zugänglichen Müllcontainer entdeckt, darunter auch solche aus der Sozialverwaltung, die dem Sozialgeheimnis unterlagen. In Frankfurt fanden sich im "Behördenmüll" von Oberfinanzdirektion, Versorgungsamt, Wohnungsamt und Arbeitsgericht Durchschriften von Bescheiden und Anträgen, Verhandlungsprotokolle mit Zeugenaussagen, Entwürfe zu Schreiben usw.

Beide Vorfälle sind lediglich Beispiele für generell verbreitete Mängel bei der datenschutzgerechten Beseitigung von Akten, amtlichen Dokumenten, aber auch von vorbereitenden Papieren der Behördenmitarbeiter, über die ich in jedem Jahr berichten muß. Bei der Nachprüfung stellt sich immer wieder heraus, daß generelle Anweisungen der Behördenleitung über die Aktenvernichtung vielfach existieren und entsprechende Geräte angeschafft worden sind, dennoch aber nicht eingehalten bzw. benutzt werden. So verfügen beispielsweise sowohl die Stadt Gießen als auch die Oberfinanzdirektion über Reißwölfe.

Mag auch die Sorglosigkeit einzelner Mitarbeiter zu derartigen Versäumnissen führen, gehen die Ursachen für solche Vorkommnisse dennoch tiefer. Die Bediensteten anzuleiten und zu motivieren, auch die Beseitigung der im Zusammenhang mit der Sachbearbeitung anfallenden Unterlagen als wichtige Aufgabe des Datenschutzes und damit auch ordnungsgerechter Verwaltung anzusehen, ist eine permanente Führungs- und Organisationsaufgabe, die sich nicht in gelegentlichen Rundverfügungen, Hausanweisungen o.ä. erschöpfen kann.

Ebensowenig ist es mit der formellen Verpflichtung der Mitarbeiter auf die jeweils geltenden Geheimhaltungsbestimmungen getan. Verantwortung trifft erst dann den einzelnen Mitarbeiter, wenn organisatorische und technische Maßnahmen in hinreichender Weise getroffen worden sind. So nutzt beispielsweise das Vorhandensein eines Reißwolfes und die Verpflichtung, ihn zu benutzen, dann nichts, wenn er in einem abgeschlossenen Nebenraum steht.

Immerhin haben solche Vorfälle insofern einen positiven Effekt, als sie aufgrund der Reaktionen der Datenschutzkontrollinstanzen und einer aufmerksamen Öffentlichkeit die Bedingungen für den ordnungsgemäßen Umgang mit "Aktenmüll" ins Bewußtsein rufen und über den unmittelbaren Anlaß hinaus die Effizienz der generell getroffenen Weisungen in Frage stellen. Denn gerade dort, wo seit Jahren alles scheinbar reibungslos abläuft, besteht am ehesten die Gefahr von Schlamperei und dem Einschleifen datenschutzwidriger Praktiken. Um keine Mißverständnisse aufkommen zu lassen: Selbstverständlich ist zu wünschen, daß derlei Vorkommnisse nicht wieder auftreten, zumal sie immer auch - häufig gravierende - Verstöße gegen die Bestimmungen über den Datenschutz und die Datensicherung darstellen. Ich habe daher auch nur dort von einer Beanstandung abgesehen, wo organisatorische und technische Maßnahmen bereits getroffen waren, und nur das Fehlverhalten einzelner Mitarbeiter vorlag.

Der Hessische Finanzminister und der Sozialminister haben die erwähnten Vorfälle jeweils für ihren Geschäftsbereich zum Anlaß genommen, durch besonderen Erlaß auf das Datengeheimnis und die datenschutzgerechte Vernichtung nicht mehr benötigten Schriftguts hinzuweisen (vgl. Antwort des Sozialministers auf eine mündliche Frage in der 30. Plenarsitzung der 11. Wahlperiode am 30. Oktober 1984). Danach dürfen Schriftstücke mit personenbezogenen Daten erst dann in Müllcontainer, Papier- oder Abfallkörbe geworfen werden, wenn diese Daten zuvor unkenntlich gemacht worden sind. Die Landesregierung hat in diesem Zusammenhang zugesagt, soweit erforderlich zusätzliche Aktenvernichtungs-Geräte anzuschaffen.

2.3.2
Datenpanne trotz Statistikgeheimnis

Das Statistische Bundesamt übermittelte an den Fachbereich Geographie der Johann Wolfgang Goethe-Universität in Frankfurt für Forschungszwecke ein Datenband mit regionalen Ergebnissen der Wahlen zum Deutschen Bundestag. Im Hochschulrechenzentrum wurde festgestellt, daß sich hinter dem Datenfile mit den Wahlergebnissen zwei weitere files befanden. Als zu erkennen war, daß diese Datensätze personenbezogene Angaben enthielten, wandte sich das Hochschulrechenzentrum an mich, um zu klären, wie weiter zu verfahren sei.

Bei der Überprüfung des Vorfalls im Hochschulrechenzentrum habe ich mir das fragliche Band auszugsweise ausdrucken lassen. Hinter dem ordnungsgemäß mit "e.o.f." (d.h. "end of file") abgeschlossenen Datenbestand aus den Bundestagswahlen waren auf dem Band Anschriften und numerisch geordnete Daten aufgezeichnet, die als Angaben aus der Kartei des produzierenden Gewerbes (PRODGEWKAT) identifiziert werden konnten. Damit stand fest, daß im Rechenzentrum des Statistischen Bundesamtes ein zuvor nicht gelöschtes Band mit statistischen Einzelangaben zum Überschreiben benutzt und ohne Abgangskontrolle zum Versand an die Universität gelangt war. Auf diese Weise wurden ungefähr 70.000 Datensätze, die als Einzelangaben dem Statistikgeheimnis unterlagen, unbeabsichtigt vom Statistischen Bundesamt übermittelt. Die Aufmerksamkeit von Mitarbeitern des Hochschulrechenzentrums Frankfurt hat wesentlich dazu beigetragen, daß der Schaden begrenzt werden konnte.

Nach sofortiger Unterrichtung des Bundesbeauftragten für den Datenschutz und des Präsidenten des Statistischen Bundesamtes fand noch am gleichen Abend eine Prüfung bei diesem Amt durch den Bundesbeauftragten statt. Das Band und den Ausdruck bei der Universität Frankfurt hatte ich sofort in Verwahrung genommen und umgehend dem Bundesbeauftragten für den Datenschutz übersandt.

Der Vorfall zeigt wieder einmal auf eindrucksvolle Weise, welche Risiken bei der Verwendung ungelöschter Magnetbänder im Datenträgeraustausch entstehen können. Ich habe wiederholt in früheren Tätigkeitsberichten auf dieses Problem hingewiesen und nehme diesen Vorgang zum Anlaß, erneut festzustellen: Datenbänder müssen vor ihrer weiteren Verwendung entweder gelöscht werden oder es sind beim erneuten Beschreiben vom file-Ende bis zum Bandende alle eventuell noch vorhandenen Daten mit Nullen zu überschreiben, um auf diese Weise das Band "aufzufüllen". Dies muß auch und gerade dort gelten, wo spezielle Geheimhaltungsvorschriften einen besonderen, über die allgemeinen Datensicherungsmaßnahmen hinausgehenden Schutz gewährleisten sollen, wie dies besonders für das Statistikgeheimnis gilt.

2.3.3
Gesperrte Meldedaten im Adreßbuch

2.3.3.1
Wiesbaden

2.3.3.1.1
Übermittlung geschützter Anschriften: Ursachen

Zu Beginn des Jahres 1984 wurde ich in zwei Fällen mit fehlerhaften Übermittlungen personenbezogener Daten aus den Melderegistern von Gemeinden an Adreßbuchverlage befaßt. In einem Fall - es handelt sich dabei um die Erstellung des Adreßbuchs der Landeshauptstadt Wiesbaden - beschäftigten sich sowohl der Hessische Landtag als auch die Medien ausführlich mit den dabei zutage getretenen Mängeln.

Dem lagen folgende Ereignisse zugrunde:
Im Oktober des Jahres 1983 waren Meldedaten der Stadt Wiesbaden an einen Verlag zum Zwecke der Herstellung eines Adreßbuchs weitergegeben worden. In dem übermittelten Datenbestand befanden sich auch Datensätze, die nach § 34 Abs. 5 des Hessischen Meldegesetzes (HMG) einer Auskunftssperre unterliegen. Die Offenbarung dieser Daten gegenüber Dritten ist deshalb unzulässig, weil sie "das Leben, die Gesundheit, die persönliche Freiheit oder vergleichbare schutzwürdige Belange der Betroffenen gefährden könnte".

Ausgelöst wurde die Datenübermittlung durch die versehentliche Eingabe einer falschen Kennzeichnung des Auswertungsempfängers im Kommunalen Gebietsrechenzentrum (KGRZ) Wiesbaden. Dadurch erhielt der Verlag einen Datensatz, der zwar einzelne weniger bedeutsame Auskunftssperren berücksichtigte, nicht aber die für die Betroffenen wesentlich wichtigere Sperre nach § 34 Abs. 5 des Hessischen Meldegesetzes. Aufgrund dieser Übermittlung wurden etwa 4.000 Exemplare des Adreßbuchs mit den gesperrten Daten von über 500 Einwohnern gedruckt. Etwa 500 Exemplare wurden Ende Dezember 1983 ausgeliefert. Alle diese Exemplare konnten durch Bemühungen der Stadt und des Rechenzentrums von den Empfängern zurückgeholt werden und wurden anschließend sofort vernichtet.

Für die unzulässige Datenübermittlung war eine Reihe von Faktoren verantwortlich. Zunächst: Das landeseinheitliche Verfahren "Grundstufe Einwohnerwesen" sieht zwar im Programm "Allgemeine Auswertungen" einen auf meinen ausdrücklichen Wunsch eingefügten Verfahrensschritt ("Routine") vor, der bei der Verarbeitung gesperrter Datensätze einen Warnhinweis auf die erste Seite der Ergebnislisten druckt. In dem speziell für die Übermittlung an den Adreßbuchverlag modifizierten Programm war jedoch eine solche Warnung nicht vorgesehen, die den bei der Durchführung des Verarbeitungsauftrags beschäftigten Mitarbeitern des Rechenzentrums die Gefahr der Übermittlung gesperrter Daten verdeutlicht hätte. So erhielten sie auf dem Bildschirm des Terminals keinen Hinweis darauf, daß durch das manuell eingefügte Auswahlkriterium auch gesperrte und besonders sensitive Daten übermittelt würden. Technische oder organisatorische Maßnahmen, die eine solche Warnfunktion ebenfalls erfüllt hätten - wie etwa die Kontrolle durch einen weiteren Mitarbeiter oder einen Vorgesetzten -, waren nicht vorgesehen.

Und weiter: Die Stadt Wiesbaden unterließ es, sich durch eine Überprüfung des Arbeitsergebnisses zu vergewissern, daß das KGRZ auftragsgemäß die gewünschten Einwohnerdaten zusammengestellt hatte und insbesondere die nach § 34 Abs. 5 HMG gesperrten Daten nicht übermittelt würden. Nach § 3 Abs. 1 des Hessischen Datenschutzgesetzes war die Meldebehörde der Stadt Wiesbaden als speichernde Stelle dafür verantwortlich, daß die datenschutzrechtlichen Bestimmungen eingehalten wurden. Diese Verantwortung trifft die speichernde Stelle auch dann, wenn personenbezogene Daten in ihrem Auftrag durch eine andere Stelle, hier das KGRZ Wiesbaden, verarbeitet werden (§ 4 Abs. 1 HDSG). Diese Verpflichtung konnte auch nicht durch Vertrag auf das Rechenzentrum übertragen werden, da sie sich unmittelbar aus dem Gesetz ergibt. Konkret bedeutet dies, daß die Kommune als speichernde Stelle nicht nur den Auftragnehmer "unter besonderer Berücksichtigung der Eignung der von ihm getroffenen technischen und organisatorischen Maßnahmen (§ 10 Abs. 1 HDSG) sorgfältig auszuwählen" hat, sondern daß sie auch im konkreten Fall die Verarbeitung durch den Auftragnehmer zu überwachen hat.

Während bei Standardauswertungen, die in einem vom Hessischen Datenverarbeitungsverbund beschlossenen Verfahren produziert werden, die speichernde Stelle das Ergebnis nicht im einzelnen überprüfen muß, kann in Sonderfällen eine Pflicht zur besonderen Überwachung bestehen. Im vorliegenden Fall handelt es sich um eine besondere Auswertung für ein Adreßbuch. Deshalb war besondere Sorgfalt darauf zu verwenden, daß sowohl die nach § 35 Abs. 5 des Hessischen Meldegesetzes eingeräumten allgemeinen Sperren von Auskünften an Adreßbuchverlage beachtet werden würden als auch und besonders - angesichts der besonders schutzwürdigen Belange der Betroffenen - die nach § 34 Abs. 5 HMG erlassenen Sperren zum Schutz von Leben, Gesundheit und persönlicher Freiheit. Das im Juni 1982 in Kraft getretene neue Hessische Meldegesetz betont, daß Meldedaten nur unter strikter Beachtung der zum Schutz des Bürgers eingerichteten Auskunftssperren verarbeitet werden dürfen. Eine fehlerhafte Übermittlung gerade an einen Adreßbuchverlag bewirkt eine weite Verbreitung der Daten und muß deshalb unbedingt vermieden werden.

Ich beanstandete deshalb die fehlerhafte Datenübermittlung sowohl gegenüber der Stadt Wiesbaden als auch gegenüber dem Kommunalen Gebietsrechenzentrum Wiesbaden.

2.3.3.1.2
Reaktionen, Diskussion im Landtag

Um eine Wiederholung dieses oder ähnlicher Vorfälle zu verhindern, schlug ich folgende Maßnahmen vor:

- Bei der Verarbeitung von Meldedaten ist durch Programm sicherzustellen, daß auch auf dem Bildschirm im Rechenzentrum oder an anderer geeigneter Stelle ein Hinweis erscheint, daß gesperrte Daten verarbeitet werden sollen.

- Vor der Übermittlung eines Gesamtdatenbestandes (z.B. an Adreßbuchverlage) hat das Rechenzentrum als Auftragnehmer besondere Kontrollen durchzuführen.

- Sollen Meldedaten an nichtöffentliche Stellen übermittelt werden, hat die speichernde Stelle wenigstens durch Stichproben zu prüfen, ob die Auskunftssperren nach § 34 Abs. 5 HMG berücksichtigt wurden. Werden lediglich geringe Untermengen des Gesamtdatenbestandes übermittelt, die durch freigegebene und nicht mehr modifizierte Programme erzeugt wurden, kann die Stichprobe entfallen.

In seiner Sitzung vom 11. Januar 1984 beschäftigte sich der Innenausschuß des Hessischen Landtags mit dem Vorfall. Er nahm die Berichte der Stadt Wiesbaden, des KGRZ Wiesbaden sowie meine Darstellung entgegen und überwies den Vorgang an die Arbeitsgruppe "Datenverarbeitung" des Ausschusses. Diese befaßte sich in ihrer Sitzung vom 17. Februar 1984 ausführlich mit den Vorgängen. In der Diskussion wandte sich insbesondere die Stadt Wiesbaden gegen die Feststellung, sie habe ihre Überprüfungspflicht nicht ordnungsgemäß wahrgenommen und wandte ein, der Fehler läge allein beim Kommunalen Gebietsrechenzentrum. Fehlerhafte Programme seien allein von den Rechenzentren bzw. vom Hessischen Datenverarbeitungsverbund zu vertreten. Der Hessische Datenschutzbeauftragte habe auch insofern eine umfassende Überprüfungspflicht. Während der Sitzung des Ausschusses verdeutlichte ich noch einmal meinen gegenteiligen Standpunkt. Die Arbeitsgruppe faßte folgende Beschlüsse:

"Aus Anlaß der Weitergabe von Adressen im Zusammenhang mit dem Adreßbuch der Stadt Wiesbaden schlägt die Arbeitsgruppe Datenverarbeitung dem Innenausschuß vor, die Hessische Landesregierung und den Datenschutzbeauftragten zu bitten, die Rechtslage bei der Verarbeitung von Daten durch die Kommunalen Gebietsrechenzentren klarzustellen und in einer entsprechenden Information an die Städte und Gemeinden weiterzuvermitteln.

Die Hessische Landesregierung und der Datenschutzbeauftragte sollen darüber hinaus gebeten werden, dem Innenausschuß einen Bericht über die Maßnahmen vorzulegen, die auf der Grundlage der bereits vom Hessischen Datenschutzbeauftragten und von den Kommunalen Gebietsrechenzentren gemachten Vorschläge getroffen worden sind, um die Wiederholung solcher und ähnlicher Fälle zu verhindern."

Der Innenausschuß schloß sich dieser Empfehlung in seiner Sitzung vom 29. Februar 1984 an. Darauf wandten sich der Hessische Minister des Innern und ich in einer übereinstimmenden Erklärung an alle Städte und Gemeinden. Der hierzu ergangene Erlaß des Hessischen Ministers des Innern wurde im Staatsanzeiger veröffentlicht (StAnz. 19/84 S. 938). In diesem Erlaß wird noch einmal ausdrücklich festgestellt, daß "speichernde Stellen" alle Behörden und sonstigen öffentlichen Stellen des Landes, der Gemeinden und Gemeindeverbände sind, die personenbezogene Daten speichern oder durch andere speichern lassen (§ 2 Abs. 3 Nr. 1 HDSG). Werden die Daten im Auftrag durch ein Rechenzentrum gespeichert, dann wird der Auftragnehmer nicht zur speichernden Stelle; diese Eigenschaft hat auch weiterhin nur der Auftraggeber.

Der Erlaß weist darüber hinaus darauf hin, daß der Auftragnehmer gesetzlich verpflichtet ist, die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung insbesondere des § 10 Abs. 1 Hessisches Datenschutzgesetz zu gewährleisten. Der Auftraggeber hat bei der Auswahl des Auftragnehmers darauf zu achten, ob die von diesem getroffenen Maßnahmen zur Gewährleistung der genannten Anforderungen geeignet sind.

Der Minister stellt darüber hinaus in seinem Erlaß fest, daß bei den Kommunalen Gebietsrechenzentren und der Hessischen Zentrale für Datenverarbeitung aufgrund der dort getroffenen und vom Datenschutzbeauftragten überwachten Maßnahmen von dieser Eignung ausgegangen werden kann. Dadurch werde die auftraggebende speichernde Stelle allerdings nicht von ihrer Verantwortung für die Richtigkeit und Rechtmäßigkeit der Datenverarbeitung entbunden. Art und Umfang der Maßnahmen, die zur ordnungsgemäßen Abnahme der Auftragsergebnisse erforderlich sind (z.B. Stichproben), richteten sich nach den Umständen des Einzelfalles, insbesondere auch danach, ob und inwieweit durch mögliche Fehler schutzwürdige Belange der Betroffenen beeinträchtigt werden können.

2.3.3.1.3
DV-technische Konsequenzen

In einer Reihe von Sitzungen befaßten sich sowohl der Landesautomationsausschuß als auch der Kommunale Automationsausschuß mit organisatorischen und programmtechnischen Verbesserungen, um derartige unzulässige Datenübermittlungen zu verhindern. Insbesondere wurden im Koordinierungsausschuß der Rechenzentren eine Reihe von Beschlüssen gefaßt, die dieses Ergebnis sicherstellen können:

- So wurden die für die einzelnen Verfahren federführenden Rechenzentren beauftragt, die jeweiligen Verfahren hinsichtlich ihrer sicherheitstechnischen Vorkehrungen zu überprüfen.
- Der Arbeitskreis Einwohnerwesen wurde einberufen, um programmtechnische Sicherheitsmaßnahmen im Verfahren Einwohnerwesen zu erarbeiten.
- Anstelle von numerischen Schlüsseln für die Auswertungsempfänger wurden "sprechende Schlüssel" eingeführt, um sogenannte "Zahlendreher", d.h. versehentliche Ziffernverwechslungen, zu vermeiden.
- Unabhängig vom Auswertungsempfänger sollen Einwohnerdatensätze mit einer Auskunfts- und Übermittlungssperre zunächst in keine Auswertung einbezogen werden. Eine "Entsperrung" der einzelnen Datensätze soll durch den Sachbearbeiter jeweils im Einzelfall vorgenommen werden.
- Durch eine entsprechende Programmroutine soll weiterhin sichergestellt werden, daß bei Auswertungen für private Dritte die Auskunftssperren wegen Adoption und die Totalsperre nach § 34 Abs. 5 des Hessischen Meldegesetzes nicht entsichert werden können.
- Durch geeignete Schriftstücke (Listenaufkleber, Karteikarten), die einer jeweiligen Auswertung beigefügt werden, wird die Gemeinde darauf hingewiesen, welche Auskunftssperren durch die DV-technischen Steuerungsinformation entsichert wurden.

Das Kommunale Gebietsrechenzentrum Gießen wurde mit der Realisierung dieser Maßnahmen bis zum 30. Juni 1984 beauftragt. Darüber hinaus beschloß der Koordinierungsausschuß betriebsinterne Überprüfungen in den einzelnen Rechenzentren, vor allem die Ergebnisüberprüfung durch einen zweiten Sachbearbeiter.

2.3.3.2
Minderjährige im Adreßbuch

Bei einer anderen Kommune gelangten entgegen der Vorschrift des § 35 Abs. 4 HMG nicht nur die Daten der volljährigen Einwohner an den Adreßbuchverlag, sondern auch die Anschriften derjenigen Personen, die das 18. Lebensjahr noch nicht vollendet hatten. Aufgrund eines technischen Fehlers im Rechenzentrum - auf die "Vorlaufkarte" der Arbeitsvorbereitung wurde die im Gesetz vorgesehene Einschränkung nicht aufgenommen - kam es zu dem Verfahrensfehler. Das Rechenzentrum erkannte den Fehler auf einem Probeausdruck, der zu Prüfzwecken erstellt wurde, nicht. Die Gemeinde ihrerseits versäumte, anhand eines Ausdrucks nachzuprüfen, ob im Datensatz nur volljährige Einwohner erfaßt worden waren. Vielmehr übergab sie die Magnetbänder ohne vorherige Kontrollmaßnahmen an den Adreßbuchverlag.

Das Rechenzentrum hat mir versichert, es wolle die offenbar gewordenen Mängel bei der Überwachung des Arbeitsablaufes durch eine Reihe von Maßnahmen für die Zukunft verhindern. Für das angewandte Verfahren wurden insbesondere folgende organisatorische Vorkehrungen getroffen:

- Die Übertragung der Auswahlkriterien vom schriftlichen Auftrag auf die Vorlaufkarte wird bei Auswertungen, die für Dritte bestimmt sind, von einem zweiten Bediensteten überwacht. Die Überprüfung ist schriftlich zu vermerken.

- Bei Daten, die der Erstellung von Adreßbüchern dienen sollen, wird bei Weitergabe von Magnetbändern ein Listenausdruck mit dem Gesamtinhalt des Bandes an die auftraggebende Verwaltung (speichernde Stelle) zur Überprüfung weitergegeben.

Wie bereits im Wiesbadener Fall kam auch hier die Gemeinde ihrer Überprüfungspflicht nicht ausreichend nach. Sie hätte als speichernde Stelle durch eine stichprobenhafte Überprüfung feststellen müssen, ob nur die Datensätze der volljährigen Einwohner für die Auswertung durch den Adreßbuchverlag übermittelt worden waren. Auch in diesem Fall habe ich die fehlerhafte Übermittlung beanstandet.

Beide Fälle lehren vor allem zweierlei: Obwohl die Rechenzentren des Hessischen Datenverarbeitungsverbundes über einen hohen Standard der Datensicherung verfügen, ist es notwendig, im Rahmen der Verfahrensentwicklung und -überprüfung immer wieder programmtechnische und organisatorische Vorkehrungen zu durchdenken, die solche Fehlerquellen ausschließen. Es war erfreulich festzustellen, mit welcher Intensität und Schnelligkeit sich die Rechenzentren um eine Verbesserung der Verfahren sowie der organisatorischen Datensicherung bemüht haben.

Deutlich wurde auch, daß sich die Gemeinden - ebenso wie wahrscheinlich auch andere Stellen der Verwaltung -durch das technische Wissen und den bei den Rechenzentren gesammelten Sachverstand dazu verleiten lassen, die Arbeitsergebnisse nicht mehr zu kontrollieren, sondern deren Richtigkeit einfach zu unterstellen. Selbstverständlich wäre jede Gemeinde überfordert, wollte sie jedes Programm im einzelnen überprüfen. Soweit jedoch nicht Routineauswertungen, sondern besondere Auswertungen von den Auftragnehmern ausgeführt werden, muß sich jede speichernde Stelle auf ihre grundsätzliche Verantwortung für die Richtigkeit der personenbezogenen Datenverarbeitung besinnen. Dementsprechend ist sie gehalten, durch geeignete organisatorische Vorkehrungen - namentlich Stichproben - weitgehend sicherzustellen, daß durch die Weitergabe der Ergebnisse nicht schutzwürdige Belange betroffener Einwohner verletzt werden.

2.4
Hochschulen

2.4.1
Hochschulstatistik

2.4.1.1
Kritik aufgrund des Volkszählungsurteils

Das Hochschulstatistikgesetz (in der derzeit noch gültigen Fassung der Bekanntmachung vom 21. April 1980, BGBl. I S. 453; zu dem jetzt vorliegenden Änderungsentwurf vgl. Ziff. 3.2.5) sieht vor, daß alle sechs Jahre eine individualisierte Erhebung des wissenschaftlichen und künstlerischen Personals der Hochschulen durchgeführt wird. Im Jahre 1983 sollte die Erhebung mit dem Stichtag 20. Oktober 1983 stattfinden. Die Hochschulen waren aufgefordert, die Erhebungsbogen bis zum 13. Januar 1984 an das Statistische Landesamt zurückzuschicken. Im gleichen Zeitraum fand das Verfahren zum Volkszählungsgesetz 1983 vor dem Bundesverfassungsgericht statt. Offenbar angeregt durch die Diskussion über dieses Verfahren in der Öffentlichkeit haben sich zahlreiche Mitglieder hessischer Hochschulen, die von der Erhebung betroffen waren, sowie auch der Hauptpersonalrat beim Hessischen Kultusminister an mich gewandt und erhebliche Zweifel an der Gewährleistung des Datenschutzes bei der Erhebung geäußert. Hierbei erschien vielen Betroffenen jene Verpflichtung besonders bedenklich, das Deckblatt zum Erhebungsbogen, auf dem Namen und Adressen der Auskunftspflichtigen vermerkt waren, an das Statistische Landesamt zurückzuschicken, um Rückfragen zu ermöglichen.

Meine Intervention hatte zunächst zur Konsequenz, daß der Hessische Kultusminister - im Hinblick auf die noch vor dem Urteil des Bundesverfassungsgerichts zur Volkszählung deutlich werdende Problematik des § 15 Hochschulstatistikgesetz - auf dem Verwaltungsweg durch Erlaß eine Verfahrenskorrektur vornahm. Noch am 7. Dezember 1983 wies er die Hochschulen an, von einer Nutzung der bei dieser statistischen Erhebung gewonnenen Daten für ihre verwaltungsinternen Zwecke abzusehen.

Doch konnte dieser - im Vorgriff auf die zu erwartende Entscheidung des Bundesverfassungsgerichts herausgegebene - Erlaß trotz dieser Verwendungsbeschränkung für die erhobenen Daten eine verfassungskonforme und damit auch datenschutzrechtlich unbedenkliche Durchführung der Hochschulstatistik nicht garantieren, da das Hochschulstatistikgesetz selbst nicht den Kriterien gerecht wird, die das Bundesverfassungsgericht für eine statistische Rechtsgrundlage statuiert hat. Ich habe daraufhin dem Hessischen Ministerpräsidenten folgende Bedenken und Kritikpunkte mitgeteilt:

1. Die in § 5 HSchStatG angeordnete Individualerhebung des wissenschaftlichen Personals in einer Periodizität von sechs Jahren mit einer Auskunftspflicht des einzelnen Betroffenen ist unverhältnismäßig. Das gleiche Ziel ließe sich auch mit einer anonymen, nicht personenbezogenen Erhebung erreichen, wie das Beispiel der nichtindividualisierten Erhebung des technischen Verwaltungs- und sonstigen Personals zeigt (§ 6 HSchStatG). Die Gesetzesbegründung läßt im übrigen die Notwendigkeit unterschiedlicher Erhebungsweisen bei den Personalgruppen der Hochschulen nicht erkennen. Für die Zwecke der Hochschulplanung sind die "Angaben zur Person" im Zusammenhang mit dem Namen jedenfalls nicht erforderlich, zumal Alter, Geschlecht und Staatsangehörigkeit auch anonymisiert werden können.

2. Eine Verpflichtung zur Angabe von Namen und Dienstanschrift auf dem Deckblatt des Erhebungsbogens ist durch den Wortlaut "Angaben zur Person" nicht gedeckt. Wie aus der Erläuterung zur Erhebung der Merkmale "Name" und "Dienstanschrift" auf dem Deckblatt hervorgeht, haben diese Angaben lediglich Hilfsfunktionen zur "Prüfung der Vollständigkeit und für Rückfragen". Einen statistischen Zweck erfüllen sie nicht.

   Die Individualisierung der Statistik bleibt auch in der Auswertungsphase durch die Kombination von Landescode, Hochschul- und Paginiernummer bestehen. Der Zweck der individualisierten Bestandsstatistik bleibt daher auch ohne Erhebung von Name und Dienstanschrift erfüllbar.

   Im übrigen mangelt es dem Erhebungsmerkmal "Angaben zur Person" an der verfassungsrechtlichen Bestimmtheit, um einen Eingriff in das informationelle Selbstbestimmungsrecht zu rechtfertigen. Der besondere Stellenwert der Erhebungsmerkmale "Name" und "Adresse", der auch in der Wertung von § 11 Bundesstatistikgesetz (BStatG) zum Ausdruck kommt, verlangt eine Bestimmtheit dieser Merkmale im Gesetz selbst. Fehlt es an dieser Anordnung durch die statistische Rechtsvorschrift, dann ist ein Verzicht auf die Erhebung dieser Einzelangaben verfassungsrechtlich geboten. Kurzum: Die Auskunftspflicht des § 13 Ziff. 2 HSchStatG erstreckt sich nicht auf Name und Dienstanschrift.

3. Der Erlaß des Kultusministers hat zwar auf meine Initiative hin im Vorgriff auf die Entscheidung des Bundesverfassungsgerichts die Aussetzung der Anwendung von § 15 Abs. 2 HSchStatG in verfassungskonformer Weise angeordnet. Gleichwohl ist die Aufklärung der Auskunftspflichtigen auf dem Deckblatt des Erhebungsbogens mißverständlich. Damit ist der Aufklärung, zu der das Bundesverfassungsgericht die statistischen Ämter verpflichtet hat, keineswegs Genüge getan. Die gesetzliche Bestimmung von § 15 Abs. 4 ist insoweit nicht hinreichend, da das informationelle Selbstbestimmungsrecht gebietet, den Bürger darüber aufzuklären, was wann wo bei welcher Gelegenheit über ihn verarbeitet wird. Dazu gehört auch die gesetzliche Möglichkeit, statistische Einzelangaben für Verwaltungszwecke der Hochschulen zu verwenden.

4. § 15 Abs. 2 verstößt im übrigen gegen den Grundsatz der Normenklarheit als Teil des Rechtsstaatsprinzips. Hier hätte schon nach § 11 Abs. 3 BStatG im Hochschulstatistikgesetz bestimmt werden müssen, an welche Stellen unter Angabe des Verwendungszweckes statistische Einzelangaben ohne Nennung von Name und Anschrift übermittelt werden dürfen. Eine Wiederholung des Normtextes von § 11 Abs. 3 BStatG reicht daher nicht aus. Diese Vorschrift verlangt vielmehr die Konkretisierung des Empfängerkreises, des Umfangs der übermittelbaren Daten und des Verwendungszweckes in der die Statistik anordnenden Rechtsvorschrift. Zweck dieser Vorschrift soll es sein, dem Auskunftspflichtigen Transparenz über die Verwendung seiner Daten zu verschaffen. Diese Absicht des Gesetzgebers wird durch § 15 Abs. 2 konterkariert.

5. Zu den vom Bundesverfassungsgericht geforderten grundrechtssichernden Maßnahmen hätte auch eine Regelung des Erhebungsverfahrens in den und durch die Hochschulen gehört. Besondere Sicherungsmaßnahmen für die Gewährleistung des Statistikgeheimnisses durch organisatorische und technische Verfahren in den Hochschulen sind durch das Statistische Landesamt bzw. den Kultusminister nicht angeordnet worden. Mit anderen Worten: Das Verfahren der Erhebung im einzelnen wurde den Hochschulen überlassen. Die Abschottung der statistischen Angaben von den übrigen Verwaltungsdaten war daher nicht durch entsprechende Regelungen gewährleistet.

6. Schließlich und letztlich war mir weder die Durchführung der Erhebung noch der Erhebungsvordruck bekannt, um die Erhebung und ihr Verfahren im Sinne eines vorverlagerten Grundrechtsschutzes präventiv prüfen zu können. Ich habe daher der Landesregierung empfohlen, wegen der bestehenden datenschutzrechtlichen Bedenken die Erhebung des wissenschaftlichen und künstlerischen Personals der Hochschulen in der vorgesehenen Form auszusetzen und auf eine Novellierung des Hochschulstatistikgesetzes hinzuwirken, die den Kriterien des Volkszählungsurteils Rechnung trägt, damit auch in Zukunft die Hochschulplanung in einem verfassungskonformen Rahmen weitergeführt werden kann.

2.4.1.2
Verfahrenskorrektur für die Übergangszeit

Mit Hinweis auf die Durchführung der Erhebung in anderen Ländern, die Bundeseinheitlichkeit der Datenbasis und das Hochschulstatistikgesetz als trotz des Verfassungsgerichtsurteils noch gültiger Rechtsgrundlage hat die Landesregierung im April die von mir bereits im Januar empfohlene Aussetzung der Erhebung abgelehnt. Nach ihrer Auffassung war die Lösung der verfassungsrechtlichen Problematik allein Sache einer Novellierung des Hochschulstatistikgesetzes. Gleichwohl haben Kultusminister und Statistisches Landesamt meine Ausführungen zum Anlaß genommen, für die Übergangszeit über einen vertretbaren Modus der Durchführung nachzudenken. Sie haben sich dabei über folgende Verfahrensweise verständigt:

1. Auf die Durchführung der Erhebung wird nicht verzichtet; die rechtlichen Möglichkeiten bei Verweigerung werden jedoch nicht ausgeschöpft, d.h. es wird bei einer Verweigerung kein Bußgeld erhoben.

2. Die vom Hessischen Statistischen Landesamt verteilten Erhebungsunterlagen werden insoweit verändert, als von den bereits bei den Hochschulen eingegangenen Unterlagen der Name und die Dienstanschrift in geeigneter Form entfernt bzw. unkenntlich gemacht werden und es zugelassen wird, daß die Bogen der Auskunftspflichtigen auch ohne Deckblatt angenommen werden.

3. Die Hochschulen und die Auskunftspflichtigen werden vom Hessischen Statistischen Landesamt in geeigneter Form von dem vorgenannten technischen Verfahren in Kenntnis gesetzt und nochmals darauf hingewiesen, daß mit Erlaß vom 7. Dezember 1983 (6 A 6.2 - 908/007 - 422) einer zentralen Zielsetzung des Urteils des Bundesverfassungsgerichts gefolgt wurde.

Noch vor dieser pragmatischen Verfahrensempfehlung der Landesregierung hat der Bundesminister für Bildung und Wissenschaft die verfassungsrechtliche Notwendigkeit einer Neufassung des Hochschulstatistikgesetzes festgestellt.

Im Dezember 1984 hat die Bundesregierung einen Novellierungsentwurf vorgelegt, der eine Reihe der Vorgaben des Volkszählungsurteils berücksichtigt (vgl. dazu unten Ziff. 3.2.5).

2.4.2
Studentendaten

2.4.2.1
Fehlende Rechtsgrundlage für die Verarbeitung

Auch bisher schon stand außer Zweifel, daß für die Erfassung und Speicherung der Studentenstammdaten, die für die Begründung, Veränderung und Beendigung des Studentenstatus von Bedeutung sind, eine Rechtsgrundlage existieren muß, die neben dem Hochschulstatistikgesetz die Aufgabenzuweisung an die Hochschulen für die Studentenverwaltung detailliert regelt. Zwar enthält das Hessische Hochschulgesetz vom 6. Juni 1978 hierzu eine Reihe von allgemeinen Bestimmungen, die aber in der administrativen Praxis bisher nicht so umgesetzt worden sind, wie dies notwendig wäre. Bis heute werden zur Datenerhebung und Speicherung die "Allgemeinen Vorschriften für die Studierenden an den Universitäten des Landes Hessen vom 29. Oktober 1971" (AVS) als Rechtsgrundlage herangezogen, eine Rechtsverordnung, die noch aufgrund des § 62 des früheren Universitätsgesetzes vom 12. Mai 1970 verkündet und in Kraft gesetzt worden ist.

Von der seit 1978 in § 27 Abs. 2 und § 35 Abs. 8 des Hessischen Hochschulgesetzes gegebenen Verordnungsermächtigung hat der Hessische Kultusminister nie Gebrauch gemacht. Da mithin in den letzten Jahren versäumt worden ist, die Verarbeitung der - im Sinne des Volkszählungsurteils zwangsweise erhobenen - Studentendaten durch Rechtsnorm zu regeln, ist nunmehr eine Situation entstanden, die weder mit dem Recht auf informationelle Selbstbestimmung noch mit dem Hessischen Datenschutzgesetz auf Dauer vereinbart werden kann. Auf diese Gefahr habe ich rechtzeitig hingewiesen.

Der Kultusminister hat daher bereits Anfang 1984 unter Hinweis auf das Urteil des Bundesverfassungsgerichts die Hochschulen gebeten, die für die unterschiedlichen Verwaltungszwecke notwendigen Daten aufzulisten. Ziel dieser Initiative sollte ein abschließend festgelegter Datenkatalog für die Studentenverwaltung sein. Obwohl die Hochschulen aufgefordert waren, ihre Berichte bis zum 25. März 1984 abzugeben, hat mir der Minister bis heute weder die Ergebnisse noch einen entsprechenden Verordnungsentwurf vorgelegt. Diese Entwicklung veranlaßt mich erneut zu der Feststellung, daß eine Weiterverwendung der nach §§ 4, 7, 8 und 9 des derzeit noch gültigen Hochschulstatistikgesetzes erhobenen Daten für administrative Zwecke der Hochschulen aus verfassungsrechtlichen Gründen und demzufolge auch datenschutzrechtlich unzulässig ist.

2.4.2.2
Konsequenzen für das geplante "Studentenoperationssystem"

Die fehlende Rechtsgrundlage hat auch erhebliche Bedeutung für die Frage, ob das für die Studentenverwaltung von der HIS-GmbH entwickelte sog. Studentenoperationssystem (HIS-SOS II) in Hessen derzeit überhaupt wie geplant implementiert werden kann. Die vom Unterausschuß Hochschule des Landesautomationsausschusses für die Entwicklung und Einführung dieses automatisierten Studentenverwaltungssystems eingesetzte Arbeitsgruppe hat sich meine Bedenken zu eigen gemacht und auf den bisher nur vorläufigen Charakter des Datenkatalogs in HIS-SOS II hingewiesen. Dieser Datenkatalog steht in der Tat unter dem Vorbehalt einer Verarbeitungsregelung, die bis zur Einführung dieses Systems in Kraft gesetzt sein muß. Insofern führen die schleppenden Arbeiten an einer Rechtsgrundlage auch zur Beeinträchtigung der administrativen Leistungsfähigkeit von Hochschulen und Wissenschaftsverwaltung.

Von besonderer Bedeutung ist die bereichsspezifische Regelung der Verarbeitung von personenbezogenen Daten in Hochschulen einschließlich der Studentendaten auch angesichts der Umgestaltung der Hochschulstatistik in eine Sekundärstatistik, die ja keine Erhebung direkt bei den Hochschulangehörigen mehr vorsieht, sondern sich auf den Verwaltungsdatenbestand der Hochschulen stützen muß (vgl. dazu unten Ziff. 3.2.5).

2.5
Gebührenpflicht für Auskunft:
Hemmnis für Datentransparenz

Die Gebührenpflicht für Auskünfte über die zu einer Person gespeicherten Daten ist in Hessen nicht, jedenfalls nicht vollständig, abgeschafft. Diese Feststellung wird bei jedem Verwunderung auslösen, der die klare Aussage von § 18 Abs. 4 HDSG liest: "Die Auskunftserteilung ist gebührenfrei". Das hessische Parlament hat mit Wirkung vom 1. November 1980 die Gebührenerhebung für Auskunftserteilungen an anfragende Bürger aufgehoben (Art. 1 des Änderungsgesetzes vom 14. Oktober 1980, GVBl. I S. 377). Die potentielle Abschreckungswirkung der Gebühr für den einzelnen, der wissen will, welche Daten über ihn gespeichert sind, um möglicherweise seine Rechte auf Berichtigung oder Löschung geltend zu machen, sollte beseitigt werden. Dieses nach wie vor gültige, auch von mir immer wieder angeführte Argument für die kostenlose Dateninformation nötigt zur Aufmerksamkeit für die Tatsache, daß es nach wie vor hessische öffentliche Stellen gibt, die Auskunftsgebühren entweder zu erheben beanspruchen oder gar tatsächlich anfordern.

2.5.1
Auskunftsentgelt bei Arbeitnehmerdaten?

Eine rechtliche Sondersituation besteht zunächst für die im öffentlichen Dienst Beschäftigten, die bei ihrem Arbeitgeber bzw. Dienstherrn die Mitteilung ihrer Daten beantragen. Soweit die Datenverarbeitung dienst- oder arbeitsrechtliche Rechtsverhältnisse betrifft, ist das Hessische Datenschutzgesetz in seinen materiellen Vorschriften (§§ 11, 12, 16 bis 19) nicht anzuwenden, also auch nicht die Bestimmung des § 18 über die Auskunft einschließlich des Wegfalls der Gebührenpflicht. Vielmehr gelten nach § 3 Abs. 4 HDSG die auch für private Firmen und Vereine einschlägigen Normen der §§ 23 ff. des Bundesdatenschutzgesetzes; Motiv für diese Abweichung war das Bestreben nach einer einheitlichen datenschutzrechtlichen Behandlung der Arbeitsverhältnisse im öffentlichen Dienst und in der Privatwirtschaft.

Nach § 26 Abs. 3 Satz 1 BDSG kann aber grundsätzlich ein Entgelt jedenfalls für die der speichernden Stelle durch die Auskunftserteilung direkt entstehenden Kosten verlangt werden. Zwar ist mir bisher kein Fall bekannt geworden, in dem eine hessische Dienststelle die Mitteilung der gespeicherten Angaben an einen Bediensteten von einer derartigen Kostenerstattung abhängig gemacht hätte. Immerhin behält sich jedoch beispielsweise die Zentrale Vergütungs- und Lohnstelle (ZVL) in Kassel, die die Bezügedaten fast aller Arbeitnehmer im hessischen Landesdienst verarbeitet, diese Möglichkeit ausdrücklich vor, auch und gerade wenn sie in ihren Auskunftsbescheiden den Satz aufnimmt, daß sie auf die Erhebung dieses Entgelts verzichte.

Diese widersprüchliche Rechtslage -als Bürger kostenfreie, als Beschäftigter möglicherweise entgeltliche Auskunft - bedarf bei der anstehenden Novellierung des Hessischen Datenschutzgesetzes dringend der Korrektur. Nach meiner Auffassung gehört die Entgeltlichkeit der Auskunft generell abgeschafft, gleichgültig ob Bundesverwaltung, Landesverwaltung oder Privatwirtschaft betroffen sind. Jedenfalls kann das hinter der Regelung des § 26 Abs. 3 Satz 1 BDSG stehende Motiv, die angebliche Gefahr zu verhindern, daß Privatunternehmen mit Auskunftsersuchen von Kunden, Vertragspartnern usw. "überschwemmt" werden, nicht - aufgrund der pauschalen Verweisungsregelung in § 3 Abs. 4 HDSG - auch für die Beschäftigten hessischer öffentlicher Stellen Geltung beanspruchen.

2.5.2
Gebührenpflicht bei der Rentenversicherung

Bei der Abwicklung des Auskunftsantrages eines in der gesetzlichen Rentenversicherung versicherten Bürgers, der mich eingeschaltet hatte, mußte ich feststellen, daß die Landesversicherungsanstalt Hessen dafür eine Gebühr von DM 10,--erhebt. Nach meinen Ermittlungen ist diese Praxis Ausfluß einer bundesweiten Handhabung sämtlicher Rentenversicherungsträger, die sich dabei auf folgende rechtliche Argumentation stützen: Für alle Sozialversicherungsträger, auch die landesunmittelbaren wie die LVA, gilt aufgrund der Verweisung in § 79 Abs. 3 des 10. Buchs des Sozialgesetzbuchs (SGB X; in Kraft getreten am 1. Januar 1981) der 2. Abschnitt des Bundesdatenschutzgesetzes. Anders ausgedrückt: Auch alle Sozialbehörden der Länder haben hinsichtlich der materiellen Datenschutzfragen wie der Zulässigkeit von Speicherung und Übermittlung, der Ansprüche auf Berichtigung und Auskunft usw. nicht das jeweilige Landesdatenschutzrecht, sondern das Bundesgesetz anzuwenden. Hintergrund dieser - im Gesetzgebungsverfahren umstrittenen und von mir seinerzeit ausdrücklich abgelehnten (vgl. 9. Tätigkeitsbericht, Ziff. 3.3) - Regelung ist der Wunsch nach Einheitlichkeit des Datenschutzrechts für den gesamten Bereich der Sozialverwaltung auf Bundes-, Landes- und kommunaler Ebene.

Während aber zwischen dem 2. Abschnitt des BDSG und den Landesdatenschutzgesetzen in der Mehrzahl der Regelungsfragen Übereinstimmung besteht, gilt dies gerade für die Entgeltlichkeit der Auskunft nicht. § 13 Abs. 4 Satz 1 BDSG statuiert nach wie vor die Gebührenpflichtigkeit der Auskunftserteilung. Im Gesetzgebungsverfahren des Jahres 1980 sind meines Wissens die Konsequenzen dieser Rechtsvereinheitlichung für die Sozialbehörden in den Ländern, die wie Hessen für ihre öffentlichen Stellen die Kostenerstattung bereits abgeschafft hatten, nicht bedacht worden.

Allerdings besteht auch bei Anwendung des § 13 Abs. 4 BDSG keineswegs eine Automatik der Gebührenerhebung. Auch und gerade von Behörden der Sozialverwaltung verlange ich, daß sie sorgfältig prüfen, ob die Auskunft nicht kostenfrei erteilt werden kann oder sogar muß.

So sieht § 3 Nr. 3 der Datenschutzgebührenordnung (DSchGebO vom 22. Dezember 1977, BGBl. I S. 3153) eine Ausnahme von der Gebührenpflicht bei "einfachen schriftlichen Auskünften" vor. Zu Recht weist die Amtliche Begründung zur Datenschutzgebührenordnung (zu § 3) auf die Aufgabe der Behörden hin, das Verfahren so zu gestalten, daß der Aufwand möglichst gering bleibt und damit die Voraussetzungen der Kostenlosigkeit der Dateninformation erreicht werden. Es bedeutet einen Vorteil gerade der automatisierten Datenverarbeitung, daß eine Auflistung der gespeicherten Daten mit geringem Aufwand ausgedruckt werden kann. In diesem Zusammenhang ist es bezeichnend, daß es schon bald nach Inkrafttreten des Bundesdatenschutzgesetzes eine Reihe von Empfehlungen, so des Bundesinnenministers und des Deutschen Städtetages, gegeben hat, die zur großzügigen Handhabung der Kostenfreiheit nach § 3 DSchGebO auffordern.

Darüber hinaus regelt § 4 DSchGebO, daß von der Einziehung der Gebühr ganz oder teilweise abgesehen werden kann, wenn sie nach Lage des einzelnen Falles eine besondere Härte bedeuten würde. Nicht schematisch vorzugehen, sondern diesen Tatbestand zu prüfen, bestand gerade im Ausgangsfall Veranlassung: Der Antragsteller hatte als Anschrift das Wohnheim eines Berufsförderungswerkes angegeben, was auf ein geringes Einkommen schließen lassen konnte.

Noch ein wichtiger Punkt: Die auskunftspflichtigen Stellen trifft nicht nur die Pflicht, die mögliche Befreiung von der Gebühr zu prüfen. Sie haben auch den Antragsteller darüber zu informieren, unter welchen Voraussetzungen (z.B. Angabe von Suchmerkmalen o.ä.) er seine Datenmitteilung kostenlos erhalten kann.

Ich habe die LVA Hessen auf diese Rechtssituation hingewiesen und sie gebeten, ihre Auskunftspraxis entsprechend zu organisieren. Gerade bei den vielfach sehr sensitiven Sozialdaten müssen die Sozialleistungsträger alles Interesse haben, den Eindruck zu vermeiden, der Bürger werde unnötigerweise mit bürokratischen Hemmnissen wie der vorherigen Gebührenzahlung in der Geltendmachung seiner Informationsinteressen behindert. In diesem Zusammenhang ist allerdings festzuhalten, daß mir aus Hessen bisher kein anderer Fall bekannt geworden ist, in dem eine andere Stelle der Sozialverwaltung einem auskunftsuchenden Bürger ein Entgelt abverlangt hat.

3. Regelungsdefizite

3.1
Informationstechnik

3.1.1
Bildschirmtext

Stand das Jahr 1983 noch im Zeichen der Beratung des Staatsvertrages über Bildschirmtext (ausführlich dazu 12. Tätigkeitsbericht Ziff. 3.4.1), war 1984 gekennzeichnet durch den Konflikt der Datenschutzbeauftragten mit der Deutschen Bundespost über die Gewährleistung des Datenschutzes. Die Notwendigkeit einer gesetzlichen Regelung, die technische Sicherheit des Systems, die Geltung des Staatsvertrages, das Informationsverhalten der Bundespost sowie nicht zuletzt die Frage der Kontrollkompetenzen von Landesbehörden beim Bildschirmtextsystem waren die Hauptpunkte der kontrovers geführten Debatte.

3.1.1.1
Einführungsstand

Hintergrund dieser Diskussion ist nicht zuletzt die Entwicklung bei den Teilnehmerzahlen: Mitte Dezember 1984 verzeichnete der Bildschirmtext 19.379 Teilnehmer, darunter 3.224 Anbieter; zum gleichen Zeitpunkt des Vorjahres waren es 6.666 Teilnehmer, davon 2.442 Anbieter.

An das Bildschirmtextsystem sind derzeit 37 externe Rechner angeschlossen, 510.426 Bildschirmtextseiten wurden am 10.12.1984 zum Abruf bereitgehalten. Die ursprünglich prognostizierte Zahl von einer Million Teilnehmer bis 1986 wird heute in den Bereich purer Spekulation verwiesen. Kurzum: Die Nachfrage nach dem Dienstleistungsangebot Bildschirmtext ist heute weit geringer, als selbst Skeptiker erwartet hatten. Die noch im Januar 1984 von Pessimisten geäußerte Teilnehmerzahl von 40.000 bis Ende 1984 (vgl. Btx-Aktuell Nr. 88 vom 15. Januar 1984 S. 1) wurde gerade zur knappen Hälfte erreicht. Neben den nicht gerade günstigen ökonomischen Rahmenbedingungen sind vor allem die überkomplexe Software-Entwicklung sowie die zur Zeit noch prohibitiven Kosten der Hardware für den nichtkommerziellen Teilnehmer Faktoren, die auf die Verbreitung von Btx nicht ohne Einfluß geblieben sind. Vor allem die nicht ausgereifte technische Entwicklung des Systems ist ursächlich für die erhebliche Verzögerung der bundesweiten Einführung von Bildschirmtext.

War der bundesweite Start bereits zur Funkausstellung 1983 in Berlin geplant, verschob sich der Beginn des eigentlichen "Wirkbetriebes" im CEPT-Standard auf Juli 1984: Die Ulmer Leitzentrale sowie die ersten regionalen Vermittlungsstellen gingen in Betrieb.

Die Situation in Hessen stellt sich nach den Plandaten der Oberpostdirektion Frankfurt, deren Bezirk fast deckungsgleich mit dem Gebiet des Bundeslandes Hessen ist, so dar, daß am Ende dieses Jahres mit dem Ortsnetz Bad Hersfeld und dem dazugehörigen Nahbereich ganz Hessen zum Nahtarif an das Btx-System angeschlossen sein sollte.

Trotz dieser zur Zeit nicht gerade optimistisch stimmenden Situation überschlagen sich die Prognosen. Nach der Diebold- Studie "Bildschirmtext 85", die sich mit der wirtschaftlichen Bedeutung und Marktentwicklung bis 1990 beschäftigt, wird die Zahl der Informationsanbieter 1990 auf etwa 100.000 wachsen. Für die beiden nächsten Jahre erwartet Diebold jeweils eine Verdoppelung der Anbieterzahlen. Selbst bei ungünstig verlaufender ökonomischer Entwicklung rechnet Diebold mit knapp einer Million Teilnehmern Ende 1988 und für Ende 1990 mit über zweieinhalb Millionen Btx-Teilnehmern. Ob diese Einschätzung Wunschdenken oder realistisches Kalkül ist, kann erst die Zukunft zeigen.

3.1.1.2
Notwendigkeit bundesrechtlicher Datenschutzregelungen

Für die Entwicklung der rechtlichen Rahmenbedingungen resultiert daraus jedenfalls, daß sie den Gegebenheiten einer Massenkommunikation standhalten müssen, wollen sie nur begrenzende oder gar direkt steuernde Wirkung entfalten. Nicht weniger wichtig ist diese Prognose für die Definition des erforderlichen Standards technischer und organisatorischer Datensicherheit in diesem offenen Kommunikationssystem.

Vor allem zu diesen beiden Punkten haben die Datenschutzbeauftragten in zwei Entschließungen vom 27./28. März und vom 6./7. Juni 1984 ihre Haltung - vornehmlich auch zum gegenteiligen Standpunkt der Bundespost - klar formuliert (vgl. den Wortlaut dieser Beschlüsse Ziff. 5.1 und 5.2).

Dabei standen besonders die widersprechenden Rechtsauffassungen immer unter dem belastenden Vorzeichen der - bewußt im Interesse einer raschen und effektiven Einführung des Bildschirmtextdienstes ausgeklammerten und verfassungsrechtlich nicht ausgetragenen - Auseinandersetzung über die Gesetzgebungskompetenz zwischen Bund und Ländern für die individualisierbaren Sparten der Massenkommunikation. Dieser verfassungsrechtlich offenen Situation entspricht das Nebeneinander von landesrechtlichen Regelungen in Gestalt des Btx-Staatsvertrages sowie der dazu mittlerweile in allen Ländern in Kraft getretenen Transformationsgesetze und den bundesrechtlichen Benutzungsbestimmungen im Fernmelderecht. Das Ausklammern der Kompetenzfrage läßt sich aber im politischen System des kooperativen Föderalismus nur dann durchhalten, wenn Bund und Länder, ohne die verfassungsgerichtliche Durchsetzung ihrer Kompetenzen anzustreben, die gegenteiligen Auffassungen respektieren.

Die Erklärung der Deutschen Bundespost gegenüber den Ministerpräsidenten der Länder vom 2. März 1983, die Datenschutzregelungen des Staatsvertrages zu akzeptieren, war Ausdruck eines solchen "medienpolitischen modus vivendi", wonach eine Bundesbehörde, die ihre Aufgabe in ausschließlicher Bundeskompetenz in eigener Verwaltung ausführt, in materieller Hinsicht landesrechtliche Vorschriften zum Nutzungsbereich eines Postdienstes anerkennt und anwendet. Diese - auf der Ebene politischer Deklaration - von Kooperationsbereitschaft geprägte Haltung wurde jedoch von der Bundespost in dem Augenblick verlassen, in dem es um die Konkretisierung dieser Verpflichtung und ihre administrative Umsetzung ging. So lehnt sie nach wie vor die Aufnahme von mit Art. 9 des Staatsvertrages deckungsgleichen Bestimmungen in das Fernmeldebenutzungsrecht ab, obwohl sie sich, wie erwähnt, bereits durch ihre Verpflichtung nach § 4 Postverwaltungsgesetz öffentlich-rechtlich an die materiellen Regelungen dieser Vorschrift im Länderabkommen gebunden hat. Dabei steht außer Zweifel, daß das Benutzungsrecht der Deutschen Bundespost für Bildschirmtext nur noch für wenige Experten, mit Sicherheit aber nicht für den Postkunden jenes Maß an Normenklarheit besitzt, das das Bundesverfassungsgericht verlangt. Verfassungsrechtliche Argumente, die sich aus dem Recht auf informationelle Selbstbestimmung herleiten, werden jedoch von der Bundespost deshalb nicht akzeptiert, da sie Btx grundsätzlich als freiwillige Dienstleistung ansieht, auch wenn Btx, wie sich aus den Prognosen ergibt, auf einen im Ergebnis für jeden Bürger unverzichtbaren Massendienst hin geplant und eingerichtet ist.

3.1.1.3
Informationsdefizit und Datenschutzkontrolle

Die Entwicklung weg vom Konsens und hin zur juristischen Formalisierung der Streitfragen hat den Konflikt erneut verschärft. Die Datenschutzbeauftragten der Länder haben daraufhin die Ministerpräsidentenkonferenz in ihrer Entschließung vom 6./7. Juni 1984 gebeten, auf die Einhaltung und strikte Beachtung dieser "Geschäftsgrundlage" des Btx-Staatsvertrages hinzuwirken. Diese Bitte der Datenschutzbeauftragten beruht auf der Besorgnis, daß die landesrechtlichen Vorschriften zur Kontrolle des Datenschutzes sonst leerlaufen und die durch Landesrecht mit der Kontrolle beauftragten Behörden ihre Aufgaben nicht effektiv wahrnehmen können. Die Bundespost akzeptiert nämlich nur die Überwachung durch den Bundesbeauftragten für den Datenschutz, der seinerseits landesrechtlich keinerlei Befugnisse hat.

Ein vielversprechender Ansatz zur Einbeziehung der zuständigen Landesbehörden waren eine von der Deutschen Bundespost angebotene Informationsveranstaltung im Mai und ein gemeinsames Expertengespräch im November.

Leider hat die Bundespost jedoch erneut ihre Auffassung bekräftigt, daß sie die zur technischen Überprüfung des Btx-Systems erforderlichen Informationen nur im Benehmen mit dem Bundesbeauftragten für den Datenschutz zu erteilen bereit ist. Sie hält es für weder zulässig noch erforderlich, den Landesbeauftragten bzw. den Aufsichtsbehörden für Btx solche Informationen zu geben, die eine wirksame Überwachung der Einhaltung des Datenschutzes bei Anbietern ermöglichen. Der Bundesbeauftragte wiederum sieht sich aus Rechtsgründen nicht in der Lage, die Landesbeauftragten für den Datenschutz über solche Verfahrensbestandteile von Btx zu unterrichten, über die ihm Unterlagen von der Deutschen Bundespost als vertraulich überlassen worden sind.

Die Datenschutzbeauftragten der Länder kamen dadurch in die Situation, ohne Kenntnis der vollständigen Unterlagen die bisher fehlende System- und Risikobeschreibung des Bildschirmtextes aufgrund der fragmentarisch von der Bundespost vorgelegten Materialien konstruieren und dann von ihr verifizieren bzw. falsifizieren lassen zu müssen. Ist eine solche Situation schon bei herkömmlichen Anlagen der Datenverarbeitung und Datenübertragung für Kontrollinstanzen unannehmbar, muß dies erst recht für ein hochkomplexes, offenes, in ständiger Veränderung und Optimierung befindliches Kommunikationssystem wie Btx gelten. Ohne Vorlage einer schriftlichen Systemdokumentation, des Pflichtenhefts und des Host-Handbuchs muß das Btx-System als "nicht prüffähig" bezeichnet werden. Zu dem gleichen Resultat kommt im übrigen auch der Regierungspräsident in Darmstadt als eine der Aufsichtsbehörden für Btx im privaten Bereich. So heißt es in einem Bericht an den Hessischen Minister des Innern vom 25. Juli 1984 lapidar: "Die für die Wahrnehmung meiner Kontrollaufgaben nach dem Btx-Staatsvertrag erforderlichen Informationen habe ich nicht erhalten".

3.1.1.4
Aufgetretene Mängel

Trotz dieser unvollständigen Informationen sind Defizite im technischen System erkennbar geworden, die mit dem Btx- Staatsvertrag nicht in Einklang stehen.

3.1.1.4.1
Abrechnungsmodus

Dies gilt insbesondere für den Modus der Abrechnung, der nicht mit Art. 9 Abs. 2 und 3 Btx-Staatsvertrag übereinstimmt. Die Steuerung der Abrechnung über die Leitseite eines Anbieters birgt im Gegensatz zur Intention dieser Schutznorm die Gefahr in sich, daß letztlich doch Rückschlüsse auf das Teilnehmerverhalten, und zwar im Hinblick auf die Wahl verschiedener Angebote, gezogen werden können.

Denn: Der in der Bildschirmtext-Leitzentrale für die Abrechnung kostenpflichtiger Seiten verwendete Gutschriften- und Entgeltsatz ordnet die Teilnehmernummer des Anfragenden derjenigen Leitseite eines Anbieters zu, über die der Teilnehmer in das Programm des Anbieters gelangt ist. Zusammen mit dem Zeitstempel, der den Zeitpunkt des Anfalls der Gebühr feststellt, wird das Teilnehmerverhalten dann um so wahrscheinlicher für den Anbieter rekonstruierbar, je mehr das Angebot in Leitseiten aufgeteilt wird. Auf diese Weise kann das Angebot inhaltlich ausdifferenziert und zusammen mit dem Zeitstempel die Inanspruchnahme bestimmter Angebote durch die Teilnehmer abgeleitet werden.

Bedenklich stimmt hierbei, daß die Bundespost, um den "Komfort" für den Anbieter zu erhöhen, in der zweiten Ausbaustufe ab Mitte 1985 je Anbieter bis zu 300 Leitseiten zur Verfügung stellen will. Begrenzt wird die damit verbundene Gefahr der Registrierung von Teilnehmerverhalten nicht durch das technische System, das die Deutsche Bundespost zur Verfügung stellt, sondern allenfalls dadurch, daß es sich nicht jeder Anbieter leisten kann, beliebig viele der vergleichsweise teureren Leitseiten anzubieten.

Wie immer man diese einschränkende Wirkung des Anbieterinteresses bewerten mag, unverzichtbar ist, daß schon die Ausgestaltung des Btx-Systems selbst die Möglichkeit der Rekonstruktion des Teilnehmerverhaltens ausschließen muß. Die Deutsche Bundespost sollte daher einen Abrechnungsmodus zu entwickeln versuchen, der von der Steuerung über die Leitseite abgeht und damit dem Btx-Staatsvertrag gerecht wird.

3.1.1.4.2
Zugriffsrecht

Weitere Risiken bestehen darin, daß Unberechtigte durch mißbräuchliche Nutzung der Anschlußkennung oder durch unbefugte Verwendung des persönlichen Kennworts zu Lasten des berechtigten Teilnehmers Btx nutzen und Gebühren bzw. Forderungen entstehen lassen können. Derzeit umfaßt das persönliche Kennwort mindestens 4 und höchstens 8 Stellen. Es entspricht damit nicht den Anforderungen, die man unter den aktuellen Bedingungen der Datenverarbeitung von einer Zugangssicherung durch Kennwort erwarten muß.

Erst von 1987 an muß die Struktur des Passwortes eine Reihe von Bedingungen erfüllen, die verhindern sollen, daß Dritte allzu leicht die Kennworte ausforschen können. Immerhin beruht der in den Medien vielbeachtete Vorfall, daß Mitglieder des "Chhaos-Computer-Clubs" unberechtigt das Gebührenkonto der Hamburger Sparkasse belastet haben, auf dieser Schwachstelle, wenn man der Sachverhaltsversion der Deutschen Bundespost folgt. Hinzu kommt, daß die persönlichen Kennwörter unverschlüsselt im Mitbenutzersatz gespeichert werden.

Die Erfahrungen zeigen bereits heute, daß erst die Verwendung intelligenter Chipkarten den Sicherheitsstandard offener Netze entscheidend verbessern kann. Die Bundespost hat in diesem Zusammenhang bereits begonnen, in Kooperation mit der Gesellschaft für Zahlungssysteme den Einsatz von Chipkarten zu untersuchen, und Betriebs- sowie Systemversuche in Aussicht gestellt.

3.1.1.4.3
Mitteilungsdienst

Ein weiterer Vorfall, ausgelöst ebenfalls durch den "Chaos-Computer-Club", hat auf eine weitere Schwachstelle des Btx-Systems hingewiesen, die die Deutsche Bundespost genauso zum sofortigen Handeln veranlaßt hat: Der Absender einer vom Empfänger bereits gespeicherten Mitteilung kann diese nachträglich ändern, ohne daß dies dem Empfänger signalisiert wird. Da der Mitteilungsdienst, z.B. bei Bestellungen, rechtsgeschäftliche Willenserklärungen enthalten kann, stellt eine solche Möglichkeit ein erhebliches Risiko dar. Zwar hat die Deutsche Bundespost daraufhin die zu dieser Manipulation notwendigen Decoderzeichen gesperrt, ist aber dabei auf den Protest solcher Anbieter gestoßen, für die die Editierung von Seiten dadurch erheblich erschwert worden ist.

3.1.1.5
"Hacking"

Über diese öffentlich bekannt gewordenen Vorfälle hinaus werden zur Zeit noch weitere Risiken der unbefugten Verwendung dieses offenen Kommunikationssystems mit der Bundespost erörtert. Diese Diskussion muß ständig geführt und in dem Maße weiterentwickelt werden, in dem das gesellschaftlich vorhandene Wissen um Nutzung und Verwendung von Kommunikationssystemen zunimmt. Anders ausgedrückt: Der Sicherheitsstandard ist immer eine Relation zwischen dem gesellschaftlich vorhandenen Wissen und den immanent vorhandenen Verarbeitungsschranken der Systeme.

Das Beispiel des "Chaos-Computer-Clubs" weist insofern auf eine neue Phase der Datenverarbeitung hin, als es einen Verbreitungsgrad von Handlungswissen über den Computer in der Gesellschaft anzeigt, der auch die Frage der technischen Sicherheit in einem neuen Licht erscheinen läßt:
Die Möglichkeiten des "hacking", derzeit eher noch "sportliche" Aktivität vor allem der Alternativszene, stellen neue Fragen z.B. im Hinblick auf sicherheitsempfindliche Sektoren, deren Rechner und ihrer Verletzlichkeit durch Nutzung, Veränderung und Zerstörung von Programmen und Speicherinhalten. Gleiches gilt für große Datenbanken der sozialen Sicherungssysteme oder medizinische Datenbanken. Auch das Problem der Vernetzung und der Online-Verbindungen verschiedener Rechner im öffentlichen Bereich ist im Hinblick auf die Verletzlichkeit anders zu beantworten als bisher.

Eine wichtige Konsequenz ergibt sich aus dieser Entwicklung auch für die Institutionen der Datenschutzkontrolle: Die Anforderungen an das technische Know-how des Datenschutzes werden noch mehr in den Vordergrund rücken. Zu den rechtlichen Rahmenbedingungen müssen die technischen hinzutreten; die Zuordnung von technischen zu rechtlichen Phänomenen stellt die "Technikvermitteltheit" des Datenschutzrechts her, deren Notwendigkeit sich beim Bildschirmtext zeigt.

3.1.1.6
Überwachung nach dem Abhörgesetz?

Ein Sonderproblem bildet die Überwachung des Datenverkehrs über Bildschirmtext nach dem Abhörgesetz (Gesetz zu Artikel 10 Grundgesetz, G 10) und nach § 100a Strafprozeßordnung (StPO). Nach Auffassung der Bundesregierung ist Btx rechtlich als Fernmeldeverkehr zu qualifizieren. Er genießt damit auch den Schutz des Fernmeldegeheimnisses. Bei Vorliegen der gesetzlichen Voraussetzungen ist daher eine Überwachung dieses Fernmeldeverkehrs nach dem G 10 oder nach § 100a StPO möglich (vgl. Parl. Staatssekretär Spranger, Bundestag 10. Wahlperiode / 58. Sitzung S. 122 f.).

Demgegenüber habe ich schon bei den Beratungen des Bildschirmtext-Staatsvertrages auf die Notwendigkeit hingewiesen, dort ein eigenes Mediengeheimnis zu verankern. Angesichts der Tatsache, daß die Länder Btx nicht als Fernmeldedienst, sondern als neues Medium definieren, würden sie sich selbst widersprechen, wenn sie bei der Überwachung von Btx durch die G 10-Kommission Bundesrecht für anwendbar erklärten. Feststeht, daß dieser Kompetenzkonflikt nicht zu Lasten des Bürgers und seiner Grundrechte ausgehen darf.

Die Datenschutzbeauftragten von Bund und Ländern haben bereits in ihrem Beschluß vom 11. Dezember 1980 ihre Bedenken dagegen zum Ausdruck gebracht, das G 10 auf den Bildschirmtext anzuwenden. Der Bundesbeauftragte für den Datenschutz hat seine Bedenken gegenüber der Auffassung der Bundesregierung noch einmal in einem Schreiben an den Bundesminister des Innern erläutert, in dem er darauf hinweist, daß die Vorschriften des G 10 weder nach dem Wortlaut noch nach ihrer Entstehungsgeschichte auf Bildschirmtext Anwendung finden können. Selbst Bundesbehörden, die die generelle Kompetenzfrage bei Btx anders beantworten als die Länder, kommen hier zum gleichen Resultat.

Ich habe den Hessischen Ministerpräsidenten auf diese Problematik hingewiesen. Es wäre wünschenswert, wenn die Landesregierung verdeutlichen könnte, daß sie die Auffassung der Bundesregierung zur Überwachung des Bildschirmtextsystems nicht teilt. Die Rechtsunsicherheit im Hinblick auf mögliche Grundrechtseinschränkungen ist mit der Verfassung nicht zu vereinbaren.

3.1.2
TEMEX

Der geplante TEMEX-Dienst der Deutschen Bundespost - sein Name leitet sich von der englischen Bezeichnung TELEMETRIC EXCHANGE ab - soll das Fernwirken bzw. Fernmessen u.a. im einzelnen Haushalt über das Telefonnetz ermöglichen. Als Anwendungsfälle werden unter anderem genannt:

- Vorrats- und Verbrauchsmessung und -steuerung bei Heizungsanlagen, Strom-, Wasser- und Gasversorgung;
- Einbruchs- und Diebstahlssicherung über Fernalarm;
- Überwachung hilfs- und pflegebedürftiger Personen.

Im Zusammenhang mit den Beratungen zu meinem 12. Tätigkeitsbericht hatte ich im Landtag die datenschutzrechtlichen Probleme von TEMEX erläutert und meinen Standpunkt dargelegt, wie ihn die Datenschutzbeauftragten in einer gemeinsamen Entschließung vom 6. Juni formuliert haben:

"Weil Fernwirksysteme erlauben, von außen in einer Wohnung Wirkungen auszulösen, Messungen vorzunehmen und Beobachtungen anzustellen, berühren sie maßgeblich die durch Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG geschützte Privatsphäre und das Grundrecht der Unverletzlichkeit der Wohnung (Art. 13 GG). In diese Grundrechte darf nur in engen gesetzlichen Grenzen unter strikter Wahrung des Grundsatzes der Verhältnismäßigkeit bzw. mit ausdrücklicher Einwilligung des Betroffenen eingegegriffen werden.

Um eine Verletzung dieser Grundrechte auszuschließen und ausreichenden Datenschutz zu gewährleisten, müssen vor Einführung von Fernwirkdiensten daher eindeutige gesetzliche Regelungen geschaffen werden, die auch die von der Verfassung vorgesehene Kompetenzverteilung zwischen Ländern und Bund berücksichtigen. Solange derartige bereichsspezifische Regelungen fehlen, dürfen Telefon-Fernwirkdienste nicht eingeführt werden."

Der Landtag hat sich meiner Position angeschlossen und die Landesregierung gebeten, "vorhandene rechtliche Möglichkeiten auszuschöpfen, die eine Einführung des TEMEX-Dienstes ohne Beteiligung des Landes ausschließen" (vgl. Beschluß Nr. 16, Beschlußempfehlung des Innenausschusses, Drucks. 11/1551).

Kurz darauf legte der Bundesminister für das Post- und Fernmeldewesen den Entwurf der 25. Änderungsverordnung zur Fernmeldeordnung vor, die in § 38c den Temexdienst regeln sollte. Die dort vorgesehene Regelung bestätigt im wesentlichen die im Beschluß der Datenschutzbeauftragten geäußerten Bedenken. Die Konsequenz daraus hat der Verwaltungsrat der Deutschen Bundespost auf seiner Plenarsitzung am 25. Juni 1984 gezogen: Er hat die Beschlußfassung über die Einführung des Temex-Dienstes bei den Beratungen über die 25. Verordnung zur Änderung der Fernmeldeordnung mit Rücksicht auf die noch offenen Fragen des Datenschutzes zurückgestellt (vgl. Bulletin der Bundesregierung Nr. 76/S. 674 f. vom 28. Juni 1984). Allerdings führt die Bundespost - an Orten außerhalb Hessens, etwa in München und Ludwigshafen - eine Reihe von Betriebs- und Systemversuchen durch.

Der Entwurf des § 38c verzichtet schlechthin auf eine bereichsspezifische Datenschutzregelung für Fernwirkdienste. So finden z.B. die Fragen der Einwilligung des Teilnehmers und ihr Widerruf, die Abschaltbarkeit der Endeinrichtung oder das für den Teilnehmer wichtige Anzeigen des Meß-/Schaltvorgangs zum Endgerät keine Erwähnung, ganz zu schweigen von einer Bestimmung über Verbindungs- bzw. Abrechnungsdaten sowie ihrer Verwendung und Löschung.

Mit Ausnahme der Begrenzung der Speicherung von Verbrauchsdaten auf einen Zeitraum von bis zu drei Arbeitstagen in § 38c Abs. 6 enthält die von der Post vorgeschlagene Formulierung keine Nutzungsregelung mit privatrechtsgestaltendem Charakter. Mithin wird die gesamte Nutzung der Vertragsgestaltung zwischen Anbieter und Teilnehmer überlassen. Angesichts der zumindest lokalen Monopolstellung der meisten Anbieter, etwa der Energieversorgungsunternehmen, ist dieser Regelungsverzicht nicht akzeptabel.

Regelungsbedarf ergibt sich keineswegs nur wegen der umfangreichen Datensammlungen, die bei der TEMEX-Hauptzentrale und damit bei der Bundespost entstehen können. Ich sehe die kritischen Datenschutzfragen auch und gerade im landesrechtlich zu regelnden Nutzungsbereich, etwa bei den vielfach öffentlich-rechtlich ausgestalteten Benutzungsverhältnissen der Energieversorgungsunternehmen mit Anschluß- und Benutzungszwang, der auch die Zähleinrichtungen für den Strom- und Wasserverbrauch einbezieht. Auch bei den Anbietern können durch das Fernmessen massenhaft Daten gespeichert werden, die Verbrauchsgewohnheiten des Bürgers, seine Anwesenheit in der Wohnung usw. offenlegen können.

Geeigneter Anknüpfungspunkt für eine Regelung in Hessen könnte die anstehende Novellierung des Hessischen Datenschutzgesetzes sein. Ich habe angeregt, Fernwirken und Fernmessen in die Legaldefinitionen der Datenverarbeitungsphasen einzubeziehen sowie besondere Zulässigkeitsvoraussetzungen und Verfahrensbedingungen in das HDSG aufzunehmen. Eine erste landesgesetzliche Normierung der datenschutzrechtlichen Aspekte von TEMEX ist im Berliner Kabelpilotprojektgesetz vom 25. Juli 1984 getroffen.

3.2
Statistik

3.2.1
Die amtliche Statistik vor neuen Regelungsaufgaben

Strukturen staatlichen Informationshandelns stehen im Mittelpunkt intensiver Diskussionen, die sich die Auswertung des Volkszählungsurteils vom 15. Dezember 1983 (Entscheidungssammlung des Bundesverfassungsgerichts, Bd. 65, S. 1 ff.) zum Ziel gesetzt haben. Selten zuvor hat es eine Entscheidung des Bundesverfassungsgerichts gegeben, die aus der Distanz von nunmehr gut einem Jahr in ihren Konsequenzen so unterschiedlich beurteilt worden ist.

Die Bundesregierung, die Innenministerkonferenz, der Innenausschuß des Deutschen Bundestages, Landtage wie Landesregierungen, sie alle haben legislative und administrative Konsequenzen beraten und zumeist entsprechende Initiativen ergriffen. Die Konferenz der Datenschutzbeauftragten von Bund und Ländern hat einen umfangreichen Forderungskatolog an Politik und Verwaltung formuliert, dessen Umsetzung wohl noch einige Zeit erfordern wird.

Am unmittelbarsten aber waren die Konsequenzen für die amtliche Statistik: Wesentliche Statistikgesetze, wie z.B. der Mikrozensus und das Hochschulstatistikgesetz, entsprachen nicht den verfassungsrechtlichen Anforderungen. Sie stand daher insgesamt vor der Alternative der verfassungskonformen Auslegung und Durchführung vieler Statistikgesetze oder der völligen Aussetzung wichtiger Teile der Statistik. Die Reaktionszeiten des Gesetzgebers schienen jedenfalls aus der Sicht der amtlichen Statistik zu lang, wollte man nicht den Verzicht auf statistische Information für eine Übergangszeit in Kauf nehmen.

Um dieser Situation zu entgehen, wurde der sogenannte "Übergangsbonus" ins Spiel gebracht. Dieser Begriff bedeutet, daß jedem Verfassungsgerichtsurteil eine Art Moratorium immanent ist, das der Verwaltung und dem Gesetzgeber eine gewisse Reaktionszeit einräumt, um die verfassungsgerichtliche Entscheidung umzusetzen. Damit soll gleichzeitig die bisherige Praxis bis zum Tätigwerden der Legislative legitimiert, mit anderen Worten die Funktionsfähigkeit der öffentlichen Verwaltung in diesem Übergangszeitraum nicht gefährdet werden. Den Forderungen des Datenschutzes wurde dementsprechend dieser "Übergangsbonus" zunächst entgegengehalten.

Unter diesen Umständen galt es klarzustellen, daß die Ausführungen des Urteils, die sich nicht nur mit der Volkszählung, sondern mit der Statistik und ihren verfassungsrechtlichen Rahmenbedingungen überhaupt auseinandersetzen, insoweit für alle Statistiken und ihre Durchführung unmittelbar verbindlich sind. Sie sind damit auch und zugleich verfassungsrechtlicher Prüfungsmaßstab für die gesamte amtliche Statistik. Ein "Übergangsbonus" kann daher nur die verfassungskonforme Durchführung einer Statistik im Rahmen des Normtextes unter Beachtung der Grundsätze des Volkszählungsurteils bedeuten. Diese Möglichkeit aber bietet sich nicht in allen Fällen an, wie z.B. beim Mikrozensus oder bei der Hochschulstatistik. Die Bindungswirkung der Entscheidungsgründe erzwingt dann einen Verzicht auf die Durchführung einer mit dem Recht auf informationelle Selbstbestimmung unvereinbaren Norm mit der Konsequenz für den Gesetzgeber, selbst tätig zu werden.

Leider wird das Volkszählungsurteil generell immer noch nicht als Chance für eine grundsätzliche Neuorientierung der amtlichen Statistik, sondern nach wie vor als Restriktion verstanden. Die Verrechtlichung, die sich zur Zeit anbahnt, bringt für den Bürger nicht, wie von vielen erwartet, eine qualitative Einschränkung der statistischen Befragung, nicht etwa eine geringere Belastung mit Auskunftspflichten, sondern im Gegensatz zu früher lediglich präzisere Regelungen und ein mehr an begleitenden grundrechtssichernden Verfahren. Eine Einschränkung der amtlichen Statistik in ihrem Erhebungsumfang und im Hinblick auf ihre Methoden ist bisher nicht auszumachen. Diese Tendenz läßt sich bei fast allen zwischenzeitlich vorgelegten Gesetzentwürfen beobachten.

Die Reflexion über Nutzen und Funktion der amtlichen Statistik im Hinblick auf politisches Handeln muß vor jeder gesetzlichen Initiative stehen: Die Auskunftsbereitschaft großer Teile der Bevölkerung steht jedenfalls nicht unter dem Vorbehalt irrationaler Vorurteile, vielmehr entspricht sie einer realistischen Einschätzung von politischen Kosten und Nutzen statistischer Information. In diesen Zusammenhang gehören auch die Fragen von Auskunftszwang und Kooperation des Bürgers, von Verhältnismäßigkeit und Methodenwahl, gegebenenfalls auch Überlegungen zu einer grundlegend neuen Institutionalisierung amtlicher und wissenschaftlicher Statistik, die von fachlichen und politischen Vorgaben unabhängiger wäre als heute.

Ob und inwieweit sich die amtliche Statistik nach dem Volkszählungsurteil auf diese Fragen eingelassen hat, wird an den vorliegenden Gesetzentwürfen zur Volkszählung und zum Mikrozensus wie auch zur Hochschulstatistik in ganz unterschiedlicher Weise deutlich.

3.2.2
Volkszählung 1986

3.2.2.1
Erhebungsprogramm

Das Erhebungsprogramm des "Entwurfs eines Gesetzes über eine Volks-, Berufs-, Gebäude-, Wohnungs- und Arbeitsstättenzählung" (Volkszählungsgesetz 1986 - VZG '86, vgl. Bundesrats-Drucksache 553/84)) entspricht nach Ansicht seiner Autoren "im wesentlichen" (vgl. Vorblatt zur Drucks. a.a.O.) dem des Volkszählungsgesetzes 1983. Nach Ansicht der Bundesregierung wird damit den Anforderungen des Volkszählungsurteils des Bundesverfassungsgerichts in vollem Umfange Rechnung getragen. In diesem Urteil werde "das Erhebungsprogramm des Volkszählungsgesetzes 1983 für zulässig erklärt und als Vorbedingung für die Planmäßigkeit staatlichen Handelns bezeichnet. Zur Sicherung des Rechts auf informationelle Selbstbestimmung sind nach dem Urteil jedoch ergänzende verfahrensrechtliche Vorkehrungen für die Durchführung und Organisation der Datenerhebung erforderlich" (vgl. Vorblatt a.a.O). Kurz: Beim "Erhebungsprogramm" bleibt alles beim alten, nur das Verfahren wird grundlegend neu und detailliert geregelt. Daher sieht der Entwurf des VZG '86 gegenüber dem VZG '83 folgende Neuregelungen vor:

1. Unterscheidung zwischen Erhebungsmerkmalen (Angaben, die zur statistischen Verwendung bestimmt sind) und Hilfsmerkmalen (Angaben, die lediglich der Durchführung der Zählung dienen) (§ 3 VZG).
2. Konkrete Bezeichnung der Erhebungssachverhalte (§§ 5 - 7 VZG).
3. Personelle und organisatorische Trennung der Erhebungsstellen von anderen Verwaltungsstellen (§ 9 VZG).
4. Vorschriften über Auswahl und Aufgaben der Zähler mit Ausschluß von Interessenkollisionen (§ 10 VZG).
5. Vorschriften über Erhebungsvordrucke und die Form der Auskunftserteilung (§§ 13 und 15 VZG).
6. Ausschluß der Übermittlung von Einzelangaben für den kommunalen Vollzug und den Melderegisterabgleich.
7. Verzicht auf Regelungen zur Übermittlung von Einzelangaben für Aufgaben oberster Bundes- und Landesbehörden sowie für wissenschaftliche Zwecke.
8. Besondere Trennungs- und Löschungsvorschriften (§ 15 VZG).

Ganz zweifellos stellen diese Punkte im Hinblick auf die verfassungsgerichtlichen Vorgaben einen erheblichen Fortschritt in der Statistikgesetzgebung dar, der auf andere Statistiken nicht ohne Auswirkungen bleiben wird. Von besonderer Bedeutung ist etwa die Differenzierung von Erhebungsmerkmalen, die zur statistischen Auswertung bestimmt sind, und Hilfsmerkmalen, die im Gegensatz dazu der Durchführung der Zählung dienen. Diese Unterscheidung hat Konsequenzen für die Trennung und Löschung der beiden Datenarten und hat auch Einfluß auf die Gestaltung der Erhebungsvordrucke.

Damit wird zum ersten Mal eine strikte funktionale Differenzierung von statistischen Einzelangaben vollzogen und klar gesetzlich definiert. Auf diese Weise entsteht eine eindeutige Zweckbindung dieser beiden Datenarten innerhalb der amtlichen Statistik. Der Entwurf des gleichzeitig in den Bundestag eingebrachten Mikrozensusgesetzes (vgl. dazu unten Ziff. 3.2.3) zeigt, daß beabsichtigt ist, diese Zweckbindung zum generellen Strukturprinzip der amtlichen Statistik zu machen. Bemerkenswert ist auch, daß Familien- und Vornamen der Haushaltsmitglieder nicht zu den Erhebungsmerkmalen gerechnet werden. Auch die Adresse wird grundsätzlich nur temporär bis zu einer Zuordnung des jeweiligen Haushalts zu der kleinräumigen Gliederungseinheit der "Blockseite" gespeichert.

3.2.2.2
Erhebungsstellen

Trotz dieser bemerkenswerten Neuorientierung im Hinblick auf die grundrechtssichernden Verfahren bleiben doch - neben der unzureichenden Behandlung der Frage nach der Erforderlichkeit einer Totalerhebung in der Begründung des Regierungsentwurfs - noch weitere Fragen offen. Die erste betrifft die noch zu treffenden landesrechtlichen Regelungen für die Einrichtung der Erhebungsstellen (vgl. § 9 VZG '86). Ob und inwieweit etwa kleinere Gemeinden jeweils für sich eine von der übrigen Gemeindeverwaltung "personell und organisatorisch" getrennte Erhebungsstelle einrichten können, ist zweifelhaft. Vorstellbar wäre auch die Zusammenfassung mehrerer kleiner Kommunen oder die Einrichtung der Erhebungsstellen bei den Landkreisen. Jedenfalls: Der generelle Verweis auf noch zu treffende landesrechtliche Regelungen in diesem wichtigen Verfahrensabschnitt stellt den Entwurf unter den Vorbehalt dieser - noch nicht einmal in ihrer Kontur erkennbaren - Bestimmungen. Zweifel sind angebracht, ob eine Totalerhebung wie die Volkszählung durch unterschiedliche Erhebungsorganisationen in den Ländern nicht methodisch gefährdet wird. Detaillierte Vorgaben des Bundesgesetzgebers sind daher notwendig. Die Hessische Landesregierung jedenfalls hat sich bisher nicht dazu geäußert, wie sie sich die Organisation der Volkszählung auf der Gemeindeebene vorstellt. Sie wartet offenbar den weiteren Verlauf des Gesetzgebungsverfahrens ab.

Nicht weniger wichtig für die Beurteilung der Verfassungskonformität einer zukünftigen Volkszählung wird die Regelung der "informationellen Gewaltenteilung" auf der gemeindlichen Ebene sein, die ebenfalls dem Landesrecht zugewiesen ist; ihre Ausgestaltung wird nicht zuletzt auch entscheidend sein für die Motivation von Städten und Gemeinden, sich an der Durchführung der Volkszählung überhaupt zu beteiligen. § 14 Abs. 1 des Regierungsentwurfs macht die Zulässigkeit der Übermittlung statistischer Einzelangaben ohne Hilfsmerkmale u.a. davon abhängig, daß durch Landesrecht eine "Trennung der zur Durchführung statistischer Aufgaben zuständigen Stelle von anderen kommunalen Verwaltungsstellen sichergestellt und das Statistikgeheimnis durch Organisation und Verfahren gewährleistet ist". Auch hier sind Vorstellungen über Inhalt, Form und Kontext einer zukünftigen Regelung von der Landesregierung bisher nicht geäußert worden.

Für eine Beurteilung aus der Sicht des Datenschutzes entsteht damit ein Junktim zwischen Bundes- und Landesgesetz, denn erst beide zusammen bilden das Normprogramm der Volkszählung.

3.2.2.3
Erhebungsvordrucke

In zwei weiteren entscheidenden Punkten jedoch ignoriert die Bundesregierung die vom Bundesverfassungsgericht definierten Kriterien. So enthält der Gesetzentwurf keine Bestimmung über Form und Inhalt der Erhebungsvordrucke. Nicht einmal die vom Bundesverfassungsgericht ausdrücklich erwähnte Möglichkeit, den Inhalt der Fragebögen durch Rechtsverordnung festzulegen, wird aufgenommen. Ich habe daher die Landesregierung gebeten, im Verlauf der Beratungen des Bundesrates dafür Sorge zu tragen, daß Inhalt und Form der Erhebungsvordrucke in der Anlage zum Volkszählungsgesetz festgelegt werden. Einen entsprechenden Änderungsvorschlag zu § 13 Abs. 1 des Entwurfs habe ich dem Hessischen Ministerpräsidenten unterbreitet. Erst eine solche Einbeziehung der Erhebungsvordrucke trägt den verfassungsrechtlichen Erfordernissen Rechnung. Danach hat der Gesetzgeber selbst dafür Sorge zu tragen, daß der Inhalt des Fragebogens mit dem Gesetz übereinstimmt; dies kann nicht durch die gesetzesausführenden Statistikbehörden bestimmt werden.

Diese Form der Feststellung der Erhebungsvordrucke als Anlage zum Gesetz gewährleistet zum einen den geforderten Parlamentsvorbehalt und sichert zum anderen die Nähe zu den Beratungen im Gesetzgebungsverfahren. Zugleich vermeidet sie ein erneutes kompliziertes Verfahren des Verordnungsgebers. Ganz und gar unplausibel wird der Verzicht auf die gesetzliche Festlegung des Fragenkatalogs beim Vergleich mit dem neuen Entwurf zum Mikrozensusgesetz (Bundestags-Drucks. 10/2600 vom 10. Dezember 1984), der hierfür eine Rechtsverordnung der Bundesregierung mit Zustimmung des Bundesrates vorsieht (vgl. § 10 Abs. 1 Satz 3). Was beim Mikrozensus als selbstverständliche Verfahrenssicherung gilt, muß erst recht für die Volkszählung gelten.

3.2.2.4
Mündliche Auskunftspflicht gegenüber dem Zähler

Darüber hinaus habe ich der Landesregierung empfohlen, sich für eine Streichung des § 13 Abs. 2 Satz 2 des Entwurfs zum VZG '86 einzusetzen. Die in dieser Bestimmung geregelte mündliche Auskunftspflicht gegenüber dem Zähler - im Hinblick auf die Angaben nach § 10 Abs. 6 des Entwurfs - befrachtet die beabsichtigte Volkszählung 1986 mit einem von vornherein vermeidbaren verfassungsrechtlichen Risiko. Zwar gibt es sinnvollerweise eine Befugnis des Zählers zur mündlichen Befragung, keineswegs aber darf ihr eine mündliche Auskunftsverpflichtung des Bürgers korrespondieren. Vielmehr ist der Auskunftspflichtige nach Auffassung des Verfassungsgerichts berechtigt, den ausgefüllten Erhebungsvordruck in verschlossenem Umschlag an die Erhebungsstelle zu senden: "Diese Erhebungsmethode vermeidet die Gefährdungen, die durch die Einsichtnahme der Zähler in die personenbezogenen Angaben der Bürger entstehen" (Bundesverfassungsgericht, a.a.O. S. 57 f.).

Doch damit nicht genug: Die Fassung des Regierungsentwurfs käme auch mit dem Gebot der Normenklarheit in Konflikt. Durch die Überschrift "Auskunftspflicht" zu § 12 des Entwurfs muß der betroffene Bürger den Eindruck gewinnen, daß hier die Auskunftspflicht abschließend geregelt ist. Dieser Eindruck wird durch die Verfahrensregelung in § 12 Abs. 4 und 5 noch verstärkt. Trotzdem wird ein wesentlicher Teil der Auskunftsverpflichtung, nämlich die in der amtlichen Statistik ungewöhnliche Sondervorschrift für eine mündliche Auskunftspflicht, in § 13 unter der Überschrift "Erhebungsvordrucke" aufgenommen. Bedenkt man, daß die Nichterfüllung der Auskunftspflicht als Ordnungswidrigkeit geahndet wird, ergeben sich aus dieser - für den Bürger nicht leicht durchschaubaren -Regelung gewichtige Zweifel an der Zulässigkeit dieser Sanktion im Hinblick auf das "nulla-poena-Prinzip" des Grundgesetzes.

3.2.2.5
Verschiebung?

Die Beratungen in den Ausschüssen und im Plenum des Bundesrates lassen eine äußerst kontroverse Diskussion des Volkszählungsgesetzes im weiteren Lauf des Gesetzgebungsverfahrens erwarten. Dabei gibt es gute Argumente, die schon heute eine Verschiebung der Volkszählung um mindestens zwei Jahre als empfehlenswert erscheinen lassen. Zum einen stellt der kurzfristig auf den 23. April 1986 festgesetzte Termin für die Durchführung der Volkszählung die Parlamentsberatungen unter den Einfluß des Sachzwangs bereits zuvor investierter Mittel sowie bereits eingeleiteter organisatorischer Vorbereitungen.

Zweiter wichtiger Aspekt: die internationalen Verpflichtungen der Bundesrepublik. So hat der Wirtschafts- und Sozialausschuß der Vereinten Nationen den Mitgliedstaaten empfohlen, alle zehn Jahre eine Weltbevölkerungs- und Wohnungszählung unter Berücksichtigung der bisherigen internationalen Empfehlungen zu Volks- und Wohnungszählungen durchzuführen. Der nächste Weltzensus ist auf das Jahr 1990 festgelegt worden. Die Volkszählung in der Bundesrepublik Deutschland mit dem Weltzensus zu synchronisieren hätte die Vorteile der internationalen Vergleichbarkeit der Datenbasis sowie des Einhaltens dieser UNO-Verpflichtung. Ein 1986 durchgeführter Zensus wäre nichts anderes als eine "nachgeholte" 83er Zählung. Eine Synchronisierung hätte dann zur Konsequenz, daß 1990 erneut eine Totalerhebung der Bevölkerung durchzuführen wäre oder aber die Daten von 1986 zu extrapolieren bzw. hochzurechnen wären.

3.2.3
Mikrozensus

Anders als die Volkszählung hat der Mikrozensus wegen seines detaillierteren und umfassenderen Fragenkatalogs schon früh zu Verfassungsbeschwerden Anlaß gegeben, die aber noch im Mikrozensus-Beschluß (Entscheidungssammlung des Bundesverfassungsgerichts, Band 27, S.1 ff.) zurückgewiesen worden sind, wenn auch mit grundsätzlichen Ausführungen zum allgemeinen Persönlichkeitsrecht, die nach wie vor Teil der Verfassungsrechtsprechung sind. Gleichwohl haben sich in der Vergangenheit bei jeder Mikrozensusbefragung Bürger an mich gewandt, weil sie sich durch diese Statistik in ihrem Persönlichkeitsrecht beeinträchtigt glaubten. Bei keiner Statistik ist die anfängliche Verweigerungsquote (bis zu 10 %) so hoch. Auf diese Probleme habe ich im 9. Tätigkeitsbericht (Ziff. 2.3.3) bereits grundsätzlich hingewiesen.

Im Zusammenhang mit dem beim Bundesverfassungsgericht anhängigen Verfahren über das Volkszählungsgesetz 1983 hatte die Bundesregierung wegen des hohen verfassungsrechtlichen Risikos zunächst auf administrativem Wege, danach durch Verordnung die Durchführung des Mikrozensus für 1983 ausgesetzt. Nach der Volkszählungsentscheidung vom 15. Dezember 1983 war offensichtlich, daß der Mikrozensus 1984 nur mit erheblichen Modifikationen verfassungskonform durchzuführen gewesen wäre. Nach Intervention der Datenschutzbeauftragten in den Ländern sowie auch einem entsprechenden Beschluß der Konferenz der Datenschutzbeauftragten entschloß sich die Bundesregierung, den Mikrozensus 1984 auszusetzen und die Novellierung des Gesetzes anzugehen. Am 10. Dezember 1984 haben die Fraktionen von CDU/CSU und F.D.P. mit Formulierungshilfe durch den Bundesminister des Innern den Entwurf eines "Gesetzes zur Durchführung einer Repräsentativstatistik über die Bevölkerung und den Arbeitsmarkt" (Mikrozensusgesetz, Bundestags-Drucks. 10/2600) eingebracht, der im Vergleich zu dem von der Bundesregierung eingebrachten Entwurf zum Volkszählungsgesetz bereits einige Fortschritte enthält. Im übrigen gelten in weiten Teilen ähnliche Argumente wie beim Entwurf für ein Volkszählungsgesetz. An meiner grundsätzlichen Beurteilung des Mikrozensus hat sich seit meinem 9. Tätigkeitsbericht nichts geändert. Allerdings hat sich im Gegensatz zur damaligen Stellungnahme der Landesregierung (Drucks. 9/4479, zu 2.3.3) der verfassungsrechtliche Prüfungsmaßstab entscheidend verändert. Die Auskunftspflicht ist nach wie vor nicht überzeugend begründet. Das Erhebungsprogramm läßt auch im neuen Gesetzentwurf an Normenklarheit zu wünschen übrig. Aufgenommen ist ebenfalls die kritikwürdige mündliche Auskunftsverpflichtung gegenüber dem Interviewer im Hinblick auf die Hilfsangaben. Besonders hervorgehoben zu werden verdienen - im Gegensatz zum Regelungsvorschlag für die Volkszählung - die Bestimmung über Testerhebungen mit freiwilliger Auskunftserteilung sowie die Tatsache, daß der Fragenkatalog in den Erhebungsvordrucken durch Verordnung der Bundesregierung mit Zustimmung des Bundesrates festgelegt wird.

3.2.4
EG-Arbeitskräftestichprobe

Kritisch zu bewerten dagegen ist die Einbeziehung der EG-Arbeitskräfte-Stichprobe in § 14 des Entwurfs des Mikrozensusgesetzes. Die Erhebungsmerkmale sind in großen Teilen mit denjenigen des Mikrozensus austauschbar bzw. ergänzen sich. Die Verweisung in § 14 sieht vor, daß grundsätzlich alle Verfahrensbestimmungen des Mikrozensusgesetzes auf die durch unmittelbar geltende Rechtsakte der Europäischen Gemeinschaft angeordnete Stichprobenerhebung über Arbeitskräfte "entsprechende" Anwendung finden, soweit die Merkmale (Erhebungs- und Hilfsmerkmale) mit denen der Arbeitskräftestichprobe übereinstimmen und sich aus den Rechtsakten der EG nichts anderes ergibt. Daß diese Verweisungsregelung unklar ist, läßt sich an wenigen Beispielen zeigen. Die "entsprechende" Anwendung der Auskunftspflicht, die ein überragendes Allgemeininteresse am Beantwortungszwang für den Bürger voraussetzt, läßt sich dann schwer nachvollziehen, wenn man weiß, daß in etwa der Hälfte aller EG-Mitgliedsstaaten diese Repräsentativstichproben auf freiwilliger Basis erfolgen. Problematisch ist auch, wie die kasuistisch definierte Auskunftspflicht für den Mikrozensus (§ 9 Abs. 1) überhaupt "entsprechend" auf andere Stichproben übertragen werden soll. Und weiter: Während in § 10 noch angeordnet wird, daß die Erhebungsvordrucke des Mikrozensus keine Frage über persönliche und sachliche Verhältnisse enthalten dürfen, die über die Merkmale nach den §§ 5 und 6 hinausgehen, können nach § 14 Abs. 2 Mikrozensus und EG-Stichprobe zur gleichen Zeit mit gemeinsamen, sich ergänzenden Erhebungsunterlagen, d.h. also auch mit zusätzlichen Angaben durchgeführt werden. Konsequenz: Die Generalverweisung in § 14 bietet keine ausreichenden grundrechtssichernden Maßnahmen bei der Durchführung der EG-Statistik.

Besonders problematisch ist die Frage nach der Regelungsbedürftigkeit der Auskunftspflicht. Selbst wenn man § 10 Abs. 1 Bundesstatistikgesetz für anwendbar hält, muß die Erforderlichkeit der Auskunftspflicht bei jeder neuen statistischen Erhebung nach dem neuesten Stand der wissenschaftlichen Methodendiskussion geprüft werden; so verlangt es das Bundesverfassungsgericht. Auch nach Auffassung des Bundesministers der Justiz muß der Gesetzgeber selbst eine bewußte Entscheidung über Auskunftspflicht oder Freiwilligkeit treffen. Diese unabdingbare Voraussetzung für einen verfassungsrechtlich legitimen Eingriff in das informationelle Selbstbestimmungsrecht des Einzelnen ist bei der einschlägigen EG-Verordnung (KOM (84) 343 endgültig) nicht erfüllt. Die Verordnung läßt, wie auch in der Vergangenheit, die Auskunftspflicht ungeregelt und verschiebt damit die Entscheidung auf die Mitgliedsstaaten. Weder der Rat der Europäischen Gemeinschaft noch der deutsche Gesetzgeber sind jemals mit dieser - für eine verfassungskonforme Statistik notwendigen - Frage nach der Verhältnismäßigkeit der Auskunftspflicht für die EG-Statistik befaßt gewesen. Eine generelle Verweisung wie im § 14 genügt nicht angesichts der Tatsache, daß im einzelnen noch unbestimmte künftige Statistikverordnungen der EG in Bezug genommen werden. Im Gegenteil, im Bundesstatistikgesetz oder im Verfahren der Rechtsetzung der EG ist zu garantieren, daß eine Prüfung dieser Frage im Einzelfall durch den jeweiligen Statistikgesetzgeber erfolgt.

Darüber hinaus läßt auch das Erhebungsprogramm in Art. 4 der Verordnung eine hinreichende Bestimmtheit vermissen. Schon in der Vergangenheit haben verschiedene Datenschutzbeauftragte darauf hingewiesen, daß mehrere in den Erhebungsformularen vorgesehene Fragen nicht mit dem Normtext der EG-Verordnung vereinbar waren. Die zum Teil sehr offene Fassung des Erhebungsprogramms in der EG-Verordnung führt in Verbindung mit dem Schlüsselverzeichnis, das den statistischen Ämtern der Mitgliedsstaaten zur Formulierung der Fragen vorgegeben wird, zu einer faktisch über den Normtext hinausgehenden Erweiterung der Erhebungsmerkmale durch die EG-Kommission. Trotz dieser bereits 1983 vorgetragenen Bedenken ist die EG-Stichprobe 1984 erneut in einer Form erhoben worden, in der mindestens sechs Fragen nicht durch die speziell für diese Erhebung erlassene Verordnung 276/84 gedeckt waren. Im Ergebnis ist daher das Verfahren der EG-Statistiken nicht mit einer Verweisung auf entsprechende Anwendungen vorhandener Statistikbestimmungen, sondern unmittelbar im Bundesstatistikgesetz grundsätzlich zu regeln.

3.2.5
Hochschulstatistik

Statistikbereinigung und Anpassung an die geänderte Verfassungsrechtslage sind die Ziele, die mit dem Referentenentwurf des Bundesministers für Bildung und Wissenschaft zur Novellierung des Hochschulstatistikgesetzes (Stand: 6. Juni 1984) verfolgt werden sollen. Dies soll durch die Modifikation des Erhebungsverfahrens, d.h. den Übergang von der Primär- zur Sekundärstatistik, durch den Wegfall der bisher gestatteten verwaltungsinternen Verwendung der statistischen Einzelangaben und durch den Verzicht auf Individualerhebungen beim wissenschaftlichen und künstlerischen Personal sowie bei Abiturienten erreicht werden.

Während bis jetzt Studenten, Doktoranden und Wissenschaftler unmittelbar auskunftspflichtig waren, verzichtet der vorliegende Referentenentwurf auf die Primärerhebung bei den Betroffenen und damit auch auf die in der Vergangenheit häufig kontrovers beurteilten Angaben zur Person.

Adressaten der Erhebung sind die in § 2 Ziff. 1 bis 3 beschriebenen Institutionen anstelle der in ihnen arbeitenden und studierenden Personen. Dadurch und durch den Verzicht auf die Primärerhebung wird das ursprüngliche Ziel einer Verlaufsstatistik, wie es in der Begründung zum noch geltenden Hochschulstatistikgesetz formuliert ist, aufgegeben. Dies war um so leichter möglich, weil es in 13 Jahren Hochschulstatistik nicht zu einer einzigen Auswertung des erhobenen Datenmaterials in Form einer Verlaufsstatistik gekommen ist.

Der Entwurf gewinnt vor allem durch Kürze und Präzision: §§ 3 bis 11 Hochschulstatistikgesetz (derzeit geltende Fassung) finden sich nunmehr in einer einzigen, wenn auch umfangreichen Bestimmung des Regierungsentwurfs (§ 3) wieder. Die Erhebungseinheit der Studenten nach § 3 Abs. 1 Ziff. 1 Regierungsentwurf erfaßt im Grunde den alten Tatbestand bis auf die Angaben zur Person (§ 4 Ziff. 1 HStatG). Der Terminus "Studienverlauf" in § 4 Ziff. 2 HStatG wird allerdings aufgelöst und präzisiert.

Das Personal der Hochschulen wird nicht mehr differenziert nach wissenschaftlichem und künstlerischem Personal (§ 5 HStatG) sowie technischem und Verwaltungspersonal, sondern gemeinsam erhoben. Lediglich für Habilitierte gibt es jährlich eine gesonderte Erhebung (§ 3 Abs. 1 Ziff. 2). Für wissenschaftliches und künstlerisches Personal werden in dreijähriger Periodizität Geburtsjahr und fachlicher Schwerpunkt erhoben. Dazu kommen noch eine Haushalts-, Raum-, Gebäude- und Prüfungsstatistik sowie eine Statistik der Wohnheimplätze. Besondere Aufmerksamkeit verdient die Erhebungseinheit "Prüfungskandidaten" (§ 2 Ziff. 4 i.V.m. § 4 Abs. 1 Ziff. 3 des Entwurfs). Hier wird ausnahmsweise die neue Struktur der Hochschulstatistik als Sekundärstatistik aufgrund vorhandener Daten verlassen zugunsten einer direkten Befragung der Betroffenen.

Die Datenschutzbeauftragten von Bund und Ländern haben auf ihrer Konferenz am 16. Oktober 1984 einen Beschluß gefaßt, in dem sie anhand des vorliegenden Referentenentwurfs feststellen, daß die Bundesregierung gemeinsam mit den beteiligten Landesressorts eine im Sinne des Datenschutzes umfassende Bereinigung der Hochschulstatistik einzuleiten beabsichtigt. Nach Ansicht der Datenschutzbeauftragten verdienen dabei folgende Strukturmerkmale auch im Verlauf des Gesetzgebungsverfahrens besondere Beachtung:

"1. Die Hochschulstatistik soll in ihren Erhebungsbereichen grundsätzlich nur noch bei den Hochschulen und deren Einrichtungen aufgrund vorhandener Verwaltungsdatenbestände mit Ausnahme der Prüfungsstatistik ohne Namen und Anschrift erhoben werden.

2. Auf eine Verlaufsstatistik soll verzichtet werden.

3. Das Erhebungsprogramm soll seinem Umfang nach gegenüber dem geltenden Hochschulstatistikgesetz bereinigt und erheblich reduziert werden.

Die Datenschutzbeauftragten gehen davon aus, daß auch die Statistik der Prüfungskandidaten nicht personenbezogen erhoben werden muß. Sie würden es daher begrüßen, wenn in der Hochschulstatistik in ihrer Gesamtheit auf die Erhebung unmittelbar beim Betroffenen verzichtet würde.

Je mehr sich allerdings die amtliche Statistik auf Verwaltungsdaten gründet, um so mehr muß auf die Präzision der Befugnisnormen zur Datenerhebung im Hochschulrahmengesetz und in den Hochschulgesetzen der Länder geachtet werden. Die Verlagerung der Datenerhebung von der Statistik zur Verwaltung stellt vor allem die Landesgesetzgebung (das Landesrecht) vor neue Aufgaben. Nach Ansicht der Datenschutzbeauftragten muß nunmehr dort die Frage nach dem legitimen Umfang der Datenverarbeitung gestellt und beantwortet werden."

3.3
Arbeitnehmerdaten

Das Jahr 1984 brachte wichtige Fortschritte in der Diskussion über den Datenschutz für Arbeitnehmer.

3.3.1
Die Entwicklung in Hessen

3.3.1.1
Novellierung des Personalvertretungsrechts

Die Notwendigkeit, die Beteiligungsrechte der Betriebs- und Personalvertretungen an die veränderten Bedingungen des Umgangs mit Arbeitnehmerdaten in automatisierten Personalinformationssystemen anzupassen, habe ich immer wieder unterstrichen, zuletzt im 12. Tätigkeitsbericht (3.3.1.4.). Dort hatte ich insbesondere meine Auffassung betont, daß angesichts widersprüchlicher Gerichtsurteile durch den Gesetzgeber klargestellt werden müsse, daß dem Personalrat ein Mitbestimmungsrecht bei der Einführung und Anwendung von Verfahren zur automatisierten Verarbeitung von Beschäftigtendaten zusteht und dazu einen konkreten Formulierungsvorschlag unterbreitet.

Das "Gesetz zur Änderung des Hessischen Personalvertretungsgesetzes und des Hessischen Richtergesetzes" vom 11. Juli 1984, das am 1. Oktober dieses Jahres in Kraft getreten ist, räumt jetzt dem Personalrat ein Mitbestimmungsrecht über die "Einführung, Anwendung, Änderung oder Erweiterung von automatisierter Verarbeitung personenbezogener Daten der Beschäftigten" ein (§ 61 Abs. 1 Nr. 17 neu). Die Personalräte hessischer Dienststellen erhalten damit Möglichkeiten der Reaktion auf die Nutzung von Computern im Personalwesen, die den Standard sowohl in der Bundes- und den anderen Landesverwaltungen als auch in der Privatwirtschaft weit übertreffen.

Dazu tragen auch weitere Bestimmungen der HPVG-Novelle bei: So hat der Personalrat bei der Bestellung und Abberufung von behördlichen Datenschutzbeauftragten mitzubestimmen (§ 61 Abs. 1 Nr. 3 neu). Bei dieser Regelung geht es im Kern darum, daß der Mitarbeiter, der für die innerdienstliche Überwachung der Einhaltung des Datenschutzes zuständig ist, nicht ausschließlich ein "Mann des Vertrauens" der Dienststellenleitung ist, sondern auch auf den Konsens der Personalvertretung rechnen kann. Damit diese Vorschrift ihre volle Wirkung entfalten kann, ist allerdings eine entsprechende Korrektur auch des Hessischen Datenschutzgesetzes angezeigt, die die Bestellung eines behördlichen Datenschutzbeauftragten verbindlich vorschreibt und - wie das BDSG - auch dessen Aufgaben und Kompetenzbereich festlegt. Bisher beruht die Beauftragung einzelner Bediensteter mit Datenschutzfragen lediglich auf einem Erlaß des Hessischen Innenministers aus dem Jahr 1978; für die Kommunen kann dieser Erlaß sogar nur eine Empfehlung aussprechen.

Angesichts der raschen Entwicklung der neuen Techniken kann auch das Mitwirkungsrecht des Personalrats an der Installation betrieblicher und dem Anschluß an öffentliche Informations- und Kommunikationsnetze (§ 66 Abs. 2) wichtige Bedeutung erlangen.

3.3.1.2
Datenschutz-Symposium:
Entwicklungsstop für Personaldatensysteme

Die Fortführung der im 12. Tätigkeitsbericht (3.3.1.1) aufgeführten Automationsprojekte im Personalwesen des Landes wurde im Laufe des Jahres 1984 gestoppt bzw. ausgesetzt. Im April hatte die Landesregierung beschlossen, die im Zusammenhang mit dem Anschluß der Regierungspräsidien an die Lehrerindividualdatei vorgesehenen Maßnahmen nicht zu beginnen bzw. bereits vollzogene Schritte nicht fortzuführen. Dies geschah mit Rücksicht auf das Anfang September stattgefundene Datenschutz-Symposium der Landesregierung ("Informationsgesellschaft oder Überwachungsstaat"), dessen Auswertung für die weitere Planung abgewartet werden sollte. Auch bei den anderen Automationsmaßnahmen im Personalbereich sollte nach dem Willen der Landesregierung "restriktiv verfahren werden".

Der Hessische Landtag hat in seinen Beschlüssen vom 5. Juli zu meinem 12. Tätigkeitsbericht (vgl. Beschlußempfehlung Nr. 4 des Innenausschusses, Drucks. 11/1551) "zustimmend zur Kenntnis genommen", daß die Landesregierung die Vorbereitung von Personalinformationssystemen in der hessischen Landesverwaltung bis zur Auswertung des "...Symposiums... zurückstellen wird". Gleichzeitig hat er seine Erwartung ausgedrückt, daß nach Auswertung dieser Konferenz der weitere Ausbau der Systeme mit dem Innenausschuß und den anderen zuständigen Gremien des Parlaments diskutiert wird. Meines Wissens haben sich alle Ressorts an diese Vorgabe gehalten und die Planung bzw. Implementation der von ihnen in Gang gesetzten Vorhaben ausgesetzt. Die Landesregierung hat ihre Entscheidung zur Zurückstellung im übrigen noch einmal in einem Beschluß von Ende Oktober bekräftigt.

Daß sich der Landtag mit seinem Beschluß selbst in die Automationsplanung in einem datenschutzrechtlich so sensitiven Bereich wie dem der Personalinformationssysteme einschaltet, ist von kaum zu unterschätzender Bedeutung. Diese Maßnahme trägt auch der Vielzahl von Petitionen, Eingaben und Protesten Rechnung, die von den verschiedensten Betroffenengruppen, etwa Lehrern und Hochschulangehörigen, sowohl einzeln wie über ihre Personalvertretungen eingereicht worden sind.

Der Workshop "Personalinformationssysteme - ein Weg zur Überwachung der Arbeitnehmer?" gab auf dem Symposium Gelegenheit zu intensiver Debatte zwischen Betroffenen und Experten. Die Landesregierung hat wiederholt ihre Absicht unterstrichen, konkrete Konsequenzen aus den Erkenntnissen dieser Tagung zu ziehen. Dazu haben die anwesenden Fachleute, Parlamentarier, Wissenschaftler, Betriebspraktiker und Belegschaftsvertreter eine Fülle von Anregungen für den Ausbau des Arbeitnehmer-Datenschutzes geliefert. Allerdings ist deren Realisierung keineswegs durchweg Sache des Landesgesetzgebers; einige der vorgeschlagenen Initiativen fallen in die Kompetenz des Bundes. Zum Teil geht es auch nur um Konsequenzen aus bereits vorhandenen Datenschutzbestimungen, wie etwa dem Sozial- oder Arztgeheimnis.

Noch liegt jedoch der Auswertungsbericht der Landesregierung zum Symposium nicht vor. Für diese Auswertung genügt es im übrigen nicht, daß nur gesetzliche Regelungsvorschläge unterbreitet werden. Vielmehr halte ich für notwendig, daß jedes Ressort seine Automationspläne im Personalbereich noch einmal gründlich überprüft und sich darüber klar wird, wie es sich im einzelnen den Technikeinsatz und die damit zusammenhängenden Datenschutzvorkehrungen vorstellt. Nur mit einer solchen gründlichen Vorarbeit wäre gewährleistet, daß die vom Landtag geforderte Debatte über den weiteren Ausbau der Systeme auf einer soliden Fakten- und Entscheidungsgrundlage geführt wird.

3.3.2
Chancen und Grenzen gesetzlicher Regelungen

Das Volkszählungsurteil des Bundesverfassungsgerichts vom 15. Dezember 1983 hat auch die Diskussion um notwendige Verbesserungen beim Arbeitnehmerdatenschutz nachhaltig beeinflußt. Die Datenschutzbeauftragten der Länder und des Bundes haben in ihrer Entschließung vom 28. März 1984 konkrete Regelungsforderungen aus der Entscheidung abgeleitet. Die SPD-Bundestagsfraktion hat einschlägige Novellierungsvorschläge ebenso vorgelegt (Gesetzentwurf zur Novellierung des Bundesdatenschutzgesetzes, BT-Drucks. 10/1180 vom 27. März 1984) wie die Landesregierung Nordrhein-Westfalen (Referentenentwurf zur Änderung des Landesdatenschutzgesetzes NRW vom 10. September 1984). Meinen Standpunkt -was die Chancen und Grenzen gesetzlicher Regelungen für Personalinformationssysteme angeht - habe ich am 5. September auf dem Symposium der Landesregierung vorgetragen. Im folgenden noch einmal die wichtigsten Punkte:

1.
Datenschutz für Arbeitnehmer läßt sich mit den allgemeinen Formulierungen der Datenschutzgesetze ("Generalklauseln") nicht gewährleisten. Vielmehr sind speziell auf das Arbeitsverhältnis zugeschnittene Regelungen notwendig. Dies deshalb, weil der Arbeitnehmer einem besonders starken Informationsdruck ausgesetzt ist: Eine Vielzahl von Daten über ihn verarbeitet der Arbeitgeber für die Personalplanung ("Rationalisierung"), zur Gesundheitsüberwachung am Arbeitsplatz, aber auch für die Steuer- und Sozialbehörden. Diese Situation ist keineswegs nur in der Privatwirtschaft, sondern auch im öffentlichen Dienst gegeben.

2.
Personalinformationssysteme bringen eine qualitative Veränderung des Umgangs mit Arbeitnehmerdaten mit sich: Die automatische Verarbeitung sichert nicht nur den jederzeitigen Zugriff, sie verwandelt die einmal über die Beschäftigten erhobenen Daten in ein für die verschiedensten Zwecke beliebig nutzbares Datenmaterial. Diese "Multifunktionalität" ermöglicht den nahtlosen Übergang von der Personalverwaltung zur Personalkontrolle.

3.
Grundlage rechtlicher Regelungen des Arbeitnehmerdatenschutzes muß das - vom Bundesverfassungsgericht in seinem Volkszählungsurteil bestätigte - Grundrecht auf informationelle Selbstbestimmung sein. Die Handlungsfähigkeit des einzelnen ist nicht nur im Verhältnis Bürger - Staat gefährdet, sondern auch in der Abhängigkeitsbeziehung des Arbeitsverhältnisses: Personalinformationssysteme steigern die Steuerbarkeit des Arbeitnehmers und fördern den Anpassungsdruck am Arbeitsplatz.

4.
Individualrechte des Arbeitnehmers - z.B. auf Auskunft, auf Löschung - sind wichtig, aber die Selbstbestimmung kann im Rahmen des Arbeitsverhältnisses nur auf der Grundlage der Mitbestimmung der Gewerkschaften sowie der Betriebs- und Personalräte reale Bedeutung gewinnen. Beispiel für die notwendige Verknüpfung individueller und kollektiver Rechtspositionen ist die Einschränkung des Fragerechts des Arbeitgebers bei der Einstellung, die letztlich nur durch die Mitbestimmung des Betriebs- bzw. Personalrats bei der Ausgestaltung der Personalfragebögen (§ 94 BetrVG, §§ 75 Abs. 3 Nr. 8, 76 Abs. 2 Nr. 2 BundesPersVG) abgesichert werden kann.

5.
Schon das geltende Recht sowohl der Betriebsverfassung wie der Personalvertretung bietet eine Reihe von Anknüpfungspunkten für die gesetzgeberische Fortentwicklung des Datenschutzes bei der Verarbeitung von Arbeitnehmerdaten:

5.1 So umfaßt das Mitbestimmungsrecht über die Ausgestaltung von Personalfragebögen nicht nur die Erhebung der Daten, sondern auch deren Verwendung im konkreten betrieblichen Verarbeitungsprozeß.

5.2 In der betrieblichen wie behördlichen Praxis gibt es eine Vielzahl von Betriebs- und Dienstvereinbarungen, die die Voraussetzungen und Grenzen der Erhebung und Verwertung von Arbeitnehmerdaten detailliert festlegen.

5.3 Die Rechtsprechung, nicht zuletzt die des Bundesarbeitsgerichts (BAG), hat klargestellt, daß Personalinformationssysteme der Überwachung der Arbeitnehmer dienen können und dann der Mitbestimmung (nach § 87 Abs. 1 Nr. 6 BetrVG) unterliegen (vgl. zuletzt die Entscheidung des BAG vom 14. Septemer 1984, Az.: 1 ABR 23/82). Die Mitbestimmung bei Personalinformationssystemen darf allerdings angesichts der vielfältigen Nutzbarkeit aller Arbeitnehmerdaten nicht auf die Verarbeitung bestimmter Kategorien von Informationen - etwa die Verhaltens- und Leistungsdaten - beschränkt werden. Auch die Anknüpfung an das Vorhandensein bestimmter Auswertungsprogramme geht an der technischen Realität vorbei: Solche Programme lassen sich heute ohne besondere technische Kenntnisse dezentral entwickeln, unverzüglich auswerten und ebenso schnell wieder löschen.

6.
Eine wirksame Beteiligung der Arbeitnehmervertretungen setzt auch die Verbesserung ihrer Informationsbasis über die technischen Abläufe voraus. Dazu ist es u.a. notwendig, daß der Betriebsrat einen Sachverständigen auch ohne Zustimmung des Arbeitgebers beiziehen kann. Der betriebliche Datenschutzbeauftragte muß zur Unterrichtung des Betriebsrats verpflichtet werden.

7.
Grenze auch für die Mitbestimmung der Vertretungsorgane der Beschäftigten ist das informationelle Selbstbestimmungsrecht der Betroffenen. Von der strikten Zweckbindung der Arbeitnehmerdaten kann nicht abgewichen werden. Protokollierungsdaten dürfen nur für die Zugangs- und Zugriffskontrolle, nicht aber für die Leistungsüberwachung genutzt werden.

8.
Zur rechtlichen Absicherung des Arbeitnehmer-Datenschutzes gehören untrennbar organisatorische und technische Maßnahmen. So müssen z.B. Gesundheitsdaten der Werksärzte in einem getrennten Informationssystem verarbeitet werden. Bestimmte sensitive oder - aus dem Zusammenhang gerissen - irreführende Informationen dürfen überhaupt nicht automatisiert in einem Personalinformationssystem gespeichert werden. Dies gilt z.B. für Beurteilungsinhalte, psychologische Eignungstests usw.

9.
Die Verbesserung der individuellen Arbeitnehmerrechte ist vor allem in den folgenden Bereichen dringlich:

- Über die klarere Formulierung des Auskunftsrechts hinaus muß der Betroffene vom Arbeitgeber regelmäßig über den aktuellen Stand der Datenspeicherung informiert werden ("Kontoauszug").
- Für die Einschaltung der Aufsichtsbehörde muß ein Nachteilsverbot verankert werden. Es kann nicht hingenommen werden, daß - wie von der Rechtsprechung der Arbeitsgerichte in einigen Fällen toleriert - Beschäftigte wegen angeblichen Bruchs ihrer Schweigepflicht gemaßregelt oder gekündigt werden, weil sie Mißstände der Kontrollbehörde anzeigen.
- Die Auskunft über den Arbeitnehmer durch den früheren an den jetzigen Arbeitgeber muß von einer Einwilligung des Betroffenen abhängig gemacht werden.

3.4
Sozialversicherung

3.4.1
Ausgangspunkt: Die Modellversuche zur Leistungs- und Kostentransparenz

3.4.1.1
Die Diskussion im Landtag

Die in mehreren Bundesländern durchgeführten "Modellversuche zur Erhöhung der Leistungs- und Kostentransparenz in der gesetzlichen Krankenversicherung" haben einen Zielkonflikt sehr deutlich werden lassen: Den Zielkonflikt zwischen dem legitimen Einsatz der automatisierten Datenverarbeitung zur Effizienzsteigerung in der Sozialversicherung und dem grundrechtlichen Anspruch des einzelnen Versicherten auf Wahrung seines informationellen Selbstbestimmungsrechts. Am Beispiel des Projekts der Allgemeinen Ortskrankenkasse Main-Kinzig in Hanau hatte ich im letzten Tätigkeitsbericht (Ziff. 3.2.3) die datenschutzrechtlichen Probleme aufgezeigt, die durch die Speicherung, Verknüpfung und Auswertung großer Mengen von Gesundheitsdaten entstehen können. Dabei habe ich unterstrichen, daß die Rechtsgrundlagen - insbesondere die Bestimmung des § 223 der Reichsversicherungsordnung - nicht ausreichen, um Art und Umfang der Verarbeitung personenbezogener Versichertendaten in den Modellversuchen zu rechtfertigen.

Der Hessische Landtag hat in seinem Beschluß Nr. 14 zu meinem 12. Tätigkeitsbericht meine Rechtsposition übernommen und die Auffassung vertreten, "daß die ursprüngliche Form der Datenerfassung bei dem Modellversuch der AOK Main-Kinzig nicht durch § 223 RVO abgedeckt" gewesen sei. "Vor der Durchführung der weiteren Phasen des Versuchs und etwaiger sonstiger Datenverarbeitungsprojekte zur Kosten- und Leistungstransparenz", so lautet der Beschluß weiter, sei "jeweils in Abstimmung mit dem Datenschutzbeauftragten zu prüfen, ob die Rechtsgrundlagen ausreich(t)en" (vgl. Drucks. 11/1551).

Diesem Beschluß war eine eingehende Behandlung des Themas in den zuständigen Landtagsausschüssen vorausgegangen, bei denen auch Vertretern der betroffenen Krankenkasse und des Landesverbands der Ortskrankenkassen Gelegenheit zur Stellungnahme gegeben wurde. Die Diskussion im Parlament war allerdings Ende 1984 noch nicht abgeschlossen: Im Innenausschuß bzw. im Sozialpolitischen Ausschuß standen noch ein Berichtsantrag der F.D.P.-Fraktion (Drucks. 11/1655) und die dazu gestellten Ergänzungsfragen zur Erörterung an.

Zur Umsetzung des Beschlusses hat der Sozialminister im Oktober einen Erlaß an alle hessischen Sozialversicherungsträger bzw. deren Verbände gerichtet mit der Aufforderung, ihm derartige Vorhaben rechtzeitig zur Abstimmung mit dem Datenschutzbeauftragten mitzuteilen.

3.4.1.2
Die Abwicklung des Projekts der AOK Main-Kinzig

Anfang Mai hat mir die AOK Main-Kinzig das überarbeitete Verfahrenskonzept für das Modellvorhaben vorgelegt. Als "Handlungsfelder", also Untersuchungsbereiche, wurden die Arzneimittelinformation für Ärzte, die produktbezogene Arzneimittelberatung und die Ermittlung betriebsbezogener Krankheitsschwerpunkte definiert. Klargestellt wurde, daß der erfaßte umfangreiche sogenannte "Transparenz-Datenbestand" aus 1981 anonymisiert wird und ausschließlich der Feststellung möglicher geeigneter Fallgruppen für eine spätere detailliertere Untersuchung der Leistungs- und Kostentransparenz dient, also als statistische bzw. aggregierte Informationsbasis für eine spätere Umsetzungsphase.

Auf der Grundlage dieser Zusagen sowie eines weiteren Besuchs bei der Kasse habe ich mit Schreiben vom 13. Juli abschließend meine Anforderungen an eine datenschutzgerechte Fortführung des Modellversuchs festgelegt, wobei sich Vorstand und Geschäftsführung der AOK Hanau - von fortbestehenden Meinungsdivergenzen über die juristische Beurteilung abgesehen - sehr kooperativ verhalten haben. Die wichtigsten Punkte:

1. Gegenstand meiner Stellungnahme konnte nur die derzeit laufende Phase der Entwicklung geeigneter Auswahlprogramme aus dem anonymisierten "Transparenz-Datenbestand", die in Zusammenarbeit zwischen der Kasse und einem externen Forschungsinstitut (IGES Berlin) erfolgt, sein. Vor Eintritt in die nächste Projektphase, bei der es um die Umsetzung der gefundenen Auswahlverfahren auf konkrete Einzelfälle oder Fallgruppen mit neuem, zeitnah erfaßtem Datenmaterial geht, ist der Datenschutzbeauftragte zur Prüfung der Rechtmäßigkeit sowie der dann erforderlichen Datenschutz- und Datensicherungsmaßnahmen erneut einzuschalten.

2. Die AOK liefert das Datenmaterial an das Forschungsinstitut (IGES Berlin) in einer Form, in der die Angaben, die einen Personenbezug auf Versicherte und Ärzte erlauben (z.B. Versichertennummer, Arztnummer) verschlüsselt werden.

3. Der personenbezogene Original-Datenbestand wird bei der AOK nur so lange vorgehalten, bis notwendige Bereinigungen und Korrekturen des Datenmaterials erfolgt sind. Danach wird er gelöscht.

4. Das Forschungsinstitut führt eine zweite Verschlüsselung vor der Rücklieferung des Datenbestandes an die AOK durch, so daß eine spätere Wiederherstellung des Personenbezugs bei der AOK verhindert wird.

Die Vorgaben 1 bis 3 sind inzwischen realisiert. Derzeit findet die Aufbereitung durch das beauftragte Forschungsinstitut statt. Mit Ergebnissen wird etwa im Frühjahr 1985 gerechnet. Für den weiteren Fortgang des Modellversuchs ist auch die, in § 223 RVO vorgesehene, Mitwirkung der Kassenärztlichen Vereinigung (KV) Hessen gesichert. In einer Kooperationsvereinbarung vom 1. Juni 1984, die unter maßgeblicher Vermittlung des Bundesministers für Arbeit und Sozialordnung zustandekam, sind die Einzelheiten des Zusammenwirkens zwischen der AOK Main-Kinzig und der KV festgelegt worden. Über Ziele und Rahmenbedingungen des Projekts wurde prinzipielle Einigkeit erzielt. Allerdings behält sich die Kassenärzteschaft ihre Zustimmung zum Einstieg in die nächste Projektphase bis zur Bewertung des derzeit laufenden Auswertungsabschnitts vor. Außerdem machte sie die "irreversible Anonymisierung" der Arzt- und Versichertendaten zum Vorbehalt ihres Einverständnisses.

Im Ergebnis wird mithin das Verarbeitungskonzept in der kommenden Umsetzungsphase im nächsten Jahr sowohl mit dem Datenschutzbeauftragten als auch mit der Kassenärztlichen Vereinigung Hessen abgestimmt werden müssen. Dabei wird gemäß dem Landtagsbeschluß (s.o.) nicht zuletzt zu prüfen sein, in welchem Umfang dann personenbezogene Daten verwendet werden sollen und inwieweit dafür "die Rechtsgrundlagen ausreichen", d.h. die rechtlichen Vorgaben der RVO sowie des Datenschutzrechts beachtet sind bzw. werden können.

3.4.2
Verarbeitungsvoraussetzungen und -grenzen in der Sozialversicherung

Die Modellversuche sind - als ein Instrument zur Kostendämpfung im Gesundheitswesen - bundesweit zu einem wichtigen Thema der gesundheitspolitischen Diskussion geworden. Im Jahr 1984 haben sich u.a. der Bundesminister für Arbeit und Sozialordnung, die 59. Gesundheitsministerkonferenz, der Deutsche Gewerkschaftsbund sowie die verschiedensten Einrichtungen und Verbände der Sozialversicherung und der Ärzte zu Wort gemeldet.

Nach meiner Auffassung muß bei der künftigen Auseinandersetzung um die Verarbeitungsvoraussetzungen und -grenzen, insbesondere in der gesetzlichen Krankenversicherung, von folgenden Grundüberlegungen ausgegangen werden:

1.
Lange Zeit hat die gesetzliche Krankenversicherung eher im Hintergrund der Datenschutzdiskussion gestanden. Sie war nicht mehr als einer von vielen ebenso selbstverständlichen wie alltäglichen Anwendungsfälle der Verarbeitung personenbezogener Daten. Spätestens seit den Modellversuchen zur Erhöhung der Leistungs- und Kostentransparenz steht jedoch die gesetzliche Krankenversicherung mit im Vordergrund aller Überlegungen über Aktualität und Aufgaben des Datenschutzes. Die Modellversuche haben einerseits den Blick für die Möglichkeiten einer konsequenten Datenverarbeitung geschärft, andererseits aber auch die Notwendigkeit einer gezielten Verarbeitungsregelung verdeutlicht. Manche Streitfrage ist mittlerweile, nicht zuletzt dank der intensiven Gespräche zwischen den für einzelne konkrete Projekte zuständigen Krankenkassen und den jeweiligen Datenschutzbeauftragten, geklärt worden. Nach wie vor wird jedoch die Auseinandersetzung über Voraussetzungen und Grenzen der Modellversuche durch eine Reihe von Mißverständnissen und Fehlinterpretationen belastet.

2.
Ziel sämtlicher Modellversuche ist es, den ständig steigenden Kosten der gesetzlichen Krankenversicherung entgegenzuwirken. Sie sollen eine bessere Kenntnis der Bedingungen vermitteln, unter denen gegenwärtig Leistungen erbracht werden und damit zugleich die Grundlage für eine Politik schaffen, die, um einer langfristigen Sicherung der Leistungen willen, die Kosten dämpft. Die Modellversuche sind insofern ihrer ganzen Struktur und Funktion nach Instrumente einer auf die Zukunft der gesetzlichen Krankenversicherung angelegten Planung. In diesem Rahmen stellt sich die Frage nach der Verarbeitung von Versichertendaten und damit unterscheidet sie sich zugleich von all den Fällen, in denen beispielsweise im Hinblick auf die Überprüfung einer bereits erbrachten einzelnen Leistung auf bestimmte individuelle Angaben zurückgegriffen wird. Argumente, die im Zusammenhang mit diesen konkreten Einzelsituationen zu den Verarbeitungsmodalitäten von Versichertendaten entwickelt worden sind, lassen sich deshalb nicht auf die Bewertung der Modellversuche übertragen.

3.
Die gesetzliche Krankenversicherung ist Teil der Sozialverwaltung. Sie kann und darf daher ihre Aufgaben immer nur unter den für die Sozialverwaltung ebenso wie für die Verwaltung überhaupt geltenden Handlungsbedingungen erfüllen. Konkret: Die rechtliche Zulässigkeit der Entscheidungen zur gesetzlichen Krankenversicherung mißt sich zuvörderst an ihrer Übereinstimmung mit den Erfordernissen einer strikt rechtsstaatlich agierenden, verfassungskonformen Verwaltung. Genau diese Voraussetzung ist aber nur solange erfüllt, wie der vom Grundgesetz geforderten und garantierten informationellen Selbstbestimmung auch und gerade dort Rechnung getragen wird, wo es um die Verarbeitung der Versichertendaten im Rahmen der gesetzlichen Krankenversicherung geht. So gesehen ist der Datenschutz zwingende, in der Verfassung abgesicherte Funktionsvoraussetzung der gesetzlichen Krankenversicherung. Wie sie ihren Aufgaben nachzugehen hat, bestimmt sich infolgedessen nicht am Datenschutz vorbei oder gar im Gegensatz zu ihm, sondern ausschließlich in Kenntnis und unter strikter Beachtung seiner konstitutiven Voraussetzungen, vor allem also einer klaren Zweckbindung sowie einer für den Betroffenen jederzeit erkennbaren, nachvollziehbaren und kontrollierbaren Verarbeitung.

4.
Genau diese Erwartung läßt sich nicht erfüllen, wenn die Verarbeitung von Versichertendaten weitgehend mit mehr oder weniger allgemein gehaltenen Hinweisen auf die Aufgaben der gesetzlichen Krankenversicherung gerechtfertigt wird. Niemand kann ernsthaft bestreiten, daß den Krankenkassen keineswegs nur die Funktion eines bloßen Kostenträgers zukommt. Mit jedem Schritt auf eine Konzeption hin, die in der Tätigkeit der Krankenassen die Konkretisierung eines allgemeinen Auftrags zur Sicherstellung der Gesundheit sieht, verändern sich allerdings auch die Informationsansprüche. Spätestens in dem Augenblick, in dem präventive Gesichtspunkte in den Vordergrund rücken, fällt es zunehmend schwer, die Verarbeitungsvoraussetzungen und -grenzen präzise und nachvollziehbar zu umschreiben. Eine konsequent auf die Prävention bedachte Informationspolitik weist tendenziell stets über eine auf die medizinischen Angaben beschränkte Verarbeitung hinaus. Daten über das jeweilige soziale Umfeld des Versicherten geraten genauso in den Mittelpunkt des Interesses. Ganz abgesehen davon verstärkt eine auf präventive Ziele gerichtete Verarbeitung die multifunktionale Verwendung der Daten und erschwert damit erneut eine verläßliche Beschreibung der Verarbeitungsanlässe und -inhalte.

5.
Mangelnde Präzision kann nicht durch den immer wiederkehrenden Hinweis auf die "soziale Solidarität" als dem eigentlich tragenden Prinzip der Krankenversicherung kompensiert werden. Die "Solidarität" vermag ebensowenig wie etwa die "öffentliche Sicherheit" einen gleichsam offenen Verarbeitungsprozeß zu rechtfertigen. Der Versicherte geht mit seiner Aufnahme in die gesetzliche Krankenversicherung ohne Zweifel Bindungen ein, die sich nicht zuletzt in den Informationserwartungen der Krankenkassen und den durch sie veranlaßten Verarbeitungsprozessen konkretisieren. Nicht minder relevant ist aber, daß die gesetzliche Krankenversicherung mit ihrer Tätigkeit einen für den Betroffenen lebenswichtigen Bereich berührt. Der Versicherte ist insofern von vornherein auf die Leistungen angewiesen und deshalb von der Krankenkasse abhängig. Genaugenommen befindet er sich in einer Situation, die mit der Lage des Arbeitnehmers durchaus vergleichbar ist. Ebensowenig wie deshalb der bloße Verweis auf das bestehende Arbeitsverhältnis genügt, um Personalinformationssysteme zu legitimieren, reicht die Erwähnung der Solidarität, um eine nicht weiter präzisierte Verarbeitung von Versichertendaten zu begründen. Der Vergleich mit dem Arbeitsverhältnis macht zudem noch ein weiteres deutlich: Die Abhängigkeit des Versicherten und die sich daraus für die Verarbeitung ergebenden Folgen werden nicht deshalb behoben, weil die Versicherten Vertreter in die Aufsichtsgremien entsenden. Auch die gesetzlich garantierte Mitbestimmung der Arbeitnehmer ändert nichts an ihrer Abhängigkeit und entbindet daher nicht von der Verpflichtung, den Verarbeitungsprozeß an klare und verbindliche Bedingungen zu knüpfen.

6.
Selbst dort aber, wo an die Stelle allgemeiner Bemerkungen zur Solidarität scheinbar weitaus präzisere Hinweise, wie etwa auf die §§ 223 oder 182 Abs. 2 RVO, treten, ist die unter Datenschutzgesichtspunkten für solche Modellversuche unerläßliche Präzision der Verarbeitungsbedingungen nicht erreicht. Generalklauseln wie etwa die Formulierung, die Krankenpflege müsse ausreichend, zweckmäßig und notwendig sein, bewegen sich auf einer notwendigerweise abstrakten Ebene. Sie legen keineswegs den Handlungsspielraum verbindlich fest, sondern beschreiben nur allgemeine Handlungsziele. Für die Gewährung von Sozialleistungen gilt jedoch nicht anders als in allen weiteren Fällen einer zwangsweisen Erhebung personenbezogener Daten das Gebot einer präzisen gesetzlichen Umschreibung des Verwendungszwecks, die allein auch eine strikte, ständig überprüfbare Zweckbindung sichern kann. Die Konstruktion eines allgemeinen Auftrags zur Herstellung von Kosten- und Leistungstransparenz mit Hilfe einer Auflistung verschiedener RVO-Vorschriften genügt diesem Bestimmtheitsgebot genauso wenig, wie außerhalb der gesetzlichen Krankenversicherung vergleichbar unspezifiziert gefaßte Regelungen die Verarbeitung rechtfertigen können. Die Entscheidung des Bundesverfassungsgerichts (BVerfG) zum Volkszählungsgesetz (VZG) besagt, entgegen mancher anderslautenden Bemerkung, nichts Gegenteiliges. Das Gericht hat lediglich festgestellt, daß es im Sozialgesetzbuch ebenso wie etwa in der Abgabenordnung bestimmte, konkret auf den Datenschutz zugeschnittene Vorschriften gibt. Das BVerfG hat aber nirgends gesagt, weitere Überlegungen zu den Konsequenzen des Datenschutzes für die Sozialverwaltung überhaupt und speziell die gesetzliche Krankenversicherung seien damit überflüssig. Spätestens an den Modellversuchen erweist sich, wie sehr es darauf ankommt, über diese wenigen, sicherlich besonders wichtigen Vorschriften hinaus den Gesamtkomplex der Datenverarbeitung durch die Sozialversicherungsträger in ein dem Bestimmtheitsgebot entsprechendes gesetzliches Regelungssystem einzuordnen. Sicherlich müssen die Versicherungsträger die Chance der Selbstverwaltung nutzen, um alle ihnen mögliche Maßnahmen zur Präzisierung und Transparenz des Verarbeitungsprozesses zu treffen. Eine noch so große Bereitschaft, selbst Vorkehrungen vorzusehen, ersetzt aber nicht eine gesetzliche Regelung. Die im Rahmen der eigenen Entscheidungskompetenz getroffenen Maßnahmen sind immer nur komplementär, nicht jedoch alternativ zur gesetzlichen Festschreibung der Verwendungsziele.

7.
Alle Überlegungen zu den notwendigen Verarbeitungsbedingungen müssen von einer sorgfältigen Interessenanalyse ausgehen. Mit der einfachen Gegenüberstellung der legitimen Kostendämpfungserwartungen einerseits und der Datenschutzanforderungen andererseits ist es nicht getan. Sie verkürzt die Problemsicht und verführt zu einer einseitigen Argumentation. Zunächst: Eine Gesellschaft, die sich für eine gesetzliche Krankenversicherung entscheidet, muß sich ohne Zweifel fortlaufend mit den Leistungsbedingungen auseinandersetzen, um die Leistungsfähigkeit des Versicherungssystems zu garantieren. Sie darf aber nicht, soll ihre demokratische Struktur nicht gefährdet werden, eine umfassende Verhaltenssteuerung durch die Sozialverwaltung hinnehmen. Ferner: Die Leistungsfähigkeit der Krankenversicherung spielt auch aus der Perspektive des Versicherten eine zentrale Rolle, zumal davon nicht zuletzt seine finanzielle Belastung abhängt. So gesehen, spricht aus seiner Sicht ebenfalls viel für ein Höchstmaß an Transparenz der Kostenstruktur. Nur ist es dem Versicherten keineswegs gleichgültig, wann, zu welchen Zwecken, in welchem Umfang und mit welchen Konsequenzen auf die Angaben zu seiner Person zurückgegriffen wird. Schließlich: Der Vertraulichkeit kommt auch und gerade für den Arzt eine besondere Bedeutung zu. Sie ist, genaugenommen, elementare Voraussetzung seiner Aktivität. Insoweit ist seine Zurückhaltung gegenüber einer Verarbeitung von Gesundheitsdaten einsichtig und legitim. Sie wird dagegen dann problematisch, wenn sie die Intransparenz der eigenen, sich auf die Kostenstruktur der Versicherung auswirkenden Entscheidungen sichern soll.

8.
Bedenkt man diesen Hintergrund, dann werden Funktion und Grenzen einer am Datenschutz orientierten Verarbeitungsregelung sichtbar. Der Datenschutz ist kein Instrument der Auseinandersetzung mit der Opportunität sowie der Struktur der gesetzlichen Krankenversicherung. Wer deshalb seine Kritik am Sozialleistungssystem auf die Datenschutzebene verlagert, führt sie unter falschen Voraussetzungen. Ebensowenig geht es an, standespolitische Erwartungen als Datenschutzforderungen auszugeben. Notwendigkeit und Umfang der Verarbeitungsregelung richten sich nicht nach dem Verarbeitungsverständnis eines bestimmten Berufes. Wo daher der Datenschutz unter standespolitischen Aspekten gesehen und vereinnahmt wird, bleiben seine rechtlich allein relevanten Ansatzpunkte außer Betracht. Sie ergeben sich einzig aus der Notwendigkeit, die gesetzliche Krankenversicherung durchweg so zu organisieren, daß die Verarbeitung von Versichertendaten, wo sie nachweislich erforderlich ist, unter feststehenden, jederzeit nachprüfbaren Bedingungen stattfindet.

Konsequenterweise dürfen sich die Datenschutzbeauftragten keineswegs darauf beschränken, konkrete "Mißbräuche" aufzuzeigen oder gar erst im nachhinein abzustellen. Mit ihre wichtigste Funktion ist es im Gegenteil, die Entwicklung der Verarbeitungs-und Kommunikationstechnik kontinuierlich zu verfolgen, um mögliche Gefahren rechtzeitig offenzulegen und durch gezielte Maßnahmen aufzufangen. Datenschutz hat insofern eine präventive Funktion. Nur solange sie berücksichtigt sowie konsequent gehandhabt wird, können die Datenschutzbeauftragten die ihnen obliegende, vom BVerfG ausdrücklich bestätigte Aufgabe eines "vorbeugenden Rechtsschutzes" erfüllen. Genau darum geht es aber in erster Linie bei den Überlegungen und Vorschlägen zu den Modellversuchen.

9.
Der Datenschutz setzt Prioritäten. Der Zugriff auf personenbezogene Angaben muß, so wünschenswert er erscheinen mag, die Ausnahme bleiben. Die gesetzliche Krankenversicherung hat insofern keine Alternative. Alle Aufmerksamkeit muß sich zunächst darauf konzentrieren, wie das für die Reflexion zur Kostendämpfung notwendige Informationsmaterial mit Hilfe anonymisierter Daten gewonnen werden kann. Zudem: "Globaldaten" mögen oft kaum aussagefähig sein. Nur läßt sich mit dieser Feststellung keineswegs der uneingeschränkte Rückgriff auf personenbezogene Angaben rechtfertigen. Vielmehr gilt es festzustellen, ob und in welchem Umfang sich die Ziele der Modellversuche mit fallbezogenen Angaben, Daten also, die keinen Versichertenbezug aufweisen, erreichen lassen.

10.
Weit mehr als bisher gilt es zu prüfen, inwieweit die Erhebung und Speicherung von Versichertendaten durch die Kassen auf dem Weg über alternative Beschaffungsformen überflüssig gemacht werden könnte. DEVO und DÜVO etwa verpflichten den Arbeitgeber, eine Vielzahl vom Informationen für die Sozialversicherung zu sammeln, aufzubereiten und weiterzuleiten. Mit Hilfe besonderer Übermittlungspflichten, die - sei es gesetzlich, sei es vertraglich wie im Falle der Kassenärztlichen Vereinigungen - zu statuieren wären, ließe sich eine Information der Krankenkassen in dem erforderlichen Umfang sicherstellen, zugleich aber die Verarbeitung von Versichertendaten gezielt reduzieren.

11.
Ganz gleich welche Wege man beschreitet, der Betroffene muß in jedem Fall den Verarbeitungsprozeß überschauen können. Keinesfalls reicht es daher aus, auf die Selbstverwaltung der Krankenkassen hinzuweisen, um es dann bei einer Information der jeweiligen Selbstverwaltungsgremien bewenden zu lassen. Vielmehr gilt es auch gerade bei Projekten, die, wie die Modellversuche, Versichertendaten so detailliert verarbeiten, für eine genaue Information der Betroffenen über Anlaß, Mittel und Ziele der Verarbeitung zu sorgen. Sie ist die unabdingbare Voraussetzung einer rechtlichen Zulässigkeit der Verarbeitung.

12.
Die Verarbeitung muß unter Bedingungen erfolgen, die gezielt den Gefahren einer "Normung" des Patientenverhaltens entgegenwirken. Gemeint ist damit ein für die automatische Datenverarbeitung typisches und deshalb keineswegs auf die Verwendung personenbezogener Angaben durch die Krankenkassen begrenztes Risiko. Konkret: Jede Massenverarbeitung von Informationen wird zumeist von einem Kontextverlust begleitet. Die Folge sind abstrakte Schematisierungen und Kategorisierungen, die sehr leicht, und zwar gerade dann, wenn abweichendes Verhalten ermittelt werden soll, zu falschen, für den Betroffenen äußerst gefährlichen Etikettierungen führen. Vor allem dort also, wo, wie bei den Modellversuchen, vorhandene Daten für neue Ziele verwendet werden sollen, kommt es darauf an, die Qualität der Angaben sicherzustellen, mithin Verkürzungen zu vermeiden, die ein unzutreffendes, für den Betroffenen gefährliches Bild entstehen lassen. Mit den ständig wiederkehrenden Feststellungen, die endgültigen Entscheidungen würden von Menschen und nicht von Maschinen getroffen, argumentiert man am eigentlichen Sachverhalt vorbei. Die Entscheidung erfolgt auf der Grundlage eines Informationsmaterials, das durch die Verarbeitung schon eine bestimmte Gestalt angenommen hat und deshalb festgefügte Vorstellungen über das Patientenverhalten vermittelt, deren Hintergrund nicht mehr erkennbar und ohne weiteres korrigierbar ist. Der Datenschutz kann und darf sich unter diesen Umständen nicht für das Informationsmaterial desinteressieren, sondern muß auf eine aus der Perspektive des Betroffenen korrekte Informationsvermittlung bedacht sein, die Qualität der verwendeten Daten also sicherstellen.

3.5
Polizei

3.5.1
Datenverarbeitung im Polizeirecht - Entwicklung der Diskussion

3.5.1.1
Musterentwurf der Innenminister und Alternativentwurf

In den letzten Jahren ist über neue Regelungen für die Polizei viel diskutiert worden, und zwar nicht lediglich im Zusammenhang mit Fragen der Datenverarbeitung. Zwei Probleme stehen im Vordergrund: Zum einen geht es darum, wie konkret die Aufgaben und Befugnisse der Polizei gesetzlich geregelt sein sollten. Generell zeichnet sich die Entwicklung ab, den Anwendungsbereich der polizeilichen Generalklausel, die ursprünglich die einzige Vorschrift war, die die Handlungsmöglichkeiten der Polizei umgrenzte, einzuschränken und die häufigsten bzw. einschneidendsten Maßnahmen der Polizei - wie z.B. die Identitätsfeststellung, die Hausdurchsuchung oder auch den Schußwaffengebrauch - in präzisen Spezialvorschriften zu regeln, um so rechtsstaatlichen Anforderungen besser gerecht zu werden. Zum anderen handelt es sich um die Frage, inwieweit die derzeit der Polizei zugewiesenen Aufgaben und Befugnisse einer Erweiterung bedürfen. Am 25. November 1977 verabschiedete die Ständige Konferenz der Innenminister und -senatoren des Bundes und der Länder (IMK) den Musterentwurf eines einheitlichen Polizeigesetzes des Bundes und der Länder. Dieser Entwurf enthält detaillierte Befugnisregelungen für die Polizei. Ziel des Beschlusses der IMK war zum einen die Vereinheitlichung der in Bund und Ländern vorhandenen Vorschriften, zum anderen aber auch die Lösung als regelungsbedürftig erkannter neuer Probleme. Die polizeiliche Datenverarbeitung wird in einigen Vorschriften am Rande sozusagen "mitgeregelt", sie ist jedoch nicht speziell Gegenstand der Regelungen.

Der Musterentwurf hat zu umfassenden öffentlichen Diskussionen geführt. 1978 haben mehrere Wissenschaftler einen Alternativentwurf erarbeitet (Alternativentwurf einheitlicher Polizeigesetze des Bundes und der Länder, vorgelegt vom Arbeitskreis Polizeirecht 1979). Diesem Entwurf liegt vor allem die Auffassung zugrunde, daß der Musterentwurf in bedenklichem Umfang bereits im Vorfeld der Gefahrenbekämpfung einschneidende polizeiliche Maßnahmen ermöglicht. Er enthält auch spezielle Vorschriften über die polizeiliche Datenverarbeitung. Die Autoren sind mit Recht davon ausgegangen, daß es nicht ausreichend ist, die Datenverarbeitung durch die Polizei lediglich am Rande "mitzuregeln". Festgestellt werden muß allerdings, daß der dort vorgeschlagene Inhalt spezieller Regelungen aus heutiger Sicht nicht als ausreichend angesehen werden kann. Namentlich die Entwicklung der polizeilichen Datenverarbeitung in den letzten Jahren läßt neue Überlegungen als erforderlich erscheinen.

3.5.1.2
Hessen: Richtlinien statt Gesetz

Im Verlauf der Diskussion hat eine Reihe von Ländern neue Befugnisnormen für die Polizei erlassen. Eine umfassende Regelung der polizeilichen Datenverarbeitung ist bisher jedoch nur im Bremischen Polizeigesetz erfolgt (Bremisches Polizeigesetz vom 31. März 1983, Gesetzblatt der Freien Hansestadt Bremen, 1983, Nr. 15, S. 141). In Hessen steht eine derartige Regelung noch aus. In meinen Tätigkeitsberichten habe ich immer wieder darauf hingewiesen, daß es bereichsspezifischer Regelungen für die polizeiliche Datenverarbeitung bedarf. Im 12. Tätigkeitsbericht habe ich die Aktualität dieser Forderung mit Hinweisen auf die Anforderungen des Volkszählungsurteils des Bundesverfassungsgerichts und auf die - jetzt definitiv von der Bundesregierung beschlossene -Einführung des maschinenlesbaren Personalausweises belegt (vgl. 1.1.3.1 und 3.1.3). Freilich kann es nicht darum gehen, die derzeitige, zuweilen ausufernde Praxis der Datenverarbeitung einfach festzuschreiben. Sie muß vielmehr grundsätzlich überprüft und der Umfang zulässiger Verarbeitung durch spezielle Vorschriften konkret bestimmt und begrenzt werden.

Mit den Richtlinien für die Führung Kriminalpolizeilicher Sammlungen (KpS-Richtlinien) ist 1981 ein erster Schritt unternommen worden. Im 8. Tätigkeitsbericht (Drucks. 9/2740, 1.2.1) habe ich allerdings bereits darauf hingewiesen, daß diese Richtlinien lediglich ein Provisorium sein können. Dies gilt erst recht, wenn die Richtlinien sogar eine neue polizeiliche Aufgabe, die "vorbeugende Verbrechensbekämpfung", einführen. Zwar wird man über die Frage, ob und ggf. inwieweit im Hinblick auf die Entwicklung der Kriminalität der Polizei neue Aufgaben und Befugnisse zugewiesen werden müssen, sicherlich diskutieren müssen. Für solche Entscheidungen ist jedoch ausschließlich der Gesetzgeber zuständig. Im übrigen enthalten die Richtlinien zwar wichtige Regelungsansätze, sie bedürfen jedoch der Überarbeitung und Ergänzung: Auch wenn das Bemühen ersichtlich ist, für jede Phase der Datenverarbeitung möglichst konkrete Vorschriften zu treffen, findet sich eine Reihe von allgemeinen Formulierungen, die die Tätigkeit der Polizei mehr umschreiben als eingrenzen und daher für den Schutz des Bürgers nicht ausreichend sind. Schließlich haben auch die Veränderungen der polizeilichen Datenverarbeitung noch keine hinreichende Berücksichtigung gefunden.

3.5.2
Novellierung des HSOG - Anforderungen

Im Zusammenhang mit der Beratung meines 12. Tätigkeitsberichts hat der Hessische Landtag nunmehr die Landesregierung gebeten, bis zum Frühjahr 1985 einen Entwurf für bereichsspezifische Datenschutzregelungen im HSOG (Hessisches Gesetz über die öffentliche Sicherheit und Ordnung) vorzulegen (Beschluß Nr. 3 zum 12. Tätigkeitsbericht, vgl. Drucks. 11/1551). Ich habe dem Hessischen Innenminister in einer Reihe von Gesprächen meine Auffassung darüber dargelegt, welchen Anforderungen eine Neuregelung aus der Sicht des Datenschutzes genügen muß.

3.5.2.1
Ausgangspunkte

Ausgangspunkt ist, daß Regelungen der polizeilichen Datenverarbeitung im Landesgesetz in engem Zusammenhang insbesondere mit den Vorschriften der Strafprozeßordnung (StPO) und des Gesetzes über das Bundeskriminalamt (BKA) stehen. Hieraus folgt, daß zwar zunächst unabhängig von den genannten weiteren Vorschriften die Anforderungen an ein Polizeigesetz festgelegt werden müssen, im Anschluß daran jedoch entsprechende Änderungen auch dieser Vorschriften anzustreben sind.

Unverzichtbar ist, daß detaillierte Regelungen für jede Phase der Datenverarbeitung getroffen werden. Selbstverständlich muß dies auch für die Erhebung personenbezogener Daten gelten. Viele der in der Vergangenheit diskutierten zentralen Probleme und der an mich gerichteten Anfragen von Bürgern betrafen gerade diese Phase der Datenverarbeitung, so z.B. Fragen der polizeilichen Beobachtung, der Ausforschung von Versammlungen oder auch der Art und Weise bzw. des Umfangs von Identitätsfeststellungen. Diese Vorschriften müssen sich generell an den Prinzipien der Zweckbindung, der Normenklarheit und der Verhältnismäßigkeit orientieren. Die Notwendigkeit einer Regelung besteht weiterhin für alle Verarbeitungsformen, also unabhängig davon, ob die Daten sich etwa in einer Datei befinden oder ob sie automatisiert verarbeitet werden. Lediglich bei dem Inhalt der Vorschriften im einzelnen wird im Hinblick auf die verschiedenen Formen der Datenverarbeitung zu differenzieren sein: Soweit sich aus besonderen Formen der Verarbeitung besondere Gefährdungen ergeben, müssen hierauf abgestimmte spezielle Schutzvorschriften erlassen werden.

Ein zentraler Diskussionspunkt war und bleibt der Umfang der Tätigkeit der Polizei im Bereich der vorbeugenden Bekämpfung von Straftaten. Nach der derzeitigen Gesetzeslage obliegt der Polizei - von den Vorschriften der Strafprozeßordnung einmal abgesehen - die Aufgabe der Gefahrenabwehr, "soweit eine Störung der öffentlichen Sicherheit und Ordnung unaufschiebbar zu beseitigen oder von der Allgemeinheit oder dem einzelnen eine unmittelbar bevorstehende Gefahr abzuwenden ist" (§§ 1 Abs. 2, 44 Abs. 1 HSOG). Maßnahmen dürfen sich nur gegen "Störer" richten (§§ 12 ff. HSOG) sowie gegen sogenannte Notstandspflichtige; letztere dürfen nur unter sehr engen Voraussetzungen in Anspruch genommen werden (§ 15 HSOG).

In der Praxis geht die Tätigkeit der Polizei in erheblichem Umfang über die konkrete Gefahrenabwehr hinaus. Es muß bei der Diskussion stets im Auge behalten werden, daß es sich hierbei um Maßnahmen im Vorfeld von Gefahren handelt, d.h. gegenüber Bürgern, bei denen weder ein konkreter Verdacht auf eine Straftat noch eine konkrete Gefahr vorliegen. Regelmäßig ist eine Vielzahl unbeteiligter Personen betroffen. Wenn sich daher der Gesetzgeber dafür entscheiden sollte, der Polizei die Aufgabe der vorbeugenden Bekämpfung von Straftaten für die Zukunft gesetzlich zuzuweisen, so gilt hierfür in besonderem Maße, daß durch präzise Vorschriften dem Grundsatz der Verhältnismäßigkeit Rechnung getragen werden muß. Die Regelungen der Aufgaben der Polizei einerseits und ihrer Befugnisse andererseits dürfen nicht isoliert voneinander betrachtet werden. Je weiter die Aufgaben gefaßt werden, desto konkreter müssen die zu ihrer Erfüllung eingeräumten Befugnisse im Gesetz festgelegt werden. Auf keinen Fall kann es akzeptiert werden, daß die Polizei im Bereich der vorbeugenden Bekämpfung von Straftaten mit generalklauselartigen Formulierungen zur erweiterten Datenverarbeitung berechtigt werden soll. Die Befugnis zur Erhebung und Speicherung von Daten zum Zwecke der vorbeugenden Bekämpfung von Straftaten muß auf schwere, im Gesetz im einzelnen aufgeführte Delikte begrenzt werden, für deren Bekämpfung sie unerläßlich erscheint.

3.5.2.2
Vorrang der offenen Datenerhebung

Insbesondere auch im Zusammenhang mit dem Aufbau von ZEVIS, dem Zentralen Verkehrsinformationssystem des Kraftfahrt-Bundesamtes, und dem geplanten Direktanschluß der Polizei (vgl. hierzu auch Abschn. 3.5.4) ist in der letzten Zeit die Frage in den Vordergrund gerückt, auf welche Weise die Polizei grundsätzlich ihre Daten erheben kann, ob es ihr etwa freisteht, dieselben Daten beim Betroffenen selbst oder bei anderen Stellen, offen oder verdeckt zu erheben. Sicherlich kann es in vielen Fällen dem Interesse des Bürgers entsprechen, wenn er nicht immer wieder dieselben Daten vor den verschiedenen Behörden angeben muß, sondern diese Stellen die Daten unter sich austauschen und den Betroffenen nur einmal behelligen. Im Regelfall erfährt der Bürger auch anschließend zumindest implizit von diesem Datenaustausch, denn es findet immer ein Kontakt zwischen ihm und den Behörden statt, bei dem auch diese Daten zur Sprache kommen. Ggf. kann er sich dann nach der Herkunft der Daten erkundigen und den Datenaustausch auch gerichtlich überprüfen lassen.

Anders allerdings bei der Polizei: Wenn eine Polizeibehörde Daten nicht direkt und offen beim Betroffenen erhebt, so gelangt diese Informationsbeschaffung möglicherweise nie zu seiner Kenntnis. Die Art und Weise des Vorgehens darf daher nicht im Belieben der Polizei stehen. Die Transparenz staatlicher Tätigkeit muß auch im Bereich der Polizei so weit wie möglich gewährleistet sein. Eine Datenerhebung, die direkt und offen beim Betroffenen erfolgt, ermöglicht es diesem, sich über die Maßnahme zu informieren und gegebenenfalls Rechtsschutz dagegen zu suchen. Erfährt er von der Datenerhebung nicht, so läuft sein Recht auf informationelle Selbstbestimmung leer. Der Grundsatz muß daher lauten: Daten sind in erster Linie direkt beim betroffenen Bürger und offen zu erheben. Anders darf nur dann verfahren werden, wenn sonst der Zweck der konkreten polizeilichen Aufgabenerfüllung vereitelt würde. Dieses Regel-Ausnahme-Verhältnis muß im Gesetz eindeutig niedergelegt werden. Besondere Bedeutung hat dies für die Art und Weise der Identifizierung von Bürgern (vgl. zu diesem Problem auch Ziff. 2.2.4).

3.5.2.3
Video-Aufnahmen und polizeiliche Beobachtung

In den letzten Jahren haben sich immer wieder zahlreiche Bürger an mich gewandt wegen der Datenerhebung bei Demonstrationen. Wegen der besonderen Gefahren für die Ausübung der Grundrechte, auf die auch das Bundesverfassungsgericht im Urteil zur Volkszählung hingewiesen hat, bedarf es ergänzend zu den allgemeinen Regelungen der Datenerhebung einer besonderen Schutzvorschrift für Demonstrationen. Der gegenwärtige Umfang der Datenerhebung muß eingeschränkt werden. Personenbezogene Daten dürfen nur dann erhoben werden, wenn bestimmte Tatsachen die Annahme rechtfertigen, daß von der Versammlung oder einzelnen Teilnehmern erhebliche gegenwärtige Gefahren für die öffentliche Sicherheit ausgehen.

Erforderlich ist auch eine besondere Vorschrift zum Einsatz von Video-Geräten bei Demonstrationen. Eine Vielzahl der an mich gerichteten Anfragen hatte Video-Aufnahmen durch die Polizei zum Gegenstand. In welchem Umfang die Polizei derzeit Video-Geräte einsetzt, wurde besonders deutlich an einem Fall aus dem November 1983: Am Buß- und Bettag veranstalteten Christen aus dem Rhein-Main-Gebiet in Frankfurt einen ökumenischen Bußgang. Etwa 800 evangelische und katholische Christen nahmen daran teil. Straftaten wurden nicht begangen. Während des Bußgangs wurden die Teilnehmer aus einem Polizeiwagen heraus gefilmt. Ich habe dem Innenminister mitgeteilt, daß ich ein solches Verhalten für unzulässig halte. Das Beispiel zeigt, daß die gegenwärtige Praxis des Einsatzes von Video-Geräten eingegrenzt und diese Einschränkung im Gesetz eindeutig festgelegt werden muß.

Auf die Probleme der "Polizeilichen Beobachtung" bin ich bereits im letzten Tätigkeitsbericht eingegangen (12. Tätigkeitsbericht, Ziff. 3.1.3.2.2). Sie dient der Sammlung von Erkenntnissen über den Betroffenen, etwa seine Kontakte, Reisen, benutzte Fahrzeuge usw. Die Daten derjenigen Bürger, für die die Polizeiliche Beobachtung angeordnet wurde, sind im INPOL-Fahndungsbestand gespeichert, der im übrigen in erster Linie die Daten derjenigen Personen enthält, die zur Festnahme oder Aufenthaltsermittlung ausgeschrieben wurden. Wenn die Polizei diese Bürger z.B. an der Grenze kontrolliert und dabei durch eine INPOL-Abfrage feststellt, daß für sie die Polizeiliche Beobachtung angeordnet wurde, so nimmt sie die Betroffenen nicht fest, sondern informiert die sachbearbeitende Polizeidienststelle unter Angabe des Ortes, der Zeit und der Umstände der Kontrolle darüber, daß sie diese Personen angetroffen hat. Von dieser Maßnahme erhält der Bürger keine Kenntnis. Die auf diese Weise erhobenen Daten werden von der jeweiligen sachbearbeitenden Dienststelle zusammengeführt mit dem Ziel, Bewegungsbilder der betroffenen Personen herzustellen, die unter Umständen zu weiteren polizeilichen Maßnahmen führen.

Im Zusammenhang mit der Polizeilichen Beobachtung stellt sich zunächst die Frage, unter welchen Voraussetzungen eigentlich die Fahndungsdaten von der Polizei abgefragt werden können. Nach wie vor ist der Beschluß der Innenministerkonferenz vom September 1977 nicht aufgehoben, der vorsieht, daß alle Personen, die der Polizei bei der Erfüllung ihrer Aufgaben bekannt werden - so z.B. auch bei Verkehrskontrollen nach der Straßenverkehrszulassungsordnung (StVZO) oder bei der Aufnahme von Anzeigen - routinemäßig durch Abfrage der Fahndungsdatei überprüft werden sollen (s. hierzu auch 12. Tätigkeitsbericht 3.1.3.3.1). Dementsprechend erhebt jeder Beamte bei seiner Aufgabenerfüllung sozusagen "nebenbei" auch Daten für die Polizeiliche Beobachtung. Im Zuge des Ausbaus der technischen Infrastruktur der Polizei sowie voraussichtlich auch durch die Verwendung des maschinenlesbaren Personalausweises wird die Dichte der polizeilichen Kontrollen erheblich zunehmen. Aus diesen Gründen haben die Maßnahmen der Polizeilichen Beobachtung eine erhebliche gesellschaftspolitische Dimension: Theoretisch können in Zukunft Bewegungsbilder von einem umfangreichen Personenkreis ohne größeren Aufwand hergestellt werden. Es bedarf daher auf jeden Fall einer konkreten und begrenzenden gesetzlichen Regelung. Eine Abfrage der Fahndungsdatei ist im Rahmen von Identitätsfeststellungen unter den im HSOG festgelegten Voraussetzungen zulässig. Sie darf nicht bei jedem anderen beliebigen Anlaß vorgenommen werden, sonst werden die Vorschriften des HSOG umgangen. Im übrigen bin ich nach wie vor der Auffassung, daß eine routinemäßige Abfrage der Fahndungsdatei bei jedem Kontakt mit dem Bürger unverhältnismäßig ist. Der Beschluß der Innenministerkonferenz muß daher aufgehoben werden. Darüber hinaus muß das Verfahren der Anordnung der Polizeilichen Beobachtung im Gesetz präzise festgelegt und der in Betracht kommende Personenkreis konkret begrenzt werden. Die Anordnung darf nur für einen kurzen Zeitraum erfolgen. Über eine Verlängerung der Beobachtung muß der Richter entscheiden.

3.5.2.4
Dateierrichtung und Datenaustausch

Nicht zuletzt muß im Gesetz das Verfahren der Errichtung von Dateien geregelt werden. Im 11. Tätigkeitsbericht (3.2.2.2) habe ich bereits auf den Hintergrund dieser Forderung, die ständige Zunahme polizeilicher Dateien, hingewiesen. Insbesondere muß für jede Datei eine Errichtungsanordnung vorgeschrieben werden, die namentlich über den Zweck und die Rechtsgrundlagen der Datensammlung, den aufzunehmenden Personenkreis, die Art und den Umfang der zu speichernden Informationen und die Dauer der Aufbewahrung Auskunft gibt.

Bei der Regelung der Datenübermittlung sind vor allem zwei Gesichtspunkte von besonderer Bedeutung: Zum einen muß der gegenwärtige Umfang des Informationsaustausches zwischen Polizei und Verfassungsschutz eingeschränkt werden. Datenübermittlungen dürfen nur in engen Grenzen zugelassen werden, die den unterschiedlichen Aufgabenstellungen der Polizeibehörden einerseits und der Verfassungsschutzbehörden andererseits Rechnung tragen. Ein geeigneter Maßstab sind die Übermittlungsregelungen nach dem Gesetz zu Art. 10 Grundgesetz.

Zum anderen muß sichergestellt werden, daß die Vorschriften des Bundeszentralregistergesetzes nicht in der Praxis durch Datenübermittlungen von der Polizei an andere Stellen unterlaufen werden (vgl. hierzu den konkreten Fall in Ziff. 2.2.2).

3.5.3
Der maschinenlesbare Personalausweis

Das Thema "maschinenlesbarer Personalausweis" bildete einen Schwerpunkt meines letzten Tätigkeitsberichts (Ziff. 3.1). Ähnlich wie bei der Volkszählung 1983 entzündete sich um den Ausweis bereits im Vorjahr eine breite Diskussion, die sich mit den möglichen Folgen einer solchen Art von Legitimationspapier, ihren Chancen und Gefahren auseinandersetzt. Nicht die angestrebte "Fälschungssicherheit" des Dokuments, sondern vielmehr seine Maschinenlesbarkeit weckten Befürchtungen, hier könnte eine neue Qualität der Kontrolle von Bewegungen jedes einzelnen Bürgers durch die Sicherheitsbehörden erreicht werden, die durch den angestrebten Gewinn an Sicherheit nicht gerechtfertigt wäre. Die öffentliche Ausübung einer Reihe von Grundrechten - ich nenne allein die Versammlungs-, die Demonstrations- und die allgemeine Bewegungsfreiheit - würde damit über Gebühr eingeschränkt. Aufgrund des Volkszählungsurteils wurde der ursprüngliche Einführungszeitpunkt, der 1. November 1984, aufgehoben. Regierungskoalition (s.u.), SPD und GRÜNE legten eigene Gesetzentwürfe vor.

3.5.3.1
Maschinenlesbarkeit wofür?

Völlig unbefriedigend wurde bislang die Frage beantwortet, ob der neue Ausweis überhaupt notwendig ist. Da im wesentlichen nur die Polizei Lesegeräte erhalten soll, muß man sich vor allem die mit diesen Geräten möglichen Veränderungen einer polizeilichen Überprüfung verdeutlichen: An die Stelle der manuellen Eingabe der dem Ausweis entnommenen Daten durch einen Polizeibeamten träte beim automatisierten Verfahren das Ablesen durch das Lesegerät selbst. Zweifellos würde dadurch das Prüfungsverfahren um einige Sekunden oder Minuten beschleunigt werden. Der Polizei würden damit schnellere und umfassendere Kontrollmöglichkeiten eröffnet. Nur: In welcher Situation können diese Möglichkeiten genutzt werden? Sollen überhaupt häufiger Kontrollen stattfinden? Wenn ja, warum?

Bis zum Frühjahr 1984 wurde immer wieder auf die geplante Vermehrung der Kontrollen an den Grenzen hingewiesen. Nachdem Frankreich und die Bundesrepublik Deutschland sowie im Anschluß daran auch eine Reihe von anderen westlichen Nachbarstaaten entschieden haben, die Grenzen ihrer Länder teilweise zu öffnen und Grenzkontrollen abzubauen, entfällt dieses maßgebliche Motiv für die Einführung des maschinenlesbaren Personalausweises. Es dürfte keine Schwierigkeiten bereiten, die dann nur noch stichprobenhaft vorzunehmenden Kontrollen über das traditionelle Verfahren der Eingabe in Tastengeräte vorzunehmen.

Vermehrte Kontrollen im Inland - hier müßten der Grund ebenso wie der betroffene Personenkreis konkret umschrieben werden - dürfen ohne besonderen Anlaß nicht vorgenommen werden. Allein der Hinweis auf den abstrakten Fall, irgendwann einmal könne eine Lage entstehen, die ein automatisiertes Lesen von Ausweisen erforderlich mache, erfüllt nicht die Anforderungen des Bundesverfassungsgerichts an Eingriffe in das informationelle Selbstbestimmungsrecht. Der Grundsatz der Verhältnismäßigkeit läßt auch den mit dem technischen Mittel einer automatisierten Speicherung verbundenen Eingriff nur zu, wenn er durch ein überwiegendes Allgemeininteresse gerechtfertigt werden kann, das ich derzeit nicht erkennen kann. Mit Interesse habe ich deshalb festgestellt, daß bereits in der Debatte des Bundestages zur Frage der Einführung des maschinenlesbaren Personalausweises sowohl die Vertreter der Regierungskoalition als auch der Bundesminister des Innern ihre Bereitschaft erkennen ließen, die Einführung eines maschinenlesbaren Ausweisdokuments noch einmal zu überdenken.

3.5.3.2
"Junktim" mit Regelungen für die Sicherheitsbehörden

Bereits in meinem letzten Tätigkeitsbericht habe ich in Übereinstimmung mit meinen Kollegen der Länder und des Bundes gefordert, daß die Verwendung dieses Dokuments durch die Sicherheitsbehörden an die Schaffung bereichsspezifischer Vorschriften für die personenbezogene Datenverarbeitung bei den Sicherheitsbehörden zu knüpfen ist. Diese Voraussetzung wurde auch von den die Regierungskoalition tragenden Fraktionen grundsätzlich anerkannt. Auch sie sind bereit, Datenschutzvorkehrungen auf einer gesetzlichen Grundlage im gesamten Sicherheitsbereich zu treffen. Hierzu gehört die Zusammenarbeit zwischen dem Bundesgrenzschutz und den Sicherheitsdiensten, ein Gesetz für den Militärischen Abschirmdienst, eine Neuregelung des Verfassungsschutzgesetzes und des Bundeskriminalamtsgesetzes. Eine klare Äußerung zu der ebenfalls notwendigen Änderung der Strafprozeßordnung wäre ebenfalls erforderlich. Auf Landesebene käme eine entsprechende Novellierung der die Gefahrenabwehr regelnden Polizeigesetze hinzu.

Nach den Verlautbarungen der Koalitionsfraktionen soll der maschinenlesbare Ausweis erst dann eingeführt werden, wenn sich beide Fraktionen über gesetzliche Neuregelungen für die Sicherheitsbehörden "verständigt" haben und "soweit wie möglich entsprechende Gesetze in erster Lesung eingebracht oder verabschiedet wurden". Sicherlich ist mit dieser Verknüpfung ein wesentlicher Schritt in Richtung auf eine umfassende Sicherung des Datenschutzes getan. Nur: Solange nicht erkennbar ist, welche Inhalte in diese Regelungsvorschläge aufgenommen werden sollen, kann die formale Ankündigung allein nicht genügen. Ein abschließendes Urteil wird freilich erst dann zu treffen sein, wenn die erforderlichen Entwürfe dem Parlament und der Öffentlichkeit zugänglich sind.

3.5.3.3
Einzelbewertung des Gesetzentwurfs der Regierungskoalition
(BT-Drucks. 10/2177)

3.5.3.3.1
Geschlossene Regelungslücken

Hervorzuheben ist die geplante Festlegung des Inhalts der für das automatische Lesen vorgesehenen Zone des Dokuments. Damit wird der Kritik an dem bisherigen Gesetz, die Maschinenlesbarkeit werde im Gesetz selbst nicht erwähnt, obwohl es sich hierbei um ein wesentliches, vom Gesetzgeber selbst vorzugebendes Merkmal handele, entsprochen.

Eine Vorschrift über die Führung der Personalausweisregister bei den Landespersonalausweisbehörden soll sowohl bundesweit den in diesen Registern zu speichernden Datenkatalog festlegen als auch die Zwecke, denen das Register zu dienen hat. Auch die Löschungsfrist für die Daten dieser Register wird festgeschrieben.

In engem Zusammenhang hiermit steht die Regelung der "Verteilung und Nutzung der Daten im Personalausweisregister". Uneingeschränkte Zustimmung verdient die Festlegung, die Personalausweisbehörden dürften ihre Daten nur nach Maßgabe dieses Gesetzes, anderer Gesetze oder Rechtsverordnungen erheben, übermitteln, sonst verarbeiten oder nutzen. Damit wird ein eindeutiger Gesetzesvorbehalt eingeräumt. Zu beachten ist auch die Einschränkung, daß eine anfragende Stelle nur dann Daten aus den Personalausweisregistern erhält, wenn sie ohne die Kenntnis dieser Daten nicht in der Lage wäre, eine ihr obliegende Aufgabe zu erfüllen und die Daten "bei den Betroffenen nicht oder nur mit unverhältnismäßig hohem Aufwand erhoben werden können oder nach der Art der Aufgabe, zu deren Erfüllung die Daten erforderlich sind, von einer solchen Datenerhebung abgesehen werden muß." Diese Formulierung stimmt im wesentlichen mit § 18 Abs. 2 des Melderechtsrahmengesetzes überein.

3.5.3.3.2
Mangelnde Zweckbindung

Nach dem Urteil des Bundesverfassungsgerichts zur Volkszählung 1983 genießt der Grundsatz der Zweckbindung der Daten Verfassungsrang. Der Entwurf sieht im Gegensatz hierzu vor, daß die Personalausweisregister nicht nur zur Ausstellung der Personalausweise und der Feststellung ihrer Echtheit, zur Identitätsfeststellung einer Person, die einen Personalausweis besitzt oder für die er ausgestellt ist, und zur Durchführung dieses Gesetzes (des Personalausweisgesetzes) und der Ausführungsgesetze der Länder dient, sondern nahezu allen öffentlichen Stellen der Bundesrepublik Deutschland als Auskunftsquelle zur Verfügung steht. Bereits in meinem letzten Tätigkeitsbericht (Ziff. 3.1.7) habe ich gefordert, daß dies auf Polizeidienststellen eingeschränkt werden muß. Anderenfalls erhielte das Personalausweisregister den Charakter eines "Parallelmelderegisters" für eine Vielzahl von Stellen -eine Entwicklung, die der Zweckbindung zuwiderliefe. Allein zulässiger Übermittlungsgrund an andere Behörden sollte die Überprüfung der Richtigkeit der in einem vorgelegten Personalausweis enthaltenen Daten sein. So beschränkt, wäre die Übermittlung an eine konkrete, vom Personalausweisgesetz vorgesehene Kontrollmaßnahme - die Identitätsüberprüfung einer bestimmten Person - geknüpft.

In diesem Zusammenhang stößt auch der vorgesehene gegenseitige Abgleich von Personalausweis- und Melderegistern ohne begrenzende Voraussetzungen auf erhebliche Bedenken. Er verwischt die Grenzen der unterschiedlichen Zwecken dienenden Dateien und führt letztlich zu einem verfassungswidrigen Zusammenschalten beider Register. Notwendig wäre vielmehr, Übermittlungen an konkrete Verwaltungsverfahren - etwa die Ausweisausstellung - zu knüpfen, und damit eine auch für den Betroffenen transparente, zweckgebundene Übermittlungspraxis festzulegen.

3.5.3.3.3
Verantwortlichkeit für die Übermittlung

Nicht hingenommen werden kann die vorgesehene Regelung, nach der nur die eine Personalausweisbehörde um Informationen ersuchende Behörde - also die die Angaben anfordernde Stelle - die Verantwortung dafür trägt, daß die mitzuteilenden Daten unter Berücksichtigung der gesetzlichen Vorschriften übermittelt werden. Damit würde ein datenschutzrechtliches Grundprinzip außer Kraft gesetzt: Das Datenschutzrecht sieht - im Unterschied zur Regelung der Amtshilfe - eine doppelte Verantwortung von Absender und Empfänger für die Rechtmäßigkeit der Datenübermittlung vor. Die datenabgebende Stelle ist verpflichtet zu prüfen, ob die Übermittlung für den vom Empfänger angegebenen Zweck auch erfolgen darf. Dieser Grundsatz, der übrigens auch im Melderechtsrahmengesetz ausdrücklich festgehalten ist, garantiert die Wachsamkeit beider beim Datenaustausch beteiligten Behörden für einen umfassenden Datenschutz.

3.5.3.3.4
Verwendung der Seriennummer und im privaten Bereich

Zu begrüßen ist hingegen, daß die Verwendung der Seriennummer des Personalausweises durch den Entwurf eingeschränkt wird. Ein Abruf personenbezogener Daten aus beliebigen Dateien und die Verknüpfung von Dateien mit Hilfe der Seriennummer des Personalausweises wird untersagt. Die Seriennummer verliert dadurch in jedem Fall die Funktion als potentielles Personenkennzeichen. Vorzugswürdig wäre allerdings ein Verbot der Speicherung der Seriennummer in allen Dateien außerhalb des Personalausweisregisters. Insofern halte ich auch das vorgesehene ausdrückliche Verbot einer Speicherung der Seriennummer in den örtlichen Melderegistern für wichtig, eine Regelung die der hessische Landesgesetzgeber auf mein Anraten hin bereits in das Landesmeldegesetz aufgenommen hat.

Eine notwendige Korrektur des jetzigen Gesetzestextes liegt darin, daß nach dem Entwurf der Personalausweis im nichtöffentlichen Bereich ausdrücklich "weder zum automatischen Abruf personenbezogener Daten noch zur automatischen Speicherung personenbezogener Daten verwendet werden" darf. Damit wurde die Forderung der Datenschutzbeauftragten des Bundes und der Länder erfüllt, privaten datenverarbeitenden Stellen sowohl die Errichtung als auch die Erschließung von Dateien in automatisierter Form mit Hilfe des Ausweises zu untersagen.

3.5.3.3.5
Zugriff der Polizei auf Personalausweisdaten

Das Gesetz sieht bislang - in der Fassung, die ursprünglich am 1. November 1984 in Kraft treten sollte - vor, daß der Ausweis zur Einrichtung oder Erschließung polizeilicher Dateien verwendet werden darf, soweit diese für die "Fahndung aus Gründen der Strafverfolgung und der Gefahrenabwehr durch die hierfür zuständigen Behörden betrieben werden". Diese Fassung stieß auf berechtigte Kritik. Insbesondere der Begriff der "Fahndung" ist zu ungenau, um den Anwendungsbereich klar einzugrenzen. Weder im Recht der Strafverfolgung noch der Gefahrenabwehr finden sich hierfür eindeutige Festlegungen. Es ist deshalb zweifellos ein Fortschritt, wenn in dem vorliegenden Entwurf präzisiert wird, ein automatisierter Abruf dürfe für Zwecke "der Fahndung oder Aufenthaltsfeststellung aus Gründen der Strafverfolgung, Strafvollstreckung oder der Abwehr von Gefahren für die öffentliche Sicherheit" vorgenommen werden, wenn die hiervon betroffenen personenbezogenen Daten "im polizeilichen Fahndungsbestand geführt" werden. Diese Konkretisierung verliert allerdings ihren Sinn, wenn durch die hierfür vorgesehenen Vorschriften nicht eindeutig der Bestand an Dateien gekennzeichnet wird, der "der Fahndung" dient.

In vielen Fällen wird der automatisierte Abruf zu dem Ergebnis kommen, daß der betroffene Bürger in den polizeilichen Dateien bisher nicht gespeichert ist. Solche "Negativ-Anfragen" dürfen nach dem vorliegenden Entwurf nur in bestimmten Ausnahmefällen gespeichert werden. Eine Aufnahme der überprüften Daten und Speicherung in einer Datei darf nur erfolgen, "wenn bestimmte Tatsachen die Annahme rechtfertigen, daß dies

1. zur Aufklärung einer der in § 100a der Strafprozeßordnung genannten Straftaten oder
2. zur Verhütung einer solchen unmittelbar drohenden Straftat führen kann und die Aufklärung oder Verhütung ohne diese Maßnahme aussichtslos oder wesentlich erschwert wäre".

Eine solche Maßnahme darf nur durch den Richter, in bestimmten Sonderfällen allerdings auch durch die Staatsanwaltschaft oder - sofern dies zur Verhütung einer unmittelbar drohenden, in § 100a der Strafprozeßordnung genannten Straftat notwendig ist - auch durch einen "von der obersten Dienstbehörde besonders ermächtigten Beamten" getroffen werden. Diese Anordnung muß schriftlich ergehen und den oder die Betroffenen - soweit dies möglich ist - bezeichnen. Soweit sich die Anordnung gegen einen Personenkreis richtet, muß sie diesen nach konkreten Merkmalen oder Eigenschaften bestimmen, ebenso die Art und Dauer der Maßnahme.

Diese Vorschrift ist gleichwohl noch zu weit gefaßt. Die pauschale Übernahme des in § 100 a StPO erwähnten Tatbestandskatalogs kann nicht überzeugen, vor allem wenn man berücksichtigt, daß ein wesentlich größerer Personenkreis von der Registrierung betroffen wäre. Nach § 100a StPO muß nämlich eine Person als Täter oder Teilnehmer an einer der genannten Straftaten verdächtig sein. Nach der geplanten Regelung im Personalausweisgesetz ist dies jedoch nicht erforderlich. Dort würde eine Speicherung nicht "täterbezogen", sondern "tatbezogen" erfolgen. Personen aus dem gesamten "Tatumfeld" und damit in nur sehr schwer abgrenzbarem Umfang wären von einer solchen Maßnahme betroffen. Die in der schriftlichen Anordnung festzuhaltenden Merkmale oder Eigenschaften des Personenkreises sind in keinerlei Weise im Gesetzentwurf präzisiert. Ein solcher, relativ offener Tatbestand widerspricht den Erfordernissen der Bestimmtheit und der Transparenz, die das Bundesverfassungsgericht in seinem Volkszählungsurteil als Voraussetzungen für jede rechtmäßige Einschränkung des Rechts auf informationelle Selbstbestimmung aufgestellt hat. Gleiches gilt auch für die Frage, ob die Betroffenen - entsprechend § 101 StPO - von der Maßnahme zu benachrichtigen sind, "sobald dies ohne Gefährdung des Untersuchungszwecks geschehen kann". Eine solche Vorschrift ist für die Speicherung von "Negativ-Anfragen" nicht vorgesehen.

3.5.4
Das Zentrale Verkehrsinformationssystem des Kraftfahrtbundesamtes (ZEVIS)

3.5.4.1
Positionen der Bundesregierung, des Bundestags und des Landtags

Schon in meinem 9. Tätigkeitsbericht für 1980 (Drucks. 9/4032 Ziff. 2.1.1) habe ich dazu Stellung genommen, daß in Hessen örtliche Polizeidienststellen einen Direktzugriff auf die Daten der in ihrem Zuständigkeitsbereich liegenden örtlichen Kraftfahrzeugzulassungsstellen erhielten. Der vom Bundesverkehrsminister im Jahr 1983 vorgelegte und 1984 weiterentwickelte Entwurf zur Änderung des Straßenverkehrsgesetzes zieht die Konsequenzen aus der damals geäußerten Kritik, dieses Verfahren sei mit den geltenden Gesetzen nicht zu vereinbaren. Er will den durch das Urteil des Bundesverfassungsgerichts zur Volkszählung 1983 bekräftigten Auftrag erfüllen, eine bereichsspezifische Regelung für die Verarbeitung personenbezogener Daten bei den örtlichen Straßenverkehrsbehörden und dem Kraftfahrtbundesamt zu schaffen. Es geht dabei um die Führung der örtlichen und zentralen Dateien der ca. 30 Mio. Fahrzeuge mit amtlichen Kennzeichen einschließlich der Angaben über ihre Halter, das zentrale Fahrzeugregister der Mopeds und Mofas mit Versicherungskennzeichen und um das Verkehrszentralregister mit Eintragungen der Bußgeldbehörden und Strafgerichte über ca. 3,8 Mio. "Verkehrssünder".

Nach dem Entwurf sollen nicht nur die Straßenverkehrsbehörden selbst, sondern insbesondere die Polizeibehörden des Bundes und der Länder einen möglichst schnellen und direkten Zugriff auf die regional und bundesweit gespeicherten Dateien der Straßenverkehrsbehörden erhalten. Aus hessischer Sicht würden damit regional bereits bestehende Zugriffsmöglichkeiten um eine bundesweite Dimension ergänzt, wenn nicht durch diese ersetzt. Diese Konzeption lag bereits den Entwürfen des Jahres 1983 zugrunde; dazu habe ich in meinem 12. Tätigkeitsbericht (Ziff. 4.3) ausführlich Stellung genommen. Da weder die Zielrichtung noch die Struktur des Entwurfs in der Zwischenzeit wesentlich abgeändert wurden, treffen die damals erhobenen rechtlichen Einwände auch für die jüngste, am 1. Dezember 1984 vorgelegte Fassung unverändert zu.

Nach wie vor ist die sogenannte *P-Abfrage vorgesehen. Meine damalige Warnung, durch diese Abfrageart könnten die beim Kraftfahrtbundesamt gespeicherten Daten gleichsam als "Bundesadreßregister" aller Kraftfahrzeughalter von den Polizeidienststellen verwendet werden - während im Meldewesen ein solches Zentralregister aus datenschutzrechtlichen Gründen vom Gesetzgeber abgelehnt wird - hat der Hessische Landtag aufgegriffen. In seinen Beschlüssen zum 12. Tätigkeitsbericht bittet er die Landesregierung, "bei der Abfassung ihrer Stellungnahme zur Novellierung des Straßenverkehrsgesetzes die Bedenken des Datenschutzbeauftragten gegenüber einer Einführung der sogenannten *P-Abfrage zu berücksichtigen" (Beschluß Nr. 18, vgl. Beschlußempfehlung des Innenausschusses, Drucks. 11/1551). Jüngste Äußerungen der Hessischen Landesregierung in der Öffentlichkeit lassen erkennen, daß sie sich meiner Einschätzung der *P-Abfrage anschließt.

Auch der Innenausschuß des Deutschen Bundestages hat in seiner Beschlußempfehlung an den Bundestag nachhaltig Bedenken gegen die *P-Abfrage geltend gemacht (Bundestags-Drucks. 10/1719, S. 5). Seine Empfehlung lautet wie folgt: "Der Einführung einer sogenannten *P-Abfrage im Online-Verfahren, d.h. der Möglichkeit, den zentralen Bestand der Kraftfahrzeuge mit Versicherungskennzeichen mittels Namensangabe im Online-Verfahren zu erschließen, kann der Deutsche Bundestag beim gegenwärtigen Sachstand nicht - auch nicht für ein Testverfahren - zustimmen." Der Bundestag folgte dieser Empfehlung in seiner Sitzung vom 20. September 1984. Seither ist die Erprobung von ZEVIS ausgesetzt.

3.5.4.2
ZEVIS als "komfortables" Auskunftssystem

Im Rahmen von ZEVIS werden beim Kraftfahrtbundesamt (KBA) folgende Dateien geführt:

- Eine Datei der Fahrzeuge mit amtlichen Kennzeichen, geordnet nach dem Kennzeichen.
- Eine Datei der Fahrzeuge mit amtlichen Kennzeichen, geordnet nach Hersteller und Fahrgestellnummer, einschließlich der in den letzten 5 Jahren endgültig ausgeschiedenen Fahrzeuge.
- Eine Datei der Fahrzeuge mit Versicherungskennzeichen.
- Eine Namensdatei des Verkehrszentralregisters, einschließlich der Daten über entzogene, gesperrte und versagte Fahrerlaubnisse.

Diese Dateien werden in einem Datenbanksystem zusammengefaßt, das im Vergleich zum bisherigen System zwar keine neuen Daten enthalten soll, durch den Ausbau der Abfragearten jedoch eine wesentlich bessere Nutzung zuläßt. Aus der Sicht des Datenschutzes sind es vor allem die den externen Nutzern eingeräumten Auskunftsmöglichkeiten, die zu Kritik Anlaß geben.

Ein Teil des Systems wurde in der Erprobungsphase bereits realisiert. Schon heute sind die Fahrzeugdatenbestände der Länder Baden-Württemberg, Bayern, Rheinland-Pfalz, Saarland und Schleswig-Holstein sowie der Zulassungsstellen Bonn und Düsseldorf in das System aufgenommen. Gleiches gilt für die Gesamtdatei der Fahrzeuge mit Versicherungskennzeichen und die Datei der Personen, die nicht im Besitz einer Fahrerlaubnis sein können (wegen Entzugs usw.).

Über eine Anfrageberechtigung im Direktzugriff verfügen jetzt bereits die Polizeidienststellen der erwähnten Länder und Orte sowie Berlins und Hamburgs, das Bundeskriminalamt und die Grenzschutzdirektion in Koblenz. Die Zahl der Anfragen beläuft sich derzeit schon auf ca. 200.000 im Monat.

Im Direktzugriff dieser Behörden stehen die erwähnten Daten bereits in den Anfragearten *H und *K:

- Die *H-Anfrage sieht die Eingabe des Kennzeichens, der Fahrgestellnummer oder des Versicherungskennzeichens vor, um die Halterdaten (Name, Vorname, Geburtsname, Geburtsort und Anschrift) zu erschließen.
- Die *K-Anfrage erweitert diese Auskunft um die Fahrzeugart, den Hersteller, den Typ, das Kennzeichen und die Fahrgestellnummer sowie die Farbe des Fahrzeuges.
- Über eine weitere Anfrageart *A können Kennzeichen mit ein bis zwei Unbekannten eingegeben werden, worauf dann eine Liste der möglichen Kennzeichen ausgegeben wird.
- Schließlich gewährt die Anfrage *F Auskunft auf die Frage, ob zu einem bestimmten Namen "Negativinformationen", etwa der Entzug der Fahrerlaubnis mit der dazugehörigen Frist, vorliegen.

Im Unterschied zu diesen Anfragearten ist die sogenannten *P-Abfrage noch nicht realisiert.

Sie würde es ermöglichen, über die Eingabe des Namens eines Fahrzeughalters Auskunft darüber zu erhalten, welche Fahrzeuge auf ihn zugelassen sind. Natürlich können über diese Abfrageart auch die übrigen Personalien eines Halters - Geburtstag und -ort, Vornamen, Geschlecht und Anschrift - festgestellt werden.

3.5.4.3
Aufhebung der "Entpolizeilichung"?

Es ist bezeichnend, daß die im Probelauf eingerichteten Direktschaltungen auf ZEVIS nicht einzelnen örtlichen Kraftfahrzeugzulassungsstellen, sondern durchweg Dienststellen der Polizei zur Verfügung gestellt wurden. Es ist nur konsequent, daß sich deshalb sowohl der Bundestag wie auch das hessische Parlament intensiv mit den Grundproblemen einer Direktanbindung der Polizeidienststellen an diese Dateien beschäftigten.

So wurde kritisch darauf hingewiesen, daß mit dem Direktzugriff auf ZEVIS dieses Informationssystem praktisch in den Polizeibereich - sowohl zu Zwecken der Strafverfolgung wie auch der Gefahrenabwehr - integriert werden würde. Eine solche Entwicklung aber steht im Gegensatz zu der in den frühen Jahren der Bundesrepublik vollzogenen "Entpolizeilichung", d.h. der Trennung der "allgemeinen" von den "besonderen" Polizeibehörden, die organisatorisch selbständig als "Ordnungspolizei" ihre Aufgaben wahrnehmen sollten. Im Zuge dieser Entwicklung wurden auch die Straßenverkehrsbehörden organisatorisch von den allgemeinen Polizeibehörden getrennt. Diese Maßnahme ist für den Datenschutz deshalb so wichtig, weil Verwaltungseinheiten, die wie die Straßenverkehrsbehörden auf die Erfüllung einer konkreten und spezifischen Aufgabe beschränkt sind, viel leichter dem Gesichtspunkt der Zweckbindung der personenbezogenen Datenverarbeitung Rechnung tragen können als Abteilungen einer zentral geführten Großverwaltung. Die zuweilen skizzierte Gefahr, mit der Einrichtung einer Direktschaltung der Polizei auf die Daten der Straßenverkehrsbehörden werde die "Repolizeilichung" der Ordnungsbehörden eingeleitet, ist deshalb nicht von der Hand zu weisen. Keinesfalls könnte eine Entwicklung hingenommen werden, die Register um Register der Ordnungsbehörden dem Direktzugriff der Polizei zugänglich machen würde.

3.5.4.4
Die *P-Abfrage

3.5.4.4.1
ZEVIS als Bundesadreßregister?

Mit der Einrichtung der Direktzugriffe ist die Gefahr verbunden, daß bereits bestehende und vom Gesetzgeber mit anderer Zielsetzung geschaffene Datenschutzregelungen unterlaufen werden. Dies gilt insbesondere für die *P-Abfrage, die der Polizei erlaubt, durch Eingabe des Namens einer Person in Sekundenschnelle festzustellen, welche Fahrzeuge auf diese Person zugelassen sind und welche weiteren personenbezogenen Angaben ZEVIS über diesen Bürger enthält (s.o.). Auch wenn eine *P-Abfrage nach dem Entwurf nur erfolgen darf, um im Einzelfall "Personen in ihrer Eigenschaft als Halter von Fahrzeugen, Fahrzeuge eines Halters oder Fahrzeugdaten festzustellen oder zu bestimmen", so wäre das Register über diese Abfrage ohne Zweifel als "Ersatzmelderegister" aller Halter verwendbar. Die - nach den bisherigen Erfahrungen mit den übrigen Abfragearten - dann auch in diesem Bereich zweifellos ansteigenden Abfragezahlen lassen nachträgliche Überprüfungen, ob im Einzelfall bei einer Abfrage die Eigenschaft einer Person als Halter eines bestimmten Fahrzeugs oder nicht doch die Ergänzung seiner Personalien im Vordergrund stand, als nahezu aussichtslos erscheinen.

Damit besteht die Gefahr, daß durch diese Abrufart vom Gesetzgeber für das Meldewesen geschaffene datenschutzrechtliche Regelungen und Strukturen ihre Bedeutung verlieren. So wäre die Absage des Bundestages an ein zentrales Bundesmelderegister und der meisten Landesgesetzgeber an Landesadreßregister für die 23 Mio. Kraftfahrzeughalter praktisch wirkungslos. Dies gilt umso mehr, als die ZEVIS entnommenen Daten durch örtliche Register weiter ergänzt werden können.

3.5.4.4.2
Protokollierung statt präventive Übermittlungskontrolle

In der Diskussion um die *P-Abfrage, ja um die Einrichtung von Direktzugriffsverfahren überhaupt, wird immer wieder eingewandt, die bei solchen Verfahren möglichen technischen Datenschutzvorkehrungen - insbesondere die Protokollierung jedes Zugriffs - machten den durch die Trennung der Dateien bis dahin wirksamen Schutz wieder wett. Gerade im vorliegenden Fall kann dieses Argument nicht überzeugen.

Bei einer herkömmlichen Datenübermittlung - etwa einer Anfrage durch die Polizei beim KBA mit dem Wunsch, den Namen des Halters eines bestimmten Fahrzeugs zu erfahren - ist die Polizei verpflichtet, der Verkehrsbehörde auch den Grund der Anfrage mitzuteilen. Nur so kann diese feststellen, ob die Übermittlung für die Aufgabenerfüllung der Polizei tatsächlich "erforderlich" ist. Diese geteilte Verantwortung von Empfänger und Übermittler für die Zulässigkeit jeder Übermittlung stellt ein wichtiges Grundprinzip des Datenschutzrechts dar. In Massenauskunftsverfahren mag diese Prüfung sich auf die Plausibilität der von der anfragenden Stelle angegebenen Zwecke beschränken. Nach Informationen des Kraftfahrtbundesamtes werden derzeit in einer Vielzahl von Fällen auch die Umstände der Anfrage mitgeteilt, so daß eine solche Zulässigkeitskontrolle grundsätzlich vorgenommen werden kann.

Kann die Polizeibehörde jedoch direkt zugreifen, so fällt jede präventive Prüfung der Rechtmäßigkeit einer Datenübermittlung weg. Allenfalls über eine Auswertung der die Abrufe begleitenden Protokolle wären etwaige Mißbräuche feststellbar. Sie könnten allenfalls für die Zukunft, nicht aber für die jeweilige Datenübermittlung zu Konsequenzen führen - aus der Sicht des betroffenen Bürgers eine nicht zu verkennende Verschlechterung.

Eine Reihe von Gründen läßt zudem an der Wirksamkeit einer nachträglichen Protokollauswertung Zweifel aufkommen. Schon derzeit beschaffen sich die bisher an ZEVIS angeschlossenen Polizeidienststellen (s.o) mit den übrigen Abfragearten Halter- bzw. Kfz-Angaben in rund 200.000 Fällen monatlich. Eine Ausweitung des Verfahrens auf das gesamte Bundesgebiet und die Einbeziehung der *P-Abfrage würden zu einer beträchtlichen Erhöhung dieser Zahlen führen. Da der Direktzugriff zeitraubende technische Hindernisse abbaut, stiege die Häufigkeit - im Verhältnis zu den bisher noch auf traditionellem Wege vorgenommenen Übermittlungen - noch zusätzlich. Dies wird durch die Praxis in den bereits angeschlossenen Ländern bestätigt. Die Datenschutzbeauftragten sind angesichts solcher Größenordnungen außerstande, die Rechtmäßigkeit dieser Abfragen zu überprüfen.

Dies gilt erst recht angesichts der im Pilotverfahren angewandten Protokollierungsmethode: So enthalten die Protokolle derzeit lediglich eine Kennung der anfragenden Dienststelle. Weder die anfragende Person noch der Anfragegrund werden dokumentiert. Nachträgliche Recherchen bedürfen eines beträchtlichen Aufwandes und eines ausgezeichneten Erinnerungsvermögens der beteiligten Mitarbeiter, um im konkreten Fall die Rechtmäßigkeit einer bestimmten Abfrage nachprüfen zu können.

3.5.4.4.3
Begründungsdefizit für Online-Anschluß

Kurzum: Der mit der Schaltung eines Direktzugriffs verbundene Verlust an wirksamen Datenschutzkontrollmöglichkeiten ist erheblich. Demgegenüber gilt, daß jede Beschleunigung einer Datenweitergabe angesichts der geschilderten Risiken einer besonderen Rechtfertigung bedarf. Dies gilt insbesondere dann, wenn die Rechtsstellung der betroffenen Bürger beeinträchtigt wird. So müßte die Polizei für die Einrichtung der *P-Abfrage als Online-Anschluß den Nachweis führen, daß das öffentliche Interesse hierfür gegenüber der beeinträchtigten Rechtsstellung der betroffenen Bürger Vorrang genießt. Dieser Nachweis konnte bisher nicht geführt werden und wird auch kaum zu erbringen sein. Denn nur in wenigen Fällen bedarf es eines Zugriffs im "einstelligen Sekundenbereich", wie ihn die Online-Anbindung ermöglicht. Fast immer genügt eine telefonische Anfrage beim Kraftfahrtbundesamt, die Verzögerungen lediglich um Sekunden oder allenfalls Minuten mit sich bringt. Auch daß die *P-Abfrage im traditionellen Verfahren der Übermittlung bisher wesentlich seltener genutzt worden ist als die übrigen Abfragearten, spricht gegen die Einrichtung eines Direktzugriffsverfahrens.

Meine Einschätzung wird bestätigt durch eine Stellungnahme des Polizeipräsidenten der Stadt Düsseldorf vom 26. November 1984, in der dieser zur Online-*P-Abfrage feststellt, daß sie aus der Sicht der Polizei zwar nützlich sein kann, aber nicht unabdingbar ist. Insbesondere könnten bei der Verfolgung von Straftaten die Planung und Vorbereitung der polizeilichen Maßnahmen nicht wesentlich beschleunigt werden. Dies gelte auch für die Vorbereitung von Observationen, zumal die Betroffenen zu Fahrzeugwechseln neigten. Die bisher vorhandenen Möglichkeiten einer Einzelanfrage würden demnach genügen.

3.5.4.5
Die *H-Abfrage

Bedenken habe ich auch gegen die Einrichtung von Online-Anschlüssen für die *H-Abfrage, bei der Halterdaten mit Hilfe der Eingabe des Kennzeichens ermittelt werden. Will ein Polizeibeamter die Personalien einer Person feststellen, die einen Wagen lenkt, so gewährt ihm diese Abfrageart einen schnellen und für den Betroffenen nicht erkennbaren Zugang. Zwar sind in vielen Fällen Fahrer und Halter nicht identisch. Der Zugriff auf die Straßenverkehrsdateien kann deshalb keine eindeutige Antwort auf die Frage geben, wer sich an einem bestimmten Ort zu einer bestimmten Zeit am Steuer eines Fahrzeugs befindet. Trotzdem genügt der Polizei in vielen Fällen der erste Anschein: Sie speichert trotz dieser Unsicherheit die gewonnenen Daten und vergleicht sie mit bereits vorhandenen Informationen. Der erleichterte Zugriff kann dazu verleiten, noch häufiger Abfragen auch ohne jeden Zusammenhang mit Gefahren oder Delikten im Straßenverkehr vorzunehmen. Die Grenzen solcher Zugriffe definieren derzeit weder das Strafprozeßrecht noch die Polizeigesetze mit der notwendigen Klarheit. Im Entwurf des Straßenverkehrsgesetzes selbst sind bisher keinerlei Einschränkungen vorgesehen (vgl. dazu auch Ziff. 2.2.4).

3.5.4.6
Zweckbindung der Straßenverkehrsregister

Die geplanten Dateien dürfen, folgt man dem Entwurf, für zahlreiche Zwecke verwertet werden. So sollen die gespeicherten Daten zunächst "für Auskünfte zur Verfolgung von Straftaten" zur Verfügung stehen, "die im Zusammenhang mit der Teilnahme am Straßenverkehr begangen werden"; gleiches gilt für bestimmte einschlägige Ordnungswidrigkeiten. Darüber hinaus können Angaben aber auch "für die Verfolgung von sonstigen Straftaten oder für die Strafvollstreckung", "für die Verfolgung von sonstigen Ordnungswidrigkeiten", "für die Abwehr von Gefahren für die öffentliche Sicherheit oder Ordnung" ohne jede weitere Einschränkung weitergegeben werden. Damit wird die Zweckbindung der Straßenverkehrsregister weitgehend zur Farce; sie stehen der Polizei praktisch unbegrenzt zur Verfügung. Nicht zuletzt angesichts der noch ausstehenden präzisen Regelungen für die Tätigkeit der Polizei zur Abwehr von Gefahren und zur Strafverfolgung muß dieser Katalog verringert werden. Dies gilt auch und gerade wegen der geplanten Einrichtung von Direktzugriffsverfahren, da diese - wie erwähnt - zusätzlich die wirksame datenschutzrechtliche Kontrolle erschweren.

Konkret bedeutet dies, daß die Register nicht zur Verfolgung von außerhalb des Verkehrsbereichs begangenen Ordnungswidrigkeiten zur Verfügung stehen sollten. Liegt kein Bezug zum Straßenverkehr vor, sollte nur die Abwehr erheblicher Gefahren für die öffentliche Sicherheit und Ordnung eine Übermittlungsbefugnis begründen. Eine Datenweitergabe zu Zwecken der Strafvollstreckung sollte nur dann zugelassen werden, wenn eine Überprüfung ergibt, daß die Durchsetzung der Strafvollstreckung im Einzelfall nicht unter Rückgriff auf andere Datenbestände gesichert werden kann.

Der vorliegende Gesetzentwurf wird als Antwort auf die im Urteil des Bundesverfassungsgerichts zur Volkszählung 1983 aufgestellte Forderung nach einer präzisen Zweckbindung zweifellos die Bedeutung eines "Musterentwurfs" für ein bereichsspezifisches Datenschutzgesetz erhalten. Deshalb darf der Gesetzgeber sich nicht darauf beschränken, bisher bereits praktizierte Übermittlungswege lediglich formalrechtlich abzusichern. Die Forderung nach einer konkreten Zweckbindung schließt seine Verpflichtung ein, in jedem Fall zu prüfen, auf welche Zwecke sich die Verarbeitung personenbezogener Daten in einer bestimmten Datei beschränken muß.

3.5.4.7
Nutzung durch Nachrichtendienste und Justizbehörden

Der Entwurf sieht vor, daß sowohl dem Bundesnachrichtendienst als auch dem Militärischen Abschirmdienst Daten aus dem zentralen Fahrzeugregister und den örtlichen Registern übermittelt werden dürfen. Für beide Dienste ist eine unverzichtbare Voraussetzung für Eingriffe in das Recht auf informationelle Selbstbestimmung noch nicht erfüllt: Es gibt keinerlei Rechtsnormen, die die personenbezogene Datenverarbeitung dieser Behörden regeln. Dies hat auch der Bundesinnenminister gesehen und deshalb im Entwurf selbst versucht, die Aufgaben dieser Stellen zu beschreiben, um ein Minimum an Zweckbindung für die weiterzugebenden Daten zu sichern.

Doch sind diese Formulierungen nicht nur unzureichend, sie stehen noch dazu am falschen Platz: Beide Dienste bedürfen einer eigenen gesetzlichen Regelung, die ihre Aufgaben und Befugnisse abschließend und präzise regelt. Solange solche Normen nicht vorliegen, kommt eine Übermittlung aus den Fahrzeugregistern an diese Stellen nicht in Betracht. Nur eine gesetzlich geregelte personenbezogene Datenverarbeitung beim Empfänger kann das Recht auf informationelle Selbstbestimmung der betroffenen Bürger ausreichend sichern.

Auf Bedenken stoßen schließlich die Bestrebungen, im zentralen Fahrzeugregister allgemein für Zwecke der Strafverfolgung oder der Strafvollstreckung durch die hierfür zuständigen Behörden, d.h. Staatsanwaltschaften und Gerichte, Suchvermerke und Steckbriefnachrichten über Beschuldigte oder Verurteilte, deren Aufenthalt unbekannt ist, speichern zu lassen. Die Gefahr ist unverkennbar, daß das zentrale Fahrzeugregister damit, auch was die Datenspeicherung angeht, in den direkten Zugriff dieser Dienststellen gerät und damit die Trennung von den Straßenverkehrsbehörden und deren Aufgabenstellung verwischt wird. Hier gilt es zu prüfen, ob nicht eine Regelung gefunden werden kann, die sicherstellt, daß das Kraftfahrtbundesamt als speichernde Stelle für die Führung seines Datenbestandes verantwortlich bleibt und dieser Datenbestand nicht über dessen Aufgabenstellung als Straßenverkehrsbehörde hinaus unnötig ausgedehnt wird.

3.6
Information des Bürgers

3.6.1
Mangelnde Transparenz der Datenverarbeitung

3.6.1.1
Notwendigkeit der Verbesserung

Die Wirksamkeit von Datenschutzregelungen läßt sich nicht zuletzt daran messen, inwieweit diese die Transparenz von Datenverarbeitung für den betroffenen Bürger erhöhen. Ein Maximum an Transparenz von Datenverarbeitung - das heißt möglichst umfassende Informationen über die angewendeten Verarbeitungsmethoden, die gespeicherten Daten, die Übermittlungswege und die Verknüpfungen zu anderen Verfahren - ist eine der Grundvoraussetzungen für effektive Datenschutzmaßnahmen und deren Kontrolle durch den Datenschutzbeauftragten. Darauf habe ich in den letzten Jahren immer wieder hingewiesen. Innenausschuß und Landtag haben sich dieses Problems angenommen und die Landesregierung gebeten, bei der anstehenden Novellierung des Bundesdatenschutzgesetzes und des Hessischen Datenschutzgesetzes u.a. für substantielle Verbesserungen bei der Information des Betroffenen einzutreten (Beschluß Nr. 7, Drucks. 11/1551).

Gewiß, vieles hat sich im Umfeld der Datenverarbeitung in den letzten Jahren geändert und erheblich verbessert. Andererseits: Regelungen über die Benachrichtigung des Betroffenen, wie sie der Bundesgesetzgeber in den §§ 26, 34 des BDSG zumindest für einen Teilbereich der Datenverarbeitung festgeschrieben hat, hat das Land Hessen für den öffentlichen Bereich nicht nachvollzogen. Man war der Meinung, wie im übrigen auch in allen anderen Bundesländern, eine wenn auch eingeschränkte Veröffentlichungspflicht und das durch den Datenschutzbeauftragten zu führende Dateienregister (§§ 17, 25 HDSG) genügten, um das erforderliche Mindestmaß an Transparenz zu garantieren. Rückblickend muß aber festgestellt werden, daß diese Regelungen dazu nicht ausreichen.

3.6.1.2
Veröffentlichung von Dateien

Die Veröffentlichung von Dateien durch die für die Datenverarbeitung verantwortlichen Stellen ist kontinuierlich erfolgt. Die Möglichkeit, daß diese Veröffentlichungen in den verschiedensten Publikationsorganen vorgenommen wurden - sie reichen vom Staatsanzeiger für das Land Hessen bis zum kleinsten Lokalblatt -, und die weitgehend unbestimmte Art der zu veröffentlichenden Inhalte der Datenverarbeitung - wie z.B. frei wählbare Beschreibung logisch zusammengehörender Datensätze, der Hinweis lediglich auf "regelmäßige" Übermittlungen an Dritte und das Fehlen von Angaben über die angewandten Verarbeitungsmethoden (z.B. Online) - haben, soweit sich dies aus den Erfahrungen der letzten Jahre ableiten läßt, dazu geführt, daß diese Information für den Bürger praktisch keinen Wert hat.

3.6.1.3
Das Dateienregister

Bleibt das Dateienregister. Ich habe den aktuellen Zustand dieses Registers, seine Stärken und Schwächen, seit 1979 in meinen Tätigkeitsberichten beschrieben. Unbestreitbar besitzt das Register inzwischen einen hohen Qualitätsstand und bietet z.B. dem Datenschutzbeauftragten zu Zwecken der Kontrolle umfangreiche Informationen. Es zeigt die Strukturen der Datenverarbeitung der öffentlichen Stellen und bietet Einblicke in Verfahren und Entwicklungstendenzen. Der Bürger dagegen, für den das Register in erster Linie gedacht war, denn sein gesetzlich verbriefter Anspruch auf Auskunft sollte ja erleichtert oder gar erst ermöglicht werden, kann mit diesen Informa-

tionen wenig anfangen. Grund: Das Register ist seiner Art nach vom Gesetzgeber so konzipiert, daß es als Nachschlagewerk, als eine Art "Datenatlas" genutzt werden kann. Es zeigt auf, welche öffentlichen Stellen Datenverarbeitung einsetzen und welche Daten (-arten) zu diesen Zwecken gespeichert werden; jeder Personenbezug ist (gewollt) ausgeschlossen. Hinweise auf die Sensitivität einzelner Verfahren oder der zur Verarbeitung bestimmten Daten fehlen. Datenarten werden vereinfachend zusammengefaßt und verbal - d.h. im Zweifel ungenau - beschrieben. Soweit verfahrensübergreifende Übermittlungen vorgesehen sind, ist deren Tragweite aus dem Register nicht ersichtlich.

Aber auch wenn diese Schwächen nicht wären: Wie soll ein Bürger seinen Auskunftsanspruch eigentlich realisieren, wenn ihm der Datenschutzbeauftragte auf Anfrage beispielsweise mitteilt, daß für sein soziales Umfeld (Anknüpfungspunkt ist hier der Wohnort) 50 öffentliche Stellen 150 verschiedene Dateien gemeldet haben. Eine engere Eingrenzung der für ihn relevanten Dateien und Verfahren ist aber in der Regel nicht möglich, da ja keine Angaben über die speziellen Lebensumstände des anfragenden Bürgers vorliegen. Überspitzt ausgedrückt: Einem Empfänger von Sozialhilfe mitzuteilen, daß seine Heimatgemeinde die Abgaben und Steuern auf Grundbesitz maschinell errechnet und das örtlich zuständige Finanzamt eine Datei der Einkommensmillionäre führt, ist ebenso sinnlos, wie den Millionär darauf hinzuweisen, daß zur Berechnung des auszuzahlenden Sozialhilfesatzes die Rentenhöhe gespeichert wird.

3.6.1.4
Probleme beim Auskunftsanspruch

Hinzu kommt eine weitere Schwachstelle. Der Bürger, der bei der Verwaltung Auskunft begehrt, sieht mit Recht seinen Namen als Anknüpfungspunkt dieses Verfahrens. Organisationsfachleute der Datenverarbeitung sehen dies aber oft anders. Der Namen ist eben nicht Mittelpunkt des jeweiligen DV-Verfahrens, sondern bestenfalls ein "Parameter", den es nach den vorgegebenen "Spielregeln" rationell zu verarbeiten gilt. Eine der verbreitetsten Methoden der rationellen Datenverarbeitung ist der Ersatz verbaler, also "störanfälliger" Komponenten, und dazu gehört auch der Name, durch maschinenfreundliche Zahlencodes. Bei Rückfragen an die Verwaltung sind diese oft bis zu 20-stelligen "Kontonummern" stets vollständig anzugeben (Beispiel: Grundstufe Finanzwesen - Bescheid über Grundsteuer und Benutzungsgebühren). Die Angabe des Namens allein ermöglicht es der Verwaltung eben noch lange nicht, festzustellen, ob Daten über einen bestimmten Bürger gespeichert sind. Diese Art des Auskunftsbegehrens setzt oft - und das ist tägliche Praxis - langwierige und kostenaufwendige Suchstrategien voraus. Eine denkbare Lösung, das "allwissende" Register mit Namen und Hinweisen auf alle Fakten, scheidet von vornherein aus. Diese Art einer "Super-Einwohnerdatenbank", vielleicht eines Tages technisch realisierbar, wäre das Ende jeglichen Datenschutzes.

3.6.2
Neuer Lösungsansatz: "Daten-Kontoauszug"

Wenn eine Reaktion auf eingeführte DV-Verfahren die aufgezeigten Schwierigkeiten aufwirft, gibt es noch die Möglichkeit der Aktion aus dem jeweiligen Verfahren heraus. Der Bürger wird nicht lediglich auf sein Recht hingewiesen, "Auskunft zu verlangen" und dann seinem Schicksal überlassen, sondern der Einsatz von Datenverarbeitung führt automatisch zu einer Auskunft oder korrekt zu einer "Benachrichtigung". Diese Benachrichtigung muß sich aber von der Lösung im Bundesdatenschutzgesetz deutlich unterscheiden. Es genügt eben nicht der allgemeine Hinweis, daß Daten erstmals gespeichert (§ 26 BDSG) oder erstmals übermittelt werden (§ 34 BDSG), sondern es muß ein aktueller "Kontoauszug" erzeugt werden.

3.6.2.1
Inhalt des Kontoauszugs

Der Kontoauszug muß den betroffenen Bürger ausreichend informieren. Unzulänglichkeiten der Information, wie sie z.Zt. das Dateienregister und allgemeine Veröffentlichungen enthalten, müssen ausgeschlossen werden. Das jeweilige DV-Verfahren ist also allgemeinverständlich zu beschreiben, die gespeicherten Daten sind ausnahmslos in verständlicher Form darzustellen. Soweit Schlüssel, Kennziffern oder ähnliches verwendet werden, sind diese auf ihre ursprünglichen Werte zurückzuführen. Bei einer Reihe von DV-Verfahren ergibt die Menge der gespeicherten Daten für den Betroffenen nur dann einen Sinn, wenn ihm der gesetzliche Hintergrund des Verfahrens und die daraus resultierenden Verarbeitungsparameter bekanntgegeben werden. Dies gilt insbesondere dann, wenn in DV-Verfahren aus erhobenen Daten und durch Programme vorgegebenen Parametern "neue" personenbezogene Daten maschinell errechnet werden (z.B. Lohnsteuerklasse, Höhe von einkommensabhängigen Leistungen, Abgaben und Gebühren). Besondere Verfahrensmerkmale wie Zugriffe auf externe Datenbanken und Rechner, Online-Zugriffe usw. sind, soweit notwendig, aufzuzeigen. Alle vorgesehenen Übermittlungen müssen dargestellt werden. Soweit in bestimmten Verfahren Übermittlungssperren vorgesehen sind, sind auch diese detailliert zu erwähnen.

3.6.2.2
Geeignete Verfahren

Sicher: Aus DV-technischer Sicht wäre es denkbar und optimal, unter einem einheitlichen Suchmerkmal - z.B. Personenkennzeichen - alle für einen Bürger relevanten Hinweise auf dessen in bestimmten Dateien gespeicherte Daten in einer zentralen "Kontoauszugsdatei" abzuspeichern. Dies würde aber unweigerlich dazu führen, daß jede nur denkbare Verknüpfung von unterschiedlichen Datensätzen aus verschiedenen Dateien leicht ermöglicht würde.

Alle Bestrebungen von seiten des Gesetzgebers oder der Verwaltung, einheitliche Such- oder Verknüpfungsmerkmale z.B. im Einwohnerwesen oder beim Bundespersonalausweis einzuführen, sind bisher gescheitert. Sie dürfen keinesfalls auf dem Umweg über den "Kontoauszug" neu belebt werden.

Wenn "Kontoauszüge" erstellt werden sollen, darf dies mithin nur aus dem jeweiligen Verfahren heraus geschehen. Dies bedeutet, daß auch die Suchstrategien nach bestimmten Daten - z.B. welcher Name zu welcher Kontonummer gehört - nur in dem jeweiligen Verfahren selbst durchgeführt und dazu evtl. erforderliche Tabellen nur für dieses Verfahren gespeichert werden dürfen.

Dabei müssen der mit einem "Kontoauszug" verbundene Aufwand und das erhoffte Mehr an Transparenz bzw. Information für den einzelnen Bürger in einem realistischen Verhältnis stehen. Einem Bürger in einem gesondert zugestellten, mit 80 Pfennig frankierten "Kontoauszug" mitzuteilen, wie er heißt, wo er wohnt und wann er geboren ist, und man habe diese Daten gespeichert, um ihm irgendwann einmal zu einem Jubiläum zu gratulieren, würde mit Recht Unverständnis hervorrufen. Vielmehr wäre gegenwärtig vorrangig die Information aus besonders sensitiven Bereichen wie z.B. der Verarbeitung von Sozialdaten wichtig. Von der Verfahrensseite her wäre der Einstieg bei landeseinheitlichen (auch kommunalen) DV-Verfahren, die zugleich Massenverfahren sind, denkbar.

Von der Anwendungsbreite und ihrem Inhalt her könnten sich für einen Versuch mit dem Kontoauszug eignen:

- das Sozialhilfeverfahren HES-SIAS mit allen Unterverfahren
- alle Verfahren im Gesundheitswesen (Patientenstammdatei, Finanzbuchhaltung)
- Renten- und Kostenbeiträge des Landeswohlfahrtsverbandes
- Darlehensverfahren des Landeswohlfahrtsverbandes
- Rentenauskunftsverfahren
- Verfahren Kommunales Finanzwesen (alle kommunalen Abgaben, Steuern und Gebühren, z.B. Kindergartenabrechnungen, Erschließungsbeiträge, Veranlagungskonten)
- Einwohnerwesen (Wehrerfassung, Wehrstammrolle, Lohnsteuerkartenregister, Wählerverzeichnisse)
- Kfz-Zulassung
- Ordnungswidrigkeitsverfahren.

Soweit es sich um Verfahren handelt, bei denen der Betroffene mitwirkt, indem er z.B. einen Antrag stellt, ist die Sache noch einfacher. Da in diesen Fällen ein Bescheid erteilt wird, könnte der Kontoauszug beigefügt werden und hätte für den Bewilligungszeitraum Gültigkeit. Bei Änderungen in der Person des Antragstellers oder in Verfahrensteilen erfolgt in der Regel eine neue Bescheidschreibung, also auch ein neuer Kontoauszug.

Bei bestehenden Verfahren sollten zuerst alle "Neuzugänge" mit Kontoauszügen versorgt werden. Für "Altfälle" müssen andere Lösungen gefunden werden. Umständlich und teuer wäre es, einen generellen Ausdruck aller Konten aus einem Massenverfahren zu erzeugen. Besser ist es, den Zeitpunkt abzuwarten, in dem die einzelnen Datensätze z.B. zu Terminarbeiten verarbeitet werden (Beispiel: Wahlbenachrichtigungen). Andererseits gibt es aber etwa im Einwohnerwesen Personen, die weder eine Lohnsteuerkarte erhalten noch wahlberechtigt sind (Ausländer). Sofern bei dieser Gruppe kein meldepflichtiger Vorgang (Umzug, Wegzug, Geburt eines Kindes o.ä.) eintritt, wird aus ihrem Datensatz keine Mitteilung an den Betroffenen erfolgen, dem ein "Kontoauszug" beigefügt werden könnte. Dies wären dann die Ausnahmefälle, die maschinell abgefragt und gesondert angeschrieben werden müßten.

Zusätzlicher Aufwand entstünde im Grunde genommen nur bei den datenverarbeitenden Stellen, also z.B. bei den Kommunalen Gebietsrechenzentren. Die Verwaltungen selbst wären im Regelfall weder mit zusätzlichen Personal- noch Sachkosten (Porto) belastet. Erfahrungsgemäß sind auch die Fälle, in denen die Identität eines Betroffenen vor Versendung des Kontoauszugs nochmals überprüft werden muß, gering (Namensgleichheit, gleicher Geburtstag o.ä.).

Kurzum: Der "Daten-Kontoauszug" bietet die Möglichkeit, die Transparenz der Datenverarbeitung zu erhöhen. Er muß aber unter Berücksichtigung der verfahrenstechnischen Besonderheiten gestaltet und eingesetzt werden.

4. Bilanz

4.1
Zum 12. Tätigkeitsbericht für 1983 (Drucks. 11/473)

4.1.1
Änderung des Kindergeldrechts (12. Tätigkeitsbericht Ziff. 3.2.5)

4.1.1.1
Datenaustausch zwischen Finanzbehörden und Kindergeldstellen

Die Entwicklung konzentrierte sich im Jahre 1984 auf den automatisierten Datenaustausch zwischen den Finanzverwaltungen der Länder und der Bundesanstalt für Arbeit mit ihren Kindergeldkassen (vgl. Ziff. 3.2.5.4). Am 5. Juli wurde zwischen den Länderfinanzministern und den zuständigen Bundesressorts (Bundesminister für Arbeit und Sozialordnung, Bundesminister der Finanzen, Bundesminister für Jugend, Familie und Gesundheit) sowie der Bundesanstalt für Arbeit die "Rahmenvereinbarung über einen Datenaustausch für die Berechnung des einkommensabhängigen Kindergeldes (RVDAKG)" abschließend erörtert. Sie stellt eine Empfehlung für eine bundeseinheitliche Regelung der Übermittlung von Steuerdaten an die Kindergeldkassen bei den Arbeitsämtern dar. Auf der Grundlage der RVDAKG haben der Hessische Finanzminister und die Bundesanstalt für Arbeit im November eine "Amtshilfevereinbarung" geschlossen, die ergänzende Punkte (HZD als annehmende Stelle, Kostentragung etc.) enthält. Erstmals werden von den Finanzverwaltungen Angaben aus den Steuererklärungen 1983 für das Leistungsjahr 1985 geliefert.

Die RVDAKG enthält eine detaillierte Festlegung des an dem Datenaustausch teilnehmenden Personenkreises, der Datensätze bei der Anfrage und der Rückmeldung, der Art und der Versandform der Datenträger usw. Mit dem neuen Verfahren wurde auch ein neuer Vordruck für die Ausfüllung durch die Kindergeldberechtigten eingeführt. Aus datenschutzrechtlicher Sicht sind vor allem folgende Punkte von Bedeutung:

1. Die Finanzverwaltung übermittelt der Bundesanstalt für Arbeit keine einzelnen Einkommensdaten, wenn die Einkommensgrenze des § 10 Abs. 2 des Bundeskindergeldgesetzes eindeutig über- oder unterschritten wird.

2. Grundsätzlich wird nur die Summe der Einkünfte gemeldet; es erfolgt also keine Aufschlüsselung der einzelnen Einkunftsarten des Kindergeldbeziehers. Die ursprünglich in der Rahmenvereinbarung vorgesehene Handhabung, daß jedenfalls bei solchen Steuerpflichtigen, die sog. "negative Einkünfte" geltend gemacht haben, auch die genau aufgegliederten Einkunftsarten mitgeteilt werden, wird vorläufig nicht praktiziert.

3. Antragsteller und ihre Ehegatten nehmen nur dann am Datenaustausch teil, wenn beide ausdrücklich schriftlich eingewilligt haben. Die Zustimmung kann jederzeit widerrufen werden.

4. Die Kindergeldbezieher werden ausführlich über die Modalitäten des Datenaustauschs, insbesondere auch die zur Übermittlung vorgesehenen Daten, informiert.

Die Rahmenvereinbarung und das auf ihr beruhende neue Verfahren der Ermittlung des maßgeblichen Einkommens für die Kindergeldberechnung berücksichtigt mithin zwei wichtige Grundvoraussetzungen für die Wahrung des Datenschutzes und des Steuergeheimnisses: Die übermittelten Informationen werden strikt auf den für die Bearbeitung der Kindergeldanträge erforderlichen Datensatz beschränkt. Zum anderen steht es dem Bürger frei, seine Zustimmung zu geben oder nicht. Die Formulierung des Einverständnisses auf dem Vordruck hätte allerdings präziser gefaßt werden können. Es bleibt anzumerken, daß sich die Finanzbehörden der Länder bei den Vorarbeiten für die RVDAKG intensiv für die Einhaltung des Steuergeheimnisses und die Berücksichtigung der von den Datenschutzbeauftragten in ihren Tätigkeitsberichten und zahlreichen Stellungnahmen gestellten Anforderungen für eine datenschutzgerechte Handhabung eingesetzt haben.

4.1.1.2
Alternative nach wie vor: Zusatzbescheinigung über die Einkommenshöhe

Dennoch bleiben Kritikpunkte: Für alle Kindergeldbezieher, die Bedenken gegen die Teilnahme am automatisierten Datenaustausch haben, bleibt es bei dem bisherigen unbefriedigenden Verfahren, daß sie entweder ihren gesamten Steuerbescheid vorlegen müssen oder eine Kopie, bei der sie die für die Leistungsberechnung nicht maßgeblichen Daten schwärzen können ("Kopierlösung"). Doch ist zum einen der Information in den Formularen nicht genau zu entnehmen, welche Angaben noch lesbar sein müssen. Vor allem aber wird verlangt, daß die Einkunftsarten auf keinen Fall unkenntlich gemacht werden dürfen, also auch in den Fällen, in denen es auf sie gar nicht ankommt. Mit anderen Worten besteht immer die Gefahr, daß den Kindergeldkassen für die Antragsbearbeitung nicht notwendige Steuerdaten zur Kenntnis gelangen.

Wenn man bedenkt, daß sich die Finanzverwaltung im Rahmen des automatisierten Datenaustausches in der Lage sieht, prinzipiell nur die Summe der Einkünfte des Kindergeldberechtigten an die Kindergeldkassen weiterzugeben (s. o. Ziff. 2.), will mir noch weniger einleuchten, warum der Hessische Finanzminister ebenso wie seine Länderkollegen den Vorschlag nicht nur der Datenschutzbeauftragten, sondern auch der Besoldungsressorts der Länder nach wie vor ablehnt (vgl. Stellungnahme der Landesregierung zu meinem 12. Tätigkeitsbericht, Drucks. 11/1258, zu Ziff. 3.2.5.3), eine gesonderte Zusatzbescheinigung zum Einkommensteuerbescheid auszudrucken, die nur diesen kindergeldrelevanten Betrag enthält. Damit würde eine Zweiteilung des Verfahrens für den Einkommensnachweis - hier automatisierter Abgleich, dort Vorlage der Nachweise - vermieden und für alle Fallsituationen die Beschränkung auf die erforderlichen Angaben gewährleistet. Ob eine solche Lösung - wie der Finanzminister meint - mehr Aufwand verursacht als die jetzige Praxis, ist zu bezweifeln.

Dies gilt insbesondere angesichts der Tatsache, daß es für die Kindergeldbezieher im öffentlichen Dienst Hessens (vgl. zur Sondersituation der bei der öffentlichen Hand Beschäftigten 12. Tätigkeitsbericht, Ziff. 3.2.5.5) bei der bisherigen Handhabung ("Kopierlösung") bleibt. Eine Anfrage des Hessischen Ministers des Innern bei der Zentralen Besoldungsstelle und der Zentralen Vergütungs- und Lohnstelle, ob sie eine Abwicklung ihrer Kindergeldfälle entsprechend der RVDAKG in Form eines Datenaustauschs befürworten, wurde von beiden Behörden ablehnend beantwortet. Eine Verfahrensvereinfachung oder Arbeitsentlastung werde nicht erreicht. Beide Stellen haben sich vielmehr dem o.a. Vorschlag angeschlossen, daß die Finanzbehörden eine zusätzliche Bescheinigung für die Vorlage bei den Kindergeldstellen zur Verfügung stellen.

4.1.2
Patientengeheimnis in der Psychiatrie - Datenerhebung nach § 184 RVO
(12. Tätigkeitsbericht, Ziff. 3.2.4)

Aus meiner Kritik an der Verwendung des umfangreichen "Formulars zur Feststellung der Krankenhauspflegebedürftigkeit" nach § 184 der Reichsversicherungsordnung (RVO) durch die gesetzlichen Krankenkassen haben die Betroffenen inzwischen Konsequenzen gezogen. Trotz ursprünglich negativer Prognose für eine Einigung konnte zwischen den Beteiligten - den Verbänden der gesetzlichen Krankenkassen und dem Landeswohlfahrtsverband als Träger der betroffenen psychiatrischen Krankenhäuser - eine Vereinbarung über ein abgestuftes Auskunftsverfahren getroffen werden. Ich habe mich intensiv an den Vermittlungsbemühungen beteiligt. Der gefundene Kompromiß kann aus datenschutzrechtlicher Sicht insoweit begrüßt werden, als er bei aller Anerkennung des legitimen Informationsbedürfnisses der Krankenkassen die Übermittlung von Patientendaten sowohl in der Häufigkeit wie im Umfang einzuschränken geeignet ist.

Die "Empfehlung für ein gestuftes Auskunftsverfahren vor Abgabe von Stellungnahmen zur Krankenhauspflegebedürftigkeit im Sinne des § 184 RVO/§ 17 KVLG durch den Sozialärztlichen Dienst der LVA Hessen für die Krankenkassen in Hessen" hat folgenden Wortlaut:

"1. Bei Erst-/Wiederaufnahmen von Patienten in Psychiatrischen Krankenhäusern erteilen im allgemeinen die Krankenkassen auf Antrag und nach ärztlicher Begründung der Notwendigkeit eine befristete Kostenzusage. Dabei werden die vom Landesvertrauensarzt erstellten "Verweildauerrichtwerte" für die Begutachtung der Krankenhauspflegebedürftigkeit beachtet.

2. Sobald absehbar ist, daß Krankenhauspflegebedürftigkeit im Sinne des § 184 RVO/§ 17 KVLG weiterhin vorliegt, wird rechtzeitig ein Kostenverlängerungsantrag gestellt, dem eine ärztliche Stellungnahme nach beiliegendem Vordruck beizufügen ist.

In den erforderlichen Fällen schalten die Krankenkassen den Sozialärztlichen Dienst ein. Dieser kann eine gutachterliche Stellungnahme nur abgeben, wenn ihm alle für die Begutachtung relevanten Angaben (aktuelle Krankheitssymptomatik, Befunde, Krankheitsverlauf, Behandlungsmaßnahmen usw.) vorliegen. In Einzelfällen wird auf Anforderung des Sozialärztlichen Dienstes ein formloser ergänzender Arztbericht nachgereicht.

3. In solchen Fällen, in denen der Sozialärztliche Dienst in seiner Stellungnahme zum Ausdruck bringt, daß die Kriterien der Krankenhauspflegebedürftigkeit nicht vorliegen, hat die Krankenkasse die wesentlichen Ablehnungsgründe dem Krankenhaus mitzuteilen.

4. Krankenakten werden an die Krankenkassen und an die Sozialärztlichen Dienststellen nicht übersandt.

   Soweit im Widerspruchsverfahren erforderlich, werden Krankenakten - ggf. kopierte Auszüge, die Drittgeheimnisse aussparen - im verschlossenen Umschlag direkt dem Landesvertrauensarzt übersandt."

Gegenüber der bisherigen Verfahrensweise ergeben sich für mich folgende Verbesserungen:

1. Für die "Ärztliche Stellungnahme zur Begründung der Krankenhauspflegebedürftigkeit gemäß § 184 RVO", die die Verlängerung der Kostenzusicherung begründen soll, wird ein erheblich kürzeres Formular verwandt als bisher (vgl. den Abdruck des bisherigen Erhebungsbogens im 12. Tätigkeitsbericht, Drucks. 11/473, S. 49).

2. Daten von Psychiatriepatienten werden voraussichtlich seltener von den Krankenhäusern erfragt als bisher, nämlich in der Regel erst nach Ablauf einer in einer Richtlinie des Landesvertrauensarztes festgelegten Verweildauer, die je nach Krankheitsbild differiert. Die Beteiligten waren sich dabei einig, daß die in dieser Richtlinie genannten "Verweildauerrichtwerte" keine Höchstfristen darstellen, sondern einen durchschnittlichen Erfahrungswert.

3. Die Übersendung von Patientenunterlagen über den Vordruck hinaus wird eingeschränkt und damit das Erforderlichkeitsprinzip genauer beachtet. Komplette Krankenakten werden anders als bisher grundsätzlich überhaupt nicht weitergeleitet, weder an die Krankenkassen noch an den Sozialärztlichen Dienst. Eine Ausnahme besteht nur für das Widerspruchsverfahren, d.h. nach Ablehnung der Kostentragung durch die Kasse, nur für den Landesvertrauensarzt und nur für den Fall, daß kopierte Auszüge etc. nicht ausreichen.

Das neue "abgestufte Auskunftsverfahren" soll zunächst für ein Jahr eingeführt und in der Praxis erprobt werden. Für die einzelnen Krankenkassen stellt die Abmachung allerdings nur eine Empfehlung dar. Insofern kommt viel auf deren Akzeptanz der neuen Handhabung trotz fehlender Verbindlichkeit an. Ich werde mich im kommenden Jahr bei psychiatrischen Krankenhäusern ebenso wie bei einzelnen Krankenkassen über die Einhaltung des neuen Verfahrens informieren.

4.1.3
PIOS-Datei "Staatsgefährdung"
(12. Tätigkeitsbericht Ziff. 2.1.3.2; 11. Tätigkeitsbericht Ziff. 3.2.2.2.3)

Im 11. und 12. Tätigkeitsbericht hatte ich meine grundsätzlichen Bedenken gegen die geplante Datei PIOS-Staatsgefährdung dargelegt. Hierbei handelt es sich um eine sogenannte Verbunddatei, die von Bund und Ländern gemeinsam betrieben wird.

Im Vordergrund meiner Kritik standen folgende Gesichtspunkte:

- In der polizeilichen Praxis wird der Begriff des "Staatsschutzes" bzw. der "Staatsgefährdung" sehr weit ausgelegt. Als maßgeblich wird nicht lediglich die Begehung bestimmter objektiver Straftatbestände wie z.B. Friedensverrat, Hochverrat und Gefährdung des demokratischen Rechtsstaates angesehen, sondern darüber hinaus auch die Zielrichtung des Täters; jeder Straftatbestand kann daher grundsätzlich von dem einzelnen Polizeibeamten als Staatsschutzdelikt qualifiziert werden. Dies führt zu einer sehr weitgehenden, kaum präzisierbaren, damit auch schwer kontrollierbaren Etikettierung von Straftatverdächtigen.

- Charakteristisch für das PIOS-Konzept ist die Speicherung von sog. Vorfelddaten, d.h. von Daten über Personen, bei denen weder ein konkreter Straftatverdacht noch eine "konkrete Gefahr" im Sinne des Polizeirechts vorliegt. Für die Aufzeichnung von Informationen über einen derart vage beschriebenen Personenkreis besteht nicht nur keine Rechtsgrundlage (vgl. dazu 3.5.2.1), sie macht darüber hinaus die gesellschaftspolitische Problematik der "Vorverlagerung" polizeilicher Datenverarbeitung deutlich. Auch wurde das PIOS-Konzept speziell für die Bekämpfung des Terrorismus entwickelt. Den dagegen vorgetragenen Bedenken wurde die besondere Gefährlichkeit des Terrorismus entgegengehalten. Wenn eine Erweiterung dieses Konzepts auf den gesamten Bereich der Staatsschutzdelikte erfolgt, ist die Verhältnismäßigkeit der Mittel nicht gegeben.

- Der Entwurf der Errichtungsanordnung für die Datei ist zu unbestimmt.

Durch das Zusammentreffen dieser Kritikpunkte potenziert sich die Gefahr, daß hier eine umfangreiche Sammlung von Daten über politisch kritisch eingestellte Bürger entsteht.

In ihrer Stellungnahme zu meinem 11. Tätigkeitsbericht (Drucks. 10/659, zu 3.2.2.2.3) hatte die Landesregierung die vorgesehene Errichtungsanordnung als hinreichend präzise angesehen. Sie hatte entgegnet, daß etwa Ermittlungsverfahren wegen Beleidigung oder Nötigung "nicht ohne weiteres" als Staatsschutzdelikt in der Datei PIOS-Staatsgefährdung erfaßt werden sollen. Diese Ausführungen sind jedoch nicht geeignet, meine Bedenken zu widerlegen, sie bestätigen sie vielmehr. In ihrer Stellungnahme zu meinem 12. Tätigkeitsbericht (Drucks. 11/1258, zu 2.1.3.2) weist die Landesregierung lediglich darauf hin, daß die PIOS-Datei Staatsgefährdung in der geplanten Form nicht realisiert werde. Zu einem noch nicht absehbaren Zeitpunkt solle nunmehr eine "Arbeitsdatei PIOS-Innere Sicherheit" (APIS) eingerichtet werden. Diese werde sowohl die Daten enthalten, die bisher für die Datei PIOS-Staatsgefährdung vorgesehen waren, als auch diejenigen Daten, die bisher in der Datei PIOS-Terrorismus gespeichert wurden.

Anläßlich der Beratung meines 12. Tätigkeitsberichtes hat der Landtag die Landesregierung gebeten, im Innenausschuß über den Stand des Ausbaus dieser neuen Datei (APIS) und die weiteren Planungen zu berichten, insbesondere über den Personenkreis, der in dieser Datei gespeichert werden soll sowie über die vorgesehenen Löschungsfristen. Hierbei solle auch auf die vom Hessischen Datenschutzbeauftragten vorgetragenen Bedenken eingegangen werden (Beschluß Nr. 8, vgl. Beschlußempfehlung des Innenausschusses, Drucks. 11/1551). Dieser Bericht ist bisher nicht erfolgt. Der Hessische Minister des Innern hat mir jedoch inzwischen mitgeteilt, daß APIS jetzt zur Verfügung stehe, und mir den neuen Entwurf einer Errichtungsanordnung zugeleitet.

Meiner bisherigen Kritik ist in diesem neuen Entwurf jedoch nicht Rechnung getragen worden. Dies ist um so problematischer, weil in APIS noch mehr Daten, nämlich die aus dem Bereich der Terrorismusbekämpfung und die aus den sonstigen Staatsschutzbereichen, zusammengefaßt werden. Der Kreis der in APIS zu speichernden Personen ist erst recht nicht klar umgrenzt. Aufnahme finden sehr unterschiedliche und in keiner Weise miteinander vergleichbare Sachverhalte; schwerste Gewaltverbrechen stehen neben Bagatelldelikten. Ich habe daher dem Innenminister mitgeteilt, daß ich gegen eine Zustimmung Hessens zur APIS-Errichtungsanordnung und eine Beteiligung an dieser Datei grundsätzliche Bedenken habe. Er hat daraufhin seine Zustimmung nicht erteilt und seine abschließende Stellungnahme bis zum Abschluß der Erörterungen im Landtag zurückgestellt.

4.1.4
Hinweis-und Spurendokumentationssysteme
(12. Tätigkeitsbericht, Ziff. 2.1.3.3; 11. Tätigkeitsbericht, Ziff. 3.2.2.2.4)

Hinweis- und Spurendokumentationssysteme (abgekürzt "HIDOK" bzw. "SPUDOK") werden in Hessen in zunehmendem Maße eingesetzt. Sie dienen der Bearbeitung von Groß- bzw. Sammelverfahren, bei denen eine große Anzahl von Hinweisen und Spuren verarbeitet werden müssen. Der Einsatz von HIDOK erfolgt grundsätzlich für begrenzte Zeit bei der sachbearbeitenden Dienststelle. Sämtliche Hinweise, Spuren, Ermittlungsergebnisse und polizeiliche Maßnahmen werden in die jeweilige Datei eingespeichert. Mehrdimensionale Recherchen unter den verschiedensten Verknüpfungsgesichtspunkten sind mit HIDOK möglich.

Im 11. und 12. Tätigkeitsbericht habe ich die mit dem Einsatz von HIDOK verbundenen Probleme ausführlich dargelegt. Im Vordergrund stand dabei die Frage der Löschung der Daten. Nach Auffassung des Hessischen Ministers des Innern müssen alle in HIDOK gespeicherten Daten bis zum rechtskräftigen Abschluß des jeweiligen Verfahrens bzw. bis zur Verfolgungsverjährung ohne Ausnahme gespeichert bleiben, d.h. auch die Daten solcher Bürger, die nach Einschätzung der Polizei als Unbeteiligte anzusehen sind.

Diese Auffassung hat bedenkliche Konsequenzen: Im Vergleich zu HEPOLIS ist die Schwelle der automatisierten Speicherung bei HIDOK vorverlegt. In HEPOLIS werden diejenigen Personen erfaßt, gegen die ein Ermittlungsverfahren eröffnet wurde. Hingegen wird in HIDOK jeder Hinweis bzw. jede Spur ohne Ausnahme eingespeichert. Konkret bedeutet dies, daß auch die Daten jedes Bürgers, der in irgendeinem Zusammenhang mit dem jeweiligen Ermittlungsverfahren bekannt wird, aufgenommen werden, der Personenkreis ist daher erheblich weiter. Da es jedoch Jahre dauern kann, bis ein Groß- bzw. Sammelverfahren rechtskräftig abgeschlossen ist, läuft die Auffassung des Innenministers darauf hinaus, daß dieser Personenkreis vielfach länger gespeichert wird als die in HEPOLIS erfaßten Bürger.

Das Problem verschärft sich, wenn der Einsatz von HIDOK über die ursprünglich entwickelte Konzeption hinaus erfolgt, wie dies gegenwärtig bereits in Hessen der Fall ist: HIDOK wird nicht mehr lediglich für die Bearbeitung von Groß- bzw. Sammelverfahren benutzt, sondern darüber hinaus auch für die generelle Bearbeitung bestimmter Arten von Straftaten. Im 12. Tätigkeitsbericht hatte ich dargelegt, daß das LKA eine SPUDOK-Datei für Ermittlungen zu Anschlägen auf US-Einrichtungen errichtet hat. In diese Datei werden seit Ende 1981 alle Hinweise und Spuren aufgenommen, die möglicherweise im Zusammenhang mit einem derartigen Anschlag stehen. Bei den Tatverdächtigen handelt es sich um ganz verschiedene Personenkreise. Dementsprechend werden auch die jeweiligen Strafverfahren nicht verbunden. Wenn HIDOK in dieser Weise für die Bekämpfung bestimmter Arten von Straftaten eingesetzt wird, läuft dies auf eine zeitlich völlig unbegrenzte Speicherung aller darin enthaltenen personenbezogenen Daten hinaus.

In ihrer Stellungnahme zu meinem 12. Tätigkeitsbericht (zu 2.1.3.3) hat die Landesregierung an ihrer Auffassung festgehalten, daß die in HIDOK enthaltenen Daten bis zum rechtskräftigen Abschluß des jeweiligen Verfahrens ausnahmslos gespeichert bleiben müßten. Zur Frage, welche konkreten Konsequenzen dies für die Dauer der Speicherung der betroffenen Bürger hat, hat sie nicht Stellung genommen. Zu der von mir im Bericht erwähnten HIDOK-Datei für Anschläge auf US-Einrichtungen wird nur mitgeteilt, daß lediglich bei einem "erkennbaren Zusammenhang mit den unaufgeklärten Anschlägen" ein Grund bestehe, zukünftige vergleichbare Straftaten in diese Datei einzubeziehen. Diese fragmentarische Äußerung zu den von mir angesprochenen Problemen läßt allerdings die zentralen Fragen, wie die bisherige Nutzung dieser Datei zu beurteilen ist und in welchem Umfang HIDOK in Zukunft eingesetzt werden soll, weitgehend offen. Auf das Problem, daß bei dieser Art des Einsatzes von HIDOK zeitlich nicht begrenzte Speicherungen von Bürgern, u.a. auch von völlig unbeteiligten, vorgenommen werden, geht die Landesregierung nicht ein.

Im Rahmen der Beratungen zu meinem 12. Tätigkeitsbericht sind die mit dem Einsatz von HIDOK zusammenhängenden Fragen in der Arbeitsgruppe Datenschutz des Innenausschusses eingehend diskutiert worden. Im Anschluß daran hat der Landtag die Landesregierung gebeten, "dafür Sorge zu tragen, daß die Nutzung des polizeilichen Hinweis- und Spurendokumentationssystems (HIDOK/SPUDOK) nur aufgrund im Einzelfall erlassener Errichtungsanordnungen erfolgt. Diese müssen eine ständige Überprüfung und Bereinigung des Datenbestandes vorschreiben, damit insbesondere die Daten solcher Personen, gegen die sich ein ursprünglicher Verdacht nicht bestätigt hat, nach kurzer Frist gelöscht werden" (Beschluß Nr. 9 zum 12. Tätigkeitsbericht, vgl. Drucks. 11/1551). Bisher liegen mir diese Errichtungsanordnungen noch nicht vor. Eine Fortsetzuung der bisherigen Speicherungspraxis ist aber nicht hinnehmbar.

4.1.5
Auswertung von Protokolldaten der Polizei
(12. Tätigkeitsbericht, Ziff. 3.1.4)

Bei der Speicherung personenbezogener Daten auf Protokollbändern zu Zwecken der Datenschutzkontrolle (§ 10 HDSG) geraten zwei Datenschutzaspekte in Konflikt: Werden die Daten weiterhin aufbewahrt, so kann festgestellt werden, ob ordnungsgemäß und rechtmäßig zugegriffen, geändert und übermittelt wurde. Auf der anderen Seite besteht entsprechend lange die Gefahr des Mißbrauchs und der zweckwidrigen Auswertung (vgl. 12. Tätigkeitsbericht, insbes. Ziff. 3.1.4.4).

Zweck der Protokollierung kann nur die Sicherung einer fehlerfreien Datenverarbeitung und die Nachweismöglichkeit für die Datenschutzkontrolle sein. Die Daten dürfen nur für diese Zwecke genutzt werden.

Die Dauer der Aufbewahrung der Protokollbänder muß im Hinblick auf diesen Zweck konkret festgelegt werden. Dies ist insbesondere auch im Hinblick auf die in diesem Jahr beschlossene Einführung des maschinenlesbaren Personalausweises von Bedeutung, denn dieser Ausweis wird zu einer wesentlich häufigeren Datenabfrage durch die Polizei führen (ausführlich zum maschinenlesbaren Personalausweis Ziff. 3.5.3).

In ihrer Stellungnahme zum 12. Tätigkeitsbericht (Drucks. 11/1258, zu 3.1.4.4) hat die Landesregierung sich meiner Auffassung angeschlossen, daß die Protokolldaten ausschließlich zu Zwecken der Datenschutzkontrolle personenbezogen ausgewertet werden dürfen. In der Zwischenzeit hat ein ausführliches Gespräch zwischen dem Hessischen Minister des Innern und mir stattgefunden. Dabei wurde folgende Verfahrensweise festgelegt:

1. Die Protokolldaten werden künftig nicht mehr für kriminalpolizeiliche Zwecke verwandt.

2. Andere personenbezogene Auswertungen dürfen von der Polizei nur noch mit Zustimmung des Innenministers vorgenommen werden. Der Datenschutzbeauftragte ist jeweils zu unterrichten.

3. Die Log-Daten werden wie seither zu Zwecken der Datensicherung ("checkpoint restart" bzw. "recovery") sechs Wochen unverändert gespeichert. Anschließend erfolgt ein maschineller "Verdichtungslauf", in welchem alle Daten über interne Betriebszustände, die lediglich der System- und Netzwerksteuerung sowie -überwachung dienen, entfernt werden. Dies geschieht ausschließlich zur besseren Ausnutzung der Bandkapazitäten, da diese Betriebsdaten zum Zeitpunkt des Verdichtungslaufs nicht mehr benötigt werden. Die so erzeugten Datenbänder werden nicht wie bisher unbefristet, sondern nur noch drei Jahre aufbewahrt und dann gelöscht.

4.1.6
Landes- und Kommunalstatistik
(12. Tätigkeitsbericht, Ziff. 1.2.1. Nr.2)

Einer der Beschlüsse des Hessischen Landtages zu meinem 12. Tätigkeitsbericht enthielt die Bitte an die Landesregierung, "bis Oktober 1984 zu prüfen und zu berichten, inwieweit für den Bereich der Landes- und Kommunalstatistik gesetzliche Änderungen als Konsequenz aus dem Volkszählungsurteil erforderlich werden" (Beschluß Nr. 5 der Beschlußempfehlung des Innenausschusses, Drucks. 11/1551). In ihrem Bericht vom 30. Oktober hat sich die Landesregierung meiner Auffassung (vgl. 12. Tätigkeitsbericht, Ziff. 1.2.1, Nr. 2) angeschlossen und im Gegensatz zu früheren Äußerungen die Erforderlichkeit eines Landesstatistikgesetzes bejaht. Hinter diesem Standpunkt steht nicht zuletzt die Erwägung, daß künftig auch landesstatistische Erhebungen notwendig werden können, die ebenso wie die Volkszählung und der Mikrozensus auf einer Auskunftspflicht des Bürgers basieren.

Nach Auffassung der Landesregierung zeichnen sich für ein Landesstatistikgesetz bisher folgende Regelungskomplexe ab: Gesetzliche Verankerung des Statistischen Landesamtes, Kommunalstatistik, Planungsdatenbanken des Landes, Statistikorganisation (Erhebungsstellen, Abschottung vom Verwaltungsvollzug usw.), Befragungen mit und ohne Auskunftspflicht des Bürgers.

Im Hinblick darauf, daß das neue Volkszählungsgesetz die Organisation der Erhebung landesrechtlichen Bestimmungen vorbehalten wird (vgl. Ziff. 3.2.2.2), halte ich die Verabschiedung eines Landesstatistikgesetzes noch vor der Durchführung der Volkszählung - im Gesetzentwurf ist dafür der April 1986 vorgesehen - für angebracht.

4.1.7
Archivgesetz
(12. Tätigkeitsbericht, Ziff. 4.1; 11. Tätigkeitsbericht, Ziff. 2.3; 10. Tätigkeitsbericht, Ziff. 3.2)

Der Bitte des Landtags, ihm einen Vorschlag für ein Archivgesetz zu unterbreiten (Beschluß Nr. 17 zu meinem 12. Tätigkeitsbericht, vgl. Beschlußempfehlung des Innenausschusses, Drucks. 11/1551), will die Landesregierung zumindest auf absehbare Zeit offensichtlich nicht nachkommen. Der Hessische Minister für Wissenschaft und Kunst hat zu diesem Beschluß in dem Sinne Stellung genommen, er wolle sich die Erfahrungen zunutze machen, die mit den Gesetzesvorhaben in anderen Ländern gesammelt wurden. Es werde geprüft, welche Regelungen für Hessen brauchbar seien.

Dazu ist festzuhalten: Zeit für diese Prüfung gab es ebenso genug wie ausformulierte Regelungsvorschläge. Schon in meinem 10. Tätigkeitsbericht hatte ich einen Diskussionsentwurf für ein Hessisches Archivgesetz vorgestellt, der unter kompetenter fachlicher Beratung durch die hessischen Staatsarchive erarbeitet worden war (10. Tätigkeitsbericht, Drucks. 9/5873, 3.2). Der Entwurf eines Bundesarchiv-Gesetzes, der von der Bundesregierung vorgelegt worden ist und sich derzeit im Gesetzgebungsgang befindet (vgl. Bundesrats-Drucks. 371/84), enthält zahlreiche Anregungen, die - entgegen der Auffassung des Hessischen Ministers für Wissenschaft und Kunst - auch für eine landesgesetzliche Normierung von großem Interesse sind. Schließlich habe ich diesem Ressort einen Musterentwurf übersandt, der von einer Arbeitsgruppe der Datenschutzbeauftragten zusammengestellt worden ist.

Ich kann nur wiederholen: Ein Archivgesetz stellt keinen Beitrag zu einer überflüssigen Gesetzesflut dar, sondern einen unverzichtbaren Rahmen für die Regelung der Aufbewahrung und Nutzung historischer Dokumente und damit für die Gewährleistung der Geschichtsforschung.

4.2
Zum 11. Tätigkeitsbericht für 1982 (Drucks. 10/166)

4.2.1
Personaldaten und Personalakten der Lehrer
(11. Tätigkeitsbericht, Ziff. 5.1; 12. Tätigkeitsbericht, Ziff. 2.1.5)

Im Oktober 1983 hatte mir der Hessische Kultusminister seinen Erlaßentwurf zur Personalaktenführung der Lehrer zugeleitet. Im 12. Tätigkeitsbericht (2.1.5) hatte ich meine Ergänzungs- und Verbesserungsvorschläge dargestellt. Der Erlaß ist am 23. Februar 1984 ergangen (vgl. Amtsblatt des Hessischen Kultusministers, 3/84, S. 146) und enthält alle Anregungen, die ich gegeben hatte.

Kernstück des Erlasses ist die Festlegung eines abgestuften Datenkatalogs, der differenziert nach Schulen und Staatlichen Schulämtern die für die Führung der Personalnebenakten der Lehrer erforderlichen Angaben enthält. Von besonderer Bedeutung ist - angesichts der schnellen Verbreitung von Klein- und Tischcomputern an hessischen Schulen - das in dem Erlaß enthaltene Verbot, die Daten aus den Lehrerakten in schuleigene DV-Geräte einzuspeichern.

4.2.2
Gesundheitsdaten in Personalakten des öffentlichen Dienstes
(11. Tätigkeitsbericht, Ziff. 5.2; 12. Tätigkeitsbericht, Ziff. 2.1.6)

4.2.2.1
Übermittlung amtsärztlicher Zeugnisse an den Dienstherrn
(11. Tätigkeitsbericht, Ziff. 5.2.3, 5.2.4; 12. Tätigkeitsbericht, Ziff. 2.1.6.1)

4.2.2.1.1
Vorgelegte Entwürfe

In seinem Beschluß Nr. 10 zu meinem 12. Tätigkeitsbericht hat der Landtag die Landesregierung gebeten, "bis zum 31. Dezember 1984 ihre bereits zugesagten Regelungsvorschläge zur Begrenzung der Übermittlung von Gesundheitsdaten an die personalführenden Stellen vorzulegen, mit dem Datenschutzbeauftragten abzustimmen und der Arbeitsgruppe Datenschutz und Datenverarbeitung darüber zu berichten".

Der Hessische Minister des Innern hat im Oktober einen Erlaßentwurf zum "Inhalt ärztlicher Gutachten und Zeugnisse in dienstrechtlichen Angelegenheiten" vorgelegt, dem die anderen Ressorts zugestimmt haben. Dieser Erlaßentwurf sieht vor, daß

a) die personalverwaltenden Stellen den Untersuchungsauftrag an den Amtsarzt oder sonstigen die Gesundheitsprüfung vornehmenden Mediziner genau zu beschreiben haben,

b) der untersuchende Arzt in der Regel nur das zusammenfassende Ergebnis der Untersuchung übersendet und

c) zusätzliche ärztliche Informationen nur in bestimmten Ausnahmefällen angefordert werden können.

Im November hat der Innenminister weiterhin eine Ergänzung des "Erlasses betr. die Aufbewahrungsbestimmungen für Akten und sonstiges Schriftgut der Dienststellen des Landes Hessen" vom 10. August 1978 vorgelegt, der die längerfristige Aufbewahrung von ärztlichen Unterlagen aus Anlaß ärztlicher Untersuchungen für dienstrechtliche Zwecke regeln soll, soweit es sich um Untersuchungsstellen im Bereich der Landesverwaltung handelt.

Ende November schließlich hat der Hessische Minister für Arbeit, Umwelt und Soziales dem Innenminister und mir seinen "Entwurf einer Verordnung zur Änderung der Zweiten Durchführungsverordnung zum Gesetz über die Vereinheitlichung des Gesundheitswesens" zugeleitet. Dieser Regelungsvorschlag richtet sich an die Gesundheitsämter bzw. Amtsärzte. Er schreibt ihnen - entsprechend den im o.a. Erlaßentwurf enthaltenen Bestimmungen - vor, grundsätzlich nur das Ergebnis der medizinischen Eignungsprüfung an die personalführenden Stellen mitzuteilen, und zwar in Form eines einheitlichen Vordrucks. Zusätzliche ärztliche Informationen sollen dann übermittelt werden können, wenn dies sich in bestimmten Fällen, etwa bei "begründeten Zweifeln an der Vollständigkeit oder Aussagefähigkeit des Ergebnisses", als notwendig erweist und der Betroffene nach Belehrung über Umfang und Inhalt der weiterzuleitenden Angaben nicht widersprochen hat. Außerdem sind Vorschriften über die Aufbewahrungsfristen der medizinischen Dokumentation und über die Archivierung enthalten.

4.2.2.1.2.
Notwendige Änderungen

Beiden Entwürfen kann bescheinigt werden, daß sie einen großen Schritt in Richtung auf eine wirksame Begrenzung des medizinischen Datenflusses bei Untersuchungen in dienstrechtlichen Angelegenheiten darstellen und damit der Intention meiner in den letzten Tätigkeitsberichten geäußerten Auffassung sowie des Beschlusses des Landtages gerecht werden. Dennoch erscheinen mir Korrekturen bzw. Verbesserungen angebracht, die ich in meinen umfangreichen Stellungnahmen an die beiden Ressorts angeregt habe. Mir geht es, zusammengefaßt, um folgende Punkte:

1.
Die Regelungen für die personalführenden Stellen sowie für die Behörden, die die ärztlichen Prüfungen vornehmen, müssen so weit wie möglich textlich übereinstimmen, um Mißverständnisse zu vermeiden und eine einheitliche Handhabung zu gewährleisten. Dafür sind noch Korrekturen der Formulierungen erforderlich.

2.
Das Einsichtsrecht des untersuchten Bediensteten oder Stellenbewerbers in seine ärztlichen Unterlagen muß klargestellt werden. Dies ist inzwischen, jedenfalls im Erlaßentwurf des Innenministers, aufgenommen.

3.
Die Übermittlung und Anforderung weiterer medizinischer Informationen über das zusammenfassende Beurteilungsergebnis hinaus muß von der vorherigen Einwilligung des Betroffenen abhängig gemacht werden. Für die Entbindung von der ärztlichen Schweigepflicht hinsichtlich dieser zusätzlichen, in aller Regel sehr "sensitiven" Anamnese- und Diagnosedaten reicht es nicht aus, den fehlenden Widerspruch des Untersuchten als stillschweigende Zustimmung zu werten, wie es der Verordnungsentwurf des Sozialministers vorsieht. Der Betroffene muß die Möglichkeit haben, über die detaillierte Offenbarung seines Gesundheitszustands selbst zu bestimmen und sie ggf. zu verhindern, wenn er auf die vorgesehene dienstrechtliche Maßnahme (z.B. die Einstellung) verzichten will.

4.
Die Fallgruppen, in denen zusätzlich Befunde und Diagnosen angefordert bzw. weitergegeben werden, müssen genauer als bisher gefaßt werden. So ist etwa die Übermittlungskategorie der "Zweifel an der Vollständigkeit, Aussagefähigkeit oder dem Ergebnis der Untersuchung" so weit formuliert, daß nicht ausgeschlossen werden kann, daß personalverwaltende Stellen in jedem Untersuchungsfall von dieser - eigentlich als Ausnahme gedachten - Möglichkeit Gebrauch machen. Die Begrenzung dieser Sonderfälle gilt ungeachtet der Tatsache, daß ohnehin das Einverständnis des Betroffenen gegeben sein muß. Dies deshalb, weil der Untersuchte in der abhängigen Situation des Stellenbewerbers bzw. Bediensteten die Einwilligung auf Verlangen des Dienstherrn bzw. Arbeitgebers in der Regel kaum wird verweigern können.

Für die große Mehrzahl der Fälle, in denen der Gesundheitstest nach der präzisen Vorgabe des Untersuchungsauftrags durch die jeweilige Dienststelle uneingeschränkt positiv ausfällt, sehe ich ohne näheren Beleg keinen Bedarf für die Weitergabe ärztlicher Zusatzinformationen. Dagegen braucht bei einem für den Betroffenen ungünstigen Ausgang der Untersuchung, also z.B. bei der Feststellung von Verwendungsbeschränkungen oder Dienstunfähigkeit, die Einstellungsbehörde vielfach auch Befunddaten, um die Ablehnung der Einstellung, Beförderung, Versetzung usw. begründen zu können. Ich habe daher dem Innenminister ebenso wie dem Sozialminister vorgeschlagen, die Mitteilung der Beurteilungsgrundlagen der ärztlichen Entscheidung auf die Situationen eines ganz oder teilweise für den Untersuchten negativen Resultats zu begrenzen.

5.
Die Aufbewahrungsfristen für Dokumente medizinischen Inhalts, gleich ob bei den Personalverwaltungen oder bei den Gesundheitsämtern, müssen sich strikt an die allgemeine datenschutzrechtliche Vorgabe halten, daß Daten nur so lange gespeichert werden dürfen, wie sie zur Aufgabenerfüllung der jeweiligen Behörde erforderlich sind. Deshalb bedarf der Klärung, aus welchen beamten-, versorgungs- oder arbeitsrechtlichen Gründen beide Entwürfe für personalärztliche Akten vorsehen, daß sie bis zur Vollendung des 70. Lebensjahres bzw. bis 5 Jahre nach dem Tod des Bediensteten aufgehoben werden müssen. Zu begründen ist auch, warum die Gesundheitsämter für ihre Aufgabenerfüllung die Aktenbestände 30 Jahre lang zur Verfügung haben müssen. In den vorgesehenen Ausführungsvorschriften schließlich muß geregelt werden, wie die Gesundheitsämter von den Personalverwaltungen über den Ablauf der genannten Fristen informiert werden.

4.2.2.1.3.
Weiteres Verfahren

Die Vorarbeiten des Innenministers wie des Sozialministers sind jetzt soweit gediehen, daß - auch wenn der vom Landtag gesetzte Termin zum Jahresende 1984 nicht eingehalten werden konnte - bei weiterer zügiger Behandlung die endgültige Fomulierung und Abstimmung der Regelungsvorschläge im neuen Jahr rasch vonstatten gehen und der Arbeitsgruppe Datenverarbeitung und Datenschutz des Landtages bald Bericht erstattet werden kann.

Dabei darf allerdings nicht vergessen werden, daß die Regelung für die Datenverarbeitung der Gesundheitsämter durch die Änderung einer Verordnung aus dem Jahr 1935(!) nur als Übergangsregelung akzeptabel ist. Die nicht zuletzt als Konsequenz des Volkszählungs-Urteils des Bundesverfassungsgerichts notwendige umfassende bereichsspezifische gesetzliche Regelung von Datenverarbeitung und Datenschutz bei den Gesundheitsämtern steht noch aus. Auf die Erforderlichkeit solcher Bestimmungen habe ich schon früher aufmerksam gemacht (vgl. zuletzt 11. Tätigkeitsbericht Ziff. 2.1.2.2.). Zu Recht unterstreicht daher der Minister für Arbeit, Umwelt und Soziales in der Begründung zu seinem Entwurfstext, daß die vorgeschlagene Regelung im Vorgriff auf Datenschutzbestimmungen in einem künftigen Gesetz über den öffentlichen Gesundheitsdienst (ÖGD) getroffen wird.

4.2.2.2
Zweckbindung der Beihilfedaten
(11. Tätigkeitsbericht, Ziff. 5.2.2; 12. Tätigkeitsbericht, Ziff. 2.1.6.2)

4.2.2.2.1
Vermischung von Personal- und Krankheitsdaten

Beihilfeakten im öffentlichen Dienst enthalten hochsensible Krankheitsdaten der Bediensteten, teilweise übrigens auch ihrer Ehegatten und Kinder. Insofern gleichen sie den Unterlagen der Krankenkassen für die Arbeitnehmer in der privaten Wirtschaft. Wesentlicher Unterschied: Die Gesundheitsdaten, die von den Krankenversicherungen verarbeitet werden, unterliegen besonders strengen Datenschutz- bzw. Geheimhaltungsbestimmungen. Bei gesetzlichen Trägern greifen das Sozialgeheimnis und der spezielle Sozialdatenschutz (§ 35 SGB I, §§ 67 ff. SGB X). Angehörige von Unternehmen der privaten Krankenversicherung unterliegen dem strafrechtlich sanktionierten besonderen Berufsgeheimnis (§ 203 Abs. 1 Nr. 6 StGB). Die Informationsweitergabe der gesetzlichen Krankenkassen an den Arbeitgeber ist in der RVO detailliert und restriktiv geregelt: So darf beispielsweise die RVO-Kasse dem Arbeitgeber bei Arbeitsunfähigkeit des Mitarbeiters die Diagnose nicht mitteilen (vgl. § 369 b Abs. 3 Satz 2 RVO).

Nichts davon im öffentlichen Dienst: Hier erfüllt der Dienstherr gleichzeitig Arbeitgeberfunktionen und die Aufgabe der (teilweisen) Krankheitskostenerstattung; er kennt sowohl die allgemeinen Arbeitnehmerdaten als auch die Gesundheitsdaten seiner Bediensteten. Schon im 11. Tätigkeitsbericht (Ziff. 5.2.2) hatte ich auf die Gefährdung des Persönlichkeitsrechts der im öffentlichen Dienst Beschäftigten dadurch hingewiesen, daß dort - im Unterschied zum privaten Unternehmensbereich - keine strikte Trennung erfolgt zwischen den Angaben, die der einzelne zur Deckung seiner Krankheitskosten offenbaren muß, und solchen Daten, die der Arbeitgeber/Dienstherr für die Zwecke der Personalverwaltung, Gehaltsabrechnung usw. erhoben hat und verarbeitet.

Meine - auch aufgrund zahlreicher Eingaben genährte -Besorgnis, hier könnten Krankheitsdaten für dienstrechtliche Entscheidungen zweckentfremdet werden, hatte die Landesregierung in ihrer Stellungnahme zu meinem 11. Tätigkeitsbericht (Drucks. 10/659, zu Ziff. 5.2) sogar ausdrücklich bestätigt. In der Praxis zeige sich immer wieder, "daß auch aus Beihilfeakten wichtige Erkenntnisse für die schwerwiegenden Personalentscheidungen gewonnen ... werden könn(t)en". Im letzten Tätigkeitsbericht (12. Tätigkeitsbericht, Ziff. 2.1.6.2) hatte ich die Landesregierung gebeten, ihre ablehnende Haltung gegenüber einer strikten "Abschottung" der Beihilfeunterlagen zu überdenken und noch einmal die wichtigsten Grundsätze formuliert: Beihilfedaten dürfen ausschließlich zweckgebunden, d.h. nur zur Prüfung und Berechnung des Beihilfeanspruchs verwendet werden, nicht aber für sonstige Personalentscheidungen wie Beförderungen usw. Ausnahmen bedürfen der Zustimmung des betroffenen Bediensteten. Zur organisatorischen Absicherung dieser Zweckbindung ist eine getrennte Führung der Beihilfeakten von den übrigen Personalakten geboten.

4.2.2.2.2
Beschluß des Landtags - neuer Erlaß

Während die Landesregierung ihrer Stellungnahme zu meinem 12. Tätigkeitsbericht (Drucks. 11/1258, zu Ziff. 2.1.6.2) zufolge noch die Beratungen auf Bundesebene zu einer eventuellen Neuregelung des Bundesbeamtenrechts abwarten wollte, hielt der Hessische Landtag ein schnelleres Vorgehen für angezeigt. Im Beschluß Nr. 11 zu meinem 12. Tätigkeitsbericht (vgl. die Beschlußempfehlung des Innenausschusses, Drucks. 11/1551) hat das Parlament am 5. Juli 1984 die Landesregierung gebeten, "umgehend Regelungsvorschläge vorzulegen, die die strikte Zweckbindung bei der Verwendung von für die Gewährung von Beihilfen gemachten Angaben unter Berücksichtigung der vom Datenschutzbeauftragten gemachten Anmerkungen gewährleisten".

Der Hessische Minister des Innern ist dieser Bitte nachgekommen und hat mir Ende Oktober seinen Entwurf für die Änderung der Verwaltungsvorschriften zu § 107 Hessisches Beamtengesetz (StAnz. 1984, S. 779) vorgelegt; diese Vorschriften regeln den Umgang mit Personalakten. In einem neuen Abschnitt (V a) sollen die getrennte Führung sowie die strikt zweckgebundene Verwendung der Beihilfeunterlagen verankert werden. Eine Weitergabe von Informationen aus der Beihilfeakte an die Personalverwaltung soll nur mit Zustimmung des Betroffenen oder in Ausnahmefällen einer konkreten Gefahr für die öffentliche Sicherheit und Ordnung - also bei Krankheiten, bei denen auch der Arzt offenbarungsbefugt wäre - möglich sein.

Ich habe diesen Entwurf zustimmend zur Kenntnis genommen und in einer ausführlichen Stellungnahme eine Reihe von Verbesserungen des Textes angeregt. Die Novellierung der Beihilfebestimmungen sollte im neuen Jahr so schnell wie möglich in Kraft treten. Trotz dieser positiven Entwicklung bleibt jedoch festzuhalten: Regelungen für die Datenverarbeitung im Personalwesen auf untergesetzlicher Ebene können nur als Zwischenschritt dienen auf dem Weg zu einer präzisen gesetzlichen Regelung von Umfang und Zwecken der Erhebung sowie Verwendung von Arbeitnehmerdaten; dies gilt auch für das Personalaktenrecht. Die Anforderungen des Volkszählungsurteils des Bundesverfassungsgerichts vom 15. Dezember 1983 machen diesen Schritt unumgänglich (vgl. dazu oben Ziff. 3.3.2).

4.3
Zum 10. Tätigkeitsbericht für 1981 (Drucks. 9/5873)

4.3.1
Hochschul- und Klinikrechenzentrum der Justus-Liebig-Universität Gießen
(10. Tätigkeitsbericht, Ziff. 4.4.3.2)

Im Mai 1981 hatte ich die unzureichenden Maßnahmen der Datensicherung im Hochschulrechenzentrum Gießen beanstandet und darüber dem Landtag berichtet. In ihrer Stellungnahme zu meinem 10. Tätigkeitsbericht hatte die Landesregierung angekündigt, der Kultusminister werde die erforderlichen Maßnahmen durchführen, sobald die Entscheidung über die Errichtung eines Krebsregisters bei der Universität Gießen getroffen sei (Drucks. 9/6331, zu 4.4.3.2). Diese Ankündigung bezog sich auf ein Datensicherungskonzept, das im September 1981 von Vertretern der Universität sowie des Staatlichen Hochbauamts Gießen, einem Experten des Landeskriminalamts und mir gemeinsam erarbeitet worden war. Die erforderlichen Mittel hatte der Hessische Kultusminister für 1983 vorgemerkt und zudem in eine Nachtragshaushalts-Unterlage für die damals noch laufenden Baumaßnahmen am Rechenzentrum eingesetzt.

Dennoch mußte ich bei einer erneuten Datenschutz-Prüfung des Hochschulrechenzentrums im August dieses Jahres feststellen, daß keine der vorgesehenen Vorkehrungen für die Daten- und Anlagensicherung realisiert worden ist. Ich habe daraufhin im Oktober 1984 den Hessischen Minister für Wissenschaft und Kunst auf diesen unhaltbaren Zustand hingewiesen und ihn aufgefordert, mir über den derzeitigen Stand der Datensicherung zu berichten. Die Dringlichkeit sofortiger Schritte hat sich seit 1981 erheblich erhöht, bedenkt man den Ausbau der Datenverarbeitung im Bereich der Universitätsklinika und den Aufbau des regionalen Tumorregisters Marburg/Gießen mit der Konsequenz umfangreicher Speicherung von Patientendaten.

Wiesbaden, den 13. Februar 1985

gez. Prof. Dr. Simitis

5. Materialien

5.1
Erklärung der Konferenz der Datenschutzbeauftragten der Länder und des Bundes zur Einführung von Bildschirmtext vom 27./28. März 1984

Die Datenschutzbeauftragten beobachten mit Besorgnis die Entwicklung und Einführung von Bildschirmtext. Sie betonen, daß nach ihrer Ansicht den Problemen des Datenschutzes nicht genügend Aufmerksamkeit geschenkt wird. Sie haben begründeten Anlaß anzunehmen, daß die Deutsche Bundespost den von der Rundfunkkommission der Länder und den Datenschutzbeauftragten entwickelten Datenschutzbestimmungen des Bildschirmtext-Staatsvertrages nicht hinreichend Rechnung trägt.

1. Die Ministerpräsidenten der Länder haben am 18. März 1983 den Staatsvertrag über Bildschirmtext unterzeichnet. Bis auf wenige Ausnahmen sind die Zustimmungsgesetze in den Ländern in Kraft getreten. Die Zustimmung der Länder war abhängig von einer zufriedenstellenden Regelung des Datenschutzes. Die unmittelbar bevorstehende bundesweite Einführung von Bildschirmtext zwingt zur Prüfung, ob die Deutsche Bundespost die Forderungen erfüllt hat, die Grundlage der Zustimmung waren.

2. Die Deutsche Bundespost hat in ihrer Zusage offengelassen, in welchem Umfang sie die Bestimmungen des Staatsvertrages in Bundesrecht umsetzen will. Die Ministerpräsidenten der Länder hatten eine Regelung in Form von Rechtsvorschriften erwartet. Dies ist wegen der Sensitivität der anfallenden Daten - um so mehr nach dem Urteil des Bundesverfassungsgerichts zum Volkszählungsgesetz 1983 - geboten.

   Die bisher vorgenommenen Ergänzungen der Fernmeldeordnung bleiben weit hinter dem Erforderlichen zurück. Gegenüber dem Staatsvertrag fehlen insbesondere klare Regelungen zur Verarbeitung der Verbindungsdaten (Umfang der Speicherung, Zeitpunkt der Löschung). Darüber hinaus sollen die Bestimmungen festlegen, welche Abrechnungsdaten im Streitfall dem Anbieter übermittelt werden. Die jetzige Formulierung "im Rahmen der technischen und betrieblichen Möglichkeiten" ist zu allgemein.

3. Die Datenschutzbeauftragten kritisieren mit Nachdruck, daß sich die Deutsche Bundespost bisher nicht in der Lage gesehen hat, ihnen das vollständige Systemkonzept für Bildschirmtext vorzulegen. Die zur Zeit bekanntgewordenen Elemente des Bildschirmtextsystems wecken begründete Zweifel daran, ob die Deutsche Bundespost den materiellen Bestimmungen des Staatsvertrages gerecht wird. Dies gilt insbesondere für das Verbot, Abrechnungsdaten so zu speichern, daß die Art und der Zeitpunkt des in Anspruch genommenen Angebots erkennbar sind.

5.2
Entschließung der Datenschutzbeauftragten der Länder und der Datenschutzkommission Rheinland-Pfalz zu Bildschirmtext vom 6./7. Juni 1984

Ein effektiver Datenschutz bei Bildschirmtext ist abhängig von dem medienpolitischen Modus vivendi zwischen Bund und Ländern, der auf Konsens und gegenseitiges Vertrauen angelegt ist. Die Unterzeichnung des Staatsvertrages und dessen Ratifikation durch die Länderparlamente waren davon abhängig, daß die Deutsche Bundespost den im Staatsvertrag geregelten Datenschutz einhalten und für ihren Bereich entsprechende Vorschriften erlassen werde. Die Deutsche Bundespost hat dies schriftlich zugesagt. Die Reaktion der Deutschen Bundespost auf die Erklärung der Datenschutzbeauftragten, die an die Einlösung der Verpflichtung der Deutschen Bundespost erinnert, läßt befürchten, daß die Deutsche Bundespost sich von dieser gemeinsamen Geschäftsgrundlage für die Einführung von Bildschirmtext lösen will. Im Gegensatz zur einheitlichen Auffassung der Ministerpräsidenten vertritt die Deutsche Bundespost nunmehr die Ansicht, daß Bildschirmtext als Fernmeldedienstleistung bundesrechtlich verordnet sei und damit nach Art. 87 GG in der ausschließlichen Verwaltungskompetenz des Bundes stehe.

Die Datenschutzbeauftragten sind nach wie vor der Ansicht, daß die Länder für die gesamte Nutzung des neuen Mediums Bildschirmtext die Regelungskompetenz haben. Die Länder haben demzufolge den Datenschutz im Bildschirmtext-Staatsvertrag für diesen Bereich abschließend geregelt. Die Auffassung der Deutschen Bundespost, Bildschirmtext sei ausschließlich ein Fernmeldedienst (vgl. Antwort des Parlamentarischen Staatssekretärs Spranger vom Bundesministerium des Innern in der Fragestunde des Deutschen Bundestages vom 14. März 1984 auf eine entsprechende Frage des Abgeordneten Dr. Hirsch F.D.P), stimmt in mehrfacher Hinsicht mit der Bildschirmtextkonzeption nicht überein. So steht sie beispielsweise im Gegensatz zu der Tatsache, daß die Deutsche Bundespost nie ein Monopol für das Betreiben von Bildschirmtextdiensten in Anspruch genommen und entsprechenden Regelungen im Staatsvertrag nicht widersprochen hat.

Die Gefahren des neuen Kommunikationssystems für die Privatsphäre liegen in erster Linie in den technisch grundsätzlich möglichen umfassenden Sammlungen personenbezogener Daten in den technischen Einrichtungen, die zur Nutzung von Bildschirmtext bereitgestellt werden. Über diese technischen Einrichtungen wird die vollständige Kommunikation zwischen den Anbietern und Teilnehmern abgewickelt. Über diese Einrichtungen gehen alle Abrufe von Angeboten, fließen alle ausgetauschten Daten und wird die Gebührenabrechnung abgewickelt. Nutzbarkeit und Verwendungsmöglichkeit dieser Daten hängen hierbei von den der Informationstechnologie eigenen Verarbeitungs- und Verknüpfungsmöglichkeiten ab.

Angesichts dieser Gefährdung sind nach der Rechtsprechung des Bundesverfassungsgerichts durch Gesetz die organisatorischen und verfahrensrechtlichen Vorkehrungen zu treffen, um der Gefahr einer Verletzung des Persönlichkeitsrechts entgegenzuwirken. Daher ist es unverständlich, daß die Deutsche Bundespost derzeit offenbar nicht bereit ist, entweder den Staatsvertrag für sich gelten zu lassen oder entsprechende bundesgesetzliche Regelungen zu schaffen. Spätestens seit dem Urteil des Bundesverfassungsgerichts zur Volkszählung ist die Erklärung der Deutschen Bundespost, daß sie neben Verwaltungsanweisungen auch Vorschriften erlassen werde, in verfassungskonformer Weise nur als Verpflichtung zu verstehen, Rechtsnormen zu schaffen. Da die Deutsche Bundespost den Staatsvertrag nicht unmittelbar für sich gelten läßt, bestehen Regelungslücken im Bundesrecht. Die Bundespost würdigt nicht in ausreichendem Maße, daß die verschärfte Datenschutzregelung im Staatsvertrag den erhöhten Gefahren begegnen und den evtl. vorhandenen Ängsten der Bevölkerung Rechnung tragen sollte.

Eine Regelung des Datenschutzes bei Bildschirmtext kann sich nicht in einer einseitigen Verpflichtungserklärung der Deutschen Bundespost gegenüber den Ländern, in Verwaltungsanweisungen oder in Vorkehrungen im technisch-betrieblichen System erschöpfen. Selbst das Fernmeldegeheimnis - dessen Reichweite bei Bildschirmtext nicht unbestritten ist - befreit nicht von der Notwendigkeit, zusätzliche grundrechtssichernde gesetzliche Regelungen zu schaffen, die den besonderen Gefahren begegnen. Aus der Mitwirkung der Datenschutzbeauftragten bei der Schaffung der Datenschutzvorschrift im Staatsvertrag folgt eine Verantwortung gegenüber Landesregierungen und Landesparlamenten für eine ausreichende Berücksichtigung des Persönlichkeitsschutzes bei der Einführung von Bildschirmtext. Die Datenschutzbeauftragten mußten darauf vertrauen, daß die Deutsche Bundespost die den Ministerpräsidenten gegenüber abgegebene Verpflichtung einhält und ungeachtet kompetenzrechtlicher Meinungsverschiedenheiten alles tut, was für eine effektive Umsetzung der Bestimmungen des Staatsvertrages notwendig ist. Hierzu gehören eine umfassende Information über die technischen Komponenten des Bildschirmtextsystems, die vollständige Umsetzung der Datenschutzvorschriften des Staatsvertrages für die Einrichtungen der Deutschen Bundespost und die Ermöglichung einer effektiven Datenschutzkontrolle durch die zuständigen Verwaltungsbehörden der Länder. Dabei verlangt die enge Verflechtung von Netz- und Nutzungsbereich, daß alle Kontrollinstitutionen fortlaufend, unmittelbar und umfassend über die technische Ausgestaltung und Wirkungsweise des Bildschirmtextsystems unterrichtet werden. Mit einer Information aus zweiter Hand können die Datenschutzinstanzen der Länder ihrer Verpflichtung nicht nachkommen. Die Kontrolle durch unabhängige Datenschutzinstanzen ist eine wesentliche Voraussetzung eines wirksamen Grundrechtsschutzes.

Zu den nach Ansicht der Deutschen Bundespost bereits verwirklichten technisch-organisatorischen Vorkehrungen zum Schutze des Persönlichkeitsrechts der Bürger kann noch nicht abschließend Stellung genommen werden. Zwar hat die Deutsche Bundespost inzwischen mündlich die Datenschutzbeauftragten über das technische System Bildschirmtext unterrichtet, eine schriftliche Verfahrensbeschreibung einschließlich aller Datensätze steht noch aus. Erst wenn diese vorliegt, können die Datenschutzbeauftragten zum technischen System Bildschirmtext abschließend Stellung nehmen. Die Datenschutzbeauftragten sind jederzeit bereit, Datenschutzfragen des Bildschirmtextsystems mit der Deutschen Bundespost zu erörtern.