11. Wahlperiode

Drucksache **11/473**

HESSISCHER LANDTAG

19. 01. 84

Zwölfter Tätigkeitsbericht des Hessischen Datenschutzbeauftragten

Mit Schreiben vom 19. Januar 1984 legt der Datenschutzbeauftragte gemäß § 29 des Hessischen Datenschutzgesetzes vom 31. Januar 1978 dem Landtag folgenden Tätigkeitsbericht vor:

Eingegangen am 19. Januar 1984 · Ausgegeben am 2. Februar 1984

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

INHALTSVERZEICHNIS

1. Zur Situation

1.1
Entwicklungen 1983

1983 war für den Datenschutz ein wichtiges Jahr. Nie zuvor war, dank der Auseinandersetzung um das Volkszählungsgesetz, das Interesse am Datenschutz so groß, die Bereitschaft, in den Datenschutzvorkehrungen eine im Interesse des Bürgers unabdingbare Bedingung staatlicher und privater Aktivität zu sehen, so verbreitet. Nie zuvor hat sich aber auch die Tendenz so deutlich abgezeichnet, den Datenschutz zurückzudrängen, um die Verarbeitung personenbezogener Angaben zu einer immer schärferen und umfassenderen Kontrolle des einzelnen nutzen zu können.

1.1.1
Die Volkszählung und ihre Folgen

1.1.1.1
Das Volkszählungsgesetz - Entstehung und Kritik

Zunächst einige Bemerkungen zur Volkszählung. Die heftige Kontroverse über das Volkszählungsgesetz (VZG) ist mit der Verkündung der Entscheidung des Bundesverfassungsgerichts am 15. Dezember 1983 abgeschlossen. Das Gericht hat jeden Zweifel beseitigt. Das VZG ist nur noch Dokument fehlgelaufener legislativer Tätigkeit. Statt den Handlungsrahmen für die umfassendste statistische Erhebung abzugeben, erinnert es an die Handlungsgrenzen des Gesetzgebers. So unmißverständlich freilich das Verdikt des Bundesverfassungsgerichts ausgefallen sein mag, so wenig geht es an, alle weiteren Überlegungen zum VZG als schlicht überflüssig auszugeben. Wenn die Lehren aus dem Konflikt wirklich gezogen werden sollen, dann gilt es, die Geschichte des Gesetzes ebensowenig zu vergessen wie den Verlauf und die einzelnen Stationen der Auseinandersetzung um seine Geltung (vgl. dazu die Chronologie der Ereignisse, unten Ziff. 1.3). Niemand kann ernsthaft von sich behaupten, den Protest gegen die Volkszählung vorausgesehen und vorausgesagt zu haben. Nur: Die hartnäckig wiederholte Behauptung, niemand und schon gar nicht die Datenschutzbeauftragten hätten versucht, den Gesetzgeber von seiner verfehlten Entscheidung abzuhalten, ist eindeutig falsch. Schon 1979, während der Beratungen des Innenausschusses des Deutschen Bundestages, war der eigentlich kritische Punkt des VZG unmißverständlich angesprochen worden. Für mich stand damals wie heute fest: Gesetzliche Regelungen, die statistische und administrative Aufgaben vermischen, bewegen sich jenseits der Legalität. Eben deshalb hatte ich, ebenso wie übrigens der Bundesbeauftragte für den Datenschutz, den Innenausschuß des Bundestages gewarnt. Die Beratungen über das Volkszählungsgesetz dürften unter keinen Umständen dazu führen, die statistische Erhebung letztlich nur noch als höchst willkommenen Anlaß anzusehen, um die Informationswünsche staatlicher und kommunaler Verwaltung zu erfüllen. Doch die Kritik hat weder den Innenausschuß noch das Plenum beeindruckt. Allzu günstig erschien die Gelegenheit, die zahlreichen Informationserwartungen gleichsam auf einen Schlag zu verwirklichen, allzu mächtig war vor allem der Druck der Kommunen und ihrer Verbände.

Gewiß, die Kritik ist nach der Verabschiedung des Gesetzes verstummt. Kein Datenschutzbeauftragter hat jedenfalls bis zu dem Zeitpunkt, zu dem auf Landesebene die Vorbereitungen für die Durchführung der Volkszählung begonnen haben, das Gesetz in Frage gestellt. Kaum verwunderlich freilich, denn die Verabschiedung eines Gesetzes gegen den Widerspruch der Datenschutzbeauftragten ist kein einmaliger Vorgang. Das VZG ist genaugenommen nur eines von mehreren Beispielen für Regelungen, die sich über rechtzeitig geäußerte und klar formulierte Kritik hinwegsetzen. Den Datenschutzbeauftragten bleibt kein anderer Weg als die parlamentarische Entscheidung hinzunehmen. Weder steht ihnen auch nur im entferntesten das Recht zu, den Gesetzesvollzug zu unterbrechen, noch dürfen sie Funktionen für sich in Anspruch nehmen, die der Verfassungsgerichtsbarkeit vorbehalten sind. Wo jedoch, wie im Fall des VZG, die Anwendung des Gesetzes etwa den Erlaß von Verwaltungsvorschriften voraussetzt, kann und muß der Datenschutzbeauftragte die Chance nutzen, Bedenken und Kritik erneut vorzubringen.

Genau dies ist mit dem Zwischenbericht vom 14. März 1983 (Drucks. 10/573) geschehen. Er war bewußt an die Adresse des Hessischen Landtags gerichtet, weil das Parlament auf die mit der Volkszählung verbundenen Gefahren unmittelbar aufmerksam gemacht und so zugleich die Möglichkeit geschaffen werden sollte, die mittlerweile immer stärkere Kritik am VZG in einer parlamentarischen Diskussion aufzugreifen. Der Zwischenbericht stellte zugleich Forderungen auf, die in vollem Umfang in der Bremer Erklärung der Datenschutzbeauftragten des Bundes und der Länder vom 22. März 1983 (vgl. unten Ziff. 5.2.2) wiederkehrten und fast durchweg von der Landesregierung akzeptiert wurden. Der Zwischenbericht mußte freilich die allein vom Bundesverfassungsgericht zu entscheidende Frage der Verfassungsmäßigkeit des VZG ausklammern. Sie ist dann auf Anforderung des Gerichts zunächst im Zusammenhang mit der einstweiligen Anordnung (vgl. meine Stellungnahme, unten Ziff. 5.2.3) und später im Rahmen der Anhörung vor der endgültigen Entscheidung (vgl. meine Stellungnahme, unten Ziff. 5.2.4) gestellt und eindeutig beantwortet worden: Wo der Gesetzgeber die administrative Verwendung der für statistische Zwecke erhobenen Daten zuläßt und zugleich die Anonymität der statistischen Angaben durchbricht, verstößt er gegen das Grundgesetz und trifft eine eindeutig verfassungswidrige Entscheidung.

1.1.1.2
Risiken und Protestmotive

So wenig sich nun bestreiten läßt, daß die Auseinandersetzung um das VZG im Mittelpunkt der Datenschutzdiskussion gestanden hat, ja nicht zuletzt mit Rücksicht auf die Flut der Anfragen aus der Bevölkerung, die parlamentarische Debatte und die gerichtliche Verhandlung den Datenschutzbeauftragten gezwungen hat, sich fast ausschließlich ihr zu widmen, so verfehlt wäre es, die Volkszählung zum Musterfall für die Gefahren der Datenverarbeitung und damit auch für die Anwendung des Datenschutzes zu stilisieren. Ohne Zweifel hat sich der Gesetzgeber für ein Erhebungsprogramm entschieden, das weit hinter den Anforderungen früherer Volkszählungen zurückblieb. Umsonst wird man im Fragebogen nach jenen berühmten "sensitiven" Fragen suchen, die einst im Mikrozensus-Beschluß das Bundesverfassungsgericht veranlaßten, erste Grenzen für statistische Erhebungen zu ziehen. Weder galt es den eigenen Gesundheitszustand offenzulegen, noch ging es etwa darum, private Lebensgewohnheiten detailliert zu schildern. Ebensowenig läßt sich ernsthaft bestreiten, daß sich der Gesetzgeber weitgehend an längst akzeptierte und praktizierte Regeln gehalten hatte. Und schließlich: Fälle, die, soweit es um die Verarbeitungsgefahren geht, sehr viel schwerer wiegen, finden sich mühelos. Man braucht nur an die in diesem Bericht angesprochene Verarbeitung von Sozial- und Arbeitnehmerdaten zu denken.

Der Protest gegen die Volkszählung läßt sich deshalb nicht als Reaktion auf eine besonders gravierende oder gar in ihren Konsequenzen einmalige Verarbeitung personenbezogener Daten verstehen und bewerten. Verständlich wird er erst als Antwort auf die technologische Entwicklung und das Informationsverhalten des Staates. Für die Betroffenen stand nicht so sehr eine - wie auch immer näher ausgestaltete - statistische Erhebung zur Debatte, sondern die zum Symbol für die Gefahren einer immer umfangreicheren und perfekteren Datenverarbeitung gewordene Volkszählung. Mit ihr sah sich zum ersten Mal jeder Bürger mit dem Verlangen konfrontiert, Informationen zu seiner Person preiszugeben. Niemand konnte sich ausnehmen, niemand deshalb von sich behaupten, die Informationsverarbeitung sei ein Vorgang, der ihn jedenfalls nichts angehe. Deshalb ist es nicht weiter verwunderlich, wenn Vorbehalte und Ängste in einem bislang nie gekannten Maße mobilisiert wurden. Ebensowenig überrascht es aber, daß sich der Protest keineswegs auf einen bestimmten, wie immer näher beschriebenen Bevölkerungsteil beschränkte. Die Anfragen und Eingaben zur Volkszählung zeigen nur zu gut: Beruf, Einkommen, soziale Stellung, Bildungsgrad, politische Überzeugung sind allesamt Kriterien, die restlos versagen, sobald es darum geht, den Protest gegen die Volkszählung näher zu beschreiben.

So unterschiedlich der jeweilige Ansatzpunkt auch gewesen sein mag, so sehr stimmt der letztlich einzig ausschlaggebende Grund überein: die Befürchtung, die Volkszählung könnte zum Einfallstor einer schrankenlosen, durch die automatische Verarbeitung begünstigten Verknüpfung der unzähligen, im staatlichen und privaten Bereich schon vorhandenen Daten zur Person des einzelnen werden. Die Volkszählung wurde so zum Katalysator des tiefen Mißtrauens gegenüber einer in ihren Konsequenzen undurchsichtigen, in ihrer konkreten Bedeutung kaum nachvollziehbaren und in Anbetracht ihres rasanten Wandels immer unheimlicheren Informationstechnik, die einen ohnehin übermächtig erscheinenden Staatsapparat allzu leicht dazu verführen könnte, Privatheit und Individualität vollends zu zerstören. Der Protest gegen die Volkszählung ist, so gesehen, Protest gegen Technik und Bürokratie in einem.

1.1.1.3
Konsequenzen aus der Diskussion

Vordergründig war und ist davon nur die Volkszählung betroffen. Die Funktionsfähigkeit der amtlichen Statistik hängt von der Auskunftsbereitschaft der Bevölkerung ab. Selbst dort, wo - wie bei der Statistik - eine gesetzliche Auskunftsverpflichtung besteht, kommt es vor allem anderen auf die Bereitschaft der Betroffenen an, die von ihnen verlangten Informationen uneingeschränkt und korrekt zu erteilen. Die formelle Auskunftsverpflichtung läßt sich sicher erzwingen, die Kooperation des Bürgers nicht. In dem Maße, in dem er den Informationserwartungen skeptisch, ja ablehnend begegnet, wird er auch versucht sein, unvollständig oder gar unzutreffend zu antworten. Genau diese Einsicht hat die niederländische Regierung veranlaßt, von einer Volkszählung einstweilen abzusehen. Solange es nicht gelinge, die Vorbehalte gegen die Datenverarbeitung abzubauen, die Bürger also davon zu überzeugen, daß die von ihnen befürchteten Konsequenzen gar nicht eintreten könnten, habe es keinen Sinn, auf einer Erhebung zu bestehen, die der Gefahr ausgesetzt sei, falsche und damit für alle staatliche Politik untaugliche Informationen zu liefern. Kurzum, Gesetze, die wie das VZG das Statistikgeheimnis offen durchlöchern, die administrative Verwendung der statistischen Angaben unwidersprochen akzeptieren und noch dazu die Betroffenen durch ein fiktives Nachteilsverbot irreführen, untergraben die amtliche Statistik, indem sie Verständnis und Kooperation der Bürger von vornherein in Frage stellen sowie Umgehungsstrategien förmlich provozieren.

Freilich: Weil sich hinter der Reaktion auf die Volkszählung weit mehr verbirgt als nur die Auseinandersetzung mit einer bestimmten statistischen Erhebung, reicht eine bloße Überprüfung des Volkszählungsgesetzes nicht aus. Gewiß, vom Zwischenbericht an den Hessischen Landtag über die Bremer Erklärung der Datenschutzbeauftragten bis hin zur Entscheidung des Bundesverfassungsgerichts sind die für eine Korrektur wichtigsten Akzente gesetzt worden. Die radikale Trennung von Statistik und Verwaltung, die kompromißlose Garantie des Statistikgeheimnisses, gezielte Vorkehrungen, die den Respekt vor der Situation des jeweils betroffenen Bürgers und seinen Interessen auch und gerade während der Erhebung bis hin zur Anonymisierung der Daten wahren, sind Stationen auf diesem Weg. Das gleiche Mißtrauen und die gleiche Kritik, die sich bei der Volkszählung manifestierten, werden sich jedoch unweigerlich überall dort wiederholen, wo sich die Bürger mit ähnlich weitreichenden, tendenziell jeden einzelnen einbeziehenden und an die Nutzung der Informationstechnik geknüpften Informationsanforderungen konfrontiert sehen sollten. Der Protest gegen die Volkszählung ist kein einmaliger, sondern ein jederzeit wiederholbarer Vorgang, zumindest solange sich staatliche Politik nicht auch und gerade als Verpflichtung versteht, Informationsprozesse offenzulegen, Kontrollmechanismen einzurichten und uneingeschränkt zu respektieren sowie den Dialog mit dem Bürger zu suchen, um ihm Anlaß und Konsequenzen der Informationsverarbeitung verständlich und einsichtig zu machen, sich also seinen Einwänden und seiner Kritik zu stellen, um letztlich die in seiner Situation und den sich daraus ergebenden Folgen angebrachten Wege zu wählen.

Kurzum, die Konsequenz aus der Diskussion über das VZG, den Forderungen der Datenschutzbeauftragten und der Entscheidung des Bundesverfassungsgerichts wäre nicht gezogen, wollte man sich ausschließlich mit den auf statistische Erhebungen zugeschnittenen Regelungen zufriedengeben. Die Konsequenz kann und darf nur sein, in der Neuformulierung der Anforderungen an die Statistik den ersten Schritt einer kritischen Auseinandersetzung mit allen Aspekten der Informationsverarbeitung zu sehen, mit dem Ziel einer Informationsregelung, die durchweg auf den von den Datenschutzbeauftragten geforderten und vom Bundesverfassungsgericht bestätigten Grundsätzen aufbaut. Nur wo die strikte Zweckbindung der Verarbeitung personenbezogener Daten wirklich ernst genommen sowie Eingriffe in das Recht des einzelnen, selbst über die Verwendung seiner Daten zu bestimmen, tatsächlich gesetzlich abgesichert werden, kann eine die Grundrechte unterlaufende Anpassung und Gleichschaltung vermieden und das Grundgesetz auch unter den Bedingungen einer Gesellschaft, die vom technologischen Wandel geprägt ist, respektiert werden (zu den Konsequenzen aus dem Urteil des Verfassungsgerichtes im einzelnen vgl. unten Ziff. 1.2.1).

1.1.2
Selbstbestimmung und soziale Kontrolle durch Datenverarbeitung

Eines darf allerdings nicht übersehen werden: Die Voraussetzungen, unter denen sich die Datenschutzdiskussion vollzieht, haben sich gerade im Laufe der letzten zwei Jahre erheblich verschlechtert. Bis dahin stand - trotz der oft weitreichenden Meinungsverschiedenheiten über Details - fest, Ziel aller Überlegungen könne und dürfe es nur sein, den Verarbeitungsprozeß an zwingende, den Schutz des einzelnen garantierende Vorkehrungen zu binden. Seither setzt sich die Tendenz immer mehr durch, die Datenverarbeitung als Kontrollinstrument zu nutzen. Der Grund war schon im 10. Tätigkeitsbericht angedeutet worden. Die unter wachsenden ökonomischen Druck geratene Leistungsverwaltung sieht in der computergestützten Leistungskontrolle eines der wichtigsten Mittel, um die Haushaltsbelastung einzuschränken. Genaugenommen wiederholt sich damit in der Bundesrepublik eine bereits in den Vereinigten Staaten sowie in Schweden sichtbar gewordene Entwicklung. Just die Begleiterscheinung der automatischen Verarbeitung, die einst den Gesetzgeber zum Eingriff veranlaßt hatte, die immer perfektere Kontrolle des Bürgers mit Hilfe der zu seiner Person gespeicherten Daten, wird auf einmal als für die staatliche Politik unentbehrlich gepriesen. Allzu lange habe man, so heißt es immer wieder, unter dem Druck der Datenschutzdiskussion die Kontrollchancen ausgeblendet. Kein zu Leistungen an seine Bürger bereiter und verpflichteter Staat könne aber auf Dauer darauf verzichten, den Bürger zu überprüfen, um einerseits festzustellen, ob die Leistungen den gesetzlichen Voraussetzungen wirklich entsprächen und um andererseits herauszufinden, wie der wachsende Kostendruck vermindert werden könnte. Der Rückgriff auf die den gespeicherten Daten zu entnehmende Information wird also mehr und mehr als selbstverständliche Kehrseite staatlicher Sozial- und Wirtschaftspolitik ausgegeben.

Die Konsequenzen waren bereits in den beiden letzten Tätigkeitsberichten skizziert worden. So wurde das einst so gefeierte und für unabdingbar gehaltene Sozialgeheimnis plötzlich, fast ohne jede Diskussion, partiell preisgegeben. Dieser Tätigkeitsbericht bringt weitere Beispiele. Die Korrektur des Kindergeldrechts gehört ebenso dazu wie die Wirtschaftlichkeitsprüfungen in Krankenhäusern und die Modellversuche zur Erhöhung der Leistungs- und Kostentransparenz in der gesetzlichen Krankenversicherung (vgl. unten Abschnitt 3.2). Wohlgemerkt, die Regelungsziele leuchten durchweg ein. Wer wollte sich schließlich der Forderung verschließen, die Schwarzarbeit einzudämmen, die Pflegesätze auf ihre Angemessenheit zu überprüfen und die Leistungs- und Kostenstruktur im Gesundheitssektor transparenter zu gestalten. Genau darin liegt jedoch die Gefahr. Das überzeugend, ja selbstverständlich erscheinende Ziel verdrängt die Diskussion über die möglichen Auswirkungen der zu seiner Verwirklichung eingesetzten Mittel. Spätestens an den Modellversuchen der Krankenkassen wird klar: Die Leistung an den

Bürger ist zugleich potentielle Verhaltenssteuerung, die Möglichkeit dazu bietet aber die Verarbeitung der zur Person des Leistungsempfängers gesammelten Daten. Die Krankenkasse, die Versichertendaten "rastert", um dann den einzelnen Versicherten, der die unter Kostenaspekten definierte Normalität durchbricht, unmittelbar anzusprechen, mit dem Ziel, ihn zu veranlassen, sein abweichendes Verhalten zu korrigieren, normiert und typisiert Verhaltensstrukturen. Ähnliches läßt sich in anderen Bereichen unschwer wiederholen. Durchweg liefert die automatische Verarbeitung die Voraussetzungen dafür, schafft, genaugenommen, erst die Bedingungen für die gewünschte Verhaltensanpassung.

Noch einmal: Die Reflexion über diese Entwicklung darf nicht durch Hinweise auf das jeweilige, noch so willkommene Ziel verdrängt werden. Vielmehr kommt es zunächst einzig und allein darauf an, sich mit der Bedeutung sowie den Auswirkungen der mit Hilfe der automatischen Verarbeitung etablierten sozialen Kontrollmechanismen auseinanderzusetzen. Es mag sein, daß es letztlich keine Alternative zur Typisierung des Sozialversicherten sowie zu einer ebenso typisierten Leistungskontrolle gibt. Dennoch gilt es rechtzeitig und in aller Schärfe zu fragen, wie Kontrollvorkehrungen auszusehen haben, wo ihre Grenzen liegen und vor allem, welche langfristigen Konsequenzen sie für das soziale Verhalten ebenso wie für die Struktur und die Aktivität des staatlichen Apparats haben. Anders ausgedrückt: Die noch so notwendige staatliche Leistung darf nicht zur Vorstufe einer auf immer nachhaltigere Anpassung bedachten Verhaltungssteuerung werden.

Um das Bundesverfassungsgericht wieder zu zitieren: Wenn die Feststellung, eine Verwirklichung der Grundrechte vertrage sich nicht mit der konsequenten Registrierung sozialer Auffälligkeiten, ernst genommen werden soll, dann muß die erste und entscheidende Frage stets die sein, wie in Kenntnis der Leistungsverpflichtung staatlicher Verwaltung sowie der Kontrollmöglichkeiten automatischer Verarbeitung die Chance des einzelnen, seine Grundrechte wahrzunehmen, auch und gerade dort erhalten bleiben kann, wo er auf staatliche Leistungen angewiesen ist. Von einer Selbstbestimmung kann jedenfalls dann nicht mehr die Rede sein, wenn die Leistungsabhängigkeit mit Hilfe der automatischen Verarbeitung in eine Verhaltenssteuerung umschlägt, die strikte Anpassung also zum Preis für eine Leistung wird, die ihrer ganzen Geschichte und Intention nach den Sinn haben sollte, die materiellen Voraussetzungen für die Selbstbestimmung des einzelnen erst zu schaffen. Der Datenschutz ist damit an einem für die gesamte weitere Entwicklung überaus kritischen Punkt angelangt. Er steht allen Versuchen, die gespeicherten Daten immer mehr zu Kontrollzwecken zu nutzen, eindeutig im Weg. Insofern verwundert es nicht, wenn die Forderung nach Kontrolle in die Kritik am Datenschutz mündet. Ebensowenig ist aber zu übersehen, daß wegen der durchaus plausiblen Zielsetzungen der Druck, den Datenschutz einzuschränken, immer mehr zunehmen dürfte. Wenn freilich die mit Vorliebe immer wieder betonte "Gemeinschaftsbezogenheit" des Bürgers nicht zum Einfallstor restloser Steuerbarkeit werden soll, muß nach den Bedingungen, unter denen Information in einem demokratischen Sozialstaat verarbeitet werden darf, personenbezogene Daten also zugänglich und übermittelbar sein können, mehr denn je gefragt werden. Eben deshalb ist es falsch, ja unzulässig, die Diskussion über den Datenschutz auf wie auch immer verstandene "Mißbrauchsfälle" reduzieren zu wollen. Sie ist und bleibt eine Auseinandersetzung mit den sich aus der im Grundgesetz definierten Staatsstruktur und den von ihm garantierten Grundrechten ergebenden Konsequenzen für die Informationsverteilung.

1.1.3
Zur Notwendigkeit bereichsspezifischer Regelungen

Beides, die Entscheidung des Bundesverfassungsgerichts zum VZG und die zunehmenden Tendenzen, die Datenverarbeitung als Kontrollinstrument zu nutzen, verleihen der Diskussion über die Novellierung des Bundesdatenschutzgesetzes ein ganz besonderes Gewicht. Sie wird zum gleichsam natürlichen Ansatzpunkt, um sowohl die Konsequenzen aus der Entscheidung des Bundesverfassungsgerichts zu ziehen als auch die möglichen Reaktionen auf den sich ausweitenden Zugriff auf personenbezogene Daten zu prüfen. Die früheren Tätigkeitsberichte sind wiederholt und ausführlich auf die Novellierung eingegangen. Eines hat sich seither verändert: Der im Bundesministerium des Innern ausgearbeitete Novellierungsentwurf ist auf den entschiedenen Widerstand der Datenschutzbeauftragten des Bundes und der Länder gestoßen. Sie haben sich keineswegs der Novellierung widersetzt. Ihre in der Erklärung vom 4. November 1983 festgehaltene Kritik richtet sich gegen die bislang vorgelegten Vorschläge. Sie muß aber auch als Warnung verstanden werden, die Fortentwicklung des Datenschutzes ausschließlich als Korrektur des Bundesdatenschutzgesetzes zu verstehen und auszugeben. So wichtig es ist, das BDSG zu überprüfen und zu ergänzen, so wenig darf darüber die Notwendigkeit vergessen werden, den Datenschutz bereichsspezifisch auszubauen. Erst in den bereichsspezifischen Regelungen lassen sich Konflikte konkret ansprechen und ist es deshalb auch möglich, Vorkehrungen zu formulieren, die sich nicht in der Abstraktion der BDSG-Regeln verlieren, sondern an den Besonderheiten der jeweils behandelten Problembereiche orientieren. Jeder Verzicht auf bereichsspezifische Regelungen ist eine Flucht aus der im Interesse des Betroffenen und der datenverarbeitenden Stellen notwendigen, zugleich um der Rechtsstaatlichkeit des Datenschutzes willen unerläßlichen Präzision der Verarbeitungsanforderungen.

1.1.3.1
Sicherheitsbehörden

Wie dringend bereichsspezifische Regelungen erforderlich sind, zeigt sich an zwei im Tätigkeitsbericht ausführlich behandelten Beispielen, dem maschinenlesbaren Ausweis (vgl. Ziff. 3.1) sowie den Personalinformationssystemen (vgl. Ziff. 3.3). Unstreitig enthält das Personalausweisgesetz Datenschutzvorschriften; diese Bestimmungen reichen jedoch in keinem Fall aus. Der Personalausweis bleibt unter Datenschutzgesichtspunkten solange unannehmbar, wie seiner Einführung nicht strikte, den Datenschutz im polizeilichen Bereich verbindlich regelnde gesetzliche Vorschriften vorausgehen. Ganz in diesem Sinn hat der Deutsche Bundestag in seiner Entschließung vom 17. Januar 1980 die Verknüpfung des Personalausweisgesetzes mit weiteren bereichsspezifischen Vorschriften im Sicherheits- und Meldebereich betont. Diese Verknüpfung läßt sich weder auflösen noch in einer beliebigen Reihenfolge konkretisieren. Erst recht geht es nicht an, sich mit dem Hinweis auf das inzwischen verabschiedete Melderechtsrahmengesetz zufriedenzugeben sowie im übrigen auf einzelne Verwaltungsvorschriften wie etwa die KpS-Richtlinien zu verweisen. Ganz abgesehen davon, daß einzelne dieser Bestimmungen, soweit sie etwa die Amtshilfe betreffen, wohl immer noch umstritten sind, hat keine von ihnen Gesetzesqualität. Sie sind ihrer ganzen Entstehungsgeschichte nach nur Vorbereitung einer späteren gesetzlichen Regelung, erste Annäherung also und nicht definitive Antwort auf die Datenschutzanforderungen.

Spätestens mit der beabsichtigten Einführung des Personalausweises ist der Gesetzgeber jedoch gezwungen, den längst fälligen Schritt einer bereichsspezifischen Regelung für den Sicherheitsbereich zu vollziehen. Der Tätigkeitsbericht weist einmal mehr auf die Schwerpunkte einer solchen Regelung hin (vgl. insbesondere Ziff. 3.1.3.3). Ihre Notwendigkeit wird gerade durch die Entscheidung des Bundesverfassungsgerichts bestätigt. Das Recht des einzelnen, über die Verarbeitung der seine Person betreffenden Daten zu bestimmen, hört nicht im Sicherheitsbereich auf. So wichtig deshalb der Zugang zu personenbezogenen Daten für die Erfüllung der polizeilichen Aufgaben sein mag, die Polizei bleibt ebenso wie jede andere Sicherheitsbehörde an die im Grundgesetz verankerte Bedingung gebunden, Einschränkungen der informationellen Selbstbestimmung von einer gesetzlichen Regelung abhängig zu machen. Eine Alternative zu gesetzlich formulierten Verarbeitungsvoraussetzungen gibt es ebensowenig wie zu der vom Bundesverfassungsgericht genauso betonten Notwendigkeit, die Zwecke der Verarbeitung präzise zu formulieren und den Verarbeitungsumfang damit eindeutig einzuschränken.

1.1.3.2
Arbeitnehmerdatenschutz

Nicht minder wichtig ist es, die Verarbeitung von Arbeitnehmerdaten endlich gesetzlich zu regeln. Der Tätigkeitsbericht (vgl. Ziff. 3.3) läßt zunächst eines deutlich erkennen: Personalinformationssysteme sind, allen gegenteiligen Behauptungen zum Trotz, keineswegs nur in der Privatwirtschaft anzutreffen. Die gleichen Überlegungen, die Privatunternehmen veranlassen, sich der Vorteile automatischer Verarbeitung zu bedienen, von einer effizienteren Personaladministration bis hin zu einer konsequenten Personalplanung, spielen auch im öffentlichen Dienst eine entscheidende Rolle. Wo deshalb Arbeit geleistet wird, ist letztlich gleichgültig. In jedem Fall sehen sich die Arbeitnehmer mit Systemen konfrontiert, deren unbestreitbares Ziel es ist, die jeweils verfolgten Aufgaben auch und gerade durch eine zielgerichtete Verwertung ihrer Daten zu erreichen. In jedem Fall entstehen daher mit der multifunktionalen Nutzung der Daten just die Gefahren, die Betriebsverfassungs- und Personalvertretungsgesetz etwa dann ansprechen, wenn sie die Mitbestimmung bei Vorkehrungen, die zu einer Überwachung der Arbeitnehmer führen, garantieren.

Der Tätigkeitsbericht zeigt aber auch, wie wenig es angeht, den Arbeitnehmerdatenschutz in wie auch immer formulierten, allgemeinen, dem Bundesdatenschutzgesetz angehängten Bestimmungen abzuhandeln. Allzu breit ist die Palette der Probleme, von den Individualrechten der Arbeitnehmer über die notwendige Mitbestimmung der Betriebs- und Personalräte bis hin zur Kontrolle der Verarbeitung von Arbeitnehmerdaten durch die Arbeitnehmervertretung. Allzu sehr kommt es im übrigen darauf an, die verschiedenen, von der arbeitsrechtlichen Gesetzgebung und Rechtsprechung bereits formulierten Regelungsansatzpunkte aufzunehmen und fortzuentwickeln. Nur: In fast keinem anderen Bereich ist die Notwendigkeit einer gesetzlichen Regelung so evident, nirgendwo anders kommt es daher so sehr darauf an, Verarbeitungsschranken aufzurichten, die von den konkreten Verarbeitungsvoraussetzungen von Arbeitnehmerdaten ausgehen und auf sie zugeschnitten sind.

1.1.3.3
Informationstechnik

Um Bedeutung und Tragweite einer Novellierung des Bundesdatenschutzgesetzes richtig einzuschätzen, gilt es darüber hinaus, das radikal veränderte technische Umfeld des Datenschutzes sorgfältig zu berücksichtigen. Gerade deshalb enthält der diesjährige Tätigkeitsbericht einen langen, dem Bildschirmtext gewidmeten Abschnitt (vgl. Ziff. 3.4, vor allem Ziff. 3.4.2). Er verdeutlicht, wie sehr mittlerweile die Informationstechnik ein Stadium erreicht hat, das die bislang für überzeugend und ausreichend gehaltenen Ansatzpunkte der Datenschutzregelung, von der

Datei bis zu der Beschreibung der einzelnen Verarbeitungsphasen, endgültig in die Geschichte des Datenschutzes verweist. Wo dezentrale Verarbeitung, Dialogsysteme und "intelligente" Chipkarten die Realität der Datenverarbeitung bestimmen, ist für die bisherigen Datenschutzvorschriften kein Platz mehr. Deshalb geht es nicht mehr an, die immer wieder geforderte, schon präzise formulierte Regelung für den Direktzugriff weiter aufzuschieben. Vorschriften, wie sie der Novellierungsentwurf enthält, reichen in keinem Fall aus. Erst recht kommt es aber darauf an, jetzt schon Überlegungen darüber anzustellen, wie denn Datenschutz auch und gerade in Kenntnis der vom Bundesverfassungsgericht formulierten Anforderungen unter den Bedingungen einer sich ständig weiterentwickelnden Informationstechnik garantiert werden kann. Die Erfahrung der siebziger Jahre darf nicht wiederholt werden. Konkret: Der Gesetzgeber muß seine Erwartungen so rechtzeitig formulieren, daß sie in den Prozeß der Entwicklung und Nutzung des technischen Instrumentariums eingehen, ja ihn mitprägen. Anders ausgedrückt: Datenschutzbestimmungen haben nur dann eine echte Chance, wirksame Vorkehrungen zu treffen, wenn sie nicht späte Reaktion auf ein längst realisiertes technisches Instrumentarium sind, sondern zu den zentralen Entstehungsbedingungen für eben dieses Instrumentarium zählen.

1.1.4
Kritik der BDSG-Novelle

Wendet man sich nun den eigentlichen Novellierungsvorschlägen zu, dann zeigt sich alsbald, wie weit sie davon entfernt sind, den zuletzt vom Bundesverfassungsgericht nachdrücklich bestätigten Grundforderungen des Datenschutzes Rechnung zu tragen. Drei Beispiele:

1.1.4.1
Zweckbindung

Der Datenschutz steht und fällt mit der Zweckbindung der Verarbeitung. An der Bereitschaft, sie zu garantieren, messen sich deshalb Tragweite und Überzeugungskraft einer Datenschutzregelung. Das Bundesdatenschutzgesetz beläßt es bei einzelnen, allerdings durchaus in die Richtung einer Zweckbindung deutenden Hinweisen. Die Novellierungsvorschläge gehen der längst fälligen Korrektur aus dem Weg. Bestenfalls bei der Verarbeitung im nicht-öffentlichen Bereich finden sich Ansätze für eine entsprechende Formulierung. Der öffentliche Bereich wird dagegen sorgfältig ausgespart. Für beide Bereiche muß aber unzweideutig gelten: Eine Verarbeitung personenbezogener Daten darf erst stattfinden, wenn der Verarbeitungszweck zuvor unmißverständlich und für den Betroffenen ebenso wie für jeden Dritten nachvollziehbar definiert worden ist.

Eine ernst genommene Zweckbindung verpflichtet insofern dazu, die Aufgaben der jeweiligen speichernden Stelle genau zu umschreiben. Nicht von ungefähr spricht sich das Bayerische Datenschutzgesetz (Art. 16 Abs. 1) für die Festlegung des Aufgabenbereiches durch eine Rechtsnorm aus. Damit soll einerseits ein Höchstmaß an Transparenz erreicht und andererseits die Kontrolle der Verarbeitungsvorgänge erleichtert, wenn nicht sogar überhaupt erst ermöglicht werden. Kurzum, an Vorbildern fehlt es nicht. Der Bundesgesetzgeber braucht sie nur aufzugreifen und den von ihnen gewiesenen Weg konsequent weiterzugehen.

Nur dann kann es wirklich gelingen, alle Bestrebungen zurückzuweisen, doch noch einen möglichst uneingeschränkten Umlauf der Daten im öffentlichen Bereich sicherzustellen. Gewiß, derlei Ziele werden nicht zuletzt mit Rücksicht auf die Datenschutzgesetze nur selten offen verfolgt. Wie sehr sie aber nach wie vor die Informationserwartungen und das Informationsverhalten beherrschen, zeigt sich nicht zuletzt an den Bestrebungen, die Verantwortung für die Übermittlung allein demjenigen zuzuweisen, der die Angaben haben möchte. Der Sinn einer solchen Regelung liegt auf der Hand: Lästige Informationsschranken sollen abgebaut, die Zirkulation der Daten soll erleichtert werden. Spätestens daran erweist sich, wie wenig es mit einem bloßen, noch dazu sehr allgemein gehaltenen Bekenntnis zur Zweckbindung getan ist. Vielmehr bedarf es zusätzlicher Regelungen, die etwa bei der Übermittlung den Zeitpunkt genau festmachen, zu dem die Zweckbindung geprüft werden muß und die Verantwortung keineswegs beim Empfänger belassen. Die Daten müssen solange bei der speichernden Stelle bleiben, wie diese sich nicht davon überzeugt hat, welche Ziele der Empfänger bei der Verarbeitung verfolgt und ob diese Ziele von seinen rechtmäßigen Aufgaben gedeckt sind.

1.1.4.2
Auskunftsrecht

Die Novellierungsvorschläge unterlaufen das Recht des Betroffenen, Auskunft über die zu seiner Person verarbeiteten Angaben zu erhalten. Informationelle Selbstbestimmung setzt vor allem anderen korrekte und vollständige Kenntnis der Verarbeitung voraus. Solange der Gesetzgeber das Auskunftsrecht des einzelnen durch nichtssagende Generalklauseln ganz oder auch nur für bestimmte Bereiche eskamotiert, ja offen ausschließt, verstößt er gegen die sich aus dem Grundgesetz ergebenden Anforderungen an die Regelung der Datenverarbeitung. Erst recht geht es nicht an, eine generelle Befreiung von der Begründungspflicht für verweigerte Auskünfte vorzusehen. An der Auskunftspflicht entscheidet sich die Chance des Betroffenen, sich in den Verarbeitungsprozeß einzuschalten und auf ihn Einfluß nehmen zu können. Eine gesetzliche Regelung, die ihm den Datenzugang verweigert, macht aus ihm ein bloßes Informationsobjekt, nimmt ihn also nur noch als Informationslieferanten wahr.

1.1.4.3
Datenschutzkontrolle

Der Datenschutz bleibt solange folgenlose Zusicherung, wie die Verarbeitungskontrolle nicht gesichert ist. Nun mag es ohne Zweifel mehr als ein Kontrollmodell geben. Der Gesetzgeber hat freilich keine Wahl. Er muß sich, wie auch das Bundesverfassungsgericht betont, für eine unabhängige Kontrolle entscheiden und zugleich alle Vorkehrungen treffen, die eine ebenso umfassende wie wirksame Überwachung garantieren. Konsequenterweise haben sich deshalb die Datenschutzgesetze für selbständige Kontrollinstanzen ausgesprochen. Die immer mehr um sich greifenden Tendenzen, die Überwachung möglichst einzuschränken, stehen deshalb in krassem Gegensatz zu den Grundvoraussetzungen des Datenschutzes. Der Versuch, das Steuergeheimnis gegen die Kontrollbefugnis auszuspielen, ist dafür ebenso bezeichnend wie die Bestrebungen, eine Überwachung im Sicherheitsbereich nur noch beschränkt zuzulassen, oder die Intervention des Datenschutzbeauftragten von vornherein auf die Verarbeitung personenbezogener Daten in "Dateien" zu begrenzen. Umsonst wird man freilich in der Novellierung eine deutliche Absage an alle diese Tendenzen suchen. Sie nimmt im Gegenteil eine Entwicklung hin, die den Datenschutz offen in Frage stellt. Wenn aber Korrekturen des Bundesdatenschutzgesetzes einen Sinn haben sollen, so in jedem Fall dort, wo die Interpretation des Gesetzes mehr und mehr dazu genutzt wird, um seine Ziele ins Gegenteil zu verkehren. Gewiß, die Erfahrungen sind nicht in allen Ländern gleich. Konflikte, die anderswo mittlerweile alltäglich sind, haben sich etwa in Hessen nicht wiederholt. Zur Debatte steht aber gegenwärtig einzig und allein die Novellierung des Bundesdatenschutzgesetzes. Es hat mit seinen Vorschriften die Grundlage für die entsprechenden Kontrollbestimmungen in den Landesdatenschutzgesetzen abgegeben. Insofern gehört es zu den wichtigsten Verpflichtungen des Bundesgesetzgebers, der Verkürzung der Kontrolle entgegenzuwirken.

1.1.4.4
Novellierungsinitiative auf Landesebene

Ein Mißverständnis gilt es jedoch zu vermeiden: Die Novellierungsdiskussion mag ein durchaus naheliegender Anlaß sein, um die Zweckbindung der Verarbeitung ebenso sicherzustellen wie das Auskunftsrecht des Betroffenen und die Kontrollbefugnisse der Datenschutzbeauftragten. In allen drei Fällen handelt es sich allerdings keineswegs nur um an die Adresse des Bundesgesetzgebers gerichtete Forderungen. Der gleiche Maßstab ist auch an die Landesdatenschutzgesetze anzulegen. Sicher, vieles spricht dafür, in der Novellierung des Bundesdatenschutzgesetzes die Vorstufe einer Revision der Landesdatenschutzgesetze zu sehen. Gerade weil aber durchweg Grundvoraussetzungen des Datenschutzes auf dem Spiel stehen, kann und darf der Landesgesetzgeber die eigene Tätigkeit nicht beliebig lange zurückstellen. Mit jeder weiteren Verzögerung der BDSG-Novellierung zeichnet sich deshalb die Notwendigkeit schärfer ab, die Initiative zu übernehmen, um nicht zuletzt dort, wo das Bundesdatenschutzgesetz als Vorgabe gedient hat, die Datenschutzregelung auf ihre Vereinbarkeit mit den auch und gerade vom Bundesverfassungsgericht formulierten Verarbeitungsbedingungen hin zu überprüfen und zu ergänzen.

1.2
Das Volkszählungs-Urteil des Bundesverfassungsgerichts

1.2.1
Konsequenzen für Gesetzgeber und Verwaltung

Das Bundesverfassungsgericht hat in seiner Entscheidung vom 15. Dezember 1983 die im Volkszählungsgesetz vorgesehene Verknüpfung von Statistik und Verwaltung für verfassungswidrig erklärt, jeden weiteren Versuch einer "Volkszählung" an eine Reihe inhaltlicher und organisatorischer Voraussetzungen gebunden und die verfassungsrechtlichen Grundbedingungen des Datenschutzes formuliert. Mit zu den wichtigsten Aufgaben der nächsten Monate wird es deshalb zählen, sich mit den weitreichenden Konsequenzen der Entscheidung zum Volkszählungsgesetz auseinanderzusetzen. Schon jetzt lassen sich aber bestimmte, für die Bundes- und Landesgesetzgebung besonders bedeutsame Folgerungen ziehen:

1. Eine Volkszählung darf künftig nur noch als reine Statistik durchgeführt werden. Übermittlungen von Einzelangaben aus der Volkszählung an Behörden oder Gemeinden zu anderen als statistischen Zwecken sind in Zukunft ausgeschlossen. Auch Einzelangaben dürfen jedoch nur dann übermittelt werden, wenn durch Rechtsvorschrift, Organisation und geeignete Verfahren sichergestellt ist, daß die statistische Zweckbindung der Daten strikt eingehalten wird und keine Vermischung administrativer und statistischer Aufgaben eintreten kann.

   Der Bürger hat das Recht, seine Auskunft im verschlossenen Umschlag kostenlos - auch auf dem Postwege - der Zähldienststelle zuzusenden. Er muß über seine Rechte und Pflichten schriftlich belehrt werden; er ist darüber aufzuklären, welche Angaben lediglich auf freiwilliger Grundlage erhoben werden (wie bei der vorgesehenen Volkszählung die Telefonnummer) und welche Merkmale lediglich Hilfsmittel der Erhebung sind. Grundrechtssichernde Funktion mißt das Gericht auch der Trennung der Identifikationsmerkmale (insbesondere Namen, Kennummern und Zählerlistennummern) von den übrigen statistischen Angaben bei, diese Merkmale sind zum

frühest möglichen Zeitpunkt zu löschen und bis dahin von den übrigen Angaben getrennt "unter Verschluß zu halten". Schließlich sollen Zähler nicht in ihrer Nachbarschaft eingesetzt und auf den Einsatz solcher Zähler soll verzichtet werden, bei denen im Hinblick auf ihre dienstliche Tätigkeit Interessenkonflikte nicht auszuschließen sind. Das Legalisierungsprinzip der amtlichen Statistik und die streng gesetzeskonforme Fassung der Fragebögen fordert das Gericht mit dem Hinweis auf die Absicht, alle Auskunftspflichtigen von vornherein nach Haushalten zu erfassen, obwohl das Volkszählungsgesetz nur eine persönliche Auskunftspflicht des einzelnen Bürgers vorsah. Das Urteil enthält die deutliche Empfehlung an den Statistikgesetzgeber, diese "grundrechtssichernden Maßnahmen" zu garantieren, auch wenn er nicht selbst alles regeln muß. Beim Fragebogen wird er auf die Möglichkeit seiner Feststellung durch Rechtsverordnung hingewiesen.

Doch damit nicht genug: der Gesetzgeber muß von nun an ständig prüfen, ob eine Totalerhebung nach dem jeweils aktuellen Stand der sozialwissenschaftlichen und statistischen Methoden noch verhältnismäßig ist. Seine "Methodenwahl" ist also jeweils wissenschaftlich zu legitimieren mit der Pflicht, bei geänderten Umständen gegebenenfalls von einer Befragung aller Bürger abzusehen. Die Entscheidung des Bundesverfassungsgerichts hat damit zahlreiche Bedenken - vor allem der Datenschutzbeauftragten - aufgegriffen und zukünftige Volkszählungen, wie international üblich, zu "reinen" Statistiken gemacht.

2. Auch im Hinblick auf die Landes- und Kommunalstatistik bleibt das Volkszählungsurteil nicht ohne Auswirkungen. Der Landesgesetzgeber wird nun nicht mehr umhin können, Landesstatistiken gesetzlich zu regeln (vgl. schon meinen Neunten Tätigkeitsbericht für 1980, Ziff. 2.3.1.). Die Kommunalstatistik und die Stadtentwicklungsplanung bedürfen einer gesetzlichen Grundlage und ebenso einer gesetzlich garantierten Abschottung zu der übrigen Gemeindeorganisation in der Hessischen Gemeindeordnung. Das Bundesverfassungsgericht sieht dies als ein Gebot der "informationellen Gewaltenteilung" an.

3. Das vom Gericht als "informationelles Selbstbestimmungsrecht" aufgegriffene und konkretisierte allgemeine Persönlichkeitsrecht nach Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 Grundgesetz hat über die Statistik hinaus auch für den Datenschutz insgesamt erhebliche Folgen. Aufgabe des Gesetzgebers muß es sein, durch gezielte Regelungen die Transparenz der Datenverarbeitung zu sichern und die Entstehung einer Rechtsordnung zu verhindern, in der Grundrechte nicht mehr ausgeübt werden können, weil der Bürger "nicht mehr wissen (kann), wer was wann und bei welcher Gelegenheit über ihn weiß".

   Unabdingbar ist insbesondere eine gesetzliche Regelung für die Informationsverarbeitung durch die Sicherheitsbehörden. Die polizeiliche Beobachtung und die Rasterfahndung sind nunmehr vordringlich nach den Maßstäben dieses Urteils einzuschränken; die ausufernde und sich am Rande der Rechtsstaatlichkeit bewegende Überwachungspraxis im Staatsschutzbereich ist auf ihr von der Verfassung vorgesehenes Maß einzugrenzen. Auch die von mir wiederholt angemahnte Befugnisnorm für die Sammlung und Auswertung persönlicher Daten durch das Landesamt für Verfassungsschutz ist nach den Kriterien des informationellen Selbstbestimmungsrechts endlich zu realisieren. Das Auskunftsrecht des Bürgers muß auch bei den Sicherheitsbehörden ausgebaut werden. Wohlgemerkt: Keinesfalls geht es darum, lediglich die bisherige Praxis in Gesetzesform zu fassen und damit nachträglich zu bestätigen; sie ist vielmehr von Grund auf an Hand der vom Verfassungsgericht vorgegebenen Leitlinien zu überprüfen.

4. Das Verbot des Personenkennzeichens und seiner Substitute wird die Verwaltungspraxis im Sozialleistungssektor und im Meldewesen erheblich beeinflussen. Die Schaffung kompatibler Strukturen - wie der Bundesmeldedatensatz oder die einheitliche Sozialversicherungsnummer -, die räumlich verteilte Datenbanken erschließen und verknüpfen können, ist damit unzulässig.

5. Das Urteil bleibt auch für den maschinenlesbaren Personalausweis nicht folgenlos. Schon im Hinblick auf die auch in der Entschließung des Bundestages vom 17. Januar 1980 bestätigte unabdingbare Koppelung mit Datenschutzregelungen im Sicherheitsbereich ist von seiner Einführung jedenfalls solange abzusehen, wie es an klaren gesetzlichen Vorschriften für die Speicherung und Verwendung personenbezogener Daten in diesem Bereich fehlt. Abgesehen davon muß gewährleistet sein, daß alle technischen Vorkehrungen getroffen sind, daß nicht der maschinenlesbare Ausweis zum - vom Verfassungsgericht verbotenen - Surrogat eines Personenkennzeichens werden kann. Sein rechtlicher und technischer Verwendungszusammenhang muß umgehend klargestellt werden. In diesem Zusammenhang muß die Rechtsgrundlage der polizeilichen Identitätsfeststellung, insbesondere der Einrichtung von Kontrollstellen, auf das Gefährdungspotential der massenhaften Verwendungsmöglichkeit des Ausweises hin überprüft werden.

6. Auch der vorgelegte Referentenentwurf der Bundesregierung zur Novellierung des Bundesdatenschutzgesetzes kann in weiten Teilen nicht mehr aufrechterhalten werden. Das Bundesverfassungsgericht hat die Erhebung und die Verwendung von Daten zu regelungsbedürftigen Phasen personenbezogener Datenverarbeitung erklärt. Es hat die Bedeutung der Auskunfts-, Berichtigungs- und Löschungsrechte hervorgehoben und restriktive Übermittlungsregelungen gefordert. Die Stellung der Datenschutzbeauftragten und ihre Funktion wurde

verfassungsrechtlich institutionalisiert; keine personenbezogene Datenverarbeitung darf ohne Kontrolle durch unabhängige Datenschutzbeauftragte überhaupt stattfinden. Dies gilt auch und gerade in den Bereichen, für die besondere Geheimhaltungsbestimmungen (wie z.B. in diesem Fall das Statistikgeheimnis oder auch z.B. des Steuergeheimnis) einen besonders intensiven Datenschutz vorsehen. Dies ist eine deutliche Mahnung an eine Reihe von Behörden - etwa die Finanzverwaltung -, ihre bisherige Haltung aufzugeben und wirksame Kontrollen durch die Datenschutzbeauftragten nicht weiter zu behindern.

7. Der Gesetzgeber muß sich nach diesem Urteil darüber im klaren sein, daß es mit Generalklauseln und Querschnittsgesetzgebung allein nicht getan ist. Überall dort, wo Angaben vom Bürger gefordert werden, verlangt das Gericht bereichsspezifische, auf den Verwendungszweck zugeschnittene Informationsverarbeitungsregelungen. Der Gesetzgeber hat jede dieser Regelungen nicht nur auf die rechtlichen, sondern auch auf die technischen Verwendungs- und Verknüpfungsmöglichkeiten hin zu prüfen.

1.2.2
Rückblende: Chronologie

(1) **22. November 1973**

Richtlinie des Rates der Europäischen Gemeinschaften zur Synchronisierung der allgemeinen Volkszählungen im Zeitraum zwischen dem 1. März und dem 31. Mai 1981 (73/403 EWG; Amtsblatt der EG Nr. L 347/50)

(2) **September 1978**

Regierungsentwurf für ein Volkszählungsgesetz 1981
(8. Legislaturperiode BR-Drucks. 444/78)

(3) **15. Februar 1979**

138. Sitzung der 8. Legislaturperiode des Deutschen Bundestages: Überweisung an den Innenausschuß (federführend), an die Ausschüsse für Wirtschaft, für Arbeit und Sozialordnung, für Raumordnung, Bauwesen und Städtebau (mitberatend) sowie an den Haushaltsausschuß

(4) **23. März 1979**

Anhörung der Datenschutzbeauftragten Bayerns, Hessens und des Bundes durch die Berichterstattergruppe "Statistik" des Innenausschusses des Deutschen Bundestages. Darlegung der Bedenken gegen den Melderegisterabgleich und die Vermischung administrativer und statistischer Funktionen. Gleichlautende Stellungnahme an die Hessische Landesregierung.

(5) **Juli 1980**

Scheitern des Gesetzentwurfs zum Volkszählungsgesetz 1981 nach zwei Vermittlungsverfahren. Der Bundesrat weigert sich, einem Gesetzesbeschluß des Bundestages ohne Finanzzuweisung des Bundes an die Länder zuzustimmen.

(6) **Februar 1981**

Die Bundesregierung bringt in der 9. Legislaturperiode einen neuen Volkszählungsgesetzentwurf mit dem Zählungsstichtag 19. Mai 1982 ein.

(7) **2. Dezember 1981**

Der Bundestag beschließt einstimmig - nach Einschaltung der Berichterstattergruppe Statistik - das Gesetz in der vom Innenausschuß vorgeschlagenen Fassung. Datenschutzbeauftragte wurden in dieser Beratungsphase nicht angehört.

(8) **14. Dezember 1981**

Der Rat der Europäischen Gemeinschaften gestattet der Bundesrepublik Deutschland, von dem für die übrigen Mitgliedsstaaten festgelegten Zählungstermin abzuweichen
(Richtlinie Nr. 81/1059 EWG vom 14. Dezember 1981 - ABl.der EG Nr. L 385 vom 31. Dezember 1981, S. 33).

(9) **18. Dezember 1981**

Der Bundesrat verlangt wegen der strittigen Finanzzuweisung die Einberufung des Vermittlungsausschusses.

(10) **Februar 1982**

Im Vermittlungsausschuß werden neben finanzwirksamen Maßnahmen folgende materielle Regelungen festgelegt:

1. § 9 Abs.3 VZG: Übermittlung aller Angaben aus der Volkszählung für gemeindestatistische Zwecke. Streichung des Satzungsvorbehalts (Erforderlichkeit einer Statistiksatzung) für die Gemeinden;
2. der Melderegisterabgleich und sein Umfang;
3. die Einschränkung des Rechtsschutzes durch Aufhebung der aufschiebenden Wirkung des Widerspruchs gegen die Aufforderung zur Auskunftserteilung.

(11) **4. März 1982**

Der Bundestag stimmt den Einigungsvorschlägen des Vermittlungsausschusses zu.

(12) **5. März 1982**

Der Bundesrat stimmt den Vorschlägen des Vermittlungsausschusses ebenfalls zu. Wegen der Dauer der parlamentarischen Beratungen wird der Zählungsstichtag auf Vorschlag des Innenausschusses auf den 27. April 1983 festgesetzt.

(13) **25. März 1982**

Verkündung des Volkszählungsgesetzes im Bundesgesetzblatt (BGBl. I S. 369).

(14) **21. Februar bzw. 5. März 1983**

Einlegung der Verfassungsbeschwerden des Jurastudenten Frhr. von Mirbach und der Rechtsanwältinnen Dr.Wild und Stadler-Euler

(15) **23. Februar 1983**

Der Innenausschuß des Hessischen Landtags beschließt, die Landesregierung und den Datenschutzbeauftragten zu bitten, zu Datenschutzproblemen der Volkszählung Auskunft zu geben.

(16) **14. März 1983**

Zwischenbericht des Hessischen Datenschutzbeauftragten zur Volkszählung an den Hessischen Landtag (Drucks. 10/0573 vom 14. März 1983).

(17) **16. März 1983**

Der Innenausschuß des Hessischen Landtags diskutiert den Bericht des Datenschutzbeauftragten und die Stellungnahme der Landesregierung. Die Arbeitsgruppe Datenverarbeitung und Datenschutz wird gebeten, Bericht und Stellungnahme noch einmal zu behandeln.

(18) **22. März 1983**

Die Arbeitsgruppe Datenverarbeitung und Datenschutz behandelt den Zwischenbericht.

(19) **22. März 1983**

Die Konferenz der Datenschutzbeauftragten beschließt einen 15-Punkte-Katalog erforderlicher Datenschutzmaßnahmen bei der Durchführung der Volkszählung (vgl. unten Ziff. 5.2.2).

(20) **25. März 1983**

Frist zur Stellungnahme gegenüber dem Bundesverfassungsgericht zum Antrag auf Erlaß einer einstweiligen Anordnung, die Volkszählung 1983 bis zur Entscheidung über verschiedene gegen das VZG 1983 erhobene Verfassungsbeschwerden in der Hauptsache auszusetzen. Vorlage der Stellungnahme des Hessischen Datenschutzbeauftragten (vgl. unten Ziff. 5.2.3).

(21) **2. April 1983**

Zum Antrag auf Erlaß einer einstweiligen Anordnung findet eine mündliche Verhandlung vor dem 1. Senat des Bundesverfassungsgerichts statt, in der sich auch der Hessische Datenschutzbeauftragte äußert.

(22) **13. April 1983**

Der 1. Senat des Bundesverfassungsgericht setzt die Durchführung der Volkszählung im Wege der einstweiligen Anordnung aus.

(23) **30. Juni 1983**

Frist zur Stellungnahme für das Verfahren in der Hauptsache. Zweite schriftliche, ausführliche Stellungnahme des Hessischen Datenschutzbeauftragten (vgl. unten Ziff. 5.2.4).

(24) **18./19. Oktober 1983**

Mündliche Verhandlung im Hauptsacheverfahren.

(25) **15. Dezember 1983**

Verkündung des Urteils des Bundesverfassungsgerichts zum Volkszählungsgesetz 1983 (1 BVR 209/83 u.a.) mit folgendem Tenor:

"1. § 2 Nummer 1 bis 7 sowie §§ 3 bis 5 des Gesetzes über eine Volks-, Berufs-, Wohnungs- und Arbeitsstättenzählung (Volkszählungsgesetz 1983) vom 25. März 1982 (Bundesgesetzbl. I S. 369) sind mit dem Grundgesetz vereinbar; jedoch hat der Gesetzgeber nach Maßgabe der Gründe für ergänzende Regelungen der Organisation und des Verfahrens der Volkszählung Sorge zu tragen.

2. § 9 Absatz 1 bis 3 des Volkszählungsgesetzes 1983 ist mit Artikel 2 Absatz 1 in Verbindung mit Artikel 1 Absatz 1 des Grundgesetzes unvereinbar und nichtig.

3. Die Beschwerdeführer werden durch das Volkszählungsgesetz 1983 in dem aus Nummer 1 und 2 ersichtlichen Umfang in ihren Grundrechten aus Artikel 2 Absatz 1 in Verbindung mit Artikel 1 Absatz 1 des Grundgesetzes verletzt. Im übrigen werden die Verfassungsbeschwerden zurückgewiesen.

4. Die Bundesrepublik Deutschland hat den Beschwerdeführern die notwendigen Auslagen zu erstatten."

2. Bilanz

2.1
Zum 11. Tätigkeitsbericht für 1982 (Drucks. 10/166)

2.1.1
Richtlinien zur Datenverarbeitung der Hochschulen (Ziff. 2.1.3)

Der Hessische Kultusminister hat die in meinem letzten Bericht (vgl. Ziff. 2.1.3) angemahnten "Richtlinien zur Gewährleistung des Datenschutzes und der Datensicherung bei den Datenverarbeitungseinrichtungen der hessischen Hochschulen" mit Erlaß vom 14. Januar 1983 verkündet. Ihr Inhalt entspricht mit geringfügigen Abweichungen dem Text, den ich in meinem 10. Tätigkeitsbericht als Entwurf abgedruckt hatte (Ziff. 5.1) und an dessen Formulierung ich maßgeblich beteiligt war. Die Richtlinien unterscheiden diejenigen ADV-Anlagen, auf denen personenbezogene Daten verarbeitet werden, von denen, die zur Verarbeitung naturwissenschaftlich-technischer oder Strukturdaten benutzt werden. Nur die ersteren unterliegen den Richtlinien; Voraussetzung für ihren Betrieb ist eine besondere Zulassung.

Dieses Modell der organisationsinternen und funktionsbezogenen Lizenzierung von solchen ADV-Einrichtungen, die personenbezogene Daten verarbeiten, ist der erste Versuch auf der Ebene von Verwaltungsvorschriften und Richtlinien, eine Art Zulassungsmodell für personenbezogene Datenverarbeitung, das auch hard-ware miteinschließt, auf seine Wirksamkeit hin zu testen. Dieses Modell erlaubt die Konzentration der personenbezogenen Datenverarbeitung auf einzelne Anlagen und damit gleichzeitig auch eine ökonomische und effektive Zuordnung von technischen und organisatorischen Datensicherungsmaßnahmen. Es verhindert insgesamt die "Verbunkerung" der wissenschaftlichen Datenverarbeitung, die zwar im Hinblick auf die Daten optimal gesichert, zugleich aber als Einrichtung von Forschung und Lehre soweit wie möglich frei und für jedermann zugänglich sein soll. Anhand dieses Beispiels wird zugleich zu prüfen sein, ob diese Art von Lizenzierungsmodell sich auch auf gesetzlicher Ebene in Teilbereichen empfiehlt, etwa um die Probleme des Einsatzes von Personalcomputern oder Personalinformationssystemen in den Griff zu bekommen. Das bisherige Datenschutzkonzept als "Datenverkehrsordnung" wird dadurch - um im Bilde zu bleiben -durch eine "Datenverkehrszulassungsordnung" ergänzt.

2.1.2
Die Fortentwicklung des Melderechts (Ziff. 2.2.1)

2.1.2.1
Die Ergänzung des rechtlichen Rahmens

Das Hessische Meldegesetz wurde im Juni 1982 als eines der ersten Landesmeldegesetze vom Landtag verabschiedet. Die Rolle des Vorreiters hat das Gesetz in mancherlei Hinsicht bewahren können. So hat es sich gerade jetzt in der Diskussion um die Einführung des maschinenlesbaren Personalausweises als hilfreich erwiesen, daß in den hessischen Melderegistern im Gegensatz zu der Praxis in einer Reihe anderer Bundesländer die Seriennummern von Paß und Personalausweis nicht gespeichert werden dürfen. Dieser Verzicht war nicht nur rechtlich geboten; er dokumentierte auch den Willen des Landesgesetzgebers, sich an den strengen Maßstäben eines strikten Datenschutzes zu orientieren.

Dadurch konnten verbreitete Befürchtungen zerstreut werden, über diese Nummern würde nicht nur im Meldewesen, sondern auch darüber hinaus in anderen Bereichen der öffentlichen Verwaltung ein Instrument zur Verknüpfung verschiedener Datensätze ganz im Sinne eines Personenkennzeichens geschaffen. Ebenso und wiederum im Gegensatz zu einigen anderen Bundesländern wurde die Verwendung einer verkürzten Schlüsselnummer (Ordnungsmerkmal), die das Auffinden des jeweiligen Datensatzes in den automatisierten Dateien ermöglicht, nur auf den Bereich der Meldebehörden und der Kirchen als wichtige Datenempfänger beschränkt.

Erste Erlasse - vor allem über Form, Inhalt und Verwendung des Meldescheins - wurden in diesem Jahr in Kraft gesetzt. Hingegen stehen die nach dem Gesetz notwendigen Rechtsverordnungen aus, die dem regelmäßigen Datenaustausch der Meldebehörden mit dritten Stellen zugrundeliegen sollen. Hier ist Hessen eindeutig in das "Mittelfeld" geraten. Umso mehr ist zu hoffen, daß auch diese Vorschriften und die noch ausstehenden Verwaltungsvorschriften im Verlauf des Jahres 1984 in Kraft treten können und das gesamte Regelungswerk "Melderecht" auf Landesebene abgeschlossen wird.

2.1.2.2
Praktische Probleme

Zahlreiche Kontakte meiner Mitarbeiter mit Bediensteten der Meldestellen und eine Reihe von Fortbildungsveranstaltungen verschafften mir ein Bild davon, wie das neue, datenschutzorientierte Meldegesetz von Bürger und Verwaltung aufgenommen wird. Die Tendenz der Meldestellen, die frühere Routine behutsam und schrittweise den neuen Vorschriften anzupassen, ist nicht zu übersehen. Viele Mitarbeiter in den Kommunen zögern jedoch noch, das äußerlich recht umfangreiche Regelungswerk auch im Einzelfall zu konsultieren, und überprüfen zu selten die unter dem früheren Gesetz praktizierten Verfahren auf die Übereinstimmung mit dem neuen Recht. Die Scheu vor dem Umfang des Gesetzes und seiner ungewohnten, durch den Datenschutz geprägten Struktur und Begriffe führt paradoxerweise dazu, daß die noch ausstehenden Verwaltungsvorschriften - und damit weitere Normen - vielfach vermißt werden. Hier kann nur der ständige und enge Kontakt zwischen Melde- und Aufsichtsbehörden bestehende Vorbehalte abbauen helfen. Selbstverständlich bin ich bereit, über einen entsprechenden Informationsaustausch und auch Fortbildungsveranstaltungen meinen Teil zu der Lösung dieser Probleme beizutragen.

2.1.2.3
Einzelfragen

Zieht ein Bürger innerhalb Hessens um, muß er sich nur bei der neuen Gemeinde anmelden. Eine Abmeldung ist nicht mehr nötig. Seine frühere Gemeinde erfährt somit oft recht spät von der Zuzugsgemeinde die Daten des umgezogenen Bürgers. In manchen Fällen führte dies zu Schwierigkeiten - insbesondere dann, wenn konkretes Verwaltungshandeln an einen bestimmten Stichtag geknüpft ist. Dies gilt für das Wahlrecht ebenso wie die Lohnsteuerkartenausstellung. Die Wohltat für den Bürger - er muß bei einem Umzug nur einmal bei einer Meldebehörde vorsprechen -ist sicher zu begrüßen. So weit dadurch Informationslücken bei der Gemeinde entstehen, in der er bislang seinen Wohnsitz hatte, muß durch ein möglichst schnelles Rückmeldeverfahren der Zeitraum zwischen der Anmeldung bei der neuen Gemeinde und der Information der Wegzugsgemeinde geringer werden. Dadurch werden auch mögliche Belastungen des Bürgers selbst vermieden.

Aus einer Reihe von Gemeinden wird berichtet, das Ausfüllen des Meldescheines mit seinen bis zu acht Durchschlägen für jeden einzelnen umgezogenen Bürger bereite offensichtlich Schwierigkeiten. Die Zahl der Durchschläge gibt dabei ebenso zu Klagen Anlaß, wie der Umfang der erhobenen Daten für jeden Einwohner. Diese Mängel werden nicht selten dem Datenschutz angelastet - zu Unrecht. Sicherlich entspricht das neue Verfahren, nach dem jeder Empfänger eines Durchschlags - wie etwa das Statistische Amt oder die Kirchen - nur sein Exemplar erhält, datenschutzrechtlichen Forderungen. Dadurch wurde das alte "Umlaufverfahren" abgelöst, nach dem ein komplett ausgefüllter Datensatz nacheinander an mehrere Empfangsstellen weitergegeben wurde. Dadurch konnte jede Stelle nicht nur ihre Daten entnehmen, sondern erhielt auch Einblick in alle übrigen Daten.

Die große Zahl der Empfänger regelmäßiger Übermittlungen ist jedoch der eigentliche Grund für den Umfang des Durchschreibesatzes. Der Datenschutz beeinflußt Zahl und Interesse möglicher Empfänger an den Meldedaten nicht. Zudem sollte man berücksichtigen, daß das Gesetz auf ein automatisiertes Einwohnerwesen zugeschnitten ist. In einem solchen Verfahren ist es ohne weiteres möglich, daß die Gemeinde nur einmal und auf einem Formular oder sogar dem Bildschirm den gesamten Datensatz erhebt und speichert. Für jeden Adressaten werden dann jeweils besondere Ausdrucke mit den notwendigen Daten angefertigt. Insofern ist es voraussichtlich eine Frage der Zeit, bis auch dieses Problem gelöst wird.

Eine Reihe von Meldebediensteten berichtete mir, daß die Praxis der Übermittlung an die Sicherheitsbehörden noch immer nicht den neuen Regelungen entspricht. Ein Einsichtsrecht von Polizei und Verfassungsschutz in das Melderegister gibt es nicht, auch wenn mancher Bedienstete dieser Stellen eine uneingeschränkte Einsichtnahme in die Meldedaten beansprucht. Vielmehr dürfen die Meldebehörden nur im Einzelfall die konkret angeforderten Daten nach der in § 31 des Meldegesetzes vorgesehenen Prüfung der rechtlichen Zulässigkeit übermitteln.

Nach § 34 Abs. 2 S. 2 des Meldegesetzes hat die Meldebehörde den betroffenen Einwohner davon zu unterrichten, wenn einem Dritten eine erweiterte Melderegisterauskunft über seine Daten erteilt wurde. Auch der die Auskunft begehrende Datenempfänger ist zu nennen. Dies gilt lediglich dann nicht, wenn der Datenempfänger gegenüber der Meldestelle nicht nur ein berechtigtes, sondern auch ein rechtliches Interesse - insbesondere zur Geltendmachung von Rechtsansprüchen - glaubhaft gemacht hat. Die Abgrenzung beider Arten von "Interessen" ist sicher nicht einfach. Im Gegensatz zum "rechtlichen Interesse" begründet ein allgemein wirtschaftliches, kulturelles oder ideelles Anliegen (etwa der Familienforschung) schon ein "berechtigtes Interesse". Ein konkreter Rechtsanspruch muß nicht gegeben sein oder behauptet werden. Nach meiner Feststellung wird dieser Pflicht zur Benachrichtigung nur im Ausnahmefall nachgekommen. Hier sollte sichergestellt werden, daß die Aufsichtsbehörden ein praktikables Verfahren vorschlagen und gegenüber den Meldebehörden durchsetzen.

2.1.2.4
Der Bundesmeldedatensatz - Ersatz für das Personenkennzeichen?

Ein Ereignis im Bereich des Meldewesens war nur am Rande Gegenstand der Diskussion um die Weiterentwicklung von Melderecht und Datenschutz. Möglicherweise handelt es sich dabei jedoch um den Grundstein für eine umfassende Vereinheitlichung der Datenverwaltung im Gesamtbereich der öffentlichen Verwaltung und darüber hinaus. Gemeint ist der bundeseinheitliche "Datensatz für das Meldewesen (DSMeld)", der am 21. Oktober 1982 von der Bundesvereinigung der Kommunalen Spitzenverbände in Zusammenarbeit mit dem Unterausschuß "EDV im Einwohnerwesen" des Arbeitskreises II der Ständigen Konferenz der Innenministerien der Länder herausgegeben wurde.

2.1.2.4.1
Zweck

Dieser Einheitsdatensatz legt - zunächst in einem "einheitlichen Bundes-/Länderteil" - in einzelnen Datenblättern genau fest, wie bestimmte Datenarten (Familienname, Geburtstag, Wohnort u.a.) durch eine festgelegte Anordnung, zulässige Länge und Inhaltsgestaltung für die automatisierte Verwendung niederzulegen sind. Mit anderen Worten: Durch eine vereinheitlichte Schreibweise und Anordnung des Datensatzes wird gewährleistet, daß dieselben Daten durch die gleichen Zugriffs-, Übermittlungs-und Veränderungsmechanismen verarbeitet werden können. Sinn dieser Vereinheitlichung auf Bundesebene ist es, Massendatenübermittlungen zwischen Landes- und Bundesbehörden sowie zwischen Behörden verschiedener Länder automatisiert durchführen zu können. Könnten die Länder weiterhin völlig autonom den technischen Rahmen ihrer Datenverarbeitungssysteme im Meldewesen bestimmen, wäre ein reibungsloser automatisierter Datenaustausch aufgrund der wahrscheinlichen Unterschiede der Systeme nicht ohne weiteres möglich. § 20 des Melderechtsrahmengesetzes sieht deshalb vor, daß die Bundesregierung zur Steuerung der Datenübermittlung von den Meldebehörden an Stellen der Bundesverwaltung und der Übermittlung von Meldedaten zwischen Meldebehörden verschiedener Bundesländer auch die Form der Übermittlung festlegen darf und hierzu auf "jedermann zugängliche Bekanntmachungen sachverständiger Stellen" - gemeint ist der Bundesmeldedatensatz - verweisen kann (Abs. 3). Folgerichtig verpflichtet die "Verordnung zur Durchführung von regelmäßigen Datenübermittlungen zwischen Meldebehörden verschiedener Länder" (1. Meldedaten-Übermittlungsverordnung des Bundes - 1. BMeldDÜV) die Meldebehörden zur Verwendung des Bundesmeldedatensatzes als zwingend vorgeschriebene Übermittlungsform für die Rückmeldung zwischen Meldebehörden verschiedener Bundesländer. Auch die derzeit erst im Entwurf vorliegende 2. Meldedaten-Übermittlungsverordnung des Bundes, die die Übermittlung von den Meldebehörden an die Kreiswehrersatzämter, den Rentendienst der Deutschen Bundespost und die Bundesanstalt für Arbeit regeln soll, verpflichtet die Gemeinden, diese Übermittlungsform zu verwenden.

2.1.2.4.2
Folgen

Die Festlegung eines bundesweit einheitlichen Meldedatensatzes für - wie es zunächst scheint - zwei eng umgrenzte Bereiche hat jedoch weit über den unmittelbaren Regelungsgegenstand hinaus Bedeutung. Es wäre unsinnig, würde eine Meldebehörde ihre Daten vor einer Übermittlung an die genannten Empfänger jeweils in die geforderte Form "umgießen" müssen. Sie wird vielmehr diese Form von vornherein als Grundlage für ihre Datenverwaltung überhaupt wählen. Es ist nur folgerichtig, wenn der Einheitsdatensatz bereits zusätzliche "Freifelder" für Daten der jeweiligen Landesverwaltung vorsieht. Der Bundesmeldedatensatz wird damit indirekt zur technischen Grundlage für das gesamte Meldewesen aller Bundesländer und darüber hinaus auch für die Datenverwaltung derjenigen öffentlichen Stellen, die regelmäßig Daten von den Meldebehörden erhalten. Eine Reihe von Bundesstellen wurde bereits im Zusammenhang mit dem Entwurf der 2. Bundesmeldedatenübermittlungsverordnung erwähnt (s.o. 2.1.2.4.1 a.E.). Die parallele Entwicklung innerhalb der Länder ist bereits abzusehen. Statistische Ämter, Personalausweisbehörden, Schulämter, Ausländerämter, Standesämter und auch die Kirchen erhalten regelmäßig länderintern Meldedaten. Aber auch private Stellen - etwa Auskunfteien, Großversandhäuser und Kreditschutzorganisationen - könnten daran denken, ihre Auskunftsverlangen an die Meldebehörden unter Verwendung dieser Form zu automatisieren. Der Bundesmeldedatensatz würde damit zum Standard der Datenverwaltung in weiten Bereichen von Verwaltung und Wirtschaft.

2.1.2.4.3
Auswirkungen auf die Struktur des Datenschutzes

Gerade an diesem Beispiel zeigt sich, daß ein richtig verstandener Datenschutz sich nicht nur als Instrument zur Verhütung individuellen Mißbrauchs verstehen darf. Zunächst als technisch verstandene Vorgabe für einen bestimmten, begrenzten Bereich konzipiert, erhält der Bundesmeldedatensatz weit über den eigentlichen Zweck hinaus eine eminente Bedeutung. Er führt zu weitgehend identischen technischen Strukturen in den verschiedensten Bereichen der Verwaltung. Durch die Standardisierung wird vieles "machbar": Bestimmte Auswertungen oder Datenverknüpfungen zum Zwecke der Kontrolle, Fahndung oder anderer Arten von Überwachung können in der entsprechenden politischen Situation rasch eingerichtet werden - die Schaffung entsprechender Rechtsgrundlagen ist dann nur eine Frage der Zeit. Ob bewußt oder unbewußt, bisher bestehende "Insellösungen" der Datenverarbeitungsstrukturen vermittelten aus der Sicht des Datenschutzes ein beträchtliches Potential politischer Legitimation. Gerade die Diskussion um die Volkszählung hat gezeigt, daß das Argument, bestimmte Auswertungsverfahren seien technisch nicht machbar, erheblich glaubwürdiger ist als der Hinweis, die technischen Strukturen erlaubten zwar ein bestimmtes unerwünschtes Verfahren, die betroffenen Stellen würden diese Möglichkeit aber nicht nutzen. Nur die bewußte, vorsorgliche Aufteilung der Informationsverarbeitung in strukturell miteinander nicht verknüpfbare Teilelemente beweist wirkungsvoll, ob die datenverarbeitenden Stellen den Datenschutz wirklich ernst nehmen oder mit der Einrichtung technischer und organisatorischer Sicherungsinstrumente auf niedriger Ebene - etwa einer individuellen Zugangs- oder Abgangskontrolle bei den Datenverarbeitungsinstanzen - gleichsetzen. Mechanismen dieser "niedrigeren" Ebene können jederzeit und kurzfristig aufgehoben werden. Ihr Funktionieren hängt zudem auch von dem guten Willen der direkt betroffenen Personen ab. Deshalb habe ich bereits mehrfach auf die Gefahren hingewiesen, die durch die Speicherung der Seriennummer von Personalausweis und Paß und durch die Verwendung einheitlicher Strukturen der Datenverwaltung entstehen können (vgl. 11. Tätigkeitsbericht, Ziff. 2.2.1.2 sowie in diesem Bericht Ziff. 2.1.2.1 und Ziff. 3.1.2.2).

Auf den Bundesmeldedatensatz bezogen heißt dies: Die Zugriffs- und Verwertungsstrukturen lassen durch die Vereinheitlichung des Mediums bundesweite Auswertungsverfahren zu, die bisher an dem Problem der Masse der Daten und der Geschwindigkeit der Verarbeitung scheiterten. Die Entscheidung, ob diese Auswertungen durchgeführt werden, fallen dann bestenfalls je nach der aktuellen politischen Lage. Von diesem Blickwinkel aus ist die Einführung des Bundesmeldedatensatzes mehr als nur einer der täglich feststellbaren kleinen Schritte zur Erweiterung der Datenverarbeitungskapazität und damit auch des Kontrollpotentials über den Einzelnen. Sie ist nicht weniger als der Grundstein für eine neue Ära technischer Vereinheitlichung der Datenverwaltung im Bereich der öffentlichen Stellen von Bund, Ländern und Gemeinden. Damit schafft sie die technische Infrastruktur für eine bundesweite Meldedatenbank - ein meines Erachtens höchst gefährliches und bedrohliches Resultat für den Datenschutz. Welche Konsequenzen diese Entscheidung im einzelnen haben wird, hängt von der kritischen und wirkungsvollen Beobachtung dieser Entwicklung durch die Parlamente, die Datenschutzinstanzen und die Öffentlichkeit ab.

2.1.3.
Informationsverarbeitung und innere Sicherheit (Ziff. 3.2)

2.1.3.1
Kriminalaktennachweis (Ziff. 3.2.2.1.2)

Im letzten Tätigkeitsbericht habe ich über die geplante Einführung des bundesweiten Kriminalaktennachweises (KAN) - eines automatisiert geführten Verzeichnisses der beim Bund und bei den Ländern geführten kriminalpolizeilichen Akten - berichtet und meine Einwände gegen den vorgesehenen Umfang der Übermittlung "hessischer" Daten in den KAN dargelegt (Ziff. 3.2.2.1.2). In erster Linie ging es dabei um die vorhandenen Altbestände an Kriminalakten. Ich habe vor allem Bedenken dagegen geäußert, daß eine Reihe von Straftatbeständen für die pauschale Überspielung in den KAN vorgesehen sind, bei denen keineswegs sicher ist, daß jedes diese Straftatbestände betreffende Ermittlungsverfahren tatsächlich die Aufnahmekriterien für den KAN erfüllt. Mit anderen Worten: Bei der Einspeicherung in den KAN geht man lediglich von gewissen Erfahrungswerten aus, obwohl es sich im Einzelfall durchaus um einen Sachverhalt handeln kann, der für eine zentrale Speicherung beim Bundeskriminalamt keinen Anlaß bietet. Damit wird das 1981 von den Innenministern beschlossene Konzept für den KAN unterlaufen. In diesem Konzept wird unterschieden zwischen Daten, die nur für ein Bundesland relevant sind und daher nur der Polizei dieses Landes zur Verfügung stehen sollen und solchen, die überregionale Bedeutung haben; nur diese sollen im KAN zentral gespeichert werden.

Sowohl die Landesregierung in ihrer Stellungnahme zu meinem Bericht (Drucks. 10/659, zu 3.2.2.1.2) als auch der Innenminister in einem späteren Gespräch haben darauf hingewiesen, daß aus den derzeit vorhandenen Beständen an Kriminalakten die für den KAN vorgesehenen Fälle maschinell ausgewählt werden sollen und bei einer derartigen Verfahrensweise die Auswahlkriterien nicht in der gewünschten Genauigkeit befolgt werden könnten. Eine Nachbereinigung der hessischen Datenbestände im KAN sei jedoch genauso wie bei HEPOLIS gewährleistet. Diese Argumentation kann ich jedoch nicht akzeptieren. Ich möchte noch einmal betonen, daß der Vorteil rationeller Datenverarbeitung nicht den Verzicht auf die Einhaltung gesetzlicher Bestimmungen und diese konkretisierende Richtlinien rechtfertigt. Die Verfahrensweise beim Aufbau von HEPOLIS ist in diesem Zusammenhang nicht vergleichbar, da es sich hierbei um das erste Informationssystem der Polizei handelte.

Zu bedenken sind ferner auch folgende Gesichtspunkte: Die vorgesehene pauschale Überspielung stellt nicht lediglich eine geringfügige, sondern eine sehr beträchtliche Erweiterung des KAN-Beschlusses der Innenministerkonferenz dar, da insbesondere alle Straftaten mit sexuellem Bezug, alle(!) Fälle von Diebstahl, Betrug und Urkundenfälschung - unabhängig von den jeweiligen konkreten Umständen - in den zentralen Nachweis eingegeben werden sollen.

Auch ist es eine erhebliche Beeinträchtigung des Bürgers, wenn Informationen über eine ihn betreffende Kriminalakte nicht nur in Hessen, sondern im ganzen Bundesgebiet jederzeit abrufbar sind.

Und schließlich: Eine rasche und vollständige Nachbereinigung der in den KAN eingegebenen Datenbestände ist keineswegs gewährleistet. Geplant ist derzeit lediglich folgendes: Im Rahmen der laufenden Sachbearbeitung soll vom Sachbearbeiter jeweils geprüft werden, ob die betreffende Kriminalakte tatsächlich die KAN-Kriterien erfüllt; anderenfalls soll sie aus dem KAN wieder herausgenommen werden. Darüber hinausgehende Bereinigungen sind nicht vorgesehen. Betroffen sind damit von der Bereinigung nur diejenigen Fälle, in denen entweder das polizeiliche Ermittlungsverfahren noch nicht abgeschlossen ist oder in denen der Betroffene erneut in den Verdacht gerät, eine Straftat begangen zu haben. Dies ist auf keinen Fall ausreichend.

Nach wie vor habe ich auch erhebliche Bedenken dagegen, daß die Daten jedes Tatverdächtigen, der in zwei verschiedenen hessischen Gemeinden eine Straftat begangen haben soll, in den KAN überspielt werden sollen, weil damit angeblich das KAN-Kriterium der erneuten Straffälligkeit des Beschuldigten "außerhalb seines Wohn- oder Aufenthaltsbereichs" erfüllt ist. Die Auffassung der Landesregierung, es sei in diesem Zusammenhang ohne Bedeutung, ob Ländergrenzen überschritten würden oder nicht, widerspricht der Grundkonzeption des KAN.

In der Zwischenzeit ist die Realisierung des KAN in Hessen weiter fortgeschritten. Im Datenbestand von HEPOLIS sind diejenigen Kriminalakten gekennzeichnet worden, die in den KAN übermittelt werden sollen. Das Ergebnis sieht so aus: In HEPOLIS sind z.Z. die Daten von etwa 550 000 Personen gespeichert, über die in hessischen Polizeidienststellen eine Kriminalakte vorliegt. Von diesen 550 000 Personen sind etwa 223 000 für den KAN vorgesehen, d.h. nahezu 50 v.H. des Gesamtbestandes. Hier zeigt sich deutlich, daß meine Einwände gegen die Art und Weise der Realisierung des KAN in Hessen berechtigt waren und meine Befürchtung eingetreten ist, daß unverhältnismäßig viele Daten in den KAN eingegeben werden. Hinweisen möchte ich - im Hinblick auf die durch den KAN geschaffenen überregionalen Möglichkeiten des Datenzugriffs durch die Polizei - noch einmal darauf, daß nach der Kriminalstatistik für das Jahr 1982 (Bulletin der Bundesregierung vom 23. April 1983, Nr. 38 S. 333) etwa 65 v.H. der Tatverdächtigen in der Tatortgemeinde, etwa 9 v.H. im Landkreis des Tatortes und etwa 14 v.H. im Bundesland des Tatortes wohnen, also nur bei einem kleinen Prozentsatz der Betroffenen Wohn- und Tatort in verschiedenen Bundesländern liegen. Die sich nunmehr klar abzeichnende Entwicklung steht nicht im Einklang mit den Beschlüssen der Innenminister von 1981.

2.1.3.2
PIOS-Datei "Staatsgefährdung" (3.2.2.2.3)

Meine Bedenken hinsichtlich der geplanten Datei "PIOS-Staatsgefährdung" hatte ich im Abschnitt 3.2.2.2.3 dargelegt. Diese Datei wird zu einem erheblichen Anteil sog. "unbewertete" Daten enthalten. Die Speicherung der Daten soll erst der Klärung der Frage dienen, ob ein Tatverdacht bzw. eine konkrete Gefahr zu bejahen ist. Sie ist ein Instrument der "Verdachtsverdichtung". Eine derartige Speicherung von Vorfelddaten ist generell sehr problematisch (s. hierzu auch Ziff. 3.1.3.2.2). Umso mehr ist jedenfalls darauf zu achten, daß der Kreis der Personen, die in einer derartigen Datei gespeichert werden sollen, präzise abgegrenzt wird. Aber dies ist hier gerade nicht der Fall, insbesondere deshalb nicht, weil der Begriff der "Staatsgefährdung" in der Praxis sehr extensiv ausgelegt wird.

2.1.3.2.1
Sachstand

Dem Hessischen Innenminister hatte ich meine Einwände mitgeteilt und ihm ein gemeinsames Gespräch über die geschilderten Probleme vorgeschlagen. Die Landesregierung hat in ihrer Stellungnahme zu meinem Bericht (Drucks. 10/659, zu 3.2.2.2.3) sowie in ihrem späteren Antwortschreiben meine Kritik als unberechtigt bezeichnet. Sie hat sich hierbei vor allem auf den Wortlaut der Errichtungsanordnung für diese Datei berufen. Die Arbeitsgruppe Datenverarbeitung und Datenschutz des Innenausschusses des Landtags hat ihre Diskussion bis zur konkreten Einführung der Datei zurückgestellt. In der Zwischenzeit hat mir der Innenminister auf meine Bitte noch einmal konkret die Verfahrensweise in der Praxis dargestellt. Seine Ausführungen konnten meine Bedenken nicht ausräumen. Da voraussichtlich im nächsten Jahr mit dem Betrieb der neuen PIOS-Datei begonnen wird, halte ich eine wesentliche Eingrenzung der geplanten Datenspeicherungen für unerläßlich.

2.1.3.2.2
Begriff der "Staatsgefährdung" konturenlos

Zentrales Problem der geplanten neuen PIOS-Datei ist nach wie vor die Frage, welcher Sachverhalt als "staatsgefährdend" bzw. als "Staatsschutzangelegenheit" anzusehen ist. Der Begriff der "Staatsschutzangelegenheit" wird in der Praxis sehr weit gefaßt. Dies trifft nicht nur für Hessen zu. Besonders deutlich wird dies u.a. an der polizeilichen Kriminalstatistik für das Jahr 1982 (Bulletin der Bundesregierung vom 23.4.1983 Nr. 38 S. 333). Aus dieser Statistik geht hervor, daß Delikte wie z. B. Friedensverrat, Hochverrat, Straftaten gegen ausländische Staaten, landesverräterische Agententätigkeit usw. lediglich 30,7 v.H. der polizeilichen Meldungen von Staatsschutzdelikten ausmachen. 69,3 v.H. entfallen auf sogenannte "sonstige" Staatsschutzdelikte, d.h. allgemeine Delikte, die aufgrund besonderer Umstände des Einzelfalls von der Polizei als Staatsschutzdelikte eingestuft werden. Hierzu zählen z.B. auch Meineid, Beleidigungstatbestände, Verunglimpfung des Andenkens Verstorbener, Körperverletzung, Nötigung und einfache Sachbeschädigung. In der gegenwärtigen Praxis kann grundsätzlich jedes Delikt als Staatsschutzdelikt qualifiziert werden. Entscheidend wird die polizeiliche Einschätzung des subjektiven Motivs des Verdächtigen. Diese Abgrenzung des Kreises der Staatsschutzangelegenheiten erscheint mir konturenlos. Ich sehe nach wie vor lediglich einen engen Kreis von schwerwiegenden, gegen den Bestand der Bundesrepublik bzw. ihrer Länder gerichteten objektiven Straftatbeständen als geeignet an, den Begriff der "Staatsschutzangelegenheit" zu konkretisieren.

Im letzten Tätigkeitsbericht habe ich bereits darauf hingewiesen, daß es häufig auch sehr schwierig ist, das Motiv eines Beschuldigten zuverlässig festzustellen; dies gilt insbesondere für den Beginn der Ermittlungen. Es besteht die Gefahr, daß alle Ermittlungsverfahren, die im Zusammenhang mit politischen Demonstrationen stehen oder irgendeinen sonstigen realen oder vermuteten politischen Hintergrund haben, pauschal als Staatsschutzangelegenheit qualifiziert und die Betroffenen damit vorschnell und undifferenziert als (potentiell) "staatsgefährdende" Personen etikettiert werden. Diese Befürchtungen kann ich auch nach dem Gespräch mit dem Hessischen Innenminister nicht als widerlegt ansehen.

2.1.3.2.3
Errichtungsanordnung zu unbestimmt

Die Frage der Definition des Begriffs "Staatsschutzangelegenheit" spielt nicht lediglich eine Rolle bei der geplanten neuen PIOS-Datei, sondern auch bei anderen Dateien bzw. polizeilichen Meldediensten. Sie ist jedoch gerade bei der PIOS-Datei von besonderer Bedeutung, da in ihr auch zahlreiche Daten über das Umfeld der Betroffenen, u.a. auch deren Kontaktpersonen, gespeichert werden sollen. Die Gefahr ist nicht von der Hand zu weisen, daß hier im Ergebnis eine umfangreiche Sammlung der Daten von auf irgendeine Art und Weise kritisch eingestellten Bürgern entsteht. Vorkehrungen hiergegen können nur durch eine präzise Errichtungsanordnung für die Datei getroffen werden, in der lediglich einzelne schwerwiegende objektive Straftatbestände als Anknüpfungspunkt für eine Speicherung aufgeführt werden.

Die Hessische Landesregierung sieht in ihrer Stellungnahme eine Konkretisierung des Begriffs der "Staatsschutzangelegenheit" als nicht erforderlich an und weist im übrigen auf den restriktiven Wortlaut der Errichtungsanordnung der geplanten Datei hin. Entgegen der Auffassung der Landesregierung ist jedoch gerade der Wortlaut dieser Errichtungsanordnung nicht geeignet sicherzustellen, daß lediglich schwerwiegende oder überregional bedeutsame Delikte aus dem Staatsschutzbereich gemeldet und aufgenommen werden, da Nummer 11 der Errichtungsanordnung auf die subjektiven Motive des Verdächtigen bzw. dessen Hintergrund abstellt und damit weit und unbestimmt gefaßt ist. Dort ist festgelegt, daß - über die zuvor aufgezählten Verfahren wegen Friedensverrat, Hochverrat usw. hinaus - auch alle anderen Straftaten erfaßt werden, sofern wegen der Angriffsrichtung, dem Motiv des Täters oder dessen Verbindung zu einer Organisation der Verdacht besteht, daß die Tat

- gegen die freiheitliche demokratische Grundordnung, den Bestand und die Sicherheit des Bundes oder eine Landes gerichtet ist,
- eine ungesetzliche Beeinträchtigung der Amtsführung von Mitgliedern verfassungsmäßiger Organe des Bundes oder eines Landes zum Ziel hat,
- durch Anwendung von Gewalt oder darauf gerichtete Vorbereitungshandlungen auswärtige Belange der Bundesrepublik Deutschland gefährdet oder eine solche Gefährdung zum Ziel hat.

So ist auch die Landesregierung lediglich in der Lage, in ihrer Stellungnahme darauf hinzuweisen, daß Delikte wie z.B. Beleidigung und einfache Nötigung "nicht ohne weiteres" in der Datei erfaßt werden. Ich halte diese vagen Abgrenzungen für untragbar - gerade auch in Anbetracht der Schwierigkeiten, den subjektiven Hintergrund zuverlässig feststellen zu können, und angesichts der geplanten Speicherung von Daten über das Umfeld der Betroffenen.

2.1.3.3
Hinweis- und Spurendokumentationssysteme (Ziff. 3.2.2.2.4)

Bei der Darstellung der Tendenzen der polizeilichen Datenverarbeitung im letzten Jahresbericht (Ziff. 3.2.2) hatte ich aufgezeigt, daß zunächst als automatisierte Datei in Hessen lediglich das Hessische Polizeiinformationssystem "HEPOLIS" existierte, inzwischen jedoch die Möglichkeiten der automatisierten Datenverarbeitung im Polizeibereich auf vielfältige Weise genutzt werden. In diesem Zusammenhang habe ich auch auf den zunehmenden Einsatz von Hinweis- und Spurendokumentationssystemen und die damit verbundenen Probleme hingewiesen.

2.1.3.3.1
Besonderheiten von HIDOK

HIDOK wird in Hessen gegenwärtig auf verschiedene Weise genutzt. Datenschutzrechtliche Probleme wirft insbesondere der Einsatz von HIDOK für die Bearbeitung von Groß- bzw. Sammelverfahren auf. Hier wird jeweils für begrenzte Zeit aus besonderem Anlaß bei der sachbearbeitenden Arbeitsgruppe bzw. Sonderkommission eine automatisierte Datei errichtet, in die sämtliche Daten, die im Rahmen des Ermittlungsverfahrens anfallen, eingespeichert werden. Zur Zeit sind bei verschiedenen hessischen Polizeidienststellen insgesamt sechs derartige Dateien eingesetzt. Ferner besteht für alle Länder die Möglichkeit, das Hinweis- und Spurendokumentationssystem (genannt SPUDOK) des Bundeskriminalamts (BKA) zu benutzen. Der Einsatz von SPUDOK ist für Fälle terroristischer Gewaltkriminalität von bundesweiter Bedeutung vorgesehen. Zur Zeit bedient sich das Hessische Landeskriminalamt zweier SPUDOK-Dateien. Sie betreffen die Ermittlungen im Zusammenhang mit dem Attentat auf den Hessischen Wirtschaftsminister Karry und mit den Anschlägen auf US-Einrichtungen. Direkten Zugriff auf diese Dateien haben das Landeskriminalamt (LKA) und das BKA, nicht jedoch die Polizeidienststellen anderer Länder. Sofern auch in anderen Bundesländern zahlreiche Hinweise oder Spuren bekannt werden, können auch diese Länder die Möglichkeit des Direktzugriffs auf die SPUDOK-Dateien erhalten.

Im Vergleich zu HEPOLIS weisen die Datenspeicherungen in HIDOK (bzw. SPUDOK) folgende Besonderheiten auf:

Zum einen sind umfangreiche Freitextspeicherungen und mehrdimensionale Recherchen unter den verschiedensten Verknüpfungsgesichtspunkten möglich. Zum anderen ist in HIDOK ein erheblich weiterer Personenkreis gespeichert. Während in HEPOLIS lediglich die Daten derjenigen Personen festgehalten werden, gegen die tatsächlich ermittelt wird, d.h. bei denen der Tatverdacht zumindest einen gewissen Konkretheitsgrad erreicht hat, werden in HIDOK die Daten jeder Person eingegeben, die im Zusammenhang mit dem jeweiligen Ermittlungsverfahren in irgendeiner Weise bekannt wird. Dies gilt z.B. für jeden Hinweis aus der Bevölkerung auf bestimmte Personen, unabhängig davon, ob sich dieser Hinweis in irgendeiner Weise bestätigt. Zwar trifft es zu, daß die Speicherung aller im Rahmen des Ermittlungsverfahrens anfallenden Hinweise und Spuren keine grundsätzlich neue Verfahrensweise darstellt. Durch die Automatisierung erhält diese Verfahrensweise jedoch eine neue Dimension, die besondere Gefährdungen mit sich bringt.

Weil die Schwelle der Einspeicherung von Daten hier im Vergleich zu HEPOLIS wesentlich vorverlagert ist, habe ich im letzten Bericht dargelegt, daß ständige Aktualitätsprüfungen und Bereinigungen der in HIDOK gespeicherten Datenbestände besonders dringlich sind. Da hier eine Vielzahl Unbeteiligter gespeichert wird, muß - soweit die Speicherung überhaupt zulässig ist - eine Löschung der Daten sobald wie möglich erfolgen.

2.1.3.3.2
Keine Anwendung der KpS-Richtlinien?

Die Landesregierung hat in ihrer Stellungnahme (zu 3.2.2.2.4) meine Forderungen als unbegründet angesehen. Sie geht dabei zunächst mit Recht davon aus, daß die Richtlinien für die Führung kriminalpolizeilicher personenbezogener Sammlungen (KpS-Richtlinien) auf die Führung der Kriminalakten zugeschnitten sind und hier eine nicht völlig vergleichbare Sachlage vorliegt. Allerdings führt sie dann weiter aus, daß die KpS-Richtlinien ungeeignet seien für Akten, die lediglich sachorientiert geführt würden. Als sachgerechter Anknüpfungspunkt für die Vernichtung komme bei ungeklärten Fällen nur die Verfolgungsverjährung in Betracht. Die Landesregierung vertritt damit offensichtlich die Auffassung, daß die Datenspeicherung in HIDOK sogar noch über die in den KpS-Richtlinien festgelegten Fristen (je nach Fall 10, 5 bzw. 3 Jahre) hinaus erfolgen kann.

Dieser Auffassung muß ich mit Nachdruck widersprechen. Es ist vielmehr umgekehrt davon auszugehen, daß die Fristen der KpS-Richtlinien für die HIDOK-Datenbestände erheblich zu lang sind. Diese Fristen stellen im übrigen auch lediglich Regelaussagen dar; eine Berücksichtigung der jeweiligen Umstände des Einzelfalles ist ausdrücklich vorgeschrieben. Bereits der Ausgangspunkt der Landesregierung, daß es sich bei der Einspeicherung in HIDOK um eine sachorientierte - im Gegensatz zur personenbezogenen - Speicherung handelt, ist unzutreffend. Zwar ist Anlaß für den Einsatz von HIDOK jeweils eine konkrete Straftat bzw. ein konkreter Straftatenkomplex, im Rahmen der Ermittlungen wird jedoch eine Vielzahl personenbezogener Daten gespeichert, so vor allem die Daten von Personen, die möglicherweise als Tatverdächtige in Betracht kommen, aber auch Hinweisgeber und Zeugen. Auf die Daten dieser Personen kann auch direkt zugegriffen werden.

2.1.3.3.3
Notwendigkeit von Aktualitätsüberprüfungen und Bereinigungen

In ihrer Stellungnahme (s.o.) weist die Landesregierung auf noch vorgesehene Gespräche zwischen dem Hessischen Landeskriminalamt und dem Datenschutzbeauftragten über HIDOK hin. Der Hessische Landtag hat in seiner Sitzung vom 21. Juni 1983 die Landesregierung und den Datenschutzbeauftragten gebeten, im Rahmen der Diskussion über den 12. Tätigkeitsbericht erneut zu der Frage der Löschungsfristen bei HIDOK Stellung zu nehmen. In der Zwischenzeit habe ich noch einmal im Hessischen Landeskriminalamt die geschilderten Probleme erörtert. In der Frage der Aktualitätsüberprüfungen und Bereinigungen der in HIDOK gespeicherten Datenbestände konnte jedoch keine Einigung erzielt werden.

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 Personen, die selbst von der Polizei als unbeteiligt angesehen werden. Zur Begründung dieser Auffassung werden vor allem folgende Gründe angeführt: Im Zuge der Ermittlungen müsse von Anfang an darauf geachtet werden, daß zu einem späteren Zeitpunkt - vor allem zum Zeitpunkt einer eventuellen Hauptverhandlung - umfassender Aufschluß darüber besteht, welche Hinweise und Spuren zu welchen Ermittlungen und unter Umständen zu einer Anklage geführt hätten. Außerdem gingen neue Gerichtsentscheidungen davon aus, daß die Staatsanwaltschaft unter Umständen auf Wunsch des Beschuldigten im Rahmen des Hauptverfahrens Spuren- und Hinweisakten dem Gericht vorlegen müsse. Schließlich müßten auch Hinweise, die sich als unbedeutend herausgestellt hätten, gespeichert bleiben, damit die Polizei nicht unter Umständen denselben Hinweis noch einmal überprüfen müsse.

Diese Argumentation überzeugt nicht. Bei einer Erörterung des Löschungsproblems ist zunächst generell im Blick zu behalten, daß seit der Verabschiedung der Datenschutzgesetze die Zulässigkeit der Speicherung personenbezogener Daten nicht mehr die Regel ist, sondern die Ausnahme, die einer konkreten Begründung bedarf. Die Datenschutzgesetze verbieten eine Speicherung von Daten "auf Vorrat", d.h. eine Speicherung allein aus dem Grund, daß die Daten möglicherweise einmal später gebraucht werden könnten. Dies gilt auch für die Polizeibehörden. Zwar ist es hier sicherlich im Einzelfall nicht ganz einfach, die Grenzlinie zu ziehen; dies ändert jedoch nichts daran, daß die Polizeibehörden ebenso wie andere Behörden rechtlich dazu verpflichtet sind, ihren Datenbestand ständig daraufhin zu überprüfen, inwieweit er noch für ihre Aufgabenerfüllung erforderlich ist. Auch bei der in den KpS-Richtlinien vorgeschriebenen Aussonderung von Kriminalakten kann selbstverständlich nie vollkommen ausgeschlossen werden, daß die Polizei nicht die Daten in einem Einzelfall später doch noch einmal brauchen könnte. Nichtsdestoweniger ist eine Aussonderung nach bestimmten Fristen aus rechtsstaatlichen Gründen geboten. Für HIDOK gilt dies entsprechend. Unabhängig davon, wie hier die Grenzlinie im Einzelfall zu ziehen ist, kann es jedenfalls nicht hingenommen werden, daß alle personenbezogenen Daten - auch dann, wenn sie sich als falsch bzw. vollkommen unbedeutend erwiesen haben - langfristig gespeichert werden.

Was die eventuelle Pflicht der Staatsanwaltschaft zur Vorlage von Spurenakten im Hauptverfahren angeht, so ist zunächst darauf hinzuweisen, daß diese Fälle außerordentlich selten vorkommen werden. Die hierzu ergangenen Gerichtsentscheidungen (Bundesgerichtshof vom 26.5.1981, Neue Juristische Wochenschrift 1981, S. 2267; Bundesverfassungsgericht vom 12.1.1983, Neue Juristische Wochenschrift 1983, S. 1043) befassen sich auch nur mit der eventuellen Pflicht der Staatsanwaltschaft zur Vorlage vorhandener Spurenakten. Sie behandeln dagegen weder die Frage der automatisierten Speicherung der in den Spurenakten enthaltenen Daten noch den Aspekt, welche Daten die Staatsanwaltschaft aus rechtlichen Gründen aufbewahren darf bzw. vernichten muß. Aus den Entscheidungen kann daher keineswegs geschlossen werden, daß alles, was der Staatsanwaltschaft bzw. der Polizei im Zusammenhang mit einem Ermittlungsverfahren irgendwie zur Kenntnis gelangt, auf jeden Fall langfristig aufbewahrt werden muß.

2.1.3.3.4
Unzulässigkeit zeitlich nicht begrenzter Speicherung

Konsequenz der Auffassung des Hessischen Ministers des Innern ist, daß die Daten einer Vielzahl - auch nach Auffassung der Polizei unbeteiligter - Personen über lange Zeit gespeichert sind. Zu bedenken ist, daß sich Groß-bzw. Sammelverfahren über viele Jahre hinziehen können. Nach der Auffassung der Landesregierung könnten in diesem Fall alle Daten erst dann gelöscht werden, wenn das letzte Strafverfahren rechtskräftig abgeschlossen ist. Dies kann natürlich, wenn alle Instanzen ausgeschöpft werden, auf eine über zehn Jahre hinausgehende Speicherungsfrist hinauslaufen. Wenn einer der Tatverdächtigen nicht gefaßt wird, bleiben alle personenbezogenen Daten auch darüber hinaus auf unabsehbare Zeit gespeichert. Dies steht eindeutig im Widerspruch zu den in den KpS-Richtlinien getroffenen Fristenregelungen: Personen, gegen die konkrete Ermittlungen geführt werden und über die demzufolge eine Kriminalakte angelegt wurde, bleiben nach den KpS-Richtlinien regelmäßig 10 bzw. 5 oder 3 Jahre (je nach der Schwere des Falles und dem Alter des Betroffenen) gespeichert. In HIDOK dagegen könnte jeder unbedeutende Hinweis auf unbestimmte Zeit gespeichert bleiben, zumal dann, wenn der Kreis der in einer Datei zusammengefaßten Fälle weit gezogen wird.

Die Problematik zeigt sich etwa an der SPUDOK-Datei, die vom LKA für Ermittlungen zu den Anschlägen auf US-Einrichtungen eingesetzt wird. In diese Datei werden seit Ende 1981 alle Hinweise und Spuren aufgenommen, die möglicherweise in einem Zusammenhang mit den Anschlägen stehen. Bei den Tatverdächtigen handelt es sich um ganz verschiedene Personenkreise, die auch nicht demselben politischen Hintergrund zuzurechnen sind. Dementsprechend werden auch die jeweiligen Strafverfahren nicht verbunden. Sofern weitere Anschläge auf US-Einrichtungen erfolgen, ist geplant, auch für diese Ermittlungen die Datei zu benutzen, sofern sie möglicherweise in irgendeinem Zusammenhang mit einem zuvor verübten Anschlag stehen könnten. Da vermutlich nicht damit gerechnet werden kann, daß zu irgendeinem Zeitpunkt überhaupt keine Anschläge auf US-Einrichtungen mehr verübt werden und der Hessische Minister des Innern eine Löschung aller Daten erst nach rechtskräftigem Abschluß des letzten Strafverfahrens für möglich hält, bedeutet dies im Ergebnis, daß alle in dieser HIDOK-Datei gespeicherten Personen zeitlich unbegrenzt gespeichert sind.

Ich halte diese Praxis für rechtlich nicht zulässig und im Hinblick auf den Verhältnismäßigkeitsgrundsatz für untragbar. Zusammenfassend möchte ich daher noch einmal feststellen: Für die Datenspeicherung in HIDOK können auf keinen Fall längere Speicherungsfristen als die in den KpS-Richtlinien vorgesehenen Regelfristen gelten, sondern es sind im Gegenteil ganz erheblich verkürzte Fristen vorzusehen. Aktualitätsüberprüfungen und Bereinigungen müssen regelmäßig durchgeführt werden.

2.1.4
Krebsregister (Ziff. 2.1.4 und 3.3.2; vgl. auch 10. Tätigkeitsbericht, Ziff. 3.4)

2.1.4.1
Epidemiologische Krebsregister

Die Konferenz der Gesundheitsminister hat auf ihrer Sitzung am 17. und 18. November 1983 in München "Grundsätze zur Krebsregistrierung" verabschiedet, deren Berücksichtigung den Landesgesetzgebern empfohlen wird, die ein Krebsregistergesetz vorbereiten und verabschieden wollen.

Das Ziel hat sich seit dem Modellgesetzentwurf des Bundesministers für Jugend, Familie und Gesundheit für ein Krebsregistergesetz in den Ländern aus dem Jahr 1982 nicht geändert: Angestrebt wird nach wie vor die Einrichtung regionaler, über die Bundesrepublik verteilter, epidemiologischer Krebsregister mit einer ausreichenden Population. Nur die Mittel haben sich geändert, wenngleich - und dies ist bemerkenswert -mit entscheidenden Modifikationen zugunsten des Datenschutzes. Im Gegensatz zum Musterentwurf wird nunmehr einvernehmlich von der Notwendigkeit einer grundsätzlichen Einwilligung des Patienten in die Verarbeitung seiner Daten in epidemiologischen Krebsregistern ausgegangen, wobei eng eingegrenzte Ausnahmetatbestände eine Speicherung im Einzelfall auch ohne vorherige Zustimmung zulassen.

Damit hat die Diskussion um epidemiologische Krebsregister zu einer deutlichen Annäherung der Positionen von Datenschutzbeauftragten und Gesundheitsministerien geführt. Die Anforderungen an epidemiologische Krebsregister sind ja durch die Datenschutzbeauftragten der Länder und des Bundes klar abgesteckt worden (vgl. Beschluß vom 14. Dezember 1981, abgedruckt im 10. Tätigkeitsbericht, Ziff. 3.4).

Im Ergebnis wird auch die Hessische Landesregierung durch diesen Beschluß der Gesundheitsministerkonferenz bestätigt, bewegt sich doch ihr Gesetzentwurf vom letzten Jahr (1982) in weiten Teilen auf der Kompromißlinie dieses Beschlusses (zu meiner Auffassung vgl. 11. Tätigkeitsbericht, Ziff. 2.1.4). Anknüpfend an den hessischen Entwurf hat die Gesundheitsbehörde der Freien und Hansestadt Hamburg in Zusammenarbeit mit dem Hamburgischen Datenschutzbeauftragten einen Referentenentwurf erarbeitet. Wie Ankündigungen in der Presse zu entnehmen war, will demnächst auch der Hessische Sozialminister einen überarbeiteten Gesetzentwurf in den Landtag einbringen.

Die organisierte Ärzteschaft lehnt dagegen regionale epidemiologische Krebsregister rundweg ab. Aus der Sicht der Bundesärztekammer und des Verbandes der Niedergelassenen Ärzte Deutschlands (NAV) besteht keine Notwendigkeit für solche Datenbanken. Damit bestätigt sich meine schon im 10. Tätigkeitsbericht geäußerte These, daß es nicht nur um ein Problem des Datenschutzes und der ärztlichen Schweigepflicht geht, sondern auch um eine fachinterne Kontroverse zwischen Praktikern und Wissenschaftlern um den Stellenwert der medizinischen Forschung. Auch läßt sich immer wieder feststellen, daß die häufig ins Feld geführten strikten berufsrechtlichen Informationsschranken in der Praxis durch die von vielen Ärzten gebilligte unzutreffende Vorstellung eines "Schweigepflichtverbundes" - nach der der Datenaustausch zwischen Medizinern unbegrenzt zulässig sei - unterlaufen wird.

Unter diesen Umständen überrascht es nicht, daß bei klinischen Tumorregistern, die unter der Regie der Ärzteschaft selbst eingerichtet werden, Datenschutzbedenken gar nicht oder nur sehr leise zu vernehmen sind. Doch bestehen die Gefahren einer zentralisierten Krebsregistrierung zunächst unabhängig davon, ob die Ärzteschaft selbst oder Einrichtungen mit medizin-statistischem Forschungsansatz derartige Dokumentationen betreiben. Entscheidend sind in beiden Fällen Art und Qualität der rechtlich definierten Rahmenbedingungen und der Verfahren, die den Schutz der persönlichen Integrität des einzelnen gewährleisten.

2.1.4.2
Tumorzentren - klinische Krebsregister

2.1.4.2.1
Aufbaustand und Aufgaben

Der Bundesminister für Arbeit und Sozialordnung hat parallel zu den Aktivitäten des Bundesministers für Jugend, Familie und Gesundheit zur Initiierung epidemiologischer Krebsregister in den Ländern ein Programm zur Verbesserung der Krebsbehandlung entwickelt, das die Förderung von Tumorzentren und onkologischen Schwerpunkten zum Gegenstand hat. In Hessen sind gegenwärtig zwei Tumorzentren sowie zwei onkologische Schwerpunkte im Aufbau: Das Tumorzentrum Marburg/Gießen mit den Universitätsklinika Marburg und Gießen sowie das Tumorzentrum Rhein-Main in der Universitätsklinik Frankfurt am Main. Hinzu kommen in Kassel die Städtischen Kliniken und das Rote-Kreuz-Krankenhaus sowie die Städtischen Kliniken in Darmstadt als onkologische Schwerpunkte.

Mit dieser Förderung wird zunächst die Einrichtung einer - prinzipiell bundesweit kompatiblen - klinischen Tumordokumentation in den Tumorzentren und Schwerpunkten angestrebt; sie ist derzeit in vollem Gange. Gefördert wird dabei die Beschaffung von Hard- und Software sowie die Einstellung von geeignetem Dokumentationspersonal. Ziel dieser Tumordokumentation ist vor allem die Unterstützung und Verbesserung der Behandlung des Patienten in der Klinik bis hin zur Nachsorge durch den niedergelassenen, behandelnden Arzt. Sie soll weiter die Klinikorganisation unterstützen und eine vergleichbare, nach identischen Kriterien geordnete Datenbasis für die medizinische Forschung bieten. Der Umfang der je Patient gespeicherten Daten übersteigt den ursprünglich für das Register in Gießen vorgesehenen Datensatz, da eine onkologische Behandlung weitaus mehr und detailliertere Daten erfordert als die deskriptive Epidemiologie.

2.1.4.2.2
Datenschutzerfordernisse
Der Beschluß der Datenschutzbeauftragten

Die Arbeitsgruppe Wissenschaft und Forschung der Konferenz der Datenschutzbeauftragten hat sich unter meinem Vorsitz mit den Datenschutzproblemen der Tumorregistrierung befaßt (zu meiner Position vgl. 11. Tätigkeitsbericht, Ziff. 3.3.2.2 und 3.3.2.4) und einen Beschlußvorschlag erarbeitet, den die Konferenz daraufhin am 4. November 1983 verabschiedet hat. Darin heißt es:

"Der Aufbau und die Einrichtung klinischer Krebsdokumentationen in den Ländern muß nach Ansicht der Datenschutzbeauftragten der Länder und des Bundes sowie der Datenschutzkommission Rheinland-Pfalz durch Datenschutzkonzeptionen ergänzt werden, die der besonderen Sensitivität dieser Datensammlungen gerecht werden.

Die Datenschutzbeauftragten erwarten von den Trägern, die den Aufbau dieser Krankheitsdokumentation fördern und betreiben, neben fachlichen Vorgaben für die Förderung dieser Projekte, im Interesse der betroffenen Patienten auch die Festlegung datenschutzrechtlicher Rahmenbedingungen, die unbedingt eingehalten werden müssen.

Dazu gehört vor allem, daß die Verantwortung für die Einhaltung aller Vorschriften des Datenschutzes eindeutig feststeht. Die unterschiedlichen Bezeichnungen wie "Tumorzentrum e.V.", "Onkologischer Schwerpunkt" haben die Konturen der datenschutzrechtlichen Verantwortlichkeit mehr verwischt als klar umrissen.

Für die Datenschutzbeauftragten kommt als speichernde Stelle in diesem Sinne nur die behandelnde Einrichtung oder Person in Betracht. Gegen diese richten sich auch die subjektiven Rechte der Patienten nach den Datenschutzgesetzen und anderen Vorschriften zur Sicherung ihrer persönlichen Integrität. Aufgaben und Befugnisse in Bezug auf die Verwendung der klinischen Krebsdokumentation der behandelnden Einrichtungen werden durch den Behandlungsvertrag bestimmt und begrenzt. Dort, wo eine klinische Krebsdokumentation gesondert von der individuellen Patientendokumentation zur Optimierung der Krebsbehandlung und Nachsorge besteht, wird auch ihr Inhalt, Umfang sowie Übermittlung und Speicherungsdauer durch den Behandlungszusammenhang definiert. Über eine klinische Krebsdokumentation ist der Patient bei der Aufnahme einer Behandlung aufzuklären, die erste Speicherung seiner Daten ist ihm mitzuteilen.

Werden die Daten für ein bestimmtes Forschungsprojekt über den Behandlungszusammenhang hinaus personenbezogen genutzt, ist in jedem Fall eine Einwilligung nach Aufklärung ("informed consent") des betroffenen Patienten erforderlich, es sei denn, die Patientendaten sind anonymisiert bzw. aggregiert.

Die Datenschutzbeauftragten werden auf strenge Maßnahmen der technischen und organisatorischen Datensicherung achten und deren Einhaltung kontrollieren.

Sollte sich im Laufe der Entwicklung zeigen, daß der Behandlungsvertrag bzw. der Behandlungszusammenhang keine geeigneten Kriterien für eine ausdifferenzierte Dokumentation bietet, ist auch die Notwendigkeit gesetzlicher Regelung bei der Eingriffsintensität einer derartigen personenbezogenen Informationsverarbeitung nicht auszuschließen. Je mehr sich die klinische Dokumentation aus dem Behandlungszusammenhang löst, umso mehr müssen die Grundsätze und Kriterien auch für diese Krebsdokumentation Geltung erlangen, die die Datenschutzbeauftragten zu dem Modellentwurf für ein Krebsregistergesetz verabschiedet haben."

Auf der Grundlage dieses Beschlusses werde ich gemeinsam mit den hessischen Tumorzentren ein konkretes Datenschutzkonzept entwickeln. Eine entsprechende Arbeitsgruppe ist bereits eingerichtet worden.

2.1.5
Personaldateien und Personalakten der Lehrer (Ziff. 5.1)

Angesichts der unterschiedlichen Praxis und der verbreiteten Unsicherheit über Art und Umfang der zulässigen Sammlung und Verwendung von Lehrerdaten bei den Schulen und Staatlichen Schulämtern hatte ich in meinem 11. Tätigkeitsbericht unter Ziff. 5.1 dem Hessischen Kultusminister empfohlen, hierzu einen präzisen, klarstellenden Erlaß herauszugeben und für die Erarbeitung eines solches Erlasses meine Hilfe angeboten. Im Oktober hat mir der Kultusminister den Entwurf eines entsprechenden Erlasses zugeleitet. Darin wird zum einen das Prinzip bekräftigt, daß die bei Schulen und Schulämtern zu führenden Personalnebenakten ausschließlich solche Informationen über das Schulpersonal enthalten sollen, die für die konkrete Aufgabenstellung von Schulämtern und Schulleitungen notwendig sind. Zum anderen enthält der Entwurf einen im einzelnen aufgeschlüsselten Datenkatalog, bei dem jeweils angegeben ist, inwieweit das Schulamt bzw. die Schule dieses Datum aufzeichnen dürfen.

Zu dem Erlaßentwurf habe ich ausführlich Stellung genommen und dabei folgende Anregungen und Hinweise gegeben:

(1) Neben den Personalnebenakten im formellen Sinn sollten auch die bei Schulämtern und Schulen manuell geführten Lehrerkarteien ausdrücklich in den Geltungsbereich des Erlasses einbezogen werden. Nur dann wird nämlich die intendierte Eingrenzung des Datenkatalogs voll wirksam. Hinzu kommt, daß die Abgrenzung schon deshalb schwierig ist, weil vielfach die Karteikarten auch in die Akten eingeheftet werden.

(2) Die Einschränkung des Datenkatalogs muß zu organisatorischen und bürotechnischen Konsequenzen führen, auf die im Erlaß hingewiesen werden bzw. die vom Kultusminister in Angriff genommen werden müßten. Notwendig ist die Vorbereitung bzw. Verwendung von im Datenumfang reduzierten Formularen, Karteikarten usw., die den Vorgaben des Erlasses entsprechen und erst eine praktikable Realisierung möglich machen.

(3) Die Gelegenheit sollte genutzt werden, diejenigen Praktiken des Umgangs mit Lehrerdaten ausdrücklich zu untersagen, die zu Beschwerden Anlaß gegeben haben und mit der Zielsetzung des Erlasses nicht vereinbar sind. So sollte z.B. klargestellt werden, daß Schulämter und Schulen keinesfalls den in der Landesverwaltung bei Einstellungen üblichen umfangreichen Fragebogen benötigen. Auch halte ich die Erforderlichkeit einiger in der Datensatzbeschreibung des Entwurfs enthaltenen Angaben (z.B. "wirtschaftliche Verhältnisse") noch für überprüfungsbedürftig.

(4) Und schließlich: Angesichts der zunehmenden Verbreitung schuleigener DV-Anlagen erscheint mir der Hinweis dringlich, daß die Befugnis der Schule zur Erhebung und Verwendung bestimmter Lehrerdaten im Rahmen von Personalnebenakten keineswegs die Befugnis umfaßt, diese Angaben in die schuleigenen Computer einzuspeichern. Die Führung von Lehrerdateien in Schulcomputern bedarf mit anderen Worten - wenn sie überhaupt in bestimmtem Umfang für zulässig erklärt werden soll - einer Regelung zumindest durch einen besonderen Erlaß.

Ich begrüße es, daß der Hessische Kultusminister meine Empfehlung aufgegriffen hat und hoffe, daß ein nach meinen Anregungen ergänzter bzw. geänderter Erlaß nach Abstimmung mit den zuständigen Gremien, Personalräten usw. möglichst bald im kommenden Jahr ergehen kann. Angesichts der zunehmenden Verwendung von DV-Anlagen in Schule und Unterricht, die vom Kultusminister ja gefördert wird, erscheint mir allerdings darüber hinaus eine Regelung des Gesamtkomplexes "Datenschutz in der Schule" angebracht. Ganz gleich, ob Lehrer- oder Schülerdaten betroffen sind, könnte ich mir hierfür eine bereichsspezifische Regelung im Schulverwaltungsgesetz vorstellen, wie sie etwa von der Schulrechtskommission des Deutschen Juristentages vorgeschlagen worden ist. Daran mitzuwirken, bin ich gerne bereit. (Zu den Datenschutzerfordernissen bei der automatisiert geführten Lehrerindividualdatei vgl. unten Abschnitt 3.3.1, vor allem Ziff. 3.3.1.3).

2.1.6.
Gesundheitsdaten in Personalakten des öffentlichen Dienstes (Ziff. 5.2)

2.1.6.1
Übermittlung amtsärztlicher Zeugnisse an den Dienstherrn

Unter Ziff. 5.2.4 hatte ich meine Erwartung geäußert, daß im Laufe des Jahres 1983 für Hessen eine Neuregelung beim Umgang mit Gesundheitsdaten in Personalakten des öffentlichen Dienstes eingeführt werden könne, die den Forderungen der ärztlichen Schweigepflicht sowie des Datenschutzes Rechnung trägt. Diese Erwartung gründete sich auf die Übereinkunft mit den beteiligten Ressorts, d.h. dem Innenminister und dem Sozialminister, sowohl über die Zielrichtung einer entsprechenden Regelung als auch über das weitere Verfahren ihrer Ausarbeitung. Im Oktober 1982 war nämlich vereinbart worden, für Hessen eine Neuregelung in Anlehnung an die auf Bundesebene vereinbarte Verfahrensweise in Angriff zu nehmen, nach der nur das (amts-)ärztliche Zeugnis mit dem Ergebnis der Beurteilung an die personalbearbeitende Stelle zu übermitteln ist, der ärztliche Untersuchungsbogen mit den medizinischen Daten dagegen bei den Gesundheitsämtern verbleibt. Nach einer Bestandsaufnahme bei den Gesundheitsämtern und deren Anhörung sollten Bestimmungen vorbereitet werden, und zwar durch den Sozialminister für die Gesundheitsämter und durch den Innenminister für die personalbearbeitenden Stellen der Landesverwaltung; die entsprechenden Entwürfe sollten zwischen den Ressorts bereits Anfang 1983 abgestimmt werden (vgl. dazu die Stellungnahme der Landesregierung zu meinem 11. Tätigkeitsbericht, Drucks. 10/659, zu 5.2.3).

Zu meinem Bedauern haben mir die genannten Ministerien in diesem Jahr weder einen Regelungsentwurf - auf welcher Normebene auch immer - vorgelegt, noch haben sie mir einen Zeitplan für die Erarbeitung einschlägiger Vorschriften unterbreitet.

Das von der Landesregierung als hauptsächliche Schwierigkeit angeführte Problem der Aufbewahrung der medizinischen Einstellungsunterlagen bei den Gesundheitsämtern erscheint mir keineswegs so schwer lösbar, daß damit die weitere Verzögerung einer Regelung gerechtfertigt werden könnte. Dies gilt umso mehr, als die Trennung zwischen ärztlichen Aufzeichnungen und dem der Dienststelle zu übersendenden Ergebnis inzwischen für eine Gruppe von Landesbediensteten gilt, auf deren gesundheitliche Eignung es besonders ankommt - die Polizeibeamten. Die bundeseinheitliche Polizeidienstvorschrift 300 über die "Ärztliche Beurteilung der Polizeidiensttauglichkeit und der Polizeidienstfähigkeit" ist inzwischen mit Wirkung vom 1. Januar 1983 auch für die hessische Polizei in Kraft gesetzt worden (Erlaß des Hessischen Ministers des Innern vom 21. Januar 1983, StAnz. 7/1983 S. 482). Danach werden bei der Einstellung in den Polizeivollzugsdienst die Vorgeschichte, der Befund der Auswahl- und Einstellungsuntersuchungen, Fehlerbezeichnungen und die abschließende Beurteilung in einem ärztlichen Gutachten zusammengefaßt, das nur den Ärzten und ihrem Hilfspersonal zugänglich sein darf (Ziff. 2.5.1). Der Einstellungsbehörde ist dagegen nur ein "Ärztliches Tauglichkeitszeugnis" zu überlassen, das das abschließende Beurteilungsergebnis (polizeidiensttauglich oder - untauglich) enthält (Ziff. 2.5.2). Die gleiche Handhabung gilt für die Untersuchung vor der Berufung in das Beamtenverhältnis auf Lebenszeit (Ziff. 3.2).

Da über die Zielsetzung und den Regelungsbedarf in dieser Frage zwischen der Landesregierung und mir Einvernehmen besteht, erscheint mir die Erwartung angebracht, daß die in Angriff genommenen Vorarbeiten alsbald abgeschlossen werden und mir die zuständigen Ressorts so rechtzeitig ihre Vorschläge zur Stellungnahme zuleiten, daß das Verfahren bei der Übersendung amtsärztlicher Stellungnahmen jedenfalls im kommenden Jahr abschließend festgelegt werden kann.

2.1.6.2
Zweckbindung der Beihilfedaten

In diesem Zusammenhang erinnere ich auch noch einmal an meine Forderung (vgl. Ziff. 5.2.2), daß Beihilfeakten mit ihren medizinischen Inhalten von den allgemeinen Personalakten, die zu Zwecken der Personalverwaltung angelegt sind, getrennt zu führen sind und ohne ausdrückliche Einwilligung des Bediensteten für eine Einsicht des Dienstherrn im Zusammenhang mit Personalentscheidungen (z.B. Beförderung) nicht zur Verfügung stehen. Dieses Thema hat 1983 wegen der neuen Gebührenordnung für Ärzte (GOÄ) noch an Aktualität gewonnen: Da ärztliche Leistungen nach der neuen GOÄ teilweise ausführlicher begründet werden müssen, enthalten die zur Beihilfe einzureichenden Rechnungen vielfach mehr bzw. eingehendere Diagnosen. Zahlreiche Eingaben und Anfragen belegen die Besorgnis vieler im öffentlichen Dienst Beschäftigter, daß ihre Gesundheitsdaten für Maßnahmen der Personaladministration zweckentfremdet werden könnten. Eine Reihe von Personalräten hat die Position der Landesregierung erheblich befremdet, wonach es "nicht recht verständlich" sei, warum der Dienstherr Informationen aus den Beihilfeakten nicht für andere Entscheidungen verwerten können solle (vgl. Stellungnahme zum 11. Tätigkeitsbericht zu 5.2).

Nach meinem Dafürhalten sollte daher die Landesregierung ihre ablehnende Haltung zur Notwendigkeit einer einschlägigen Regelung noch einmal überdenken.

2.2
Zum 9. Tätigkeitsbericht für 1980 (Drucks. 9/4032)

2.2.1
Neufassung der "Mitteilungen in Strafsachen" (MiStra) (Ziff. 4.2.3)

Aufgrund der MiStra - einer Verwaltungsvereinbarung der Landesjustizverwaltungen und des Bundesministers der Justiz - unterrichten Gerichte und Staatsanwaltschaften bestimmte andere öffentliche Stellen über die Einleitung eines Ermittlungsverfahrens bzw. die Erhebung der öffentlichen Klage und den jeweiligen Verfahrensausgang. Vorgeschrieben sind eine Vielzahl von Mitteilungen, die sehr vielfältige Lebensbereiche betreffen. Um nur einige Beispiele zu nennen: So werden bei einem Verfahren gegen Richter, Beamte und Angestellte des Bundes oder eines Landes die Dienstvorgesetzten informiert, bei Verfahren gegen Wirtschaftsprüfer, öffentlich bestellte und vereidigte Sachverständige und Steuerberater die zuständige oberste Landesbehörde und die entsprechende Berufskammer, bei Verfahren gegen Ärzte, Apotheker und Heilpraktiker ebenfalls die oberste Landesbehörde und die betroffene Berufskammer, bei Verfahren gegen Inhaber von Gewerbescheinen das Ordnungsamt, bei Verfahren gegen Studierende und Inhaber akademischer Grade der Präsident der Hochschule, bei Verfahren nach dem Betäubungsmittelgesetz die zuständige oberste Landesbehörde, das Landeskriminalamt, das Bundeskriminalamt und die Bundesopiumstelle. Diese Beispiele zeigen, daß es sich hier um ganz erhebliche Datenflüsse handelt. Die Mitteilungen können Maßnahmen des Empfängers auslösen, die für die Betroffenen sehr schwerwiegend sind, so z.B. die Durchführung eines Disziplinarverfahrens oder die Untersagung der Berufsausübung.

2.2.1.1
Die Stellungnahme der Datenschutzbeauftragten von 1980

In meinem 9. Tätigkeitsbericht (Ziff. 4.2.3) habe ich dargelegt, daß die MiStra-Bestimmungen nach übereinstimmender Ansicht der Datenschutzbeauftragten des Bundes und der Länder einer gesetzlichen Grundlage bedürfen und dringend auf die Notwendigkeit der zahlreichen Mitteilungen hin überprüft werden müssen. Seit Inkrafttreten der MiStra hat sich die Datenschutzdiskussion wesentlich weiterentwickelt. Nach und nach ist es in das allgemeine Bewußtsein gerückt, daß Datenübermittlungen Eingriffe in Grundrechte darstellen und deshalb zum einen gesetzlich geregelt und zum anderen strikt am Verhältnismäßigkeitsprinzip gemessen werden müssen. Verwaltungsvereinbarungen können daher heute für derartige Datenübermittlungen nicht mehr als ausreichend angesehen werden. Im übrigen erweist sich bei genauer Durchsicht der vorgeschriebenen Mitteilungen, daß diese wesentlich eingeschränkt werden können und müssen. Dabei geht es selbstverständlich nicht darum, den derzeit vorgesehenen Empfängern die Erfüllung der ihnen zugewiesenen Aufgaben zu erschweren bzw. unmöglich zu machen. Es geht vielmehr um eine sorgfältige Überprüfung der Frage, welche Daten die Empfänger der Mitteilungen tatsächlich für ihre Aufgaben benötigen.

2.2.1.2
Der neue Entwurf

Die Notwendigkeit einer Überprüfung der MiStra ist auch Gegenstand einer Diskussion zwischen den Landesjustizverwaltungen gewesen. Der Hessische Justizminister hat mir nunmehr den vom Unterausschuß MiStra der Justizministerkonferenz erarbeiteten Entwurf einer Neufassung der MiStra mit der Bitte um Stellungnahme zugeleitet. Ich begrüße es, daß dieser Entwurf einen Wegfall zumindest einiger Mitteilungspflichten und die datenschutzgerechte Überarbeitung einzelner Bestimmungen vorsieht. Gleichwohl bin ich mir mit allen Landesdatenschutzbeauftragten - der Bundesbeauftragte für den Datenschutz hat dem neuen Beschluß leider nicht zugestimmt - darin einig, daß die 1980 vorgetragenen Forderungen und Anregungen nur zu einem sehr geringen Teil aufgegriffen wurden und eine erneute Überarbeitung des Entwurfs unerläßlich ist. Aus diesem Grunde möchte ich noch einmal ausführlich auf die kritischen Hauptpunkte eingehen.

2.2.1.2.1
Reduzierung der Mitteilungsfälle

Die Mitteilungen müssen dringend weiter eingeschränkt werden. Dies gilt zunächst einmal für die Anzahl der Anlässe, die eine Mitteilung nach sich ziehen sollen. So sollten insbesondere fahrlässig begangene Straftaten grundsätzlich nicht mitgeteilt werden, denn die fahrlässige Begehung einer Straftat weist auf ein geringeres Maß an strafrechtlicher Vorwerfbarkeit hin. Vor allem dürfen fahrlässig begangene Verkehrsstraftaten nicht zu weitgestreuten Mitteilungen führen. Nur bei engem Bezug zur beruflichen Tätigkeit des von der Mitteilung Betroffenen und besonderem Gewicht des verletzten Rechtsguts sollten Ausnahmen gemacht werden. Ferner halte ich es für sehr bedenklich, daß der vorliegende Entwurf über eine Vielzahl einzelner Anlässe von Mitteilungen hinaus noch eine Reihe generalklauselartiger Formulierungen enthält, die die Möglichkeit weiterer zusätzlicher Mitteilungen eröffnen. So ist z.B. nach Nr. 2 Abs. 2 eine Mitteilung auch dann zu machen, wenn sie zwar nicht ausdrücklich vorgeschrieben ist, aber "durch ein besonderes öffentliches Interesse geboten ist". Nach Nr. 3 sind darüber hinaus Mitteilungen auf Ersuchen einer Behörde zulässig, wenn nicht "erhebliche Bedenken entgegenstehen". Ein Bedürfnis für diese weitreichenden Bestimmungen vermag ich angesichts der großen Anzahl bereits konkret angeordneter Mitteilungen nicht zu erkennen, sie bergen meines Erachtens jedoch die Gefahr in sich, daß die klaren, auf die einzelnen Situationen abgestimmten Regelungen weitgehend relativiert werden.

2.2.1.2.2
Grundsatz: Mitteilungen erst nach Verfahrensabschluß

Schließlich erscheint mir die Einleitung eines Ermittlungsverfahrens bzw. die Erhebung der öffentlichen Klage in vielen Fällen kein hinreichender Anlaß für eine Mitteilung. Die Mitteilungen in Strafsachen sollen die zu benachrichtigenden Behörden in Kenntnis von Vorgängen setzen, auf die sie im Rahmen des ihnen zugewiesenen Aufgabenbereichs zu reagieren verpflichtet sind. Ein strafrechtlich relevanter Sachverhalt läßt sich jedoch zuverlässig erst nach Abschluß des Strafverfahrens beurteilen. Vorher dürfen auch im Regelfall von den Empfängern gar keine Maßnahmen zum Nachteil des Betroffenen durchgeführt werden. Damit dem von den Mitteilungen Betroffenen keine unnötigen Nachteile entstehen, sollte der Grundsatz in der MiStra ausdrücklich festgelegt werden, daß Mitteilungen im Regelfall erst nach rechtskräftigem Abschluß des Strafverfahrens erfolgen dürfen. Soweit Mitteilungen in einzelnen Situationen vorher erforderlich sind, dürfen diese grundsätzlich erst zum Zeitpunkt der Erhebung der öffentlichen Klage gemacht werden. Erst zu diesem Zeitpunkt kann von einem hinreichenden Tatverdacht gegen den Betroffenen ausgegangen werden. Diese vorzeitige Mitteilung darf erst dann veranlaßt werden, wenn begründete Anhaltspunkte dafür vorliegen, daß die zu benachrichtigende Behörde Maßnahmen treffen muß, bevor das Verfahren abgeschlossen ist. Die Bekanntgabe der Einleitung des Verfahrens sollte auf diese wenigen Ausnahmefälle beschränkt bleiben.

2.2.1.2.3
Einschränkung des Inhalts der Mitteilungen

Erforderlich ist jedoch nicht lediglich eine Einschränkung der Anlässe, die zu einer Mitteilung führen, sondern vor allem auch eine Reduktion des Inhalts der einzelnen Mitteilungen. Zu bedenken ist, daß namentlich Urteilsgründe eine Vielzahl sensibler Daten - so etwa auch eingehende Persönlichkeitsanalysen - enthalten, und zwar häufig auch über Dritte wie z.B. Zeugen oder Opfer. Diese Daten werden vielfach vom Empfänger nicht zur Entscheidung über die ihm zur Verfügung stehenden Maßnahmen benötigt. Der Inhalt der Mitteilungen muß infolgedessen auf das im Einzelfall wirklich erforderliche Mindestmaß beschränkt werden. Das bedeutet insbesondere, daß im Regelfall die Mitteilung der Tatsache der Verurteilung oder der Abdruck des Urteilstenors genügen muß.

2.2.1.2.4
Unterrichtung des Betroffenen

Auch wenn die von mir dargelegten notwendigen Einschränkungen der Mitteilungen berücksichtigt sind, werden die Gerichte und Staatsanwaltschaften in vielen Fällen andere öffentliche Stellen unterrichten. Da diese Mitteilungen unter Umständen schwerwiegende Folgen für den Betroffenen haben können, erscheint es mir wichtig, daß er hiervon in verständlicher Form informiert wird, damit er seinerseits unter Umständen geeignete Maßnahmen treffen, z.B. eine ausführliche Schilderung des angesprochenen Sachverhalts aus seiner Sicht gegenüber dem Empfänger der Mitteilung abgeben kann. Der vorliegende Entwurf sieht zwar in Nr. 2 Abs. 2 eine Unterrichtung des Betroffenen in einzelnen Fällen vor. Ich sehe jedoch keinen Grund dafür, ihn nicht in jedem Fall generell von den erfolgten Mitteilungen in Kenntnis zu setzen. Dies ermöglicht dem Betroffenen einen klaren Überblick über die von Gericht und Staatsanwaltschaft getroffenen Maßnahmen.

2.2.1.2.5
Notwendigkeit einer gesetzlichen Regelung

Noch einmal: Die "Mitteilungen in Strafsachen" bedürfen einer gesetzlichen Grundlage. Sie greifen in die Grundrechte der Betroffenen ein und können für sie unter Umständen weitreichende Folgen haben. Aus diesen Gründen reichen Verwaltungsvorschriften nicht aus. Soweit ersichtlich, hält der Entwurf jedoch ohne Begründung daran fest, daß die Mitteilungen wie bisher lediglich in einer Verwaltungsvorschrift geregelt werden.

Dem Hessischen Justizminister habe ich eine ausführliche Stellungnahme zu den einzelnen Vorschriften des Entwurfs zugeleitet und ihn gebeten, sich für die von mir vorgeschlagenen Abänderungen des Entwurfs in der Justizministerkonferenz einzusetzen.

3.1
Der maschinenlesbare Personalausweis - Gefahren - Vorbedingungen der Einführung

3.1.1
Das neue Personalausweisgesetz des Bundes

Am 25. Februar 1983 hat der Deutsche Bundestag das 4. Gesetz zur Änderung des Gesetzes über Personalausweise verabschiedet (BGBl. I S. 194). Dieses Gesetz, das am 1. November 1984 in Kraft treten soll - vgl. auch die Neubekanntmachung vom 15. März 1983 (BGBl. I S. 289) -, sieht im Zusammenhang mit der Verordnung zur Bestimmung der Muster der Personalausweise der Bundesrepublik Deutschland vom 15. März 1983 (BGBl. I S. 291) eine völlig neue Form des Personalausweises vor. Sie ähnelt den bekannten Plastikscheckkarten, die im Bankverkehr bereits verwendet werden und erfüllt vor allem zwei Forderungen der Initiatoren des Ausweises: Die Konferenz der Innenminister des Bundes und der Länder hatte während ihrer Sitzung vom 22. Juni 1978 beschlossen, einen fälschungssicheren und maschinenlesbaren Personalausweis einzuführen.

3.1.1.1
Hintergrund des neuen Gesetzes

Dieser Beschluß stand im Zusammenhang mit der damals häufig festzustellenden Praxis terroristischer Gewalttäter, sich durch Einbrüche in die Gebäude von Personalausweisbehörden Blankettvordrucke zu beschaffen, um diese zur Herstellung falscher Personalausweisdokumente zu verwenden. Wenn auch bei den später gefaßten Tätern regelmäßig ausländische gefälschte Ausweispapiere gefunden wurden, so sollte eine mögliche Verwendung gefälschter Bundespersonalausweise durch diese oder andere Täterkreise in jedem Fall ausgeschlossen werden. Das Ziel, die Fälschung bzw. Verfälschung von Personalausweisen erheblich zu erschweren bzw. zu verhindern, stand damit im Vordergrund.

Insbesondere - aber nicht nur - das geplante Herstellungsverfahren und die Maschinenlesbarkeit des Ausweises weckten Bedenken, die die Datenschutzbeauftragten bereits frühzeitig gegenüber Bundes- und Landesregierungen sowie dem Bundestag äußerten.

3.1.1.2
Die erste Phase der Gesetzgebung bis zur Verkündung des neuen Gesetzes im März 1980

In der ersten Phase des Gesetzgebungsverfahrens im Jahre 1979 stellte der Hessische Datenschutzbeauftragte im Zusammenwirken mit dem Bundesbeauftragten und anderen Landesbeauftragten für den Datenschutz einen Forderungskatalog zusammen, dem wesentliche datenschutzrechtlichen Bedenken gegen die geplante Regelung zugrunde lagen: Durch einen gesetzlich festzulegenden abschließenden Katalog der zu speichernden Daten sollte die zusätzliche Verarbeitung verschlüsselter und für den Bürger nicht erkennbarer Daten verhindert werden. Die Datenschutzbeauftragten forderten zudem ein Verfahren, das auf die Errichtung einer zentralen Datei mit den Daten aller Personalausweisinhaber verzichtet. So sollte verhindert werden, daß an einer Stelle in der Bundesrepublik Deutschland eine Datenbank entsteht, die im Sinne eines "Bundesadressregisters" die Daten aller ausweis-

pflichtigen Bürger erfassen würde. Sie wandten sich ebenso strikt gegen einen Ausbau der Seriennummern der Personalausweise zu Personenkennzeichen, um zu verhindern, daß über einen erleichterten Zugriff auf eine Vielzahl von Dateien der verschiedensten öffentlichen Stellen Persönlichkeitsprofile der erfaßten Bürger erstellt werden könnten. Auf das gleiche Ziel richtete sich die Forderung, der Personalausweis solle insgesamt nicht zur automatisierten Errichtung oder Erschließung von Dateien verwendet werden dürfen. Dadurch sollte verhindert werden, daß jede beliebige öffentliche oder auch private Stelle die Ausweiskarte durch Lesegeräte automatisiert erfaßt und auswertet, indem sie die darauf enthaltenen Daten speichert und in einer Datei zusammenfaßt (Errichtung einer Datei) oder über die Eingabe der Karte deren Daten mit vorhandenen Beständen vergleicht und sie ggfs. zusätzlich speichert (Erschließung des vorhandenen Datenbestandes). Mit anderen Worten: Der technische Vorteil der Maschinenlesbarkeit des Ausweises sollte nur dort ausgenutzt werden können, wo besondere staatliche Belange einen schnellen Zugriff auf umfangreiche Datenbestände rechtfertigen - unter eindeutig geregelten Bedingungen der Strafverfolgung und Gefahrenabwehr.

In der im März 1980 verkündeten Fassung des Personalausweisgesetzes hat der Gesetzgeber einen wesentlichen Teil dieser Forderungen erfüllt. Der Bundestag hat sich zum gleichen Zeitpunkt die von der Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 9. November 1979 beschlossene Aufforderung an die Bundesregierung zu eigen gemacht, ein datenschutzgerechtes Melderechtsrahmengesetz und bereichsspezifische Datenschutzregelungen für die personenbezogene Datenverarbeitung bei den Sicherheitsbehörden als begleitende Maßnahmen zu schaffen. (Vgl. dazu unten Ziff. 3.1.3.1).

3.1.1.3
Die zweite Phase der Gesetzgebung bis zur Verabschiedung der revidierten Fassung im März 1983

Bevor das Gesetz am 1. Oktober 1981 in Kraft treten sollte, beherrschten vor allem zwei aus der Sicht des Datenschutzes nicht zufriedenstellend geregelte Fragen die Diskussion: zum einen forderten die Datenschutzbeauftragten weiterhin, daß der Ausweis nicht zur automatisierten Einrichtung von Dateien verwendet werden dürfe, um seine Verwendung als Ersatz für ein Personenkennzeichen auszuschließen. Der Gesetzgeber hatte sich nur zu einem Verbot der automatisierten Erschließung von Dateien bekannt (vgl. dazu unten Ziff. 3.1.6). Zum anderen wurde bald erkennbar, daß die zentrale Herstellung der Personalausweise bei der Bundesdruckerei entgegen dem Gesetzeswortlaut eine befristete Speicherung der personenbezogenen Daten der zukünftigen Ausweisinhaber vorsehen würde.

Es waren jedoch weniger datenschutzrechtliche als vielmehr vor allem ungelöste Fragen der Finanzierung des Herstellungsverfahrens, die den Gesetzgeber veranlaßten, im August 1981 den Zeitpunkt des Inkrafttretens aufzuheben und im März 1982 einen neuen Gesetzentwurf zur Änderung des Personalausweisgesetzes zu beraten. Mit diesem Entwurf sollte eine Reihe weiterer Forderungen erfüllt werden. Einmal sah er erstmals die Verpflichtung jedes Deutschen vor, einen Personalausweis zu besitzen. Damit sollte das anderenfalls zulässige Ausweichen auf den nicht maschinenlesbaren Reisepaß als Ersatzdokument verhindert werden. Die Zahl der für die Herstellung des Ausweises zu speichernden Daten sollte verringert und die bis dahin ungelöste Kostenfrage geregelt werden. Für den Datenschutz von Bedeutung war die geplante präzise Regelung der vorübergehenden und eingeschränkten Speicherung der Daten bei der Bundesdruckerei sowie die Erfüllung der Forderung, der Ausweis dürfe im öffentlichen Bereich weder zur automatisierten Erschließung noch zur automatisierten Einrichtung von Dateien verwendet werden (zur Verwendung im nicht-öffentlichen Bereich vgl. unten Ziff. 3.1.6). Damit wurde zwei weiteren zentralen Anliegen Rechnung getragen, als das Gesetz am 15. März 1983 verkündet wurde.

3.1.2
Rahmenbedingungen für die Einführung des Ausweises

3.1.2.1
Die Landespersonalausweisgesetze und das neue Paßrecht als ergänzende Vorschriften

Da das Bundesgesetz als Rahmengesetz (vgl. Art.75 Nr.5 GG) der Ausfüllung durch ein Landesgesetz bedarf, ist auch das Hessische Ausführungsgesetz zum Bundesgesetz über Personalausweise vom 17. September 1972 (GVBl. S. 147) zu novellieren. Der Hessische Landtag wird 1984 diese Aufgabe aufgreifen müssen. Die Verabschiedung des Bundesgesetzes und die anstehende Novellierung des Hessischen Personalausweisgesetzes fordern dazu auf, die bestehende Rechtslage, insbesondere aber die geplanten Vorschriften vor dem Hintergrund der erweiterten Einsatzmöglichkeiten des neuen Ausweises zu überprüfen (zu den rechtlichen Vorgaben für die Neufassung des hessischen Gesetzes vgl. unten Ziff. 3.1.7).

Der vom Bundeskabinett beschlossene Entwurf zur Novellierung des Paßgesetzes übernimmt nahezu wortgleich die datenschutzrechtlichen Bestimmungen des neuen Personalausweisgesetzes für seinen Anwendungsbereich. Auch der Paß soll in fälschungssicherer und maschinenlesbarer Form ausgegeben werden. Da sich bei der Verwendung und den Kontrollmaßnahmen für beide Arten von Dokumenten somit dieselben Probleme ergeben, gelten die folgenden Ausführungen gleichermaßen für diese Gesetzesänderung.

3.1.2.2
Zusätzliche Probleme: Internationale Maschinenlesbarkeit und Verknüpfung mit dem Melderegister

Gerade im internationalen Bereich wird die Verwendung maschinenlesbarer und fälschungssicherer Dokumente seit längerem angestrebt. So wurde bereits im Jahre 1980 von der Internationalen Zivilen Luftfahrtorganisation (ICAO-International Civil Aviation Organization) ein konkret ausgearbeiteter Vorschlag für ein solches Ausweisdokument der Öffentlichkeit vorgestellt. Auch wenn die Bundesrepublik Deutschland bislang als einziger Staat der Aufforderung dieser Organisation nachgekommen ist, ein fälschungssicheres und maschinenlesbares Dokument in Form einer Plastikkarte einzuführen - übrigens eine bemerkenswerte Tatsache anläßlich der großen Zahl von Staaten, die mit wesentlich schwierigeren Problemen des Terrorismus und des organisierten Verbrechens zu kämpfen haben -, so wirft die internationale Lesbarkeit auch Probleme des internationalen und grenzüberschreitenden Datenschutzes auf. Die Bundesregierung muß sicherstellen, daß diese Art der Verarbeitung nur dann vorgenommen wird, wenn entsprechende, mit unseren Datenschutzgesetzen vergleichbare Maßnahmen die Betroffenen auch im Ausland vor einem Mißbrauch ihrer Daten schützen.

In einigen Bundesländern erhalten Befürchtungen um den geplanten Ausweis zusätzliche Nahrung dadurch, daß die Seriennummer des Personalausweises - und auch des Passes - im Melderegister gespeichert wird. Die Gefahr, daß diese Nummer die Funktion eines Personenkennzeichens erhalten kann, das als Schlüssel für die Zusammenführung der verschiedensten über jeden Bürger gespeicherten Datensätze verwendbar wäre, wächst dadurch erheblich (vgl. auch oben Ziff. 2.1.2.1 und 2.1.2.4). Umso mehr ist hervorzuheben, daß das Hessische Meldegesetz diese Möglichkeit nicht vorsieht.

3.1.3
Schwerpunkt der Kritik: Verwendungsmöglichkeiten für die Sicherheitsbehörden

Die Kritik an dem neuen Ausweis betrifft besonders die Möglichkeit, ihn für eine automatisierte Einrichtung und Erschließung von Dateien im Sicherheitsbereich zu verwenden (§ 3 Abs. 5 PAG).

Regelmäßig bei Grenzkontrollen, aber auch bei mobilen Kontrollstellen, die zur Strafverfolgung oder Gefahrenabwehr eingerichtet werden, entfällt durch die automatisierte Eingabe der Bearbeitungsschritt der manuellen Dateneingabe. Während bisher ein Beamter die Ausweisdaten in ein Übertragungsgerät eintippen mußte, übernimmt das Lesegerät diesen Schritt durch ein optisches Abtasten der Ausweisoberfläche. Zwar bedarf es weiterhin einer Kontrollperson, um die Übereinstimmung des Ausweisbildes mit dem Aussehen des Ausweisbesitzers zu prüfen, dennoch kann die Überprüfung der Daten erheblich schneller durchgeführt werden. Schon bei routinemäßigen Grenzkontrollen zu Zeiten starken Reiseverkehrs, erst recht aber bei besonderen Anlässen wie z.B. Großdemonstrationen, gewinnt dieser technische Vorteil erheblich an Bedeutung. Die schnellere Abwicklung der Datenabfrage erlaubt es, eine wesentlich höhere Zahl an Personen zu kontrollieren. Das nun ausdrücklich in der aktuellen Informationsschrift des Bundesministers des Innern zum neuen Personalausweis bestätigte Ziel, den neuen Ausweis für vermehrte Überprüfungen zu nutzen, weckt in weiten Kreisen der Bevölkerung Befürchtungen, der Ausweis könnte zu einer neuen Qualität der Verhaltenskontrolle der Bürger führen. Diese Befürchtungen stehen in einem engen Zusammenhang mit der bereits derzeit umfangreichen und ständig zunehmenden Speicherung und Verknüpfung personenbezogener Daten in den polizeilichen Informationssystemen.

3.1.3.1
Unverzichtbare Bedingung: Präzise Vorschriften für die polizeiliche Datenverarbeitung

In ihrer Stellungnahme zur Verwendung des geplanten Ausweises vom November 1979 (s.o. Ziff. 3.1.1.2) griffen die Datenschutzbeauftragten von Bund und Ländern insbesondere auch die Frage der Maschinenlesbarkeit auf. Hierzu erklärten sie:
"Die Datenschutzbeauftragten betonen jedoch, daß damit über den zulässigen Umfang von Datenspeicherungen und Datenübermittlungen im Sicherheitsbereich noch nicht entschieden ist und fordern die baldige Verabschiedung eines datenschutzgerechten Melderechts sowie die zügige Erarbeitung spezieller Datenschutzvorschriften für die Sicherheitsbehörden. Nur unter dieser Bedingung ist die Verwendung der maschinenlesbaren Ausweiskarte für Zwecke des polizeilichen Informationssystems annehmbar."

Der Deutsche Bundestag hat sich dieses "Junktim" zu eigen gemacht. Anläßlich der Verabschiedung des Personalausweisgesetzes am 17. Januar 1980 faßte er einstimmig folgenden Beschluß (vgl. BT-Drucks. 8/3498 sowie BR - zu Drucks. 17/80):

"Der Deutsche Bundestag ist der Auffassung, daß angesichts der raschen Fortentwicklung der automatischen Datenverarbeitung und deren Einsatz in der öffentlichen Verwaltung über die Verabschiedung des Gesetzes zur Änderung des Gesetzes über Personalausweise hinaus weitere Maßnahmen erforderlich sind, um einen ausreichenden Schutz der Persönlichkeitsrechte der Bürger gegen mißbräuchliche Verwendung ihrer persönlichen Daten zu gewährleisten. Die Bundesregierung wird deshalb ersucht,

1. den Entwurf eines datenschutzgerechten Melderechtsrahmengesetzes einzubringen und

2. die Arbeiten zur Entwicklung bereichsspezifischer Regelungen für die Sicherheitsbehörden nachdrücklich fortzusetzen."

Mit der Verabschiedung des Melderechtsrahmengesetzes durch den Deutschen Bundestag und des Hessischen Meldegesetzes durch das hessische Landesparlament wurde die erste Forderung des Bundestages im wesentlichen erfüllt.

Obwohl notwendig zur Erfüllung der zweiten Forderung, wurde hingegen eine ausreichende Rechtsgrundlage für die Informationsverarbeitung durch die Sicherheitsbehörden nicht geschaffen. Diesem Teil des Beschlusses kam bisher lediglich das Land Bremen insoweit nach, als es ein Polizeigesetz mit detaillierten Bestimmungen über die polizeiliche Datenverarbeitung verabschiedet hat. Die von mir bereits in einer Reihe von Tätigkeitsberichten (zuletzt im 11. Tätigkeitsbericht, Drucks. 10/166 Ziff. 3.2.1) aufgestellte Forderung nach einem datenschutzgerechten Polizeigesetz ist durch die geplante Einführung des maschinenlesbaren Personalausweises besonders aktuell und unverzichtbar geworden, weil die für die Strafverfolgung und Gefahrenabwehr zuständigen Behörden gemäß § 3 Abs. 5 PAG die wesentlichen Nutznießer des maschinenlesbaren Personalausweises sind. Ich begrüße es daher, daß der Hessische Minister des Innern in einem Schreiben an den Bundesinnenminister ausdrücklich anerkannt hat, daß bereichsspezifische Datenschutzregelungen für die Sicherheitsbehörden vor dem Inkrafttreten des neuen Personalausweisgesetzes geschaffen werden müssen.

3.1.3.2
Das spezifische Gefährdungspotential der polizeilichen Datenverarbeitung

3.1.3.2.1
Quantität und Sensitivität der gespeicherten Daten

Die Notwendigkeit einer genauen gesetzlichen Festlegung der polizeilichen Befugnisse für den Umgang mit Informationen über den Bürger ergibt sich vor allem aus folgenden Aspekten:

Zum einen gehört die Polizei zu den Verwaltungsbereichen, in denen der Einsatz der automatisierten Datenverarbeitung in den letzten Jahren besonders rasch zugenommen hat. Dies bezieht sich nicht nur auf die Quantität, sondern auch auf die verbesserten Zugriffs-, Auswertungs- und Übermittlungsmöglichkeiten (vgl. dazu ausführlich meinen letzten Tätigkeitsbericht, Ziff. 3.2.2.2). Zum anderen werden gerade von der Polizei in der Regel besonders sensible Daten verarbeitet, d.h. Informationen, deren Sammlung bzw. Weitergabe unter Umständen erhebliche Nachteile für die Betroffenen mit sich bringen kann.

Die 1981 vom Hessischen Innenminister in Kraft gesetzten Richtlinien für die Führung Kriminalpolizeilicher Sammlungen - KpS-Richtlinien - (s. hierzu 10. Tätigkeitsbericht, Drucks. 9/5873, Ziff. 2.2.2) sind zwar ein wesentlicher Schritt in die richtige Richtung und haben sich im Grundsatz bewährt. Sie reichen jedoch nicht aus: Zum einen verlangt die Entwicklung, daß - wie erwähnt - der Einsatz der automatisierten Datenverarbeitung komplexer und vielfältiger geworden ist, darauf zugeschnittene differenziertere Regelungen. Zum anderen handelt es sich lediglich um Verwaltungsvorschriften. Gerade im Sicherheitsbereich muß jedoch die Befugnis der Behörden zur Datenverarbeitung gesetzlich geregelt werden, weil die Sammlung, Auswertung und Weitergabe von Informationen in die Grundrechte der betroffenen Bürger eingreift. Unabhängig davon liegt es auch im Interesse aller Beteiligten, daß klare rechtliche Vorgaben existieren. Der neue maschinenlesbare Personalausweis macht diese Forderung dringlicher.

3.1.3.2.2
Insbesondere: Zunahme der "vorbeugenden Verbrechensbekämpfung"

Die Notwendigkeit einer präzisen gesetzlichen Regelung der polizeilichen Datenverarbeitung wird besonders deutlich anhand der Tatsache, daß die Polizei in zunehmendem Maße im Bereich der sog. vorbeugenden Verbrechensbekämpfung, d.h. im Vorfeld von Strafverfolgung und konkreter Gefahrenabwehr, tätig wird. Diese vorverlagerte polizeiliche Tätigkeit führt zu schwierigen rechtlichen Abgrenzungsproblemen und zur Speicherung erheblicher Datenmengen. Mit der Einführung des maschinenlesbaren Personalausweises verschärft sich diese Problematik, da dieser es möglich macht, Kontrollen im weiteren Umfeld von Straftaten und Verdächtigen bzw. von tatsächlichen oder befürchteten Gefahren vorzunehmen.

Ein Beispiel dafür ist die "polizeiliche Beobachtung"(PB). Die PB dient der Sammlung von Erkenntnissen über den Betroffenen - z.B. seine Kontakte, Reisen, benutzte Fahrzeuge. Das Resultat soll der Beweisführung im Zuge eines Ermittlungsverfahrens oder der Gefahrenabwehr dienen. Soll ein Bürger polizeilich beobachtet werden, dann muß nach derzeitiger Praxis weder ein substantieller Tatverdacht noch eine konkrete Gefahr im Sinne der polizeilichen Generalklausel gegeben sein. Die PB soll vielmehr erst klären, ob ein Tatverdacht bzw. eine konkrete Gefahr überhaupt vorliegen. Die heimlich erhobenen Daten werden bei einer Polizeidienststelle zusammengeführt mit

dem Ziel, Bewegungsbilder der betroffenen Personen herzustellen, die gegebenenfalls zu weiteren polizeilichen Maßnahmen führen. Die einschlägige Polizeidienstvorschrift 384.2 grenzt den zu erfassenden Personenkreis, den Anlaß einer Beobachtung und die Befugnisse im einzelnen nicht ausreichend ein. So führt die PB auch zur Sammlung vielfältiger Daten aus dem Umfeld - z.B. auch dem Bekannten- bzw. Verwandtenkreis - des betroffenen Bürgers. Eine Vielzahl Unbeteiligter gelangt so - ohne es jemals zu erfahren - in die polizeilichen Datensammlungen. Die Tatsache, daß sich der Beobachtungszeitraum nach der erwähnten Polizeidienstvorschrift über Monate, sogar über Jahre hinziehen kann, während deren der Betroffene von der Beobachtung nichts weiß, verleiht den Maßnahmen noch zusätzliches Gewicht. Die Einführung des neuen Personalausweises wird - nicht zuletzt infolge der dann verstärkt durchgeführten Grenzkontrollen - zur Sammlung von wesentlich mehr Daten über die Betroffenen bzw. deren Umfeld führen.

Zu erwähnen ist in diesem Zusammenhang die zunehmende Verwendung des Dokumentations- und Recherchesystems PIOS (Personen, Institutionen, Objekte und Sachen) durch die Polizei (vgl. auch oben 2.1.3.2). In den PIOS-Dateien sind sowohl formatierte Daten als auch Freitext gespeichert. Vielfältige Auswertungen bzw. Verknüpfungen der Datenbestände sind möglich. In diesen Dateien werden zu einem ganz erheblichen Teil sog. "Vorfelddaten" erfaßt. So können z.B. in die Datei PIOS-Terrorismus die Daten von Bürgern aufgenommen werden, die einen zufälligen, ihnen möglicherweise gar nicht bewußten Kontakt mit Angehörigen des sog. "terroristischen Umfeldes" hatten (s. hierzu auch den 4. Tätigkeitsbericht des Bundesbeauftragten, BTDrucks. 9/1243 Ziff. 2.12.1). Der Kreis der gespeicherten Personen ist kaum abzugrenzen. Der neue Personalausweis verschärft auch dieses Problem, da die Polizei durch umfangreichere Kontrollen wesentlich mehr "Vorfelddaten" gewinnen kann.

Für die Tätigkeit der Polizei im Bereich der vorbeugenden Verbrechensbekämpfung einschließlich der damit verbundenen Datenverarbeitung gibt es keine Rechtsgrundlage. Die polizeiliche Generalklausel setzt eine im Einzelfall bestehende konkrete Gefahr voraus und kann daher diese Tätigkeit im Vorfeld nicht rechtfertigen. Auch die Strafprozeßordnung sieht keine Maßnahmen zur "Verdachtsverdichtung" vor. Allerdings kann es bei der geforderten datenschutzgerechten Neufassung des Polizeigesetzes nicht darum gehen, die derzeitige polizeiliche Praxis der Datenverarbeitung einfach ungeprüft zu legalisieren. Es bedarf vielmehr der Erarbeitung verhältnismäßiger und begrenzender Regelungen. In jedem Fall darf das Mittel der vorbeugenden Verbrechensbekämpfung allenfalls zur Bekämpfung einzelner, konkret aufgeführter, schwerwiegender Straftatbestände eingesetzt werden.

3.1.3.3
Regelungsvorschläge

Einige wichtige Punkte stehen im Vordergrund:

3.1.3.3.1
Erhebung und Speicherung

Was die Datenerhebung durch die Polizei anbetrifft, so kommt - gerade auch im Zusammenhang mit dem neuen maschinenlesbaren Personalausweis - der Regelung der Identitätsfeststellung durch die Polizei besondere Bedeutung zu. Der neue Personalausweis eröffnet die Möglichkeit erheblich verstärkter Kontrollen. Der zulässige Umfang von Personenkontrollen muß daher konkretisiert und im Hinblick auf die neuen technischen Möglichkeiten klar begrenzt werden. Dabei muß auch der Abgleich mit den polizeilichen Datenbeständen geregelt werden. Die Polizei darf bei Kontrollen die Personalien des Bürgers mit ihren Informationssystemen nur vergleichen, soweit es der Zweck der Identitätsfeststellung im konkreten Fall erfordert. So benötigt z.B. die Schutzpolizei zur Erfüllung ihrer Aufgaben bei Kontrollen regelmäßig keine Angaben dazu, ob über den Betroffenen bereits eine Kriminalakte angelegt wurde. Diese Daten dürfen daher von ihr nicht abgefragt werden. Der Beschluß der Innenministerkonferenz vom September 1977, der vorsieht, daß alle Personen, die der Polizei bei der Erfüllung ihrer Aufgaben bekannt werden, routinemäßig - d.h. ohne jeden konkreten Anhaltspunkt - durch Abfrage in der Personenfahndungsdatei überprüft werden, ist unverhältnismäßig und muß daher aufgehoben werden.

Auch für die Datenspeicherung durch die Polizei bedarf es einer präzisen gesetzlichen Regelung. Werden Daten zulässigerweise erhoben, so folgt daraus nicht automatisch, daß diese Daten auch gespeichert werden dürfen. Die Speicherung stellt eine zusätzliche Beeinträchtigung des Bürgers dar, die nur dann zulässig ist, wenn sie auch tatsächlich für die weitere Aufgabenerfüllung erforderlich ist. So geht z.B. das Bundesverwaltungsgericht in ständiger Rechtsprechung davon aus, daß rechtmäßig angefertigte erkennungsdienstliche Unterlagen nur dann von der Polizei aufbewahrt werden dürfen, wenn konkrete Anhaltspunkte dafür vorliegen, daß der Betroffene künftig straffällig wird (so bereits BVerwGE 26, 169). Klargestellt werden muß auch, daß nicht rechtmäßig erhobene Daten nicht gespeichert werden dürfen. Was die einzelnen Dateien anbelangt, so muß im Gesetz bestimmt werden, daß jede Datei einer Errichtungsanordnung bedarf, in der namentlich der Zweck der Datei, der zu speichernde Personenkreis, die Art der Informationen, der Umfang vorgesehener Übermittlungen und die Dauer der Speicherung festzulegen sind. Die Verfahrensweise bei der Errichtung neuer Dateien muß klar geregelt werden. Auf diese Weise kann ein Mindestmaß an Transparenz und Kontrollierbarkeit sichergestellt werden.

3.1.3.3.2
Übermittlung

Bei der Datenübermittlung durch die Polizei muß berücksichtigt werden, daß andere Behörden sich für Auskünfte über Strafverfahren, Verurteilungen usw. grundsätzlich an das Bundeszentralregister zu wenden haben (vgl. 11.Tätigkeitsbericht Ziff. 3.2.3 sowie unten Ziff. 4.5). Die polizeilichen Datenbestände dürfen nicht an seine Stelle treten. Eine Übermittlung von Daten, die im Rahmen der vorbeugenden Verbrechensbekämpfung gewonnen wurden, muß grundsätzlich ausgeschlossen werden.

Besonders notwendig ist eine gesetzliche Einschränkung des Informationsaustausches zwischen Polizei und Verfassungsschutz. Zu bedenken ist hierbei, daß die alliierten Militärgouverneure im Jahre 1949 in ihrem sog. Polizeibrief zur Verabschiedung des Grundgesetzes die Bundesrepublik verpflichteten, Aufgaben und Befugnisse der Polizei einerseits und des Verfassungsschutzes andererseits strikt zu trennen. Dieser Grundsatz hat in den Polizei- bzw. Verfassungsschutzgesetzen seinen Niederschlag gefunden. Findet ein umfassender Informationsaustausch zwischen Polizei und Verfassungsschutz statt, so wird jedoch das Ziel der Regelungen, zwischen den unterschiedlichen Aufgaben der Behörden zu differenzieren und ihnen der jeweiligen Aufgabenstellung entsprechende Befugnisse zuzuweisen, weitgehend verfehlt, da die eine Behörde faktisch Nutznießer der Maßnahmen der anderen Behörde ist. Die derzeitige Praxis gibt zu Bedenken Anlaß. Die Datenschutzbeauftragten haben wiederholt auf dieses Problem hingewiesen (vgl. etwa Ziff.2.4 meines 9. Tätigkeitsberichtes, Drucks. 9/2740 oder Ziff. 3.12.1.1 des 3. Tätigkeitsberichtes des Bundesbeauftragten für den Datenschutz, BTDrucks. 9/93). Eine verstärkte Kontrolltätigkeit der Polizei infolge der Einführung des neuen Ausweises wird zu erhöhten Übermittlungszahlen und damit zu einer Verschärfung dieses Problems führen.

3.1.3.4
Umsetzung in die Praxis

So wichtig allerdings eine parlamentarisch verantwortete, den Grundsatz der Verhältnismäßigkeit beachtende Regelung der polizeilichen Datenverarbeitung gerade auch im Zusammenhang mit dem maschinenlesbaren Personalausweis ist, eines muß jedoch betont werden: Gesetzliche Regelungen allein reichen nicht aus. Wie ich bereits in meinem letzten Tätigkeitsbericht (Ziff. 3.2.2.2) dargelegt habe, ist im Polizeibereich eine Tendenz zur beträchtlichen Ausdehnung der gespeicherten Datenbestände festzustellen, und zwar vor allem durch die Errichtung von speziellen Zwecken dienenden automatisierten Dateien, wobei Systeme verwendet werden, die erheblich mehr Abfrage- und Verknüpfungsmöglichkeiten bieten als die ursprünglich genutzten Systeme. Die Umsetzung der Gesetzesvorschriften in die Praxis, namentlich die Frage der Errichtung neuer Dateien und ihres Datenumfanges, die Realisierung der Löschungsvorschriften und der Sicherheitsvorkehrungen gegen unbefugten Zugriff sowie gegen unberechtigte Weitergabe bedürfen der ständigen Aufmerksamkeit.

Leider war die Landesregierung bisher vielfach nicht bereit, meinen Bedenken Rechnung zu tragen (s. hierzu z.B. Ziff. 2.1.3.2 und 2.1.3.3).

Auch und gerade im Hinblick auf den maschinenlesbaren Ausweis gilt es, die datenschutzrechtlichen Probleme der polizeilichen Datenverarbeitung rechtzeitig zu diskutieren und zufriedenstellend zu lösen; die Technik darf nicht die Weichen stellen. Es darf auch in Zukunft nicht mehr geschehen, daß - wie z.B. bei der Datei PIOS-Terrorismus - zunächst große Datenmengen eingespeichert werden und erst danach Lösungen des Löschungsproblems überlegt werden, deren Realisierung sich dann über viele Jahre hinzieht.

3.1.4
Verbot zweckwidriger Auswertung von Protokolldateien
Verhinderung von Mobilitätsprofilen der Bürger

Die Eingabe des maschinenlesbaren Personalausweises - technisch präziser wäre die Bezeichnung "Bundespersonalausweis mit automatisiert lesbarer Codierzone" - in die Lesegeräte der Sicherheitsbehörden hat zur Folge, daß die auf dem Ausweis aufgebrachten Daten mit Daten der polizeilichen Informationssysteme verglichen werden. Bei diesem Abgleich speichert das System zunächst aus technischen Gründen in jedem Fall die Daten des eingegebenen Ausweises. Unter welchen Voraussetzungen und zu welchen Zwecken diese zur sog. Protokollierung der Zugriffe und Abfragen gespeicherten Angaben verwertet werden dürfen, läßt sich nur im Rahmen einer umfassenden Erklärung der Funktion automatisierter Protokollierungsverfahren beantworten.

3.1.4.1
Personenbezogene Daten auf Protokollbändern

Große Systeme der Datenverarbeitung sind technisch u. a. nur beherrschbar, wenn systeminterne Protokolle (log) über den jeweiligen Betriebszustand der Anlagenkomponenten (Maschinen und Programme) aufgezeichnet werden. Dies geschieht innerhalb des Hauptspeichers (CPU) und/oder auf externen Speichermedien (Band/Platte). Gegenstand dieser Protokolle sind Daten technischer Natur über systembedingte Betriebszustände und Nachrichteninhalte (z. B. personenbezogene Daten).
(S. auch 1. Tätigkeitsbericht, Ziff. 2.4.4 und 8. Tätigkeitsbericht, Ziff. 2.4.2).

Protokollbänder sind Dateien, die u.a. personenbezogene Daten enthalten. Als solche unterfallen sie dem Hessischen Datenschutzgesetz. Es gilt daher auch für sie § 11 HDSG, demzufolge personenbezogene Daten nur dann und nur so lange gespeichert werden dürfen, wie dies zur Aufgabenerfüllung erforderlich ist. Diese Feststellung hat folgende konkrete Konsequenzen:

3.1.4.1.1
Zweckbindung und Löschungsanspruch

Die auf den Protokollbändern gespeicherten personenbezogenen Daten können von der Polizei genutzt werden, um eine fehlerfreie Datenverarbeitung zu gewährleisten und um überprüfen zu können, ob die erforderlichen technischen und organisatorischen Maßnahmen der Datensicherung (§ 10 HDSG) getroffen und eingehalten wurden. Die auf den Archivbändern enthaltenen personenbezogenen Daten dürfen in dem Umfang und für die Dauer gespeichert werden, wie es diese Zwecke erfordern. Allerdings könnten dieselben personenbezogenen Daten in Einzelfällen auch von der Polizei zur Strafverfolgung bzw. Gefahrenabwehr gebraucht werden. Nimmt man diesen Zweck zum Maßstab, so ergibt sich ein ganz anderes Ergebnis hinsichtlich Umfang und Dauer einer zulässigen Speicherung. Könnten die personenbezogenen Daten in dem Umfang und solange gespeichert werden, bis sie für keinen dieser Zwecke mehr gebraucht werden, so würde das im Hessischen Datenschutzgesetz festgelegte Recht des Bürgers, die Löschung seiner Daten zu verlangen, wenn diese für die Aufgabenerfüllung nicht mehr benötigt werden, weitgehend relativiert werden. Die Lösung kann daher nur folgendermaßen lauten:

Zweck der Protokollierung kann nur die Sicherung einer fehlerfreien Datenverarbeitung und die Nachweismöglichkeit für die Datenschutzkontrolle (§ 10 HDSG) sein (zu den Funktionen der Protokollierung im einzelnen vgl. unten Ziff. 3.1.4.2). Die Daten dürfen nur für diese Zwecke genutzt werden. Die Dauer der Speicherung der in den Protokollen aufgezeichneten Daten muß im Hinblick auf diesen Zweck konkret festgelegt werden.

Dies gilt auch für die Aussonderung von Kriminalakten aus den Beständen der Polizei nach den KpS-Richtlinien. Die zu ihnen bis dahin in HEPOLIS gespeicherten Daten sind auch nach der Aussonderung immer noch auf den (archivierten) Protokollbändern enthalten. Würden sie auch für Zwecke der Strafverfolgung bzw. der Gefahrenabwehr genutzt, liefe das Recht des Bürgers leer, nach den in den KpS-Richtlinien festgelegten Fristen nicht mehr bei der Polizei registriert zu sein. Mit anderen Worten: Darf die Polizei die Daten der betroffenen Bürger schon nicht (mehr) in ihren speziell für ihre polizeilichen Aufgaben (Strafverfolgung und Gefahrenabwehr) eingerichteten Dateien festhalten, ist es ihr um so mehr verwehrt, die auf den Protokollbändern gespeicherten Informationen zu diesen Zwecken zu verwerten.

3.1.4.1.2
Zweckbindung und "Negativanfragen"

Im Zusammenhang mit dem neuen maschinenlesbaren Personalausweis ist diese Zweckbindung von erheblicher Bedeutung, und zwar insbesondere bei der sogenannten "Negativanfrage". Damit ist folgendes gemeint: Da die Protokolldateien alle Nachrichteninhalte enthalten, ist z.B. erkennbar - und soweit auch maschinell auswertbar -, wer wann eine Anfrage über eine bestimmte Person an das DV-System gestellt hat. Soweit diese Person in der polizeilichen Datenbank nicht gespeichert ist, gibt das System eine "negative" Auskunft an das anfragende Terminal. Auch dieser Vorgang wird Bestandteil des Maschinenprotokolls. Damit ist die abgefragte Person, über die bis zum Zeitpunkt dieser Transaktion keine Daten im System vorlagen, auf dem Log-Band gespeichert, und zwar auch dann, wenn der die Abfrage begründende Vorfall keinerlei Anlaß gab, diese Person in einer der Strafverfolgung bzw. der Gefahrenabwehr dienenden Datei, insbesondere HEPOLIS, zu speichern. Die Folge einer durch den Personalausweis verstärkten Kontrollpraxis wird die Speicherung einer wesentlich größeren Zahl von Personen aufgrund der "Negativanfrage" in den Protokollbändern sein. Wohlgemerkt: Dabei handelt es sich um Bürger, bei denen - auch aus der Sicht der Polizei - keinerlei Anlaß vorlag, sie aus Gründen der Strafverfolgung oder der Gefahrenabwehr zu registrieren, also um "unbeteiligte" Bürger.

3.1.4.2
Technischer Zweck und Umfang der Protokolle

Nachrichteninhalte und technische Darstellung von Maschinenprotokollen oder -journalen sind systembedingt und je nach Hersteller verschieden; sie unterliegen in ihrer Struktur aber ähnlichen Regeln. Die verschiedenen Kriterien, wie z. B. die Aufgabe des Journals, sein Umfang, Entstehungszeitpunkt und weitere Behandlung sollen hier in vereinfachter Form am Beispiel des Datenbanksystems beim Hessischen Landeskriminalamt dargestellt werden.

Das Hessische Landeskriminalamt setzt zur Durchführung verschiedener automatisierter Verfahren im Polizeibereich - insbesondere des polizeilichen Informationssystems HEPOLIS - ein Programmprodukt der Fa. IBM, nämlich IMS/VS (information management system/virtual storage), unter dem Systemsteuerprogramm (Betriebssystem) MVS/SP (multiple virtual storage) ein. Diese Betriebssystem- bzw. Datenbankprogramme steuern das Zusammenwirken von zwei Großrechnern mit je 6 MByte Speicherkapazität, zahlreichen Platten, Bandlaufwerken, Druckern und über hundert Datensichtgeräten, die in einem polizeiinternen Datenfernverarbeitungsnetz betrieben werden. Die Komplexität des Verfahrens ist damit vorgegeben.

Auf den Leitungswegen der Datenfernverarbeitung und innerhalb des Datenverarbeitungssystems werden ständig Daten über Betriebszustände von Einzelkomponenten, Systemsteuerdaten und Nachrichteninhalte ausgetauscht. Diese Daten werden fortlaufend auf einem Protokollband (IMS-Journal) gespeichert. Kommt es während eines Programmlaufs oder einer Transaktion zu einem fehlerhaften Abbruch der Verarbeitung (abnormal end), treten Schreib-/Lesefehler auf oder wird eine Datenbank ganz oder teilweise zerstört, verfügt das System über interne Mittel - sogenannte Wiederanlaufroutinen -, um Datenbestände vollständig und richtig wiederherzustellen. Je nach "Schwere" des aufgetretenen Fehlers laufen verschiedene Rekonstruktionsverfahren ab.

- Wird ein Programm fehlerhaft beendet oder kommt das gesamte DV-System zum Stillstand (Systemabsturz) und sind in der Datenbank keine Daten zerstört worden, wird das sog. Prüfpunkt/Wiederanlaufverfahren (checkpoint/restart) eingesetzt. Dabei wird auf dem IMS-Logband der letzte ordnungsgemäß geschriebene Prüfpunkt gesucht und die Verarbeitung der Daten ab diesem Punkt wiederholt bzw. fortgesetzt.

- Stellt das System fest, daß Daten zerstört wurden, muß ein sog. Wiederherstellungslauf erfolgen (recovery). Mit Hilfe der letzten vorhandenen Sicherungskopie der Datenbank - diese stellt ein genaues Abbild der Datenbank in einem ordnungsgemäßen Zustand zu einem bestimmten Zeitpunkt dar - wird die (zerstörte) Datenbank auf den letzten als richtig erkannten Stand gebracht. Dann werden mit dem recovery-Programm die nach dem Zeitpunkt der Sicherungskopie erstellten Logbänder erneut verarbeitet. Die Datenverarbeitung wird "richtig" nachvollzogen.

- Erkennt das System während der Verarbeitung Schreib-/Lesefehler in einem Datenbestand/Datenbankbereich, erfolgt die Protokollierung in sog. Fehlerverfolgungssätzen (trace records). Sie ermöglichen es dem Fachmann, die Fehler gezielt aufzufinden und zu analysieren.

Außer diesen Funktionen, die den ordnungsgemäßen Ablauf der Datenverarbeitung sicherstellen sollen, können mit dem Protokolldatenbestand noch weitere Aufgaben erfüllt werden:

- Statistische Auswertungen, die Auskunft über die Belastung/Auslastung des Systems bzw. von Endgeräten zu bestimmbaren Zeiten geben.

- Nachweispflichten nach § 10 (Anlage) HDSG

Noch einmal: Die im Maschinenprotokoll gespeicherten Daten dürfen nur zu diesen Zwecken und in dem hierfür benötigten Zeitraum aufgezeichnet und verwertet werden.

3.1.4.3
Archivierung der Protokolle

Im Hessischen Landeskriminalamt werden die täglich anfallenden Protokolle auf Banddateien geschrieben und vier Wochen unverändert aufbewahrt. Nach Ablauf dieser Zeit werden die Bänder erneut in das System eingegeben und in einem sog. "Verdichtungslauf" verarbeitet. D.h. durch ein Programm werden alle für die weitere Archivierung unnötigen - dies sind z.B. alle systeminternen Daten/Verwaltungsdaten - entfernt; die Bänder werden "komprimiert". Alle Nachrichteninhalte mit Angabe über z.B. den Zeitpunkt des Zugriffs und das anfragende Endgerät bleiben erhalten. Die so erzeugten verdichteten Archivbänder werden z.Z. noch auf Dauer aufbewahrt.

3.1.4.4
Notwendige Maßnahmen

Soweit personenbezogene Daten auf Protokollbändern zu Zwecken der Datenschutzkontrolle (§ 10 HDSG) gespeichert werden, geraten zwei Datenschutzaspekte in Konflikt: Werden sie weiterhin aufbewahrt, 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. Bei Abwägung dieser beiden Gesichtspunkte ist die Lösung sachgerecht, daß die personenbezogenen Daten aus "Negativanfragen" spätestens beim sog. Komprimierungslauf von den Protokollbändern gelöscht werden müssen. Damit stehen die Angaben nach der derzeitigen Praxis im HLKA höchstens vier Wochen lang zu Überprüfungszwecken (s.o.) zur Verfügung. Danach werden sie automatisch gelöscht.

Unabhängig von einer künftigen Entwicklung im Bereich der Datenbankanfragen unter Verwendung eines automatisierten Ausweislesegerätes halte ich es für unabdingbar, eine Aufbewahrungsfrist für IMS-Logbänder (soweit diese personenbezogene Daten enthalten) festzulegen, die möglichst kurz sein sollte (s. 8. Tätigkeitsbericht, Ziff. 2.4.2.5).

Ich habe dem Hessischen Minister des Innern meine Auffassung dargelegt und ihn um Vorschläge gebeten, wie eine derartige ausschließlich zweckgebundene Verwertung der personenbezogenen Daten auf den Protokollbändern sichergestellt werden kann. Sollte es sich erweisen, daß dies - aus welchen Gründen auch immer - nicht in hinreichender Weise möglich ist, müßte künftig auf die Speicherung personenbezogener Daten auf Protokollbändern ganz verzichtet werden.

3.1.5
Technische Infrastruktur - Unklarheit der Planung

Die Frage der rechtlichen Rahmenbedingungen für die Einführung des neuen Ausweises kann von den Veränderungen in der Kontrollpraxis nicht getrennt werden. Ich habe mich deshalb mehrmals an den Hessischen Minister des Innern gewandt, um ein Bild von den geplanten Verwertungsstrukturen zu erhalten. Die technischen Daten der zu beschaffenden Lesegeräte, ihre Zahl, die vorgesehenen Einsatzbedingungen sind dabei ebenso von Interesse wie die Verfahren zur Erfassung und Verwertung der gewonnenen personenbezogenen Daten.

Abgesehen von der bereits der Presse zu entnehmenden Notiz, in den nächsten vier Jahren sei die Anschaffung von 400 Geräten geplant, konnte bisher ein Rahmenplan für die Errichtung der notwendigen Infrastruktur nicht vorgelegt werden. Dies gilt auch für die Planung des Bundes. Sieht man einmal von der Feststellung gegenüber der Öffentlichkeit ab, der Ausweis solle zu einer vermehrten Kontrolle eingesetzt werden - die Gründe, warum und in welchen Bereichen dies geschehen soll, bleiben weiterhin im Dunkeln -, steht dieser Mangel an Planung im krassen Gegensatz zu den gerade in der Öffentlichkeit laut gewordenen Befürchtungen. Er belastet und erschwert nicht nur die Bewertung des Systems durch die Datenschutzbeauftragten. Das fehlende Konzept der künftigen Kontrollverfahren steht in einem unübersehbaren Widerspruch zu der Feststellung, die Maschinenlesbarkeit des Personalausweises sei unerläßlich, um wichtige Erfolge bei der Strafverfolgung und Gefahrenabwehr zu erzielen. Jeder Bundesbürger wird von der geplanten Veränderung in seinen Grundrechten berührt. Eine Zunahme und möglicherweise intensivere Verwertung der Kontrollen darf deshalb nur unter strikter Beachtung des Verhältnismäßigkeitsgrundsatzes erfolgen. Wenn keine vorbereitende Planung vorgelegt werden kann, muß dies als Indiz dafür gewertet werden, daß die gesetzlich vorgesehene Änderung entweder nicht so erforderlich ist, wie dies vorgegeben wird, oder eine Planung zwar existiert, die verantwortlichen Stellen den Stand der Entwicklung jedoch den Datenschutzbeauftragten derzeit nicht erläutern möchten. Beides wäre fatal und mit rechtsstaatlichen Grundsätzen nicht zu vereinbaren. In jedem Fall muß die Forderung der Datenschutzinstanzen nach umfassender Aufklärung über die geplanten Maßnahmen erfüllt werden.

Angesichts der jetzt klaren Position des Hessischen Innenministers, der in dem bereits erwähnten Schreiben vom 25. August 1983 an seinen Kollegen im Bund betonte, daß er im Zusammenhang mit der Einführung des Personalausweises bereichsspezifische Datenschutzregelungen für die Sicherheitsbehörden für unabdingbar halte, gehe ich davon aus, daß dieses Informationsdefizit in beiderseitigem Interesse bald behoben wird (s. bereits oben Ziff. 3.1.3.1).

3.1.6
Die notwendige Überprüfung des Bundespersonalausweisgesetzes

Neben dem Verwendungszusammenhang des Ausweises werfen auch die bereits vorliegenden oder geplanten rechtlichen Regelungen Fragen auf. (Zu der durch die Volkszählungsentscheidung des Bundesverfassungsgerichts gebotenen Überprüfung der Gesetzgebung zum Personalausweis insgesamt vgl. oben Ziff. 1.2.1, Nrn. 3-5).

Dies gilt zunächst für das bereits verabschiedete Personalausweisgesetz - insbesondere die unterschiedliche Formulierung der Nutzungsverbote in der Verwaltung einerseits und der Privatwirtschaft andererseits. Im öffentlichen Bereich darf der Personalausweis - mit Ausnahme der Sicherheitsbehörden (s.o.) - weder zur automatischen Einrichtung noch zur Erschließung von Dateien verwendet werden (§ 3 Abs. 5 Satz 1). In § 4 - der für den sog. nicht-öffentlichen Bereich gilt - fehlt dagegen die Erwähnung der "Einrichtung". Ausdrücklich untersagt ist nur die Nutzung des Ausweises zur automatischen Erschließung. Folgt man dem reinen Gesetzeswortlaut, könnten Privatunternehmen mit dem Ausweis jedenfalls Dateien anlegen, eine Auffassung, die in der Tat der Bundesinnenminister vertritt. Denkbar wäre dann z.B., daß eine Bank alle Ihre Kunden auffordert, am Eingang den Ausweis in ein Lesegerät einzuführen. Allerdings dürfen die auf diese Weise erhobenen Daten in keinem Fall zu irgendeinem Zweck erschlossen werden.

Ich halte deshalb diese abweichende Formulierung für den privaten Bereich - auch und gerade angesichts der gesetzgeberischen Intention einer umfassenden Einschränkung der Nutzung des Ausweises - für verfehlt. Kaum verwunderlich, daß sich auch in der amtlichen Begründung kein Wort der Rechtfertigung dieser Differenzierung findet. So liegt der Schluß nahe, daß es sich um ein Versehen im Gesetzgebungsverfahren handelt, das umgehend korrigiert werden sollte.

Die jetzt vom Bundesinnenminister für diese Abweichung gegebene Begründung, die Verwendung des Ausweises zur automatischen Einrichtung von Dateien im nicht-öffentlichen Bereich sei unbedenklich, da der Bürger ja nicht gezwungen werde, an diesem Verfahren teilzunehmen, geht an der Realität vorbei. Ebenso wie in bestimmten Wirtschaftsbranchen - namentlich bei Banken und Versicherungen - eine privatautonome Selbstbestimmung über die Weitergabe von Daten weitgehend illusorisch geworden ist, besteht die Gefahr, daß auch hier für den Betroffenen ein faktischer Zwang entsteht, seinen Ausweis für die Einrichtung von Dateien vorzulegen. Das Mißtrauen, das der Gesetzgeber dem in jedem Fall auf die Wahrung der Grundrechte verpflichteten Staat in § 3 Abs. 5 Satz 1 entgegengebracht hat, muß um so mehr für den privaten Bereich gelten. Gerade angesichts der Tatsache, daß § 15 Abs. 6 des von der Bundesregierung beschlossenen Entwurfs für ein Paßgesetz inhaltlich mit § 3 Abs. 5 Satz 1 bzw. § 4 PAG übereinstimmt, und für den Paß somit diese merkwürdige Differenzierung in gleicher Weise gelten soll, muß das Gesetz korrigiert werden.

3.1.7
Rechtliche Vorgaben für die Novellierung des Landespersonalausweisgesetzes

Die hessische Landesregierung hat bisher noch keinen Entwurf für ein Landesgesetz zur Ausführung des Gesetzes über Personalausweise vorgelegt. Die Personalausweisreferenten des Bundes und der Länder haben jedoch einen Formulierungsvorschlag für ein solches Gesetz ausgearbeitet, der als Muster für künftige Landesgesetze gedacht ist. Dieser Formulierungsvorschlag wurde bereits in mehreren Ländern als Grundlage für den jeweiligen Entwurf eines Landesgesetzes herangezogen. Die in diesem Vorschlag vorgesehenen Regelungen bieten deshalb schon jetzt Anlaß für eine datenschutzrechtliche Überprüfung.

Nach den darin vorgesehenen Bestimmungen besteht für einen Antragsteller, der die für die Feststellung seiner Identität notwendigen Dokumente nicht beibringen kann, die Verpflichtung, sich einem Feststellungsverfahren zu unterziehen. Als letztes Mittel ist die Durchführung erkennungsdienstlicher Maßnahmen vorgesehen. Im künftigen Landesgesetz muß eindeutig festgelegt werden, daß ed-Unterlagen nur als letztes Mittel zur Identifizierung des Betroffenen zu erstellen sind und nach der Feststellung der Identität sofort vernichtet werden müssen. Dies gilt auch, soweit diese Unterlagen an das Bundeskriminalamt weitergeleitet werden, um sie mit dort vorhandenen Daten zu vergleichen.

Nach dem Formulierungsvorschlag ist die Errichtung eines örtlichen Personalausweisregisters vorgesehen. Ebenso wie beim Melderegister sollte der Zweck dieses Registers auch im Gesetz ausdrücklich festgeschrieben werden. Da bereits das Melderegister zur Identifizierung eines Einwohners bzw. zum Nachweis seiner Wohnung für öffentliche und nicht-öffentliche Stellen zur Verfügung steht, darf das Personalausweisregister nicht zu einem Parallel-Register mit gleicher Funktion ausgebaut werden. Es kann sich dabei nur um ein Nachweis-, nicht um ein Auskunftsregister handeln. Konkret bedeutet dies, daß die darin gespeicherten Daten neben der Verwertung durch die Personalausweisbehörden allenfalls für Übermittlungen an die Polizei zur Verfügung stehen dürfen, soweit dies notwendig ist, um die Merkmale eines gestohlenen, verlorenen oder möglicherweise rechtswidrig veränderten Ausweises zu überprüfen. Keinesfalls darf das Personalausweisregister für Auskünfte an private Stellen verwendet werden, die die notwendigen Auskünfte bereits aus dem Melderegister erhalten können. Sonst könnten die Schutzmechanismen des Melderegisters unterlaufen werden. In jedem Fall ist sicherzustellen, daß die besonders sensitiven Daten derjenigen Personen, die wegen Geisteskrankheit entmündigt sind, voraussichtlich dauernd in Krankenhäusern, Pflegeheimen oder ähnlichen Einrichtungen untergebracht sind oder aus anderen Gründen der Ausweispflicht nicht unterliegen, an dritte Stellen nicht weitergegeben und gesondert gespeichert werden.

In dem geplanten Personalausweisregister sollen nach dem vorliegenden Entwurf auch "unveränderliche Kennzeichen" des Betroffenen gespeichert werden. In die Ausweiskarte werden diese Daten nicht aufgenommen. Es ist deshalb kein Grund ersichtlich, sie im Register zusätzlich zu führen. Die Aufnahme in das Register führte sonst dazu, daß die Ausweiskarte als Erschließungsinstrument für das Register herangezogen würde und damit effektiv mehr Daten zur Auswertung bereitstünden, als dies der Ausweis selbst vorsieht. Abgesehen von Vermerken nach § 2 Abs. 2 PAG, deren Sonderbehandlung wegen der Sensibilität der Daten und ihrer Konzentration bei den Grenzkontrollstellen notwendig ist, sollte eine Speicherung von Daten, die der Ausweis selbst nicht enthält, entfallen. Zur Erläuterung: § 2 Abs.2 PAG sieht vor, daß unter den Voraussetzungen des § 7 Abs.1 des Paßgesetzes - d.h. wenn Paßversagungsgründe bei dem betroffenen Ausweisinhaber vorliegen - auch der Personalausweis nicht zum Verlassen des Gebietes der Bundesrepublik Deutschland und Berlin (West) berechtigt.

In den Regelungen über das Register sollte bindend festgestellt werden, wann die für die Ausstellung des Ausweises notwendigen Unterlagen zu vernichten sind. Es erscheint angemessen, diese Unterlagen höchstens bis zum Ablauf der Gültigkeitsdauer des Personalausweises aufzubewahren und jedenfalls dann zu vernichten, wenn der alte Ausweis durch einen neuen ersetzt wurde.

In jedem Fall ist zu berücksichtigen, daß auch die Ausstellung und Vergabe vorläufiger Personalausweise einer entsprechenden Regelung bedarf.

3.2
Kostendämpfung und Sparmaßnahmen
Konsequenzen für Datenschutz, Sozial- und Patientengeheimnis

3.2.1
Datentransparenz im Sozial- und Gesundheitswesen: Zielkonflikt

Manche Themen der Datenschutzdiskussion finden sich regelmäßig in meinen Berichten wieder. Dazu gehören auch die Konsequenzen sozial- und gesundheitspolitischer Sparmaßnahmen für das Patienten- und Sozialgeheimnis sowie das Verhältnis von Ausgabenkontrolle und Vertraulichkeit der Arzt-/Patientenbeziehung bzw. der Sozialdaten. In meinem 10. Tätigkeitsbericht habe ich meine Besorgnis angesichts der drohenden Durchlöcherung des Sozialgeheimnisses geäußert (Ziff. 4.1.4), im 11. Tätigkeitsbericht die Tendenzen und Erscheinungsformen dargestellt und kritisch bewertet, die angesichts des wachsenden Datenbedarfs der Sozialverwaltung das Patientengeheimnis und die ärztliche Schweigepflicht zunehmend einschränken (Ziff. 3.3.1).

In diesem Bericht beschränke ich mich auf die im Jahre 1983 neu hinzugekommenen Fallbeispiele. Im Vordergrund stehen dabei Maßnahmen der gesetzlichen Krankenkassen zur Kostendämpfung: Wirtschaftlichkeitsprüfungen in Krankenhäusern (Ziff. 3.2.2), "Modellversuche" zur Erhöhung der Leistungs- und Kostentransparenz (Ziff. 3.2.3) sowie die Datenerhebung im Zusammenhang mit der Abgrenzung von Krankheits- und Pflegefällen (Ziff. 3.2.4). Abschließend soll der Konflikt zwischen "Verdatung" und Persönlichkeitsrecht an Hand eines Beispiels aus dem Sozialleistungsbereich, der Novellierung des Kindergeldrechts mit dem Ziel der einkommensabhängigen Minderung des Kindergeldes, aufgezeigt werden (Ziff. 3.2.5).

Zunächst zum Gesundheitsbereich:

Die als "Kostenexplosion" bezeichnete unverhältnismäßige Steigerung der Krankheitskosten hat bereits im Jahre 1977 zum Erlaß des "Krankenversicherungs-Kostendämpfungsgesetzes" (KVKG v. 27. Juni 1977, BGBl. I S. 1069) geführt. Trotzdem ist die Kostenentwicklung in manchen Bereichen - beispielsweise auf dem Gebiet der stationären Behandlung und der Kosten für Medikamente - nach wie vor unbefriedigend. Deshalb ist es nicht nur verständlich, sondern legitim, daß die gesetzlichen Krankenkassen weiterhin nach Wegen "zur Dämpfung der Ausgabenentwicklung und zur Strukturverbesserung in der gesetzlichen Krankenversicherung" (so lautet die volle Bezeichnung des KVKG) suchen. Bei einer kritischen Betrachtung der dazu angewandten Verfahren und Maßnahmen geht es daher nicht darum, dieses Ziel in Frage zu stellen, sondern allein um das Problem, welche unerwünschten - und vielleicht nicht erkannten - Auswirkungen diese Sparversuche auf das Verhältnis zwischen Arzt und Patient, insbesondere auf das Patientengeheimnis, haben können und welche datenschutzrechtlichen Vorkehrungen geboten sind, um eine Gefährdung des Patientengeheimnisses zu vermeiden.

3.2.2
Wirtschaftlichkeitsprüfungen in Krankenhäusern

3.2.2.1
Bereitschaftsdienst im Krankenhaus

Im Rahmen von Wirtschaftlichkeitsprüfungen bei verschiedenen Krankenhäusern in öffentlicher Trägerschaft wurde auch der ärztliche Bereitschaftsdienst einbezogen. Der zeitliche Umfang und die Arbeitsbelastung des ärztlichen Bereitschaftsdienstes bzw. der Rufbereitschaft sollten dadurch festgestellt werden, daß von den Ärzten die Führung von Dienstbüchern mit über den Dienst angefertigten Aufzeichnungen und deren Weitergabe an die Krankenhausverwaltung verlangt wurde.

In diesen Aufzeichnungen waren neben dem Beginn und dem Ende der Arbeitsaufnahme auch der Name und die Aufnahmenummer des Patienten sowie die Art der Behandlung eingetragen, also Angaben, die der ärztlichen Schweigepflicht (§ 203 StGB in Verbindung mit der Ärztlichen Berufsordnung) unterliegen. Insbesondere im Hinblick darauf, daß solche Wirtschaftlichkeitskontrollen häufig von privaten Prüfungsfirmen vorgenommen werden, bestand die Gefahr, daß medizinisches Datenmaterial ohne Wissen und Genehmigung der Patienten und ohne sonstige Rechtsgrundlage offenbart und damit das Patientengeheimnis verletzt werden könnte.

Ich habe in einer - auf Wunsch der Hessischen Krankenhausgesellschaft abgegebenen - gutachtlichen Stellungnahme festgestellt, daß die Kenntnis patientenbezogener Daten zu Prüfungszwecken überhaupt nicht erforderlich und damit deren Übermittlung nicht zulässig war, da anonymisierte Daten ausreichten.

3.2.2.2
Pflegesatz bei Krankenhäusern im Großstadt-Umland

Erbringen kleinere, in der Nähe einer Großstadt gelegene Krankenhäuser Leistungen über die Minimalversorgung hinaus - etwa um den Patienten ihres Einzugsbereichs die Fahrt zur städtischen oder Universitätsklinik zu ersparen -so ist der Pflegesatz höher als bei einem Krankenhaus der Grund(Minimal)-versorgung.

Bei mehreren Kreiskrankenhäusern im Rhein-Main-Gebiet hatte daher die zuständige AOK eine Wirtschaftlichkeitsprüfung veranlaßt mit dem Ziel der Feststellung, ob der erhobene Pflegesatz tatsächlich den vom Krankenhaus erbrachten Leistungen angemessen war. Auch hier stand zu befürchten, daß das Patientengeheimnis durch Übermittlung von Patientendaten an die von der AOK beauftragten Prüfer im Rahmen der Untersuchung verletzt werden würde. Wie im vorigen Fall konnten jedoch - gemeinsam mit der Krankenhausverwaltung - Verfahren gefunden werden, die es ermöglichten, für die Wirtschaftlichkeitsprüfung nur anonymisierte Listen an das jeweilige Rechenzentrum weiterzuleiten.

3.2.3
Modellversuche zur Erhöhung der Leistungs- und Kostentransparenz

3.2.3.1
Aktionsprogramm der Bundesregierung

Ein anspruchsvolles und umfangreiches Projekt zur Kostendämpfung im Gesundheitswesen sind die auf mehrere Jahre geplanten, wissenschaftlich begleiteten "Modellversuche zur Erhöhung der Leistungs- und Kostentransparenz in der gesetzlichen Krankenversicherung gem. § 223 RVO" entsprechend der Bekanntmachung des Bundesministers für Arbeit und Sozialordnung (BMA) vom 14. Oktober 1980 (Bundesanzeiger Nr. 197 vom 21. Oktober 1980), in der es heißt:

> "Das Aktionsprogramm der Bundesregierung zur Förderung von Forschung und Entwicklung im Dienste der Gesundheit betont als einen Schwerpunkt der Forschung zur Organisation und Funktionserfüllung der gesetzlichen Krankenversicherung Untersuchungen zur erhöhten Leistungs- und Kostentransparenz. Der Bundesminister für Arbeit und Sozialordnung fördert wissenschaftlich unterstützte Modellversuche zur Überprüfung von Krankheitsfällen und Unterrichtung der Versicherten nach § 223 RVO. Interessierte Krankenkassen und Wissenschaftler werden aufgefordert, ihre Bereitschaft zur Mitwirkung bei den Modellversuchen zu bekunden.
>
> Mit dem Krankenversicherungs-Kostendämpfungs-Gesetz von 1977 wurden die Krankenkassen ermächtigt, in geeigneten Fällen im Zusammenwirken mit den Kassenärztlichen Vereinigungen, den Krankenhausträgern für den jeweiligen Bereich sowie den Vertrauensärzten die Krankheitsfälle vor allem im Hinblick auf die in Anspruch genommenen Leistungen zu überprüfen und den Versicherten und den behandelnden Arzt über die in Anspruch genommenen Leistungen und ihre Kosten zu unterrichten (§ 223 RVO). Damit sollte es insbesondere ermöglicht werden, dem Versicherten und den behandelnden Ärzten die Aufwendungen durchsichtig zu machen, die mit den erbrachten Leistungen verknüpft sind, um damit Hinweise für eine gezielte Inanspruchnahme zu geben."

3.2.3.2
Der Modellversuch der AOK Main-Kinzig als Beispiel

Im Bundesgebiet wird etwa ein halbes Dutzend solcher Modellversuche in ausgewählten Krankenkassen durchgeführt. In Hessen beteiligt sich die AOK Main-Kinzig in Hanau. Mit Hilfe eines aus der Projektbeschreibung, dem Bericht über die 1. Phase des Modellversuches und den einschlägigen datenschutzrechtlichen Bestimmungen erstellten ausführlichen Fragenkatalogs und eines ganztägigen Kontrollbesuches habe ich mich an Ort und Stelle über die Einzelheiten der Durchführung des Modellversuchs informiert und die dabei angewandten Maßnahmen zum Datenschutz überprüft.

Art und Umfang der Datenspeicherung und -auswertung lassen sich stichwortartig wie folgt beschreiben:

"Um ein möglichst umfassendes Bild von der Leistungs- und Kostenstruktur sowohl über die Versicherten wie über die medizinischen Einrichtungen zu gewinnen, hat die AOK Main-Kinzig entschieden, etwa ein Drittel ihrer Versicherten in die Untersuchungen der Modellversuche einzubeziehen...". Insgesamt werden die Daten von ungefähr 33.530 Mitgliedern und 24.450 Familienangehörigen in der Stichprobe gespeichert (Bericht der AOK Main-Kinzig zur 1. Phase der Modellversuche).

Zusätzlich zu dem Stammdatensatz im Mitgliederverzeichnis der AOK sind Angaben aus folgenden Unterlagen auf den einzelnen Versicherten bzw. Arzt bezogen erfaßt und gespeichert worden: Aus den Kranken- und Überweisungsscheinen (sie werden normalerweise, nach Ärzten geordnet, bei der AOK aufbewahrt), Rezepten (sie werden üblicherweise, nach Apotheken geordnet, beim Landesverband der Ortskrankenkassen verwahrt) sowie aus den Krankenhausrechnungen (soweit über den Pflegesatz hinaus Einzelleistungen abgerechnet wurden). Keines der zusätzlich für das Modellprojekt erfaßten Daten wurde allerdings in die Mitgliederstammdatei übernommen.

Nach dem o.a. Bericht wurden "mit geringen Einschränkungen die Leistungen der medizinischen und zahnmedizinischen Behandlung sowie die Geldleistungen für die Versicherten der Stichprobe in der größtmöglichen Informationstiefe erfaßt, so daß eine nahezu vollständige Abbildung von Behandlungsursachen (Diagnosen) und Behandlungsverläufen (einzelne Leistungen in ihrer zeitlichen Folge) ermöglicht wird".

Die Datenerfassung für das Modellprojekt bezog sich ausschließlich auf das erste und zweite Quartal des Jahres 1981; sie wurde von Winter 1981 bis Mitte 1982 durchgeführt und ist einschließlich der Nacherfassung inzwischen abgeschlossen. Für die Erfassung, d.h. die Eingabe der Daten aus den Krankenscheinen, Rezepten usw. einerseits sowie die Übertragung vorhandener Diagnosen aus dem Stammdatensatz waren ca. 25 Studenten zeitweise eingesetzt, 5 davon Medizinstudenten.

Wenn der Vertragsschluß mit dem von der Bundesregierung vorgesehenen wissenschaftlichen Institut rechtzeitig erfolgt, soll die 2. Phase am 1. Januar 1984 beginnen und bis zum 31. Dezember 1985 abgeschlossen sein. In der 2. Phase sollen die bisher erhobenen und für den Modellversuch gespeicherten Daten nach Übermittlung anonymisierter Datenbänder durch die AOK vom "Institut für Gesundheits- und Sozialforschung (IGES)" in Berlin entsprechend den in der Bekanntmachung des Bundesarbeitsministeriums genannten, aber im einzelnen nicht präzisierten Zielen ausgewertet werden.

3.2.3.3
Zielkonflikt und Reaktionen

Gegen die Zielsetzung der Modellversuche wird niemand etwas einwenden können. Es leuchtet ein, daß es prinzipiell möglich sein muß, die Überweisungspraxis der Ärzte ebenso zu überprüfen wie die Kostensituation in den stationären Behandlungseinrichtungen. Die Finanzierbarkeit der Sozialleistungen stellt für den Sozialstaat - auch und gerade bei abnehmenden Haushaltsressourcen - ein zentrales Politikproblem dar, dessen Bewältigung die genaue Kenntnis der Struktur und Verteilung von erbrachten Leistungen und aufgewendeten Kosten zur Vorbedingung hat.

Doch ist kaum verwunderlich, warum die Modellprojekte so heftige Reaktionen in Presse und Öffentlichkeit, vor allem aber auch bei den Ärzten bzw. ihren Verbänden sowie den Krankenhausträgern hervorgerufen haben. Dies geschah übrigens schon bei einem ebenfalls bundesweit bekannt gewordenen Vorläufer der jetzigen Vorhaben, der breit angelegten wissenschaftlichen Überprüfung von Krankheitsfällen durch die AOK Lindau Mitte der siebziger Jahre.

Die ablehnende Haltung der Ärzte und Krankenhausträger resultiert in erster Linie aus der Besorgnis, die Krankenkassen könnten die Ergebnisse solcher Modellversuche unzulässig verallgemeinern und als Argument für eine Verschärfung ihrer Kontrolle des ambulanten wie stationären Bereichs nutzen. Auch wird immer wieder die Sorge um die Vertraulichkeit der Arzt/Patientenbeziehung angeführt.

3.2.3.4
Risiken

Die Risiken und problematischen Konsequenzen einer so umfassend wie in den Modellversuchen durchgeführten Datenspeicherung und -auswertung für die Patienten bzw. Versicherten sind auf dem Hintergrund der - inzwischen allgemein akzeptierten - Tatsache zu sehen, daß die automatisierte Informationsverarbeitung - was den Umfang, die Verfügbarkeit und Verknüpfbarkeit von Daten angeht -neue Dimensionen von Gefährdungen für den Bürger schafft. Im einzelnen ist auf folgende Gesichtspunkte hinzuweisen:

3.2.3.4.1
"Patientenprofile"

Für die Zwecke des Modellversuchs werden personenbezogene Versichertendaten zusammengeführt, die sonst bei verschiedenen Stellen gespeichert oder nicht patienten-, sondern arzt- bzw. apothekenbezogen aufbewahrt werden. Während also für die gewöhnlichen Aufgaben der AOK lediglich die "Stammdaten" des Versicherten automatisiert gespeichert und über Bildschirm abrufbar sind, kommen jetzt Angaben aus den - sonst in "Papierform" aufbewahrten - nach Ärzten geordneten Krankenscheinen und aus den - sonst beim Landesverband der Ortskrankenkassen liegenden - Rezepten hinzu. Dies ermöglicht "eine nahezu vollständige Abbildung von Behandlungsursachen (Diagnosen) und Behandlungsverläufen (einzelne Leistungen in ihrer zeitlichen Folge)" (s.o). Die versichertenbezogene Speicherung einer solchen Vielzahl von Daten führt - wenn auch im Fall der AOK Hanau für einen eingegrenzten, zurückliegenden Zeitraum - zu einer Art von "Register", mit dem ein sehr sensibler Bereich der Lebensführung des Patienten nahezu lückenlos aufgezeichnet und tendenziell - auch über den Modellversuch hinaus - für alle möglichen Auswertungen verfügbar gemacht wird.

Damit entsteht ein "Patienten- oder Versichertenprofil", welches die Krankenkase für die Erfüllung ihrer Routineaufgaben weder besitzt noch braucht. Je ausführlicher und präziser das "Versichertenprofil" ist, desto vielseitiger wird es verwendbar für eine Vielzahl von "Datenabgleichen" und "Rasterungen". Durch die Einzelangaben über bestimmte ärztliche Verrichtungen, Anwendungen bestimmter medizinischer Geräte, über Medikation u.a. könnten im Vergleich zu den bisher lediglich gespeicherten stichwortartigen Diagnosen sehr präzise Schlüsse über das Versichertenverhalten gezogen werden. Der Computer vermag dann eine Aussortierung nach beliebigen Krankheitsmerkmalen leicht zu liefern.

3.2.3.4.2
Normung des Patientenverhaltens

In einer Reihe von Angaben der Vorhabenbeschreibung für den Modellversuch (IGES-Papier G 163) sowie des Berichts der AOK Hanau finden sich auch Hinweise darauf, daß im Rahmen des Modellversuchs auf den einzelnen Versicherten eingewirkt werden soll: So sollen durch das bei der AOK eingerichtete "Gesundheitszentrum" im Hinblick auf eine Verbesserung ihrer Lebensgewohnheiten z.B. Raucher, Übergewichtige, Personen mit Bewegungsmangel oder ungünstigen Ernährungsgewohnheiten oder Personen mit hohem Blutdruck, Diabetes usw. angesprochen werden (Bericht Seite 11/12). Für Mitglieder dieser Personengruppen sind Einzelberatungen (Bericht S. 14) vorgesehen. Noch deutlicher heißt es zur Durchführung der Prüfung in der Vorhabenbeschreibung: "Die Krankenkasse unterrichtet die Versicherten und die behandelnden medizinischen Einrichtungen über die Ergebnisse der Prüfung" (IGES-Papier S. 10).

Und weiter: Mit der Errechnung eines Durchschnitts aus Erfahrungswerten über Kosten pro Patient und Jahr oder pro Behandlungsfall oder für bestimmte Arten von Erkrankungen wird eine Normung eingeleitet. Jede Entwicklung in diese Richtung läuft jedoch Gefahr, das eigentliche Ziel der Krankenbehandlung aus den Augen zu verlieren, die Hilfe zur Gesundung eines individuell geprägten und nicht normbaren Menschen. Die beim Modellversuch errechneten Durchschnittswerte könnten zu einer "Behandlungsschablone" führen, an der jeder einzelne Versicherte gemessen wird. Das für jeden Einzelfall gewonnene "Versichertenprofil" kann anhand der "Behandlungsschablone" gemessen werden: Wer vom Durchschnitt abweicht - einerlei, ob mit oder ohne sein Verschulden - gerät dann unter Anpassungsdruck. Dies wäre der typische Fall eines Ergebnisses, das nur durch den Einsatz automatischer Datenverarbeitung ermöglicht wird und ausschließlich auf Computerberechnungen beruht, also auf der Wertung von Informationen, die ohne jeden Kontextbezug - also ohne Rücksicht auf die individuelle Situation, in der sie erhoben wurden -gespeichert sind. Das Bundesverfassungsgericht führt dazu in seiner Volkszählungsentscheidung aus: "Individuelle Selbstbestimmung setzt aber - auch unter den Bedingungen moderner Informationsverarbeitungstechnologien - voraus, daß dem Einzelnen Entscheidungsfreiheit über vorzunehmende oder zu unterlassende Handlungen einschließlich der Möglichkeit gegeben ist, sich auch entsprechend dieser Enscheidung tatsächlich zu verhalten."

Und schließlich: Verfügt eine Krankenkasse über derart detailliert gegliedertes Datenmaterial über den Gesundheitszustand des einzelnen, kann dies den "Datenhunger" anderer Sozialleistungsträger wecken. Keinesfalls ist nämlich garantiert, daß die in den Modellversuchen zusammengeführten Daten auch bei den jeweiligen Kassen verbleiben. Im Rahmen des § 69 Abs. 1 Nr. 1 SGB X sind Übermittlungen zulässig, wenn die Daten zur Erfüllung der Aufgaben einer anderen Sozialbehörde erforderlich sind. Im Ergebnis wäre mithin nicht auszuschließen, daß auch andere Krankenkassen, Rehabilitationsträger oder die Versorgungsverwaltung Angaben erhalten, die weit mehr als bisher ins einzelne gehen.

3.2.3.5
Zur Rechtsgrundlage

3.2.3.5.1
§ 223 RVO: Nur Einzelfallprüfung

Für eine so umfassende Speicherung sensitiver Gesundheitsdaten, wie sie in den Modellversuchen durchgeführt wird, reicht der vom Bundesarbeitsministerium und den durchführenden Kassen herangezogene § 223 RVO als Rechtsgrundlage nicht aus. Krankenkassen dürfen nur diejenigen und nur so viele Daten speichern, wie sie zur Erfüllung ihrer Aufgaben benötigen (§ 9 BDSG in Verbindung mit § 79 SGB X). Zwar bereitet die Interpretation des § 223 RVO Schwierigkeiten, nicht zuletzt deshalb, weil sich die sehr knappe Gesetzesbegründung über die genaue Zielsetzung der Einführung dieser Bestimmung - angesichts der sonstigen inder RVO bereits vorgesehenen Prüfungsverfahren zur Feststellung der Wirtschaftlichkeit - ausschweigt. Immerhin spricht der Gesetzeswortlaut nur von "geeigneten Fällen", die vor allem im Hinblick auf die in Anspruch genommenen Leistungen von der Krankenkasse überprüft werden können. Mit dieser Formulierung ist eine "Rasterung" großer Patientenzahlen -im Fall der AOK Hanau ein Drittel der Versicherten und ihrer Angehörigen, insgesamt ca. 60.000 Personen - nicht zu rechtfertigen.

Viel näher liegt die Interpretation, daß diese Bestimmung den Kassen zusätzlich zu dem vorhandenen Kontrollinstrumentarium (durch die Kassenärztlichen Vereinigungen, vgl. § 368n RVO, durch die Prüfungsausschüsse etc.) die Möglichkeit zur Überprüfung von einzelnen Fällen und Fallgruppen geben soll, bei denen Anhaltspunkte dafür bestehen, daß sie Möglichkeiten der Einsparung bzw. Kostenminderung bieten. Anders ausgedrückt: § 223 RVO läßt nicht erkennen, daß mit ihm der gesamte detailliert geregelte Abrechnungsverkehr zwischen Ärzten und Kassenärztlichen Vereinigungen oder umfangreiche Teile davon einer zusätzlichen Kontrolle durch die Kassen unterworfen werden soll.

Bedenkt man, daß die Überprüfung durch die Kassen ja "im Zusammenwirken mit den Kassenärztlichen Vereinigungen und den Krankenhausträgern" erfolgen soll, müssen die Kriterien für die Eignung der Fälle vorher feststehen; die Kassen müssen mit anderen Worten bereits konkrete "Verdachtsmomente" auf unverhältnismäßige Kosten bzw. Leistungen haben, bevor sie die anderen Institutionen zur Zusammenarbeit auffordern können. Dem widerspricht ein Verfahren, nach dem zunächst gleichsam wahllos umfangreiche Datenmengen eingespeichert werden, um sie erst dann - in einer 2. Phase der Modellversuche - nach im vorhinein noch nicht im einzelnen definierten Gesichtspunkten "durchzurastern". Eine solche Handhabung läßt sich vor allem nicht mit den verfassungsrechtlichen Anforderungen, wie sie das Bundesverfassungsgericht in seinem Volkszählungsurteil aufgestellt hat, vereinbaren. Das Gericht verlangt zur Beurteilung der Zulässigkeit von Datenregistrierungen die vorherige Klarheit über die Verknüpfungs- und Verwendungsmöglichkeiten; die Sammlung personenbezogener Angaben auf Vorrat zu noch unbestimmten oder nicht bestimmbaren Zwecken lehnt es ab.

3.2.3.5.2
Notwendigkeit einer speziellen Regelung

Nicht haltbar ist daher auch die Rechtfertigung der Datenerfassung und -verknüpfung im Rahmen der Modellversuche mit dem Argument, alle - auch die zusätzlich gespeicherten -Informationen stünden den Kassen ohnehin zur Verfügung, wenn auch teilweise in Papierform (Krankenscheine usw.), teilweise bei anderen Stellen aufbewahrt (z.B. Landesverbände der Krankenkassen: Rezepte); die Krankenkassen werteten somit zulässigerweise nur ihre "eigenen" Daten aus. Dieses Argument verkennt die bei den Modellversuchen durch die Auswertung unter Wirtschaftlichkeitsaspekten eintretende Zweckänderung der Datenspeicherung. Die Verwendung der Daten ist auf den gesetzlich bestimmten Zweck begrenzt; das sind bei den gesetzlichen Krankenkassen vor allem die in einer Vielzahl von Bestimmungen der RVO zugewiesenen Aufgaben der Mitgliederverwaltung, Leistungsauszahlung usw.

Die für die Modellversuche notwendige zusätzliche rechtliche Grundlage, die den Verwendungszweck der von den Kassen vorgehaltenen Daten auf die Herstellung von "Profilen" einer Vielzahl von Versicherten und Ärzten ausdehnen würde, gibt aber § 223 RVO - wie ausgeführt - gerade nicht ab. Eine präzise gesetzliche Regelung und genaue Festlegung der Verarbeitungsbedingungen für die Durchführung solcher Vorhaben erweist sich aber auch und gerade angesichts der oben aufgezeigten Risiken für die Betroffenen (vgl. Ziff. 3.2.3.4) als unverzichtbar: Die Speicherung und Verknüpfung einer solchen Menge sensitiver medizinischer Angaben mit Hilfe der automatischen Datenverarbeitung bedeutet - was die Intensität des Eingriffs in die Rechtssphäre des Einzelnen angeht - gleichsam einen "Umschlag von der Quantität in die Qualität".

Eine andere Bewertung wäre denkbar, wenn es nicht darum ginge, mit der Auswertung des umfangreichen Datenmaterials konkrete "geeignete Fälle" herauszufinden, bei denen dann ggf. die Kasse den Arzt oder Versicherten informiert, sondern zunächst nur Fallgruppen herausgearbeitet werden sollen, die als Anhaltspunkte für eine spätere Überprüfung von Einzelfällen - dann in Kooperation mit den anderen in § 223 RVO genannten Institutionen - dienen können. Die Modellversuche würden dann nur im "Vorfeld", nicht aber zur Durchführung des § 223 RVO abgewickelt. In diesem Fall aber dürfte es bei den Kassen keinerlei Möglichkeiten geben, die in der wissenschaftlichen Auswertung gefundenen statistischen oder aggregierten Ergebnisse auf einzelne Patienten oder Ärzte hin zu reindividualisieren.

3.2.3.6
Zur Durchführung des Modellversuchs: Irreführende Diagnosebezeichnung

Aus meinen Feststellungen zur Durchführung des Modellversuchs bei der AOK Main-Kinzig erscheint mir ein weiterer Punkt von besonderer Bedeutung, der die Risiken der automatisierten Verarbeitung exemplarisch aufzeigt. Auf die Gefahr, die sich aus einer nur auf Computerberechnungen beruhenden Bewertung gerade von medizinischen Daten ohne Rücksicht auf ihren Entstehungshintergrund, d.h. auf die individuelle Situation des Patienten, ergibt, habe ich bereits hingewiesen (s.o. Ziff. 3.2.3.4 a.E.). Dieses Problem potenziert sich, wenn bei der Datenerfassung nicht sorgfältig genug gearbeitet wird, d.h. im konkreten Fall die Diagnosen nicht korrekt registriert werden.

Wie oben (3.2.3.2) dargestellt, müssen für den Modellversuch die über die Versicherten in der Mitgliederdatei gespeicherten Stammdatensätze um eine Reihe weiterer Angaben ergänzt werden, vor allem durch Diagnosen und Behandlungsverläufe. Die Diagnosen werden nach dem international gebräuchlichen sog. ICD-Schlüssel festgehalten. Ohne medizinische Schulung ist es kaum möglich, die jeweils richtige Diagnosebezeichnung nach dem ICD-Schlüssel aufgrund der im Krankenschein oder in Unterlagen des Krankenhauses enthaltenen Angaben einzusetzen. Bereits im Fall des Vorhabens der AOK Lindau im Jahre 1976 war deshalb heftig kritisiert worden, daß solche Codierungsarbeiten durch Aushilfskräfte und dadurch vielfach fehlerhaft ausgeführt worden waren.

Auch bei der AOK Main-Kinzig waren nur fünf der ca. 25 eingesetzten studentischen Hilfskräfte Medizinstudenten, so daß Zweifel an der Fehlerfreiheit der Datenerfassung auch dann bestehen, wenn man das Bemühen um korrekte und sorgfältige Arbeit unterstellt. Abgesehen davon stellt sich das Problem der Wahrung des Sozialgeheimnisses, wenn ärztliche Informationen einem so großen Personenkreis bekannt werden.

Vor allem aber ergab sich, daß Ausschluß- und Verdachtsdiagnosen ohne Zusatz als bestätigte Befunde festgehalten wurden. Bezeichnungen auf Krankenscheinen usw. wie z.B. "Verdacht auf Leberzirrhose" wurden bei der Codierung mit der ICD-Schlüssel-Ziffer für "Leberzirrhose" versehen. Aus dem Patienten, der aufgrund eines Krebsverdachts mit negativem Resultat untersucht wurde ("Ausschluß von Krebs"), wurde so auf den Datenbändern für die Auswertung "Krebsfall". Diese irreführende Diagnosebezeichnung beruht - wie mir mitgeteilt wurde -bezeichnenderweise darauf, daß der zur Vereinfachung der automatisierten Erfassung und zur besseren Vergleichbarkeit gedachte ICD-Schlüssel derartige Zusätze (Verdacht auf..., Ausschluß von...) gar nicht vorsieht. Für die Bildung von Durchschnittswerten mögen solche Fehler keine allzu große Rolle spielen, wohl aber dann, wenn aus solchen Versichertenprofilen "automatisch" Schlüsse und Konsequenzen für den einzelnen Betroffenen gezogen werden sollen.

3.2.3.7
Konsequenzen

Bei der Formulierung der Zielvorgaben für die Modellversuche der Krankenkassen durch den Bundesminister für Arbeit und Sozialordnung wurden Aspekte des Patientengeheimnisses und des Datenschutzes nicht ausreichend berücksichtigt. Vor allem die Kritik daran, daß eine Rechtsgrundlage für eine so umfassend wie in den Modellprojekten betriebene Verarbeitung von Versicherten-und Ärztedaten zu Zwecken der Wirtschaftlichkeitsprüfung nicht besteht, richtet sich in erster Linie an die Adresse dieses Ressorts, das das "Aktionsprogramm" unter Berufung auf diese Bestimmung initiiert hat.

Ohne eine gesetzliche Regelung, die den Verarbeitungszweck und die Verarbeitungsbedingungen für die Herstellung von Versicherten- und Arzt-"Profilen" genau angibt, können derartige "Modellversuche" allenfalls zur Vorbereitung von anonymisiertem Datenmaterial dienen, das dann zu allgemeinen, nicht auf einzelne Patienten bezogenen Maßnahmen zur Kostendämpfung ausgewertet werden kann. Es versteht sich von selbst, daß das Sozialgeheimnis nur gewahrt ist, wenn die patienten- und arztbezogenen Angaben an die Stelle oder Einrichtung, die die wissenschaftliche Auswertung vornimmt, ausschließlich in anonymisierter Form übermittelt werden (§§ 75, 76 SGB X). Bei der Erfassung ist darauf zu achten, daß Daten nicht deshalb irreführend oder gar falsch registriert werden, weil mit computergerechten, aber verkürzten Schlüsselziffern gearbeitet wird. Auch ist eine annähernde Fehlerfreiheit nur dann zu gewährleisten, wenn die Erfassung bzw. Codierung ausschließlich von mit der medizinischen Terminologie vertrauten Fachkräften durchgeführt wird.

Meine Beurteilung und die daraus im einzelnen zu ziehenden Folgerungen habe ich nicht nur der betroffenen AOK Hanau, sondern auch dem Hessischen Sozialminister als oberster Aufsichtsbehörde für die gesetzlichen Krankenkassen mitgeteilt. Über die Reaktionen der beteiligten Instanzen hinaus sollten die "Modellversuche zur Leistungs- und Kostentransparenz" eine breit geführte Diskussion anregen über das - in den nächsten Jahren sicher noch an Bedeutung gewinnende - Thema der Funktion des Sozial- und Patientengeheimnisses vor dem Hintergrund der Notwendigkeit, für die Entscheidungen von Politik und Verwaltung detaillierte Datengrundlagen zur Verfügung zu stellen.

3.2.4
Patientengeheimnis in der Psychiatrie
Datenerhebung nach § 184 RVO

3.2.4.1
Krankheit oder Pflegefall: Abgrenzung der Kostentragung

§ 184 der Reichsversicherungsordnung (RVO) bestimmt, unter welchen Voraussetzungen in der gesetzlichen Krankenversicherung "Krankenhauspflege" gewährt wird. In Verbindung mit dem Bundessozialhilfegesetz (BSHG) und den dazu erlassenen landesrechtlichen Voschriften ergibt sich, daß verschiedene Leistungsträger die Kosten für stationären Aufenthalt zu tragen haben, je nachdem, ob es sich noch um die medizinische "Behandlung" einer Krankheit des Patienten oder aber um die - bei dauerndem Siechtum notwendige - "Pflege" handelt. Diese Vorschrift hat schon zu einer Vielzahl von Sozialgerichtsprozessen und einer Reihe von Entscheidungen des Bundessozialgerichts geführt. Ihr Verständnis wird dadurch nicht gerade erleichtert, daß der darin verwendete Terminus "Krankenhauspflege" eben nicht die Pflege bei Siechtum meint, sondern die Erkennung oder Behandlung einer Krankheit oder die Linderung von Krankheitsbeschwerden. Für die letztgenannten drei Zwecke, kurz "Behandlung" genannt, sind Kostenträger die gesetzlichen Krankenkassen, überwiegend also die Allgemeinen Ortskrankenkassen. Für die Kosten der "Pflege" solcher Patienten, deren Krankheit nicht mehr behandelt oder gelindert werden kann, die aber auf Dauer hilfsbedürftig bleiben und keine eigenen Mittel haben, hat in Hessen der Landeswohlfahrtsverband (LWV) als überörtlicher Träger der Sozialhilfe aufzukommen.

Im Hinblick auf die allgemein knappen Haushaltsmittel muß es daher das Bestreben der gesetzlichen Krankenkassen und ihrer Verbände sein, die Schwelle für die Annahme eines sogenannten "Pflegefalles" besonders niedrig anzusetzen, das Bestreben des LWV andererseits, diese besonders hoch festzulegen: Ist das Leiden des Patienten durch Behandlung noch zu verbessern oder zu lindern, tragen die gesetzlichen Krankenkassen die Kosten, steht aber fest, daß dies nicht mehr möglich ist, muß der LWV die Kosten übernehmen. Zu diesem Interessengegensatz zwischen gesetzlichen Krankenkassen und Landeswohlfahrtsverband kommt eine weitere Schwierigkeit hinzu: Der LWV ist Träger der meisten psychiatrischen Krankenhäuser in Hessen. Handelt es sich also um Kosten für Psychiatrie-Patienten, so besteht hier ein qualifizierter Interessenkonflikt zwischen LWV und Krankenkassen: Bei den Kassen könnte der Verdacht entstehen, daß der LWV als Träger der psychiatrischen Krankenhäuser daran interessiert ist, möglichst viele "Behandlungs-" und möglichst wenige "Pflege-"Fälle zu haben, damit er nicht selbst auf den Kosten "sitzenbleibt".

3.2.4.2
Datenerhebung zur Feststellung des Kostenträgers
Konflikt mit dem Patientengeheimnis

Diese durch die Reichsversicherungsordnung und das Bundessozialhilfegesetz (BSHG) sowie das Hessische Ausführungsgesetz zum Bundessozialhilfegesetz (HAG/BSHG) vorgegebene Situation droht sich unter dem Druck fehlender öffentlicher Mittel nachteilig auf die Einhaltung des Patientengeheimnisses und damit des Datenschutzes in der Psychiatrie auszuwirken. Anlaß dafür sind die zwischen den Landesverbänden der gesetzlichen Krankenkassen und dem Landeswohlfahrtsverband ausgehandelten Formulare zur Erhebung von Daten bei Psychiatrie-Patienten und die Praxis ihrer Verwendung. Diese Vordrucke verlangen die Erhebung von dermaßen vielen Daten für die Entscheidung nach § 184 RVO, daß sie in der Ärzteschaft zu Bedenken wegen der Einhaltung der ärztlichen Schweigepflicht und bei einer Anzahl jüngerer Ärzte sogar zu einer Verweigerung der Ausfüllung geführt haben.

3.2.4.2.1
Die frühere Praxis: Einschränkung der Datenübermittlung aufgrund vertraglicher Pauschalvereinbarung

In der Vergangenheit konnten solche Konfliktfälle zwischen den gesetzlichen Krankenkassen und dem LWV auf wenige Einzelfälle beschränkt werden. Aufgrund einer vertraglichen Vereinbarung zwischen dem LWV und den Verbänden der gesetzlichen Krankenkassen ("Vereinbarung über die Kostenträgerschaft bei stationärer Behandlung in psychiatrischen Krankenhäusern des Landeswohlfahrtsverbandes Hessen i.d.F.v. 27. Juli 1981 - "Vereinbarung '81") wurde eine Teilung der Krankenhauskosten für Psychiatrie-Patienten zunächst für ein Jahr festgelegt, nach welcher "unabhängig davon, ob es sich um einen Behandlungs- oder Pflegefall handelt, 90 v.H. der Krankenhauspflegekosten und der aus medizinischen Gründen notwendigen Transportkosten" die Krankenkasse übernahm, die restlichen 10 v.H. der LWV trug. (§ 6 Abs. 1 der Vereinbarung). Dann erst wurde geprüft, ob es sich um einen "Pflegefall" handelte. Infolge der Entlassung vor Ablauf eines Jahres stellte sich jedoch in vielen Fällen diese Frage nicht mehr. Für die Entscheidung über die verbleibenden Einzelfälle wurde ein zwischen den Vertragspartnern vereinbartes Formular ("Ärztliche Stellungnahme zur Krankenhauspflegebedürftigkeit") vorgesehen, das als Anlage 2 der Vereinbarung '81 beigefügt war. Dabei diente ein Musterformular des Bundesverbandes der Ortskrankenkassen als Richtschnur, das allerdings - vor allem durch Fragen zu Einzelheiten der Medikation - erheblich erweitert wurde.

Der Vorläufer dieses Vordrucks mit ähnlicher Zweckbestimmung, der zum Teil auch nach Abschluß der Vereinbarung '81 noch weiterhin Verwendung fand, sah nur die Erhebung eines Mindestmaßes an für die Entscheidung über § 184 RVO notwendigen Angaben vor: Außer den Angaben über Name, Vorname, Geburtsdatum und Krankenhaus-Aufnahmenummer des Patienten war die Diagnosenummer nach dem ICD-Schlüssel einzutragen, war unter fünf Begründungen für die Notwendigkeit der stationären Krankenhausbehandlung eine anzukreuzen, außerdem die voraussichtliche Dauer des Krankenhausaufenthalts anzugeben sowie unter sechs möglichen Therapieformen eine anzukreuzen.

3.2.4.2.2
Das neue Formular zur "Krankenhauspflegebedürftigkeit"

Unter dem Druck der angespannten Haushaltslage der Sozialleistungsträger wurde die Vereinbarung '81 zum 31. Dezember 1982 gekündigt und lief nach einer Verlängerung Mitte 1983 endgültig aus. Damit erhielt das bereits der Vereinbarung '81 beigefügte, aber bislang nur in Einzelfällen benutzte "neue" Formular der "Ärztlichen Stellungnahme zur Krankenhauspflegebedürftigkeit" eine hervorragende Bedeutung:

Es wurde jetzt ohne Rücksicht auf den Ablauf der Jahresfrist auf jeden Patienten anwendbar. Die jetzigen Formulare haben den doppelten Umfang der alten, nämlich zwei DIN-A4-Seiten. Sie sehen eine außerordentlich detaillierte Erhebung von Patientendaten vor, angefangen von Angaben über frühere stationäre Aufenthalte in psychiatrischen Krankenhäusern, über die ausgeschriebene Diagnose einschließlich Symptomen und Beschwerden sowie den bisherigen Krankheitsverlauf bis hin zu den Therapiemaßnahmen. Dazu werden insbesondere Einzelheiten der medikamentösen Therapie erfragt, nicht nur aufgeschlüsselt nach Kategorien ("Antidepressiva", "Neuroleptika", "andere Psychopharmaka"), sondern auch darüber, wie oft und mit welchen namentlich bezeichneten Medikamenten therapiert worden ist. Weitere Einzelheiten lassen sich aus dem im Anschluß an diesen Abschnitt wiedergegebenen Vordruck erkennen.

Das Motiv dieses erweiterten Informationsinteresses ist angesichts der beschriebenen Konfliktsituation zwischen den Trägern der gesetzlichen Krankenversicherung und dem Landeswohlfahrtsverband klar: Das Bestreben der Krankenkassen ist es, in jedem Einzelfall des stationären Aufenthalts in einer psychiatrischen Klinik möglichst viele Daten zu erhalten. Denn: Je mehr Informationen über den Einzelfall zur Verfügung stehen, desto größer ist die Chance, daraus Anhaltspunkte für das Vorliegen eines "Pflegefalles" (oder teilstationärer Behandlungsmöglichkeit im Sinne von § 184 Abs.1 RVO) zu gewinnen und die Übernahme der Kosten damit ablehnen zu können. Unter dem Aspekt einer sparsamen Wirtschaftsführung, zu der sowohl der Landeswohlfahrtsverband als auch die gesetzlichen Krankenkassen verpflichtet sind, läßt sich ein solches Bestreben nicht einmal kritisieren. Doch darf diese Auseinandersetzung nicht zu Lasten des Patientengeheimnisses geführt werden.

3.2.4.2.3
Keine Festlegung des Datenumfangs durch § 184 RVO

Welche Angaben zur Entscheidung über die Frage, ob es sich um einen "Behandlungsfall" oder einen "Pflegefall" handelt, erforderlich sind, läßt sich aus der Vorschrift des § 184 RVO nicht unmittelbar entnehmen. Er verlangt lediglich als Voraussetzung für einen "Behandlungsfall", daß die "Aufnahme in ein Krankenhaus erforderlich ist, um die Krankheit zu erkennen oder zu behandeln oder Krankheitsbeschwerden zu lindern". Das Bundessozialgericht hat die dabei bestehenden Unklarheiten der Abgrenzung in mehreren Entscheidungen dahingehend präzisiert, daß eine notwendige Krankenhausbehandlung nicht nur das Ziel der Heilung oder Besserung der Krankheit haben kann, sondern auch, eine Verschlimmerung der Krankheit zu verhindern, das Leben zu verlängern oder die Krankheitsbeschwerden zu lindern (vgl. z.B. die Urteile des Bundessozialgerichts vom 10. Oktober 1978, 3 RK 81/77 und vom 25. Januar 1979, 3 RK 83/78). Aus den Abgrenzungsmerkmalen des § 184 RVO und der obergerichtlichen Rechtsprechung dazu lassen sich zwar Schlüsse ziehen, welche Daten aus der Krankenakte des Patienten für die Entscheidung über die Frage "Behandlungsfall" oder "Pflegefall" ggf. relevant sein könnten. Doch ist die Schlußfolgerung - die mir entgegengehalten wurde - unzutreffend, die Kassen dürften ohne weitere Anhaltspunkte über jeden Patienten im Prinzip alle in der ausführlichen Rechtsprechung der Sozialgerichte zur Definition verwandten Kriterien beim Arzt abfragen, obwohl im Einzelfall die Abgrenzung aufgrund von weniger Angaben erfolgen kann.

Meine Bedenken richten sich vor allem gegen die Ausführlichkeit der Nachfrage über die Therapiemaßnahmen und die Medikation. Zwar soll nicht verkannt werden, daß es in bestimmten Einzelfällen, wenn entsprechende Hinweise vorliegen, durchaus angezeigt sein kann, mit detaillierten Fragen nach der Medikation des Patienten die Feststellung zu ermöglichen, daß dieser beispielsweise nur noch Beruhigungsmittel erhält, also ein Pflegefall sein muß. Andererseits ist zu beachten, daß gerade durch detaillierte Angaben über die verordneten Arzneien sehr weitgehende Schlüsse über das mögliche Krankheitsbild des Patienten gezogen werden können. Deshalb geht es nicht an, daß gleichsam vorsorglich generell bei allen Patienten ein maximaler Datensatz erhoben wird. Daß man auch mit weniger Informationen auskommen kann, beweist nicht zuletzt die Tatsache, daß andere Krankenkassen knapper gefaßte Vordrucke verwenden.

Die speziellen Risiken der Erhebung gerade der extrem sensitiven psychiatrischen Daten werden besonders anschaulich, wenn man sich vorstellt, die gesamten nach dem neuen Fragebogen erfaßten Angaben würden auch in den Computern der Krankenkassen gespeichert und dann nicht im Interesse der Behandlung - wie etwa bei der geplanten automatisierten Verarbeitung der sog. "Basisdokumentation Psychiatrie" in den Krankenhäusern -, sondern unter Spar- und Kostengesichtspunkten ausgewertet. Außerdem ist immer zu bedenken, daß bei einem Leistungsträger registrierte Informationen zur Erfüllung seiner Aufgaben oder der einer anderen Sozialbehörde auch weitergegeben werden können (vgl. dazu im einzelnen auch Ziff. 3.2.3.4 über die Risiken der Datenspeicherung und -auswertung bei den Modellversuchen zur Kostentransparenz). Dies ist ein zusätzliches Argument für meine Position, die Erforderlichkeit der Erhebung von Daten in dem hier in Rede stehenden Bereich nach besonders strengen Kriterien zu beurteilen.

3.2.4.3
Reaktionen und Lösungsansätze

Ich habe dem Landeswohlfahrtsverband und den Verbänden der gesetzlichen Krankenversicherungen meine Bedenken wegen der Verwendung des Fragebogens erläutert und ihnen Gelegenheit zur Stellungnahme gegeben. Dabei habe ich dem LWV vorgeschlagen, die ursprünglichen Formulare mit dem kleineren Datensatz weiterhin so lange zu verwenden, bis eine Klärung der Rechtslage erfolgt sei. Er hat dies abgelehnt unter Hinweis darauf, daß nach den bisherigen Erfahrungen die Krankenkassen nicht bereit seien, ohne die mit dem "neuen" Formular erhobenen Angaben die Übernahme der Kosten zuzusichern. Bei einer Verweigerung der Verwendung dieses Vordrucks lasse sich bereits jetzt absehen, daß dies den LWV in ganz erhebliche finanzielle Schwierigkeiten bringen würde, die "letztlich zu einem Zusammenbruch der Versorgung führen könnten". Aus den Anwortschreiben der Verbände der gesetzlichen Krankenkassen ergab sich einheitlich die Auffassung, die bisherige Praxis, insbesondere die Benutzung des "neuen" Fragebogens, seien durch die bestehende Rechtslage gedeckt. Eine Änderung der Handhabung wurde als indiskutabel angesehen.

Auch und gerade angesichts dieser Reaktionen, die eine ausreichende und zufriedenstellende Begründung für den Umfang der Datenerhebung vermissen lassen, muß ich dagegen die derzeitige Praxis beanstanden. Der unbefriedigende Zustand sollte Anlaß -nicht nur für den Gesetzgeber - sein zu prüfen, ob die durch § 184 RVO bewirkte Abgrenzung zwischen "Behandlungsfall" und "Pflegefall" mit der Folge verschiedener Kostenträger im Hinblick auf den dadurch verursachten bürokratischen Aufwand und die Gefahren für den Schutz des Persönlichkeitsrechts in Zukunft durch eine bessere Regelung ersetzt werden könnte. Dabei war die Lösung der "Vereinbarung '81" (s.o. 3.2.4.2.1) insoweit ein durchaus akzeptabler Ansatz, als sie eine bestimmte Zeitdauer (1 Jahr) des Krankenhausaufenthaltes zur Grundlage einer Kostenteilung machte. Geht man davon aus, daß es bei der Einlieferung eines Patienten in das psychiatrische Krankenhaus -also in der "ersten Phase" seines Krankenhausaufenthalts - in aller Regel um die Erkennung, Behandlung oder Linderung einer Krankheit (§ 184 Abs. 1 RVO) geht, so kann erst zu einem späteren Zeitpunkt die Frage akut werden, ob es sich inzwischen um einen "Pflegefall" handelt. Das bedeutet, daß erst dann, wenn die "normale" Zeitdauer einer stationären Behandlung im psychiatrischen Krankenhaus für ein bestimmtes Symptombild überschritten ist, überhaupt Anlaß für die Überlegung besteht, ob eine Änderung in der Kostenträgerschaft in Frage kommt. Daraus folgt nicht nur die Unzulässigkeit einer entsprechenden Datenerhebung in allen Fällen und von Anfang an, sondern die realistische Möglichkeit, den Zeitfaktor im Rahmen einer Überprüfungsregelung zum hauptsächlichen Kriterium zu machen.

Ergänzt werden könnte eine solche "Fristen"-Regelung durch ein Verfahren der Datenerhebung, das einen Eingriff in das Patientengeheimnis weitestgehend vermeidet: Dem behandelnden Arzt könnte von der gesetzlichen Krankenkasse ein - ggf. mit dem Krankenhausträger abgestimmter - "Kriterienkatalog" an die Hand gegeben werden, aus dem er selbst erkennen kann, welcher Zusammenhang zwischen seinen Maßnahmen für den Patienten und dem daraus folgenden Ergebnis für die Einstufung als "Behandlungs"-oder "Pflegefall" besteht. Bei Erfüllung bestimmter Merkmale nach Maßgabe dieses Katalogs (z.B. dauernde Bettlägerigkeit, ausschließliche Einnahme bestimmter Arzneien, später Entlassungstermin o.ä.) hätte der Arzt selbst die Kategorie "Pflegefall" anzukreuzen. Mit einer solchen oder ähnlichen Verfahrensweise erhielte die Kasse die für ihre Entscheidung nach § 184 RVO notwendigen Angaben jedenfalls im Regelfall ohne die Übermittlung einzelner Patientendaten.

Ärztliche Stellungnahme

ZUR KRANKENHAUSPFLEGEBEDÜRFTIGKEIT

Name, Vorname des Patienten

Geburtsdatum

1. Stationärer Aufenthalt nach dem 1.4.1981 in Psychiatrischen Krankenhäusern des LWV Hessen

vom	bis	Krankenhaus
		strafrechtlich untergebracht im Krankenhaus

2. Diagnose / Befund

2.1 Diagnose / Befund (einschl. Symptome, Beschwerden):

2.2 Bisheriger Krankheitsverlauf:

3. Therapieziele

Der Patient bedarf bis auf weiteres einer regelmäßigen, ärztlich geleiteten Behandlung mit dem Ziel,

- ☐ die Krankheit zu erkennen
- ☐ die Krankheit zu heilen
- ☐ die Krankheit zu bessern
- ☐ eine drohende Verschlimmerung zu verhindern
- ☐ Krankheitsbeschwerden zu lindern
- ☐ das Leben zu verlängern

4. Therapiemaßnahmen

☐ Medikamentöse Therapie, und zwar durch

	wie oft	Name des Medikaments
☐ Antidepressiva		
☐ Neuroleptika		
☐ Antiepileptika		
☐ andere Psychopharmaka		
☐ sonstige medikamentöse Therapie (z.B. für Organleiden)		

		wie oft		wie oft
☐ Psychotherapie	☐ Einzelmaßnahme		☐ Gruppenmaßnahme	
☐ Verhaltenstherapie, Psychagogik	☐ Einzelmaßnahme		☐ Gruppenmaßnahme	
☐ Physikalische Therapie	☐ Bäder		☐ Massagen	
	☐ Krankengymnastik			
☐ Beschäftigungstherapie	☐ Arbeitstherapie		☐ Belastungserprobung	

LWV 01 - 7 - 526 (1.82 - mü)

Sonstige therapeutische Maßnahmen (welche):

Ärztliche Betreuung (Art und Umfang):

Pflegerische Maßnahmen

- ☐ Fachpsychiatrische Behandlungspflege
- ☐ Grundpflege (Hilfe beim Essen, Waschen, Betten usw.)

5. Erforderlichkeit der stationären Behandlung *)

- ☐ ambulante ärztliche Maßnahmen und die Gewährung von Grundpflege sind nicht ausreichend
- ☐ der Zustand des Patienten würde sich bei einer Entlassung in häusliche Betreuung oder bei einer Verlegung in ein Alten- oder Pflegeheim, eine Nachsorge- oder Verwahreinrichtung in medizinischer Hinsicht verschlechtern

6. Beurteilung der Therapieaussichten

Der Patient kann voraussichtlich in ..... Wochen / Monaten, ggf. in Verbindung mit ambulanter Behandlung

- ☐ nach Hause
- ☐ in ein Alten- oder Pflegeheim
- ☐ in eine Nachsorgeeinrichtung oder Verwahreinrichtung entlassen werden
- ☐ Entlassung nicht absehbar

Datum: .....

Unterschrift des Arztes: .....

***) Kriterien zum Pflegefall**

Ein Pflegefall liegt vor, wenn

a) es sich um ein Dauerleiden handelt und keines der Behandlungsziele des § 184 RVO (s. Ziff. 3) bei Anwendung von zielgerichteten ärztlichen Therapiemaßnahmen (i. S. von Ziff. 4) erreichen läßt oder

b) die Behandlung zu Hause oder in einem Alten- oder Pflegeheim oder in einer Nachsorge- oder Verwahreinrichtung in ausreichendem Maße ambulant durchgeführt werden könnte.

Es kann nicht zu Lasten der Krankenkasse gehen, wenn ein Patient aus sozialen Gründen (häusliche Verhältnisse) oder wegen Fehlens geeigneter Pflege-, Nachsorge- oder Verwahreinrichtungen nicht entlassen werden kann oder allein aus Gründen der Selbst- oder Fremdgefährdung nach dem HFEG untergebracht wird oder im Krankenhaus verbleiben muß.

- 49 -

AN 14 23

3.2.5
Änderung des Kindergeldrechts

3.2.5.1
Die Novellierung des Bundeskindergeldgesetzes (BKGG)

Ein weiteres Beispiel dafür, daß Spargesetze dazu führen, daß der Bürger in erheblichem Umfang zur erweiterten Offenlegung seiner persönlichen Verhältnisse gezwungen wird, liefert die Änderung des Bundeskindergeldgesetzes (BKGG) durch Art. 13 des Haushaltsbegleitgesetzes 1983 vom 20.12.1982 (BGBl. I S. 1857 ff.). Mit dieser Novellierung wurde die Höhe des Kindergeldes - das vorher einheitlich gewährt wurde - vom Einkommen der Eltern abhängig gemacht.

Zahlreiche bei mir eingegangene Beschwerden haben deutlich gemacht, daß diese Novellierung ein besonders krasses Beispiel für die Entwicklung gerade im Bereich der Sozialleistungen ist: Der Gesetzgeber verabschiedet unter Zeitdruck Regelungen, ohne die dadurch bewirkten Datenströme und deren datenschutzrechtliche Probleme zu berücksichtigen. Die Datenschutzbeauftragten des Bundes und der Länder waren in das Gesetzgebungsverfahren zur Novellierung des Bundeskindergeldgesetzes nicht eingeschaltet, um schon zu diesem Zeitpunkt ihre Anregungen und Vorschläge einzubringen und damit Besorgnisse in der Bevölkerung von vornherein nicht entstehen zu lassen.

3.2.5.2
Antragsverfahren für 1983: Datenkontrolle beim Finanzamt

Im Antragsverfahren für 1983 betraf die Kritik der Bürger, die sich an mich gewandt haben, vor allem zwei Punkte: Zum einen, daß sie Einzelheiten über Herkunft, Zusammensetzung und Höhe ihrer Einkünfte, die sie in aller Regel nur dem Finanzamt unter dem Schutz des Steuergeheimnisses mitteilen, jetzt auch gegenüber den Kindergeldstellen (Kindergeldkassen bei den Arbeitsämtern, Festsetzungsstellen im öffentlichen Dienst) offenlegen sollten. Besonders betroffen haben viele Antragsteller jedoch darauf reagiert, daß sie ihre Steuernummer sowie ihr zuständiges Finanzamt angeben sollten. Dies wurde in dem Anschreiben damit begründet, es sei beabsichtigt, die angegebenen Einkommensverhältnisse mit Hilfe des Finanzamts zu überprüfen. Viele Bürger haben diese für den gesamten Sozialleistungsbereich einmalige Ankündigung, ohne weitere Voraussetzungen auf ihre Steuerdaten zurückzugreifen, als allgemeines und ungerechtfertigtes Mißtrauen in ihre Ehrlichkeit und Korrektheit empfunden. Manche äußerten auch die Befürchtung, es könne einen laufenden automatisierten Datenabgleich zwischen Kindergeldstellen und Finanzämtern geben; dadurch werde das Steuergeheimnis ausgehöhlt.

Ich habe mich sofort an die zuständigen Ressorts gewandt und deutlich gemacht, daß eine ausnahmslose Überprüfung der angegebenen Einkommensverhältnisse durch Vorlage des Einkommenssteuerbescheides oder durch automatisierten bzw. listenmäßigen Datenabgleich mit den Finanzämtern unverhältnismäßig und damit unzulässig ist. Eine Rückfrage beim Finanzamt läßt das Gesetz (§ 21 Abs.4 SGB X) nur in Einzelfällen oder bei Fallgruppen zu, bei denen Anhaltspunkte auf Mißbrauch vorliegen oder Unstimmigkeiten nicht durch Nachfrage beim Antragsteller geklärt werden können. Deshalb habe ich auch die Erhebung der Steuernummer und des zuständigen Finanzamtes auf dem Vordruck, also bei allen Kindergeldberechtigten, kritisiert. Diese Angaben konnten in den genannten Zweifelsfällen nachträglich bei den Antragstellern beschafft werden. Ein allgemeines Mißtrauen gegen den Bürger darf nicht zu umfangreichem Datenaustausch zu Kontrollzwecken führen und das Steuergeheimnis mehr als notwendig durchlöchern. Diese Position haben die Datenschutzbeauftragten im übrigen in einem gemeinsamen Beschluß vom September 1983 bekräftigt.

Der Hessische Finanzminister hat mir daraufhin versichert, in Hessen werde es keinen automatisierten Datenabgleich zwischen Kindergeldstellen und Finanzämtern geben. Er hat eingeräumt, daß datenschutzrechtliche Gründe und die Wahrung des Steuergeheimnisses einer solchen Absicht entgegenstünden (s. aber unten 3.2.5.4). Einen direkten Zugriff von Kindergeldstellen auf die Datenbestände der Steuerbehörden - wie gelegentlich vermutet wird - gibt es ohnehin nicht.

3.2.5.3.
Antragsverfahren für 1984: Vorlage des Steuerbescheides ("Kopierlösung")

Bei den Anträgen für das Kindergeld 1984 ist für den Einkommensnachweis eine geänderte Regelung getroffen worden, die aber nach wie vor datenschutzrechtliche Probleme aufwirft.

Zwar werden Steuernummer und Finanzamt auf den Formularen nicht mehr erfragt, auch brauchen die Kindergeldberechtigten ihre verschiedenen Einkünfte nicht mehr selbst auszufüllen. Allerdings werden die Antragsteller aufgefordert, ihren Einkommenssteuerbescheid vorzulegen. Immerhin hat die gemeinsame Kritik der Datenschutzbeauftragten dazu geführt, daß sich die Kindergeldstellen mit der Vorlage einer Fotokopie des Steuerbescheides, auf der die für die Berechnung nicht benötigten Daten unkenntlich gemacht sind, begnügen. Auf diese Möglichkeit der Schwärzung wird in den Anschreiben zu den Kindergeldformularen ausdrücklich hingewiesen, wenn auch nicht - wie ich es im Interesse der Klarheit der Information für erforderlich halte - noch einmal auf den

Vordrucken selbst. Diese Einschränkung zeigt, daß die Vorlage des gesamten Einkommenssteuerbescheides mit allen Angaben schon deshalb nicht verlangt werden kann, weil er selbst aus der Sicht der Behörden wesentlich mehr Daten enthält, als zur Antragsbearbeitung gebraucht werden.

Diese "Kopierlösung" ist zwar ein Schritt in die richtige Richtung einer Begrenzung der beim Bürger erfragten Daten; sie macht Rückfragen bei den Steuerbehörden und gar Datenabgleiche überflüssig (s. aber unten). Dennoch bleibt ebenso wie beim Antragsverfahren für 1983 das Problem, daß den Kindergeldstellen die für die Berechnung maßgebliche "Summe der positiven Einkünfte" nicht in einem Betrag mitgeteilt werden kann, sondern in einzelne Einkunftsarten aufgeschlüsselt werden muß, die ansonsten nur im Steuerverfahren dem Finanzamt offengelegt werden. Die Schwierigkeit besteht hier darin, daß die Einkommensbegriffe von Kindergeld- und Steuerrecht nicht harmonisiert sind, so daß viele Bürger überfordert wären, wenn sie die "Summe der positiven Einkünfte" aus ihren Steuererklärungen selbst errechnen müßten.

Die Datenschutzbeauftragten haben daher ein Verfahren vorgeschlagen, bei dem die Steuerbehörden diese Summe in einer gesonderten Bescheinigung zusätzlich zum Steuerbescheid ausweisen und dem Bürger zugleich mit dem Steuerbescheid zusenden. Damit wäre das Problem endgültig gelöst, daß einer Sozialbehörde detaillierte Steuerdaten zur Kenntnis gelangen. Der Hessische Innenminister unterstützt diesen Vorschlag ebenso wie die Arbeitsgruppe der Besoldungsreferenten der Bundesländer. Motiv für die Befürwortung dieser Lösung ist dabei nicht in erster Linie der Datenschutz, sondern vor allem die erhoffte Verwaltungsvereinfachung angesichts des inzwischen fast unübersehbar gewordenen Regelungsgestrüpps im Kindergeldrecht.

Der Hessische Finanzminister hat mir gegenüber zwar den Ausdruck spezieller Kindergeld-Bescheinigungen mit der Begründung abgelehnt, die Finanzverwaltung könne die Summe der positiven Einkünfte im Sinne des BKGG wegen des steuerrechtlich anderen Berechnungsmodus des Einkommens nicht angeben. Doch bin ich noch nicht davon überzeugt, daß nicht mit einer entsprechenden Programmänderung bzw. -ergänzung des automatisierten Besteuerungsverfahrens diese Möglichkeit geschaffen werden kann. Auch steht die offizielle Antwort der Steuerverwaltungen der Länder an die für Kindergeldfragen zuständigen Ressorts - in Hessen der Innenminister - zur Realisierbarkeit dieser Lösung noch aus.

3.2.5.4
Geplanter Datenabgleich Arbeitsämter/Steuerverwaltung

Inzwischen hat sich herausgestellt, daß die Bundesanstalt für Arbeit, die für die den Arbeitsämtern angegliederten Kindergeldkassen zuständig ist, an der ursprünglichen Idee eines Datenabgleichs für ihren Zuständigkeitsbereich -also für Kindergeldberechtigte außerhalb des öffentlichen Dienstes - festhält. Um Bedenken wegen des Steuergeheimnisses auszuräumen, sollen in den regelmäßigen Datenaustausch mit den Finanzverwaltungen nur diejenigen Antragsteller einbezogen werden, die die im Vordruck enthaltene Frage bejahen, daß sie mit der Einholung der Angaben bei ihrem Finanzamt einverstanden sind. Diese Bürger brauchen dann künftig nicht mehr ihre Steuerbescheide - bzw. die gegebenenfalls teilweise geschwärzte Kopie - vorzulegen. Bei den anderen soll es beim bisherigen Verfahren bleiben. Selbst wenn man die Einverständniserklärung im Kindergeldformular für eine wirksame Befreiung vom Steuergeheimnis halten sollte, habe ich dennoch Bedenken dagegen, den Bürger mit der Verlockung, das Verfahren werde für ihn künftig einfacher, dazu zu verleiten, in einen für ihn nicht transparenten Austausch automatisiert verarbeiter Daten zwischen Behörden einzuwilligen. Dies gilt insbesondere deshalb, weil es sich um den Präzedenzfall handelt, daß erstmalig die Datenbestände der Steuerverwaltung in Hunderttausenden von Fällen für eine andere Behörde geöffnet werden sollen.

Ich habe mich in die Vorbereitungen zu diesem geplanten, wenn auch noch nicht endgültig entschiedenen Projekt eingeschaltet und werde die datenschutzrechtliche Zulässigkeit, insbesondere die zur Übermittlung vorgesehenen Datensätze sowie die Maßnahmen der Datensicherung, sorgfältig prüfen.

3.2.5.5.
Sondersituation im öffentlichen Dienst

Für Angehörige des öffentlichen Dienstes ergibt sich die Sondersituation, daß die Kindergeldanträge nicht wie bei allen anderen Empfängern von einer speziellen Sozialbehörde - den Kindergeldkassen bei den Arbeitsämtern -bearbeitet werden, sondern nach § 45 BKGG von ihrem eigenen Dienstherrn. Die Datenschutzproblematik verschärft sich insofern, als die detaillierten Angaben über das Einkommen des Bediensteten und seines Ehegatten den "für die Festsetzung der Bezüge oder des Arbeitsentgelts zuständigen Stellen", d.h. der eigenen Behörde bzw. Dienststelle zur Kenntnis gelangen. In einer Reihe von Eingaben wurde daher die Befürchtung geäußert, daß die normalerweise nur im Zusammenhang mit der Besteuerung dem Finanzamt gegebenen Informationen nicht nur der Berechnung des Kindergeldes dienen, sondern auch für Personalentscheidungen verwandt werden könnten. Auch hierin liegt eine Konsequenz der Novellierung des Kindergeldrechts, die ganz sicher vom Gesetzgeber bzw. der die Rechtsänderung vorbereitenden Ministerialverwaltung nicht erkannt worden ist. Ein Parallelproblem stellt sich übrigens bei der Beihilfe, wo der Dienstherr für die Angehörigen des öffentlichen Dienstes gleichsam die Funktionen von Arbeitgeber und Krankenkasse vereinigt (vgl. dazu oben Ziff. 2.1.6.2).

Die Datenschutzbeauftragten haben in ihrem Beschluß vom September 1983 zu dieser Frage eindeutig klargestellt, daß die für die Kindergeldbearbeitung erhobenen Daten einer strengen Zweckbindung unterliegen. Diese verbietet es demjenigen, der im Bereich des öffentlichen Dienstes mit der Bearbeitung von Kindergeldangelegenheiten betraut ist, Kindergelddaten an die mit der Bearbeitung von Personalsachen betrauten Mitarbeiter weiterzugeben oder, wenn er selbst auch mit der Bearbeitung von Personalsachen betraut ist, hierfür die Kindergelddaten zu verwenden. Bei der Erfüllung von Aufgaben nach dem Bundeskindergeldgesetz werden die Festsetzungsstellen als Sozialleistungsträger tätig; daher haben sie - auch gegenüber anderen Bediensteten oder Abteilungen der gleichen Behörde - das Sozialgeheimnis zu wahren. Dieser Hinweis auf die Zweckbindung und die Einhaltung des Sozialgeheimnisses ist inzwischen in das Gemeinsame Rundschreiben der Bundesminister für Jugend, Familie und Gesundheit sowie des Innern vom 26. November 1983 aufgenommen worden. In seinem Rundschreiben an die hessischen Kindergeldstellen vom 2. November 1983 (StAnz. 47/1983 S. 2226) hat der Hessische Innenminister diesen Hinweis zur Kenntnisnahme und Beachtung gegeben. Ich erwarte, daß die funktionsbezogene Abgrenzung von Kindergeld- und sonstigen Bedienstetendaten eingehalten wird und werde mich davon bei Gelegenheit von Überprüfungen in einzelnen Dienststellen überzeugen.

3.3
Automatisierung und Datenschutz in der öffentlichen Personalverwaltung

3.3.1
Personaldatensysteme in Hessen

3.3.1.1
Stand und Tendenzen

Über den Stand der Automatisierung der Datenverarbeitung (ADV) im öffentlichen Personalwesen Hessens habe ich zuletzt in meinem 9. Tätigkeitsbericht für 1980 informiert (vgl. Ziff. 4.4.1). Im Vorwort meines letzten Jahresberichts habe ich auf die Aktualität dieses Themas kurz hingewiesen (11. Tätigkeitsbericht, Ziff. 1.2 a.E.).

Seit 1980 hat der Einsatz der ADV für die Speicherung und Auswertung von Bedienstetendaten auch im öffentlichen Dienst erheblich zugenommen. Entsprechend hat sich die Diskussion über Nutzen und Gefahren dieser Entwicklung intensiviert. Im Verwaltungsbereich ist man dabei, den "Rückstand" gegenüber der Privatwirtschaft aufzuholen - sowohl was den Einsatz von Personaldatensystemen angeht als auch was die Debatte über deren Konsequenzen betrifft. So hat etwa der hessische Vorsitzende der Gewerkschaft ÖTV vor der Gefahr des "gläsernen Arbeitnehmers" auch in der Verwaltung gewarnt. Beleg für das wachsende politische Interesse an diesem Thema auch in Hessen ist die Absicht der Landesregierung, im Frühherbst als Beitrag zum "Orwell-Jahr 1984" eine Tagung mit Experten und Politikern durchzuführen, die gerade die Auseinandersetzung mit den Personalinformationssystemen zu einem Schwerpunkt haben wird.

Situation und Tendenzen in Hessen lassen sich in wenigen Stichworten wie folgt beschreiben:

Umfassende Personaldatensysteme gibt es - noch - nur vereinzelt (etwa bei der Hessischen Zentrale für Datenverarbeitung). Das, was irreführend als "Hessisches Personalinformationssystem (HEPIS)" bezeichnet wird, besteht aus einem vom Landespersonalamt betreuten Programmpaket, mit dem aus den Besoldungs- und Vergütungsdateien der hessischen Landesbediensteten umfangreiches statistisches Material (z.B. Tabellenbände) erstellt wird. Auf Wunsch der Ressorts können auch bestimmte personenbezogene Sonderauswertungen geliefert werden. Das aus HEPIS gewonnene Zahlenmaterial dient in erster Linie der genaueren Kenntnis der Personalstruktur sowie der Personalbedarfsplanung. Das zunehmende Interesse der öffentlichen Arbeitgeber, die Rationalisierungs- und Effizienzvorteile der ADV über personalstatistische Aufbereitungen hinaus auch für die laufende Personalverwaltung zu nutzen, zeigt sich - was die Landesverwaltung angeht - an folgenden 1983 in Angriff genommenen bzw. fortgeführten Projekten:

(1) Die "programmgesteuerte Personaldatei bei der Kanzlei des Hessischen Landtages" ist im Landesautomationsausschuß beraten und als "Pilotversuch" deklariert und gebilligt worden. Die Realisierung soll 1984 erfolgen.

(2) Gleiches gilt für das vom Hessischen Minister für Wirtschaft und Technik durchgeführte Vorhaben der "Erstellung und Fortführung einer Personaldatei der Hessischen Straßenbauverwaltung" (vgl. dazu bereits 9. Tätigkeitsbericht, Ziff. 4.1.2).

In beiden Fällen soll das von der Hessischen Zentrale für Datenverarbeitung für die eigenen Mitarbeiter entwickelte und eingesetzte "Bildschirmorientierte interne Projektsteuerungs- und -informationssystem (PSI)" übernommen und an die konkreten Gegebenheiten und Wünsche des Landtages bzw. der hessischen Straßenbauverwaltung angepaßt werden. Für beide Projekte hat der Landesautomationsausschuß den verantwortlichen Ressorts aufgegeben, "die grundsätzliche Eignung des HZD-Verfahrens, die Wirtschaftlichkeit und die Datenschutz- und Datensicherungsmaßnahmen zu klären".

(3) Auch die geplanten Veränderungen bei der "Lehrerindividualdatei (LID)" gehören in den Trend zur Nutzung der ADV für unmittelbar personaladministrative Zwecke. Diese Datei, in der alle hessischen Lehrkräfte gespeichert sind, steht derzeit nur im Zugriff des Kultusministers bzw. des ihm angegliederten Hessischen Instituts für Bildungsplanung und Schulentwicklung (HIBS). Künftig sollen auch die Schulabteilungen der Regierungspräsidenten, die für Lehrer die eigentliche personalführende Stelle sind, diesen Datenbestand im Direktzugriff benützen können.

(4) Sonderentwicklungen gibt es im Hochschulbereich. An den Universitäten Gießen und Marburg beispielsweise wird ein von der HIS-GmbH entwickeltes Personalverwaltungssystem (HIS-PVS) eingesetzt bzw. für den Einsatz vorbereitet. Im Unterausschuß "Hochschulverwaltung" des Landesautomationsausschusses laufen die Vorarbeiten für die Einführung eines landeseinheitlichen Verfahrens für den Personalbereich der Hochschulen.

Die vorgenannten Beispiele stehen in ihrer bisherigen Konzeption ausnahmslos für eine DV-Unterstützung der Personaladministration. Die Systeme enthalten keine Leistungs- und Beurteilungsdaten, die die Herstellung von Arbeitnehmerprofilen im Vergleich mit Arbeitsplatzdaten erlauben würden, was als das hauptsächliche Gefährdungsmoment der - nach einem nicht ganz einheitlichen Sprachgebrauch - als "Personalinformationssysteme" (im engeren Sinne) bezeichneten DV-Anlagen angesehen wird. Dennoch ist die sich aus der Nutzung der DV ergebende erhöhte Kontrollintensität auch bei reinen Personalverwaltungssystemen nicht zu unterschätzen. Steckt der Einsatz kompletter Personaldatensysteme - für die hessische öffentliche Verwaltung insgesamt gesehen - noch in den Anfängen, nimmt die Installierung von automatisierten Einzelanlagen zur Registrierung und Kontrolle der Leistung und des Verhaltens der Beschäftigten rapide zu. Immer mehr Behörden bedienen sich der Anlagen für die Arbeitszeiterfassung, für die Telefondatenspeicherung usw.

3.3.1.2
Informationsstand des Datenschutzbeauftragten

Bei allen Anlagen und Systemen zur Verarbeitung von Mitarbeiterdaten, die mir bekannt werden, setze ich mich für eine strikte Beachtung der Anforderungen des Datenschutzes und der Datensicherung (dazu unten 3.3.1.3) ein. Allerdings besteht ein Informationsdefizit überall dort, wo Projekte nicht entweder über die zuständigen Automationsgremien und deren Unterausschüsse laufen oder aber mir von den durchführenden Stellen bzw. deren Personalräten zur vorherigen Stellungnahme zugeleitet werden. Die gesetzlich vorgeschriebenen Meldungen zum Dateienregister werden erst nach Anlegung der Dateien erstattet. Nachträgliche Korrekturen sind jedoch schwieriger zu realisieren als rechtzeitig vor der Durchführung eines Projekts vorgetragene Anregungen und Änderungswünsche. Vor allem aus den Stadt- und Kreisverwaltungen erfahre ich häufig erst nachträglich von der Einrichtung etwa von Telefondatenanlagen, Arbeitszeiterfassungsgeräten usw. sowie von den Problemen und Konflikten zwischen Dienststellenleitungen und Belegschaften, die sich daraus ergeben. Die rechtzeitige Einschaltung des Datenschutzbeauftragten vermag nicht nur von vornherein eine datenschutzgerechte Lösung zu gewährleisten, sondern auch zur Konfliktvermeidung beizutragen.

Die DV-Leitsätze, nach denen sich die den Automationsausschüssen vorzulegenden Projektberichte zu richten haben, sind im letzten Jahr dahingehend geändert worden, daß diese Berichte nunmehr eine eingehende Beschreibung der geplanten bzw. getroffenen Maßnahmen zum Datenschutz und zur Datensicherung enthalten müssen. Zwar hat sich seitdem vielfach die Qualität des Abschnittes über den Datenschutz verbessert, dennoch muß ich darauf dringen, daß gerade bei umfangreichen Personaldatensystemen nicht nur allgemein gehaltene Absichtserklärungen abgegeben, sondern konkrete Vorkehrungen und Maßnahmen in die Berichte aufgenommen werden.

3.3.1.3
Die wichtigsten Datenschutzforderungen

Datenschutzgerechte Personaldatensysteme müssen folgende Bedingungen erfüllen, wobei ich nur die wichtigsten Maßnahmen aufzähle (vgl. bereits meinen 9. Tätigkeitsbericht, Ziff. 4.1.2):

(1) Der zur Speicherung vorgesehene Datensatz muß eindeutig festgelegt sein, ebenso die geplanten Auswertungen. Es dürfen nur solche Angaben in die Personaldateien aufgenommen werden, die für die Begründung, Ausgestaltung und Beendigung der Dienst-, Arbeits-, Ausbildungs- oder Versorgungsverhältnisse erforderlich sind. Zwar darf der Dienstherr/Arbeitgeber Mitarbeiterdaten darüber hinaus auch dann speichern und verändern, wenn er sie zur Wahrnehmung seiner berechtigten Interessen, etwa zur Personalbedarfs- oder Lehrereinsatzplanung benötigt. Letzteres ist jedoch nur dann zulässig, wenn kein Grund zu der Annahme besteht, daß schutzwürdige Belange der Betroffenen beeinträchtigt werden, m.a.W. in den Bereich ihrer Persönlichkeitssphäre im weitesten Sinne eingegriffen wird (vgl. § 23 BDSG, für hessische Bedienstete anzuwenden aufgrund der Verweisung in § 3 Abs. 4 HDSG).

Keine Bestimmung des Datenschutzrechts listet im einzelnen die Angaben auf, die ein Personaldatensystem zulässigerweise enthalten darf. Insbesondere Personalräte überschätzen häufig die Vorgaben, die den Datenschutzgesetzen direkt entnommen werden können. Auf der anderen Seite lassen sich die genannten Leitlinien mit Hilfe

arbeitsrechtlicher Normen und Grundsätze sowie einschlägiger Rechtsprechung zur Behandlung von Arbeitnehmerdaten durchaus konkretisieren: Was etwa bei der Einstellung durch das Fragerecht des Arbeitgebers nicht abgedeckt ist, darf auch nicht gespeichert werden. Ein anderes Beispiel: Nach einem Urteil des Landesarbeitsgerichts Frankfurt (Az. 4 I a BV 9/83) ist die Auswertung der Daten über krankheitsbedingte Fehlzeiten von Mitarbeitern teilweise unzulässig.

Die Beurteilung der Zulässigkeit von Speicherung und Auswertung setzt voraus, daß die Dienststellenleitungen die Aufgaben und Zwecke geplanter Personaldatensysteme präzise und detailliert definieren, damit insbesondere deutlich wird, ob bisher manuell betriebene Tätigkeiten automatisiert oder zusätzliche Aktivitäten der Personalverwaltungen wahrgenommen werden sollen.

(2) Die Zugriffsberechtigung auf die Personaldateien muß ebenfalls eindeutig festgelegt und auf Angehörige der Personalabteilung beschränkt sein. Nehmen diese unterschiedliche Aufgaben wahr oder beschränkt sich ihre Zuständigkeit auf bestimmte Teile der Belegschaft, muß der Zugriff funktionsbezogen differenziert ausgestaltet werden. Die klare Abgrenzung der für Personalangelegenheiten zuständigen Bediensteten von den Mitarbeitern mit anderen Aufgaben setzt einen präzisen Geschäftsverteilungsplan voraus. Bei Personaldatensystemen in Verwaltungen mit mehrstufigem Behördenaufbau - etwa bei der Lehrerindividualdatei oder dem Projekt der hessischen Straßenbauverwaltung - ist auf die aufgabenspezifische Abstufung der Zugriffsbefugnisse auf den verschiedenen Ebenen zu achten.

(3) Für die Sperrung bzw. Löschung nicht mehr benötigter bzw. falscher Daten (vgl. § 27 Abs. 2 und 3 BDSG) müssen entsprechende Programme vorhanden sein. Dies betrifft beispielsweise die Daten nicht eingestellter Bewerber oder von ausgeschiedenen Beschäftigten.

(4) Die Benachrichtigung der Mitarbeiter bei der erstmaligen Speicherung muß ebenso gewährleistet sein wie die Auskunftserteilung an Bedienstete über die zu ihrer Person registrierten Angaben (vgl. § 26 Abs. 1 und 2 BDSG). Das Auskunftsrecht umfaßt bei Personaldatensystemen auch die Personen und Stellen, an die ihre Daten regelmäßig übermittelt werden.

(5) Wesentliche Bedeutung kommt schließlich einer effektiven Datensicherung zu, die eine wirksame Zugangs-, Speicherungs-, Eingabe-, Übermittlungs- und Transportkontrolle zur Bedingung hat. Insgesamt ist "die innerbehördliche Organisation so zu gestalten, daß sie den besonderen Anforderungen des Datenschutzes gerecht wird" (Ziff. 10 der Anlage zu § 10 HDSG).

3.3.1.4
Reformansätze

Schon in meinem Gutachten an den Bundesarbeitsminister aus dem Jahr 1980 ("Schutz von Arbeitnehmerdaten, Regelungsdefizite -Lösungsvorschläge") habe ich darauf hingewiesen, daß ich eine Verbesserung des Arbeitnehmerdatenschutzes für dringend erforderlich halte, und ausführlich meine Argumente dargelegt. Angesichts der rapiden Entwicklung der Datenverarbeitung in Betrieben und Behörden und der zunehmend gravierender werdenden Auswirkungen auf die Beschäftigten gerade in den letzten drei Jahren hat sich die Notwendigkeit, gesetzliche Reformregelungen zu schaffen, ohne Zweifel noch verstärkt.

Allerdings unter einem Vorbehalt: Es ist in der Vergangenheit immer wieder versucht bzw. vorgeschlagen worden, verbesserte Bestimmungen zum Arbeitnehmerdatenschutz in die beabsichtigte Novellierung des BDSG aufzunehmen. Ich halte diesen Ansatz für problematisch. Datenschutz für die Beschäftigten in Betrieben und Verwaltungen ist in allererster Linie eine Frage des kollektiven Arbeitsrechts. Wer wirklich eine wirksame Kontrolle der Verarbeitung von Arbeitnehmerdaten anstrebt, muß bei der Mitbestimmung der Betriebs- und Personalräte ansetzen und dort die Voraussetzungen für strikte Verarbeitungsgrenzen schaffen. Das Bundesdatenschutzgesetz beschränkt sich dagegen darauf, dem einzelnen Betroffenen Rechte einzuräumen. Insofern gewährt es zwar auch dem Arbeitnehmer Schutzpositionen. Korrekturen des BDSG verkennen aber die Besonderheiten des Arbeitsrechts. Erinnert sei nur an die schwierigen Abgrenzungsfragen zwischen dem - im Betriebsverfassungsgesetz sowie den Personalvertretungsrechten normierten - Einsichtsrecht in die Personalunterlagen und dem Auskunftsrecht nach § 26 BDSG. Hinzu kommt, daß Änderungen im BDSG allzu leicht dazu führen können, die Reform des Arbeitnehmerdatenschutzes damit für erledigt zu erklären. Sie laufen Gefahr, den speziellen arbeitsrechtlichen Kontext völlig außer Acht zu lassen.

So gesehen, erscheint mir der Weg einer gesetzgeberischen Initiative vorgezeichnet. Es gilt zunächst, den gesetzlich eingeräumten Beteiligungsstandard der Betriebs- und Personalvertretungen an die veränderten Gegebenheiten der personenbezogenen Informationsverarbeitung in Unternehmen und Dienststellen anzupassen. Daran können und müssen dann Überlegungen anknüpfen, wie die Individualrechte der Arbeitnehmer ausgebaut werden können. Nicht selten wird ja ausgeblendet, daß das Betriebsverfassungsgesetz mit seinen Vorschriften über die Beteiligung

des Betriebsrates bei der Erhebung von personenbezogenen Daten und bei der Einführung technischer Anlagen -Bestimmungen, die von den Personalvertretungsgesetzen vielfach wörtlich übernommen wurden - aus dem Jahr 1972 stammt, als die Automatisierung der Personalverwaltung noch in den Anfängen steckte.

Auszugehen ist mithin vom Betriebsverfassungs- bzw. Personalvertretungsrecht, um dort für Klarheit zu sorgen. Zwar liegt mittlerweile eine ganze Reihe von Entscheidungen der Arbeitsgerichte vor, die ausdrücklich ein Mitbestimmungsrecht bei der Einführung von Personalinformationssystemen einräumen, ganz zu schweigen von der schon früher akzeptierten Mitbestimmung bei der Datensicherung (vgl. nur das bereits erwähnte Urtel des LAG Frankfurt vom 2. September 1983, Az. 4 I a BV 9/83). Insgesamt gesehen ist jedoch die Position der Gerichte nach wie vor uneinheitlich, was wiederum Unsicherheiten und Konflikte in Unternehmen und Behörden mit sich bringt.

Zur Beseitigung dieser Unklarheit und zur klaren Festlegung eines Mitbestimmungsrechts ist daher der Gesetzgeber gefordert. Sind auf der Bundesebene keine Korrekturen zu erwarten, macht dies einschlägige Aktivitäten auf Landesebene um so dringlicher, um zumindest für den Bereich der Verarbeitung von Arbeitnehmerdaten im öffentlichen Dienst von Land und Kommunen zufriedenstellende Lösungen zu erreichen. Dabei geht es mir vor allem darum, den derzeit im Vordergrund stehenden unfruchtbaren Streit um die Frage, ob Personaldatensysteme "dazu bestimmt sind, das Verhalten oder die Leistung der Arbeitnehmer zu überwachen" - nur dann besteht ein Mitbestimmungsrecht bei der Einführung und Anwendung, vgl. § 87 Abs. 1 Nr. 6 BetrVerfG und gleichlautend § 61 Abs. 1 Nr. 17 Hessisches PersonalvertretungsG - zu beenden. Für sachgerecht hielte ich etwa eine Formulierung, nach der ein Mitbestimmungsrecht besteht bei der "Einführung und Anwendung (1) von Anlagen zur automatisierten Verarbeitung personenbezogener Daten der Beschäftigten und (2) von sonstigen Einrichtungen, soweit diese dazu geeignet sind, das Verhalten oder die Leistung der Beschäftigten zu überwachen". Damit wäre eine klare Trennung gegeben zwischen Personaldatensystemen, deren Einsatz und Nutzung immer an die Mitbestimmung der Arbeitnehmervertretung geknüpft wäre, und sonstigen technischen Einrichtungen, bei denen die Mitbestimmung nach wie vor von der Überwachungsmöglichkeit abhängig wäre (z.B. Videokameras o.ä.).

Gegenwärtig liegt dem Landtag der Gesetzentwurf der Fraktion der GRÜNEN zur Änderung des Hessischen Personalvertretungsgesetzes (HPVG) vor. Er basiert auf Vorstellungen des Deutschen Gewerkschaftsbundes und enthält an zwei Stellen Formulierungen, die die Mitbestimmungsrechte der Personalräte im Bereich der automatisierten Verarbeitung personenbezogener Informationen zu verstärken suchen. Auch soll das für den Frühherbst angekündigte Symposium der Landesregierung (s.o.) nicht nur die "Perfektionierung der Personalinformationssysteme" und den "Ausbau der Überwachungsmöglichkeiten von Arbeitnehmern an bildschirmgestützten Arbeitsplätzen" zu Schwerpunktthemen haben, sondern dazu auch Grundlagen für gesetzgeberische Aktivitäten auf Landes- und Bundesebene schaffen. Ich hoffe daher, daß diese begrüßenswerten Ansatzpunkte aufgegriffen werden, damit konkrete Verbesserungen jedenfalls für Hessen erzielt werden.

Gerne bin ich bereit, im Rahmen der parlamentarischen Behandlung des HPVG-Entwurfs oder bei späterer Gelegenheit meine Vorstellungen im einzelnen zu erläutern und auf Wunsch Gesetzesformulierungen oder Kommentierungen zur Verfügung zu stellen.

3.3.2
Führung einer Personalkartei durch den Personalrat

3.3.2.1
Datenschutz und Personalvertretung: Probleme im Überblick

Meinungsverschiedenheiten zwischen Dienststellenleitungen und Personalräten entzünden sich immer wieder an datenschutzrechtlichen Problemen oder werden zumindest - ob zu Recht oder zu Unrecht - unter Berufung auf Bestimmungen der Datenschutzgesetze ausgetragen. Als konfliktträchtig haben sich in der Vergangenheit vor allem zwei Fragenkreise erwiesen: Zum einen die angeblich restriktiven Auswirkungen des Datenschutzrechts auf die personenbezogenen Informationsansprüche des Personalrats gegen die Dienststelle, zum anderen die Reichweite der Mitwirkungs- und Mitbestimmungsrechte bei der Einführung von Personaldatensystemen bzw. sonstigen Datenaufzeichnungsanlagen sowie bei technischen und organisatorischen Maßnahmen der Datensicherung. Auf beide Themenbereiche bin ich bereits in meinem 9. Tätigkeitsbericht (vgl. Ziff. 4.1.4) eingegangen (vgl. auch oben Ziff. 3.3.1.4). Im 11. Tätigkeitsbericht (vgl. Ziff. 2.2.2) hatte ich einen weiteren Aspekt, nämlich den der möglichen Kontrolle des Dienstherrn über die Personalvertretung, im Zusammenhang mit der Telefondatenregistrierung aufgegriffen. Dabei habe ich meine Auffassung dargelegt, daß aus der gesetzlich eingeräumten Unabhängigkeit der Personalvertretung entsprechende Konseqenzen zu ziehen sind, z.B. daß entweder die Speicherung der Telefonate des Personalrats unterbleibt oder ihm eine eigene Amtsleitung eingerichtet wird. Diese Gesichtspunkte des Datenflusses zwischen Dienststelle und Personalrat und der Geltung der Mitbestimmungsrechte sind in der Fachliteratur intensiv aufbereitet; eine Reihe von Gerichtsentscheidungen liegt dazu vor.

3.3.2.2
Datenaufzeichnung durch den Personalrat

Kaum behandelt sind dagegen bisher die datenschutzrechtlichen Rahmenbedingungen einer Speicherung und Auswertung von Daten der Beschäftigten durch den Personalrat selbst. Ich habe in einem Konflikt zwischen Leitung und Personalvertretung einer großen Landesbehörde um die Führung einer Katei der Bediensteten die Auffassung vertreten, daß sich ein Personalrat grundsätzlich zur Erfüllung seiner Personalvertretungsaufgaben vom Dienstherrn/Arbeitgeber unabhängige Dateien mit personenbezogenen Daten der Mitarbeiter aufbauen darf, d.h. nicht darauf angewiesen ist, jeweils im Einzelfall an die Personalverwaltung heranzutreten und die benötigten Angaben dort abzurufen. Dies gilt insbesondere dann, wenn der Personalrat sich Aufzeichnungen aus Personalunterlagen, die ihm entsprechend den Bestimmungen des HPVG vorliegen bzw. zur Verfügung gestellt worden sind, in eine Kartei macht. Das Recht, sich Aufzeichnungen zu fertigen, wird in der Literatur zum Personalvertretungsrecht weit überwiegend anerkannt. Erhält der Personalrat wie in vielen Fällen eine Durchschrift der einen Bediensteten betreffenden Verfügung der Dienststellenleitung, ist es ihm nicht verwehrt, diese Daten auch karteimäßig aufzubereiten, statt das zur Verfügung gestellte Schriftstück lediglich in einem Aktenordner abzuheften.

Welche personenbezogenen Angaben der Personalrat für eine sachgerechte Planung und Durchführung seiner Tätigkeit braucht und zulässigerweise in einer Datei festhalten darf, ergibt sich aus den einzelnen Aufgabenzuweisungen des HPVG. Die Kenntnis persönlicher Daten kann sich für den Personalrat u.a. zur Wahrnehmung seiner allgemeinen Überwachungsaufgabe nach § 57 Abs. 1 Satz 2 HPVG als erforderlich erweisen, aber auch z.B. für Maßnahmen zur Förderung Schwerbehinderter, zur Eingliederung ausländischer Beschäftigter oder für die Zuweisung von Dienstwohnungen. Hinzu kommen natürlich die eigentlichen Personalvorgänge selbst, wie die Einstellung, die Kündigung usw.

3.3.2.3
Grenzen der Datenhaltung

Noch einmal: Will man den Personalrat nicht auf die reaktive Behandlung von Einzelmaßnahmen beschränken, bedenkt man vielmehr auch seine Initiativrecht und seine Aufgaben der ständigen Überwachung der Einhaltung von Gesetzen und Tarifverträgen, der Anregung von Maßnamen für spezielle Teilgruppen der Bediensteten, der Sorge um eine gerechte Eingruppierungs- und Beförderungspraxis usw., muß es ihm auch möglich sein, die dafür erforderliche Datengrundlage vorzuhalten, ob sie nun vom Arbeitgeber/Dienstherrn stammt oder von den Personalratsmitgliedern selbst festgestellt bzw. erhoben worden ist. Doch müssen die Grenzen der Datenspeicherung durch den Personalrat, wie sie sich aus dem HPVG selbst ergeben, eingehalten werden. So ist etwa der Regelung des § 57 Abs. 2 Satz 3 HPVG, wonach die Einsicht in Personalakten nur mit Zustimmung des Bediensteten in Betracht kommt, zu entnehmen, daß dem Personalrat Personaldaten nicht in solchem Umfang zur Verfügung stehen sollen, daß er gleichsam eine zweite Personalakte führt. Auch wäre ein unbeschränktes Zugriffsrecht des Personalrats auf ein automatisiertes Personalinformationssystem unzulässig. Aus der Mitbestimmungs- und Überwachungsfunktion läßt sich - anders ausgedrückt - nicht ableiten, daß der Personalrat neben der Personalverwaltung der Dienststelle einen vollständigen Zweitbestand der Beschäftigtendaten führt. Hinsichtlich der Gründe, die Antragsteller bei Anträgen auf Unterstützungen und soziale Zuwendungen angeführt haben, legt § 62 Abs. 1 Satz 2 HPVG ausdrücklich fest, daß die Dienststelle dem Personalrat hierüber keine Auskünfte erteilt.

Weiterhin muß der Personalrat, wenn er eine Datei anlegt, die gesetzlichen Pflichten einer speichernden Stelle erfüllen, auch wenn er im Rechtssinne nur Teil der "speichernden Stelle" Behörde, Körperschaft usw. ist. Neben der notwendigen Zugangs-und Zugriffssicherung (vgl. § 10 Abs. 1 HDSG) muß er vor allem dafür Sorge tragen, daß die sich aus §§ 26 und 27 BDSG ergebenden Rechte der Beschäftigten ihm gegenüber gewährleistet werden. Dies gilt zum einen für das Auskunftsrecht nach § 26 Abs. 2 Satz 1 BDSG, zum anderen für die Pflicht zur Berichtigung, Sperrung und Löschung (vgl. § 27 BDSG). So sind beispielsweise nach § 27 Abs. 2 Satz 2 und Abs. 3 Satz 2 BDSG die Daten von ausgeschiedenen Mitarbeitern zumindest zu sperren und auf ihr Verlangen zu löschen, weil nach dem Ausscheiden die Kenntnis der Angaben für die Erfüllung der Aufgaben des Personalrates nicht mehr erforderlich ist - von Sonderfällen wie der Zeugnispflicht des Personalrats in Gerichtsverfahren des ausgeschiedenen Bediensteten o.ä. abgesehen. Gleiches gilt für die Daten abgelehnter Bewerber nach Beendigung des Einstellungsvorgangs. Außerdem gilt zusätzlich zur Schweigepflicht der Personalratsmitglieder das Datengeheimnis nach § 9 HDSG.

3.4
Bildschirmtext
Einstieg in eine neue Informations- und Kommunikationslandschaft

3.4.1
Der rechtliche Rahmen: Der Staatsvertrag über Bildschirmtext

3.4.1.1
Datenschutzanforderungen im Staatsvertrag

Mit der Verabschiedung des Gesetzes zum Staatsvertrag über Bildschirmtext durch den Hessischen Landtag am 21. Juni 1983 (vgl. Drucks. 10/1146 zu Drucks. 10/642 und GVBl. I 1983 S. 91 vom 5. Juli 1983) kommen neue Aufgaben auf den Datenschutz in Hessen zu. Der Staatsvertrag ist am 1. September 1983 in Kraft getreten.

Die Regelung des rechtlichen Rahmens für die Einführung des Bildschirmtextes (Btx) ist ein wichtiger Erfolg sowohl für eine föderative Medienpolitik als auch für einen auf die spezifischen Risiken dieses neuen Kommunikationsmediums zugeschnittenen Datenschutz. In seiner Rede vor dem Landtag hat der Ministerpräsident dem Datenschutz im Staatsvertrag besonderes Gewicht beigemessen. Der Hessische Datenschutzbeauftragte hat sich an der Vorbereitung der Vertragsverhandlungen - in Zusammenarbeit mit der Staatskanzlei - intensiv beteiligt und dabei die Vorschläge der Datenschutzbeauftragten der Länder und des Bundes eingebracht.

Meine weitergehenden Anregungen, die über die jetzige Fassung des Staatsvertrages hinausgingen, haben sich trotz Unterstützung durch den Ministerpräsidenten nicht durchsetzen lassen. So sollte nach meiner Auffassung vor allem auf eine Anknüpfung an den Dateibegriff generell verzichtet werden. Nur so hätte klargestellt werden können, daß es gilt, die Voraussetzungen für eine grundlegende, an der technischen Entwicklung orientierte Neukonzeption des Datenschutzes zu schaffen. Das spezifische Gefährdungsmoment besteht nämlich darin, daß alle Daten im Btx-System rechnergestützt verarbeitet werden, auch wenn sie nicht in "Dateien" im herkömmlichen Sinn, sondern in Btx-Tafeln enthalten sind. Darüber hinaus ging es mir darum, das Herstellen von Benutzerprofilen von vornherein dadurch zu verhindern, daß das bereits in den Feldversuchen in Nordrhein-Westfalen und Berlin verwandte Abrechnungsverfahren übernommen wurde. Auch halte ich nach wie vor die Sonderstellung der Kreditwirtschaft im Zusammenhang mit der Datenübermittlung an Bankenauskunftsdienste (§ 9 Abs. 6 Satz 5) für ungerechtfertigt.

Auch wenn diese Vorschläge im Staatsvertrag keine Berücksichtigung gefunden haben, sehe ich gleichwohl die Datenschutzregelung in Art. 9 als einen entscheidenden Fortschritt für den Datenschutz an. Dies gilt um so mehr, als es bis zuletzt immer wieder Bemühungen - etwa des Niedersächsischen Ministerpräsidenten oder des Deutschen Industrie- und Handelstages - gegeben hat, die darauf abzielten, die Datenschutzvorkehrungen im Staatsvertrag weitgehend zu verwässern bzw. zu beseitigen. Im einzelnen sind folgende Datenschutzmaßnahmen festgelegt:

Über die Bestimmungen des Bundesdatenschutzgesetzes und der Landesdatenschutzgesetze hinaus bestimmt Art. 9, daß Verbindungsdaten nur zum Zwecke und während der Dauer der Verbindung aus technischen Gründen temporär gespeichert werden dürfen und nach Beendigung der jeweiligen Verbindung zu löschen sind (Art. 9 Abs. 2 Nr. 1). Zur Abrechnung von Gebühren und Anbietervergütungen bestimmte Daten (Abs. 2 Nr. 2, das sind Nummer des Teilnehmers, Anschlußnummer des Anbieters, Datum, Uhrzeit von Beginn und Ende der Verbindung sowie die Vergütungssumme) werden, ohne daß dabei der Inhalt des in Anspruch genommenen Angebots kenntlich gemacht werden soll, beim Betreiber (z.B. im Bildschirmtextsystem bei der Bundespost) gespeichert und dürfen grundsätzlich nicht an Dritte weitergegeben werden. Einzige Ausnahme ist die Übermittlung von Abrechnungsdaten, wenn eine Forderung nach Mahnung nicht beglichen wird. Daraus folgt, daß der Betreiber des Btx-Systems bis zur ersten Mahnung das Inkasso von Gebühren und Anbietervergütungen übernimmt. Ausnahmen vom Übermittlungsverbot dürfen nur durch besondere Rechtsvorschriften zugelassen werden. Die Übermittlung von Verbindungsdaten ist schlechthin ausgeschlossen.

Das gesamte Bildschirmtextangebot, das personenbezogene Daten enthält, wird den strengen Übermittlungsbestimmungen der Datenschutzgesetze unterstellt. Der Schutz ist jedoch nicht lückenlos, da durch den Verweis auf das Bundesdatenschutzgesetz solche Angebote ausgenommen werden, die das "Medienprivileg" des § 1 Abs. 3 BDSG für sich in Anspruch nehmen können, die also traditionell massenmedialen Charakter haben. Wo und vor allem wie allerdings die Grenzen bei einer individualisierten Form der Massenkommunikation wie beim Bildschirmtext zu ziehen sind, müssen Bundes- und Landesgesetzgeber im Rahmen ihrer jeweiligen Presserechtskompetenzen bestimmen, wenn diese nicht allein durch die Rechtsprechung definiert werden sollen. Die bisherige Formalisierung des Pressebegriffs in Rechtsprechung und Literatur birgt bei zukünftigen Formen individualisierter Massenkommunikation die Gefahr, zum Einfallstor zur Umgehung des Datenschutzes zu werden.

Für den Vertragsabschluß über Btx sind bis auf die bereits kritisierte, unbegründete Privilegierung von Kreditgeschäften eindeutige Bestimmungen getroffen worden: Daten dürfen vom Teilnehmer nur dann abgefragt werden, soweit die Daten für das Erbringen einer Leistung, den Abschluß oder die Abwicklung eines Vertragsverhältnisses unbedingt erforderlich sind. Diese Erforderlichkeit legt auch den Umfang und die Art der zulässig erhobenen Daten fest. Die Bereitschaft des Teilnehmers, freiwillig mehr Daten über sich preiszugeben, ist insoweit unerheblich. Diese strikte Regelung kann auch nicht durch die in den Datenschutzgesetzen vorgesehene Einwilligung verdrängt werden. Sie ist mithin zwingendes Recht und kann nicht rechtsgeschäftlich abbedungen werden.

Eine gesonderte Einwilligung sieht der Staatsvertrag nur für den Fall vor, daß über die Zweckbestimmmung des Vertrages oder der Leistung hinaus die für diesen Zweck erhobenen Daten verarbeitet werden sollen. Klargestellt wird auch, daß eine Leistung nicht mit einer solchen "zusätzlichen Einwilligung" verkoppelt werden darf, etwa um die Daten an ein Direktwerbeunternehmen weiterzugeben. Ausgenommen von dieser Bestimmung sind Kreditinstitute, denen die Möglichkeit eingeräumt werden soll, auch ohne zusätzliche Einwilligung des Bankkunden dessen Daten an Kreditauskunfteien weiterzugeben. Von einer schriftlichen Einwilligung mit ihrer besonderen verbraucherschützenden Warnfunktion abzugehen, ist jedoch durch nichts gerechtfertigt, es sei denn, die Banken wollten in Zukunft den "gläsernen" Kunden, der nicht mehr punktuell, z.B. bei Abschluß eines Kreditgeschäfts, sondern andauernd auf seine Bonität und Zahlungsmoral hin überprüft wird. Die Folgen dieser Privilegierung sind absehbar: eine spezielle Datenschutzregelung für diesen Bereich, etwa nach dem Vorbild des amerikanischen "Fair-Credit-Reporting-Act", wird dann in Zukunft auch für die Bundesrepublik unverzichtbar, zumal bereits heute Beschwerden über fehlerhafte Auskünfte von Kreditauskunfteien einen Schwerpunkt in der Tätigkeit der Datenschutzaufsichtsbehörden ausmachen.

Schließlich greift Art. 9 auch diejenigen technischen Sicherungen auf, die garantieren sollen, daß der Teilnehmer nur durch eindeutiges und bewußtes Handeln personenbezogene Daten übermitteln kann. Die Betreiber müssen technisch sicherstellen, daß Verbindungsdaten nach Ende der Verbindung gelöscht werden. Sie müssen dafür einstehen, daß die zu Zwecken der technischen Datensicherung vergebenen Codes einen dem Stand der Technik entsprechenden Schutz vor unbefugter Verwendung bieten.

3.4.1.2
Kontrollzuständigkeit

Neben diesen konkreten materiellen Anforderungen an den Betrieb des Bildschirmtextsystems ist die effiziente Kontrolle der Einhaltung der Datenschutzbestimmungen des Staatsvertrages von größter Bedeutung. In dem ursprünglich von der Landesregierung vorgelegten Entwurf zum hessischen Zustimmungsgesetz war der gesamte Vollzug des Staatsvertrages den Regierungspräsidenten zugewiesen worden. Dadurch konnte die Unklarheit entstehen, wieweit meine Kontrollbefugnisse für die Verarbeitung personenbezogener Daten mit Hilfe von Btx durch öffentliche Stellen tangiert worden wären. Auch dieser Punkt konnte jedoch in den Landtagsberatungen aufgrund meiner Voschläge und zu meiner Zufriedenheit geregelt werden.

Nach den §§ 3 bis 6 des Ratifizierungsgesetzes sieht das Überwachungssystem - was den Datenschutz angeht - in Hessen wie folgt aus:

Der Hessische Datenschutzbeauftragte kontrolliert die Einhaltung der Datenschutzbestimmungen des Btx-Staatsvertrages bei öffentlichen Stellen. Bei privaten Betreibern und Anbietern vollzieht der Regierungspräsident den Btx-Staatsvertrag. Er ist auch für die Verfolgung und Ahndung von Ordnungswidrigkeiten zuständig. Der Hessische Datenschutzbeauftragte kann - analog zur Regelung in Bayern - bei der Überprüfung nichtöffentlicher Stellen beteiligt werden. Wegen der Einheitlichkeit des Btx-Systems schreibt der Gesetzgeber einen ständigen Erfahrungsaustausch zwischen Innenminister, Datenschutzbeauftragten und den Regierungspräsidenten über die Einhaltung der Datenschutzbestimmungen des Vertrages vor. Im Rahmen dieser Kooperation kann die Effektivität der getroffenen Regelungen sowie der administrativen Praxis festgestellt sowie im Rahmen des jährlichen Tätigkeitsberichts dargestellt werden.

3.4.1.3
Neukonzeption des Datenschutzes

Die Behandlung des Staatsvertrages und des Zustimmungsgesetzes hat gezeigt, daß es einen datenschutzpolitischen Grundkonsens zwischen Landtagsfraktionen, Landesregierung und dem Datenschutzbeauftragten gibt - eine Situation, die Hessen positiv von anderen Ländern unterscheidet, und die zu stabilisieren nicht zuletzt auch Aufgabe des Datenschutzbeauftragten ist. Dieser Grundkonsens darf jedoch nicht Stillstand der Datenschutzentwicklung bedeuten. Redner aller Fraktionen haben im Landtag - bei allen Unterschieden in der politischen Bewertung der technologischen Entwicklung - deutlich gemacht, daß die rechtlichen, gesellschaftspolitischen und institutionellen Rahmenbedingungen für die Einführung und Nutzung der neuen Informations- und Kommunikationstechniken in der Zukunft noch weiter definiert und konkretisiert werden müssen. Anders ausgedrückt: Isolierte Datenschutzregelungen reichen nicht aus; dem Gesetzgeber stellt sich die Aufgabe, zur Bewältigung der Risiken der neuen Systeme auch das Vertrags- und Arbeitsrecht, das Urheber-, Presse- und Wettbewerbsrecht sowie den Verbraucherschutz entsprechend anzupassen.

Ich wiederhole an dieser Stelle meine im letzten Tätigkeitsbericht dargelegte und begründete Position (vgl. Ziff. 3.1.3.3), daß das bisherige Datenschutzkonzept jetzt durch ein neues Modell ersetzt werden muß, das auch die Aspekte Datenzugang ("freedom of information"), Technologiefolgenabschätzung und Informationsverteilung einbezieht. Nur mit Hilfe einer solchen Neukonzeption kann es letztlich gelingen, das vom Bundesverfassungsgericht in seinem jüngsten Volkszählungsurteil bestätigte "informationelle Selbstbestimmungsrecht" und die vom Gericht ebenfalls geforderte "informationelle Gewaltenteilung" auch und gerade angesichts der rapiden technologischen Entwicklung zu sichern.

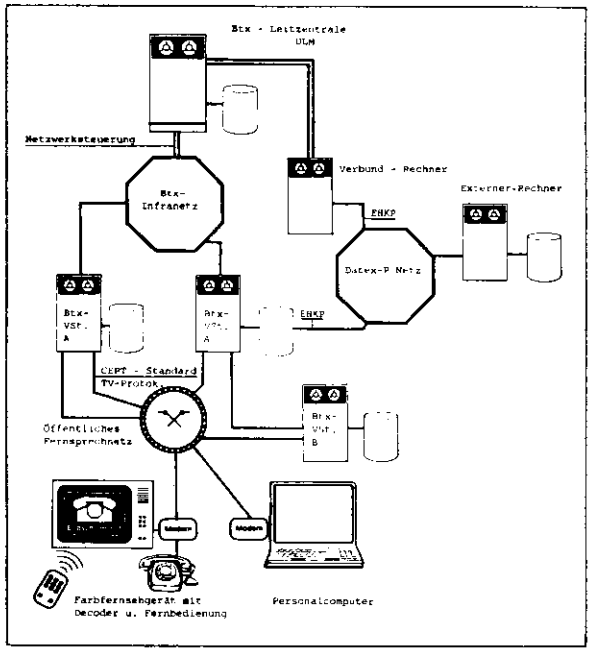
3.4.2
Bildschirmtext als neues Konzept der Informationsverarbeitung

3.4.2.1
Aktueller Ausbaustand

Bildschirmtext bzw. Videotex ist augenblicklich in 32 Ländern der Welt in Erprobung. Drei technische Btx-Normen werden dabei verwendet: CEPT (Europa), Captain (Japan), PLPS (USA).

3.4.2.1.1
Das Netzkonzept für die Bundespost

IBM Stuttgart und die Bundespost haben für den Btx-Betrieb in der Bundesrepublik ein hierarchisches Netzkonzept entwickelt. Es besteht aus der Anbieter-/Benutzerebene und der zweistufigen Postebene.



Hierarchie im Bildschirmtext - Netz

Anbieter und Benutzer stehen über das Telefonnetz der Post mit den Btx-Vermittlungsstellen (Btx-Vst) in Verbindung. Ein Modem an beiden Anschlußpunkten ermöglicht es, die Telefonleitung für den Datenaustausch zu benutzen. Ab 1984 erhebt die Post für den Bildschirmtext Gebühren, die den Telefongebühren im Nahbereichsverkehr entsprechen. Computer von Informationsanbietern können im sog. Btx-Rechnerverbund mit den Btx-Vst und der Leitzentrale in Ulm über das Datex-P-Netz Verbindung aufnehmen. Bei dieser Form der Datenfernverarbeitung werden die Regeln der EHKP (einheitliche höhere Kommunikationsprotokolle) angewendet.

Die Post baut zur Zeit 21 regionale Btx-Vermittlungsstellen auf. Diese sind nach der Planung in der Lage, gleichzeitig 600 Teilnehmer (Typ A) bzw. 100 Teilnehmer (Typ B) anzuschalten. Die Vermittlungsstellen sind mit Computern der IBM-Serie/1 ausgestattet. Sie arbeiten im Btx-Netz als Teilnehmerrechner (Verbindung Btx-Vst und Benutzer), Datenbankrechner (Btx-Seitenspeicherung) und Verbundrechner (Netzwerksteuerung mit der Leitzentrale). Mit diesem Konzept hofft die Post, bis Ende 1984 etwa 150.000 Btx-Benutzer/Anbieter anschließen zu können, die dann etwa 95 v.H. der insgesamt angebotenen Btx-Seiten direkt aus der jeweiligen regionalen Btx-Vermittlungsstelle abrufen können.

Die Leitzentrale in Ulm bildet die oberste Stufe des Btx-Netzkonzepts. Sie ist auf der Hardwareseite mit zwei Rechnern IBM 3083 ausgerüstet, die gegenseitig Backup-Funktionen übernehmen können. Bei Ausfall eines Rechners kann der zweite Rechner den Netzbetrieb aufrechterhalten. Die Leitzentrale speichert alle Btx-Seiten und steuert das Zusammenwirken aller Btx-Vst. Gleichzeitig werden hier die administrativen Aufgaben wie z.B. die Aufteilung des Gebühren-/Entgeltaufkommens zwischen Post und Informationsanbietern abgewickelt. Die ständige Aktualität des Btx-Seitenbestands in den Btx-Vst wird dadurch erreicht, daß der Computer der Leitzentrale permanent die noch "laufende" Datenbank auf ihre Aktualität überprüft und "alte" Btx-Seiten löscht. Nur der jeweils aktualisierte Bestand wird kopiert und auf das Netz gebracht.

3.4.2.1.1
Übergangslösung

Anläßlich der Internationalen Funkausstellung 1983 hat die Bundespost Bildschirmtext bundesweit gestartet. Es handelt sich hierbei vorläufig um eine Erweiterung des Berliner Pilotprojekts auf sechs Großstadtbereiche, in denen die Post sog. Einwählknoten errichtet hat, von denen Bildschirmtext im neuen CEPT-Standard zum Telefonnahtarif abgerufen werden kann. Die technische Ausstattung der Übergangslösung erlaubt allerdings derzeit nur noch die zusätzliche Anschaltung von 5.000 Teilnehmern. Bis Ende 1984 soll nach der derzeitigen Planung der Post für etwa 80 v.H. aller Telefonkunden das Btx-Netz zum Nahtarif erreichbar sein. Nach Angaben der Post liegen bereits jetzt 5.900 Anträge auf Neuzulassung zum Btx-Netz vor.

In Düsseldorf/Neuß und in Berlin sind die Pilotprojekte im britischen Prestel-Standard mit rund 8.000 Teilnehmern noch bis etwa Mitte 1984 in Betrieb. Da das IBM-Konzept vorläufig noch in einer Versuchsphase ist, wurde die Übergangslösung, d.h. die Aufschaltmöglichkeit auf die Berliner Btx-Computer, mit britischem know how (GEC-Computers und System Designers Ltd.) unter Einsatz zweier Rechner des Typs GEC 4082 realisiert. Diese Maschinen haben einen Arbeitsspeicher von 1 MB und verfügen über 108 Ausgänge (Gates).

In den Btx-Versuchen ist die Mehrzahl der künftig denkbaren Anwendungen wie Informationstransfer, Verkauf, Bankgeschäfte (Home-Banking) oder Nachrichtenaustausch zwischen zwei Benutzern realisiert worden. Die für den Bereich der öffentlichen Verwaltung besonders interessanten Datenfernverarbeitungstechniken wie Dialogverkehr, Datenfernübertragung und auch Remote Job Entry wurden in einzelnen Pilotverfahren getestet (vgl. dazu auch Ziff. 3.4.2.2.3).

3.4.2.2
Tendenzen in der Datenverarbeitung

In der Datenverarbeitung ist eine eindeutige Tendenz zur dialogorientierten Informationsverarbeitung mittels intelligenter Terminals an einem Großrechner (HOST) oder autonomer Rechner (Minicomputer/Personal Computer) mit HOST-Anschluß zu erkennen. Ich habe darüber bereits ausführlich berichtet (s. 11. Tätigkeitsbericht Ziff. 3.1, 9. Tätigkeitsbericht Ziff. 2.1). "Mehr Bürgernähe durch Dezentralisierung" lautet die Devise. Die Qualität dieses Innovationsschubs liegt nicht nur in der Ablösung überalterter Karteien, Mikrofilmorganisationen oder veralteter Datenverarbeitung im Stapel-Betrieb. In den meisten Fällen wird die durch die eingesetzte Technik erzwungene Zentralisierung der Verwaltung wieder aufgelöst und verlagert. 1982 hat eine Umfrage der Kommunalen Gemeinschaftsstelle für Verwaltungsvereinfachung (KGSt) bei 114 kommunalen Datenverarbeitungszentralen ergeben, daß reine Stapelverarbeitung (Batch) nur noch selten Anwendung findet und über 50 v.H. der befragten Rechenzentren dialogorientierte Datenfernverarbeitungsmethoden einsetzen. Bei neukonzipierten Verfahren ist die Dialogverarbeitung der Regelfall, die Stapelverarbeitung bildet die Ausnahme. Die Datenverarbeitung als Arbeitsmittel rückt näher an den Arbeitsplatz. Sie wird aber auch durch die Verwendung von Programmen mit umfangreicher Bedienerführung (Menusystem) für den einzelnen Sachbearbeiter leichter zu handhaben (Verzeichnis der in diesem Abschnitt verwandten Fachausdrücke unten Ziff. 5.4).

3.4.2.2.1
Datenfernverarbeitung mit Bildschirmtext (Btx)

Aus technischer Sicht ist Btx ein Verfahren der Datenfernverarbeitung, in dem eine Vielzahl von Datenendgeräten auf Dateien direkt zugreifen. Die hierzu notwendigen Geräte sind Fernseher, Btx-Decoder mit Tastatur oder die FS-Fernbedienung, Btx-Modem der Post und ein Telefonanschluß. Interaktive Datenverarbeitung (Dialogverarbeitung) ist grundsätzlich auch im Bildschirmtext möglich. Allerdings muß außer der Anschaffung der speziellen Geräte eine Modifizierung der bei den Verbundsrechenzentren angewandten Verarbeitungsprogramme erfolgen. Der etwas langsameren Betriebsart im Btx - das Antwort/Zeitverhalten ist schlechter - stehen aber die Vorteile der umfangreichen Grafik- und Farbgestaltung gegenüber. Außerdem öffnet Btx den Zugang zu praktisch allen Computern, soweit dies gewünscht wird.

Im Btx müssen zwei "Betriebs"arten unterschieden werden:

1. Die Kommunikation zwischen Btx-Zentrale und Benutzer als "Informationsabnehmer", d.h. Informationen/ Daten eines Anbieters werden vom Btx-Rechner der Bundespost zum Benutzer übertragen. Dies geschieht unter Verwendung des Telefonnetzes der Post.

2. Ein Anbieter arbeitet im Btx-Rechnerverbund und gestattet einem Benutzer oder einer Gruppe von Benutzern (sog. "geschlossene Benutzergruppe") den Zugang zu seinem Rechner und damit die Nutzung von Daten und Programmen. In diesem Fall fungiert der Rechner der Bundespost nur als "Vermittler" (Gateway). Dies wäre eine für den Hessischen DV-Verbund denkbare Betriebsart der Datenfernverarbeitung. Der Rechnerverbund zwischen Post und Anbieter wird über das Datex-P-Netz realisiert.

Beides sind gängige Verfahren der Datenfernverarbeitung, nämlich "Auskunftsverfahren" wie z.B. Datenbankabfragen ohne Online-Änderungsmöglichkeiten (Grundstufe Einwohnerwesen), interaktive Datenfernverarbeitung oder auch Remote Job Entry (Finanzwesen, Statistik u.a.). Neu ist an Btx das Konzept des bundesweiten flächendeckenden Netzes auf der Basis des Fernsprech- bzw. Datex-Netzes der Bundespost und die Zulassung von Datenendgeräten jeglicher Art wie z.B. Fernsehgeräte (Monitore) oder Personal Computer. Dadurch entsteht ein "offenes Netz".

3.4.2.2.2
Bürgerfreundliche Verwaltung durch Bildschirmtext?

Bürgerfreundliche Verwaltung setzt ein weitgehend dezentrales Anbieten von Leistungen voraus, d.h. die Leistung muß dort angeboten werden, wo der Bürger sie benötigt. Um die notwendige Akzeptanz eines solchen technisch zu realisierenden Versuchs zu erreichen, müßten die vom Benutzer benötigten Geräte entweder preiswert erhältlich oder in möglichst vielen Haushalten schon vorhanden sein, die Anwendung - Bedienerführung - müßte in solchen Verwaltungsprogrammen leicht erlernbar sein und verständlich dargeboten werden, und schließlich dürften nur geringe Entgelte gefordert werden. Der Einsatz herkömmlicher Datenfernverarbeitung scheiterte bei kleineren Verwaltungen nicht zuletzt oft deshalb, weil diese Kriterien nicht erfüllt werden konnten. Doch ist die technische Seite dieser Forderungen relativ leicht und schnell erfüllbar. Ein normales Fernsehgerät, ausgestattet mit einem Btx-Decoder und einer Fernbedienung, wird z.Z. für knapp über DM 2.000 angeboten. Eine alphanumerische Tastatur für Texteingaben kostet mit dem dazugehörenden Beistelldecoder ebenfalls rund DM 2.000. Wenn nicht unbedingt eine dezentrale Druckausgabe von Ergebnissen erforderlich ist, reicht jeweils eine dieser Ausstattungen bereits für bestimmte Arten der Datenfernverarbeitung über das Btx-Netz. Die Erfahrung aus

vergangenen Jahren hat gezeigt, daß die Endpreise für Btx-Decoder und Tastatur durch Großserien in kürzester Zeit auf ein Zehntel sinken können. So ist heute schon bekannt, daß der neue Valvo-Decoder auf der Basis von VLSI-Chips die Größe einer Postkarte haben wird und für wenige hundert D-Mark im Handel angeboten werden soll.

Inwieweit die Forderung nach leichter Bedienbarkeit dieser Systeme erfüllt wird, hängt von der Ausgestaltung der Benutzerprogramme durch die Bundespost ab bzw. liegt in der Verantwortung der Teilnehmer am Btx-Rechnerverbund. In den Pilotprojekten Düsseldorf und Berlin sind bereits durchaus akzeptable Lösungen getestet worden.

Nicht übersehbar ist im Augenblick die künftige Tarifgestaltung durch die Post. Die einmalige Anschlußgebühr für ein Btx-Modem und die Zuteilung einer Systemnummer beträgt zur Zeit DM 55. Zusätzlich werden als laufende Miete acht Mark je Monat berechnet, sowie die Gebühren für einen Telefonanschluß - soweit noch nicht vorhanden - und die abzurechnenden Gesprächseinheiten im Minutentakt des Telefonnahverkehrs (etwa ab Mitte 1984). Die Entgelte für abgerufene Informationen/Dienste werden von den Anbietern bestimmt und liegen z.Z. zwischen 0,5 DPf und (theoretisch) DM 9,99 je Btx-Seite. Höhere Gebühren verlangt die Post allerdings von Informationsanbietern. Diese müssen eine sog. "Btx-Leitseite" bezahlen. Sie ist der eigentliche Zugang zu dem Btx-Dienst der Bundespost. Die Gebühren hierfür hängen davon ab, ob der Anbieter nur regional oder bundesweit im Btx-Netz seine Dienste anbieten möchte (bundesweite Leitseite/Monat DM 350). Die Entgelte für die Datenübertragung zwischen einem "Anbieter"-Computer im Btx-Rechnerverbund und der nächsten Btx-Vermittlungsstelle bzw. der Leitzentrale Ulm errechnen sich nach den Gebühren für den Datex-P-Dienst der Bundespost, sie sind also von der Menge der übertragenen Informationen abhängig. Hier ist aber nach Aussagen der Post an eine "Neugestaltung" der Tarife gedacht.

3.4.2.2.3
Beteiligung öffentlicher Stellen an den Btx-Pilotprojekten Düsseldorf und Berlin

An den Btx-Versuchsanwendungen in Düsseldorf/Neuß und Berlin haben bereits zahlreiche Behörden und sonstige Stellen teilgenommen bzw. beteiligen sich derzeit noch. Sie haben fünf Kategorien von Btx-Anwendungen angeboten:

- Informationsangebote für alle bzw. viele Btx-Teilnehmer
- Informationsangebote für "geschlossene" Benutzergruppen
- Informationsangebote für einzelne Teilnehmer
- Dialog mit Rechnern (Btx-Rechnerverbund)
- Inhouse-Anwendungen (Btx auf privaten Leitungswegen).

In der Mehrzahl wurde versucht, aktuelle Informationen bürgernah zu verbreiten und über sog. Bestellseiten eine Art (Einweg-)Kommunikation mit dem Bürger aufzunehmen. Der Btx-Benutzer konnte standardisierte Informationen ähnlich einem anzukreuzenden Fragebogen über die Zifferntasten seiner Fernseh-Fernbedienung eingeben oder, wenn vorhanden, über eine Schreibmaschinentastatur (erweiterte Btx-Tastatur) Texte frei gestalten. Mit dieser Möglichkeit können sowohl Umfragen durchgeführt wie auch schriftliche Informationen auf Anforderung zugesandt werden.

Beispiele hierfür sind:

- Informationsseiten kommunaler Presse- und Informationsämter
- Informationen der Landesregierung
- Veranstaltungskalender
- Anschriften und Zuständigkeiten von Behörden und Fachämtern
- Aus- und Fortbildungsangebote
- Kataloge (Büchereien, Museen)
- Anschriftenberichtigungen durch Bürger (Bestellseiten)
- Fahrpläne öffentlicher Nahverkehrsbetriebe
- Beratungsdienste von Polizei und Feuerwehr.

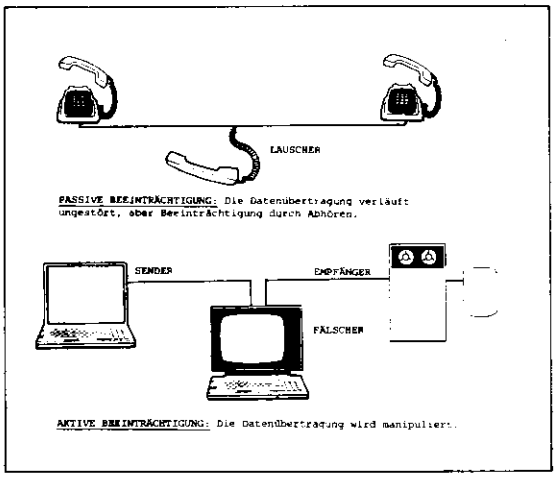
Auch aus dem Bereich der gesetzlichen Sozialversicherung und der Arbeitsverwaltung sind Versuche mit Bildschirmtext bekannt. Die Bundesversicherungsanstalt für Angestellte ist z.B. bemüht, den persönlichen Versicherungsverlauf eines Bürgers und - sofern er mindestens 55 Jahre alt ist - seine Rentenberechnung über Btx darzustellen. Sie hofft dadurch von einer Vielzahl von schriftlichen Anfragen (z.Z. etwa 450.000 im Monat) befreit zu werden. Das Bayerische Staatsministerium für Ernährung, Landwirtschaft und Forsten bietet Landwirten Informationen aus dem computergestützten "bayerischen landwirtschaftlichen Informationssystem (BALIS)" über die Btx-Zentrale Düsseldorf an. In der Praxis wurde dieses System in den Landkreisen Kaufbeuren, Landshut und Bayreuth erprobt. Bundesweit sind bereits über hundert öffentliche Stellen als Informationsanbieter im Btx-Netz.

3.4.2.3
Probleme des Datenschutzes und der Datensicherung in offenen Netzen

3.4.2.3.1
Mögliche Beeinträchtigungen des Btx-Netzes

Die Datenschutzprobleme in geschlossenen, kommerziellen Datenfernverarbeitungsnetzen und Ansätze zu deren Lösung sind hinreichend bekannt (u.a. 11. Tätigkeitsbericht, Ziff. 3.1). Im Btx-Netz erlangen sie jedoch neue Dimensionen. Seine Konzeption als offenes, d.h. jedermann zugängliches Netz erlaubt den Zugriff mit Datenverarbeitungsgeräten wie z.B. Minicomputern, deren technische Möglichkeiten allenfalls vom jeweiligen (hohen) Stand der Elektronik und dem Fachwissen des Bedieners bestimmt werden. Die physikalischen Eigenschaften des Übertragungsnetzes aber sind für den herkömmlichen Fernsprechverkehr, d.h. für die Übertragung analoger Signale konzipiert worden. Güte und Sicherheit der Datenübertragungen auf einem Übertragungsmedium wie z.B. dem Btx-Netz können durch zufällige oder systematische (physikalisch bedingte) Störungen und passive Beeinträchtigungen bzw. aktive Eingriffe beeinflußt werden. Gegen die ersteren gibt es physikalisch-technische Abhilfe wie bestimmte digitale Kodierungsverfahren oder Filtertechniken. Die bisher angewandten Sicherungsvorkehrungen gegen passive Beeinträchtigungen oder aktive Beeinflussung entsprechen aber keinesfalls den Möglichkeiten heutiger DV-Technik. Dies gilt selbst für Netze wie Datex-P, die zur digitalen Datenübertragung eingerichtet wurden.

Die Bundespost selbst sieht derzeit nach Aussage des Fernmeldetechnischen Zentralamtes keine besonderen - d.h. bisher im Fernsprechnetz nicht üblichen - Schutzmaßnahmen für das Btx-Netz vor.



Der neue Dienst "Bildschirmtext" ist besonders geeignet zum Abrufen allgemein zugänglicher Informationen aus der Btx-Zentrale. Bei der Fernabfrage dieser Daten könnten Sicherungsmaßnahmen vernachlässigt werden, soweit sie nicht den eigentlichen Netzbetrieb sicherstellen sollen. Btx erlaubt aber auch mit Hilfe einer zusätzlichen Tastatur die interaktive Datenfernverarbeitung, d.h. den Zugriff auf Daten und Programme eines externen Rechners. Für diese Art der Datenfernverarbeitung müssen die Vorkehrungen getroffen werden, die gewährleisten, daß entsprechend Art. 9 Abs. 8 des Staatsvertrages und § 10 HDSG (bzw. § 6 BDSG) der Datenschutz sichergestellt ist.

3.4.2.3.2
Zugriffssicherung

Im Bereich der Fernverarbeitung mit sensitiven Daten (z.B. der Banken) galt lange Zeit der Grundsatz, daß eine gemietete Standleitung einen höheren Schutz gegen aktive oder passive Beeinträchtigungen bietet als eine relativ offene Wählleitung, da beide Anschaltpunkte unter ständiger Kontrolle der für die Datenverarbeitung verantwortlichen Stelle sind. Erfahrungen aus den USA haben diese These widerlegt. Angriffe von "Lauschern" -sei es aus Neugier oder Spieltrieb ("Hacker") oder aus kriminellen Gründen - erfolgen in der Regel an frei zugänglichen Leitungspunkten wie Schaltkästen, Erdkabelverschlüssen oder Freileitungen bzw. im offenen Netz über beliebige Aufschaltpunkte (Telefonanschlüsse). Solange die Bundespost nicht völlig neue Netztechniken - z.B. digitalisierte Datenübertragung in optischen Leitungswegen (Glasfasertechnik) -, bei denen die Eindringschwelle für nichtautorisierte Zugriffe deutlich erhöht ist, realisieren kann, muß das Hauptaugenmerk auf die Möglichkeit der Zugriffskontrolle und vor allem auch auf die Sicherung sensitiver Datenübertragung (z.B. durch Verschlüsselungstechniken) gerichtet werden.

Dabei müssen folgende Anforderungen erfüllt werden: in einem offenen Netz muß der Absender einer Nachricht

- die Gewißheit haben, daß sie den richtigen Empfänger erreicht,
- die Zustellung beweisen können,
- daran gehindert werden, seine "Unterschrift" zu verleugnen.

Für den Empfänger muß

- der Absender eindeutig identifizierbar sein,
- der Inhalt der Nachricht authentisierbar sein,
- der Empfang einschließlich des Urhebers der Nachricht nachweisbar sein.
- Er darf aber auch keine Möglichkeit haben, den Empfang der Nachricht zu verleugnen (Quittung).

Am Beispiel eines Briefes ist dies leicht zu verdeutlichen. Der geschlossene, evtl. versiegelte Umschlag schützt die Nachricht vor Verfälschung. Die Unterschrift authentisiert den Urheber. Der Vergleich mit einer beim Empfänger oder einer neutralen Stelle hinterlegten Unterschrift (Notar) dient der Autorisierung. Die Wahl der Versendungsart, z.B. "Einschreiben mit Rückschein", stellt die Zustellung an den richtigen Empfänger und die Quittung sicher.

In Datenfernverarbeitungsverfahren geschieht die Prüfung der Authentizität heute in der Regel durch Passwort-Verfahren (PIN, Terminal-ID). Diese sind nicht immer technisch befriedigend gelöst. Erinnert sei hier an die Probleme der dezentralen oder zentralen Passwort-Vergabe, der gewollten oder ungewollten Offenbarung von Passworten - der PIN muß über das Netz gesendet werden -, um nur einige zu nennen. Die besonderen Schutz bietenden kryptographischen Verfahren dagegen bedingen den Einsatz von Ver- und Entschlüsselungsprogrammen oder speziellen Verschlüsselungsgeräten. Diese müssen - bei verschlüsseltem Datenaustausch auf den Leitungswegen - beim Anwender und im Rechenzentrum im Maschinenzugriff sein. Sie blockieren nicht unerhebliche Maschinen- und Übertragungskapazitäten, da große Rechenleistungen erbracht werden müssen. Schlüsselgeräte als Hardware-Einrichtung sind teuer und bringen u.a. Probleme des Schlüsselmanagements - d.h. alle miteinander kommunizierenden Geräte müssen über den gleichen Schlüssel verfügen - mit sich. Bei nur hundert Teilnehmern am Btx-Rechnerverbund mit etwa 10.000 Benutzern müßten z.B. eine Million persönliche Geheimzahlen oder Schlüssel verwaltet werden, wenn jeder einzelne Teilnehmer sicher sensitive Datenverarbeitung betreiben wollte. Nicht zuletzt aus diesen Gründen sind im öffentlichen Bereich, soweit es sich nicht um besonders empfindliche DV-Verfahren bestimmter Sicherheitsbehörden oder der Bundeswehr handelt, Schlüsselverfahren nicht im Einsatz.

3.4.2.3.3
Schlüsselverfahren zur Benutzeridentifikation in offenen Netzen

(1) Offene Netze, mit denen weltweite Erfahrungen vorliegen, sind das Telex-Netz und der Datenverbund der Banken SWIFT. In ihnen gelten ähnliche Verkehrsbedingungen wie im Btx-Netz. So werden z.B. Nachrichten im SWIFT-Netz, das ja dem Transfer nicht unerheblicher Geldmengen dient, mit einem internationalen Bankschlüsselverfahren abgesichert. Dies geschieht durch eine "codierte" Unterschrift. Die Banken vereinbaren bilateral die Anwendung eines geheimen Schlüsselalgorithmus (Schlüsselbuch), mit dem sensitive Inhalte der Nachrichten (z.B. Beträge, Zeit, Datum, Kontennummern u.ä.) verschlüsselt und der eigentlichen Nachricht, die im Klartext gesendet wird, als "Unterschrift" hinzugefügt werden. Der Empfänger kann dann durch Entschlüsselung die Plausibilität der Nachricht prüfen. Ein anderes, inzwischen auch im sog. Home Banking übliches Verfahren, ist die Verwendung von geheimen "Einweg"kennzahlen. Die Bank erzeugt in ihrem Rechner für jeden Kunden eine Liste von Zufallszahlen, diese wird dem Kunden auf einem sicheren Weg übersandt oder persönlich ausgehändigt und gleichzeitig als Kopie in einem Datenspeicher des Bankrechners abgelegt. Bei jeder Transaktion muß der Kunde eine neue Zufallszahl verwenden, da der Rechner einmal benutzte Zahlen in seinem Speicher löscht.

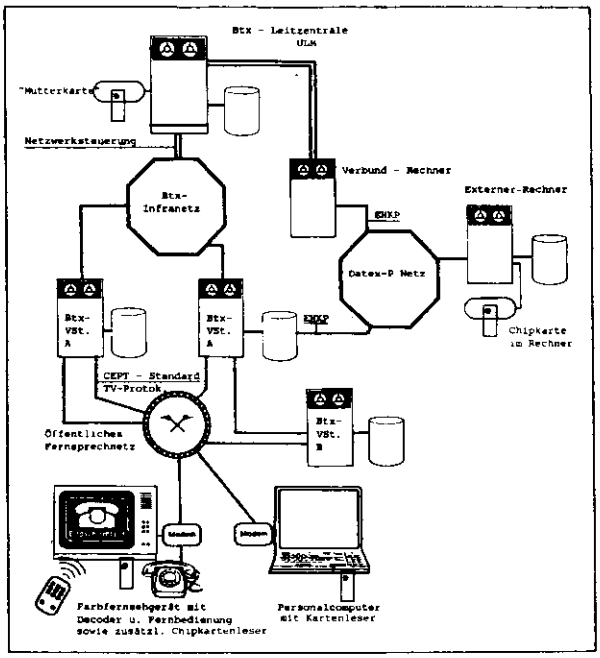
(2) Moderne Computer sind heute in der Lage, komplizierte Schlüsselalgorithmen wie z.B. den DES (American Data Encryption Standard) zu berechnen. Diese Schlüsselmethoden werden u.a. im Bankgeschäft - in den USA in den Bargeldautomaten, den Automatic Teller Machines (ATM) - verwendet, um die persönliche Geheimzahl des Kunden und die der Bank zu verschlüsseln. Die revolutionärste Entwicklung auf diesem Gebiet sind die sog. "Öffentlichen Schlüssel - Public Key". Sie bestehen aus zwei verschiedenen Teilschlüsseln, von denen einer öffentlich bekannt gemacht wird, der andere aber geheim ist. Ohne Kenntnis des geheimen Teils ist eine Rekonstruktion des Gesamtschlüssels unmöglich.

(3) Das bekannteste Beispiel eines öffentlichen Schlüssels ist der RSA-Algorithmus. Er wird auch im französischen Télétel-Versuch verwendet. Seine Stärke beruht auf der Schwierigkeit, große Zahlen zu faktorisieren, d.h. in ihre Primteiler zu zerlegen. Ohne Kenntnis der Primfaktoren ist dieser Schlüssel nicht zu brechen. Damit kann das Produkt als öffentlicher Schlüssel bekanntgemacht werden, die Faktoren sind die geheimen Schlüssel der Benutzer. Diese können dann unter Verwendung des öffentlichen Schlüssels und ihres geheimen Teils Daten/Informationen verschlüsseln, die der Empfänger auf umgekehrtem Weg mit seiner Geheimzahl entschlüsselt.

3.4.2.3.4
Alternative für das Btx-Netz: die "intelligente" Chipkarte

Die geschilderten Schlüsselverfahren bieten zwar einen vergleichsweise hohen Standard an Datensicherung, sind aber nur mit einem beträchtlichen Kostenaufwand zu realisieren. Bedenkt man, in welchem Umfang das Btx-System künftig gerade auch von der Verwaltung nicht nur als Informationsdienst, sondern auch als preiswerte Alternative zu herkömmlichen Datenfernverarbeitungsnetzen genutzt werden wird, ist die Suche nach kostengünstigeren Methoden der zuverlässigen Benutzerkontrolle, der sicheren Identifizierung geschlossener Benutzergruppen und der Verschlüsselung zwangsläufig.

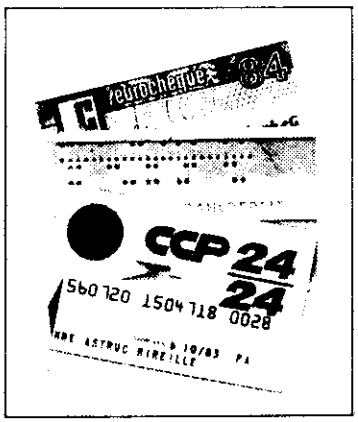
Technisch einwandfrei und preisgünstig lassen sich diese Forderungen - zumindest nach dem heutigen Stand der Erkenntnisse - auch in einem offenen Netz wie beim Bildschirmtext durch sog. "intelligente" Chipkarten lösen (dazu ausführlich der folgende Abschnitt 3.4.2.4). Sie böten außerdem die Möglichkeit, alle Zugriffe, die mit einer Chip-Karte geschehen sind, in Art eines Kontoauszugs in den Speicher der Karte zu schreiben und jederzeit durch den Besitzer ausdrucken zu lassen. Ein weiterer Vorteil wäre die "Mobilität" des einzelnen Btx-Nutzers. D.h. jedes mit einem Kartenleser ausgestattete Btx-Terminal könnte in Verbindung mit einer intelligenten Chipkarte als "eigene" Station definiert werden und wäre zur Eingabe bzw. zum Empfang oder Abruf von Daten (Mail-Box) berechtigt. Der Kartenleser könnte in den Btx-Decoder integriert werden. Der Preis für Karte und Kartenterminal wird letztlich durch die Großserie bestimmt.



CHIPKARTE IM BTX - NETZ DER BUNDESPOST

3.4.2.4
Plastikkarten als Informationsträger

Der folgende Abschnitt gibt eine ausführliche technische Darstellung der Funktionsweise und der Nutzungsmöglichkeiten von Plastikkarten als Informationsträger, insbesondere der Chipkarte. Dabei geht es nicht nur um den Aspekt der Benutzerkontrolle und der Zugriffssicherung, vielmehr zeigen die ebenfalls geschilderten in- und ausländischen Pilotversuche, welche vielfältigen Einsatzmöglichkeiten bestehen, etwa bei bargeldlosen Kartentelefonen und Warenautomaten, öffentlichen Btx-Terminals usw. Ich sehe meine Aufgabe als Datenschutzbeauftragter nicht zuletzt darin, frühzeitig über technische Entwicklungen zu informieren, die die Speicherung und Übermittlung personenbezogener Daten grundlegend verändern werden. Die massenhafte Verwendung von codierten Plastikkarten sowie vor allem der Chipkarten wird eine Vielzahl neuer - nicht nur datenschutzrechtlicher - Probleme aufwerfen, für die rechtzeitig neue Lösungen gesucht werden müssen.



3.4.2.4.1
Kartenarten

Plastikkarten als Informationsträger sind seit Jahren in vielfältigem Einsatz und erprobt (Scheckkarten von Banken, Kreditkarten, Betriebs- und Werksausweise). Ihre spezifischen Eigenschaften werden durch die Art der Informationsdarstellung auf den Karten und deren Auswertmöglichkeiten erzielt. Das Format dieser Karten ist heute in einer ISO-Norm festgelegt. Folgende Typen von Kodierungen sind dabei zu unterscheiden:

(1) **Mechanische Kodierungen**

Mechanisch kodierte Karten sind mit einer Perforation (Lochcode) oder Prägestanzung versehen. Sie können nur gelesen werden.

(2) **Optische Kodierungen**

Infrarot: Auf den Karten sind wechselnd angeordnete infrarotdurchlässige oder -sperrende Schichten angebracht. Das so erzielbare "Muster" ergibt die kodierte Information.

Ultraviolett: Die Beschichtung der Karten besitzt die Eigenschaft, daß sie bei ultravioletter Bestrahlung fluoresziert und so gelesen werden kann.

Laserkode: Bei diesen Karten werden die Informationen in Bit-Mustern aufgebracht. Ein Laserstrahl brennt winzige Vertiefungen in das Kartenmaterial ein. Die Karte kann so mit entsprechenden Geräten gelesen und beschrieben werden (Technik der Bildspeicherplatte).

Holographische Karten: Diese Kartenart wird ebenfalls durch einen Laserstrahl kodiert, wobei ein dreidimensionales Bild auf der Karte erzeugt wird. Diese Kodierung ist sehr kopiersicher und bietet viel Speicherplatz auf kleinstem Raum. Sie erfordert aber großen technischen Aufwand zum Lesen.

(3) **Magnetische Kodierung**

Magnetische Punkte bzw. magnetische Zonen: Die Speicherung der Information erfolgt in einer ferrithaltigen magnetischen Schicht, die in die Karte eingelagert ist. Diese Karte ist nur lesbar.

Magnetische Module: Das Material der Karte enthält keine magnetischen Partikel, ist aber selbst in der Lage, ein im Kartenlesegerät erzeugtes Magnetfeld so zu beeinflussen, daß Informationen dargestellt werden können.

Magnetstreifen: Dies ist die am weitesten verbreitete Form der (Scheck)karte. Die Informationen werden durch magnetisches Verändern (Beschreiben) einer Schreib-/Lesezone in der Karte gespeichert. Positionierung dieser Zone, Kodierung und die Form der Karte sind weitgehend genormt (Euroscheckkarte u.ä.).

(4) **Elektronische Karten (Smart Card/Memory Card)**

Elektronische Karten enthalten integrierte elektronische Miniaturschaltkreise mit Speicher- und Logikfunktionen - einen Chip. Sie sind selbst aktiv, d.h. sie können logische Entscheidungen treffen und sich gegen unerlaubte Zugriffe sperren. Damit unterscheiden sie sich von allen anderen Kartenarten.

Nahezu jede heute bekannte Kartenart wird z.Z. in Versuchen erprobt: Karten mit magnetischer Kodierung (Geldautomaten der Banken, Werksausweise zur Zugangskontrolle), mechanisch kodierte Karten (BANKOMAT-System), holographische bzw. infrarot kodierte Karten (z.B. Werksausweis der Farbwerke Höchst AG, Kartentelefon der Post).

Die vielfältigsten Möglichkeiten bietet nach heutigem Wissensstand die intelligente Chipkarte. Sie ist wegen der Verwendung von elektronischen Miniaturschaltkreisen am engsten mit der praktizierten DV-Technik verwandt. Alle weiteren Ausführungen beziehen sich auf diese Kartenart.

3.4.2.4.2
Die "intelligente" Chipkarte: Entwicklungsgeschichte

Patente auf Chipkarten sind seit 1968 erteilt worden. Die "intelligente" Chipkarte mit Speicher- und Logikfunktionen und Schutz gegen unbefugte Zugriffe geht auf ein Robert Moreno (Frankreich) 1974 erteiltes Patent zurück (Chip-In-Card Patents in the United States: Nilson Report Survey February 1981).

Die Chipkarten der ersten Generation hatten primär Speicherfunktionen (Transaktionsaufzeichnung). Heutige Karten (Bull, Flonic-Schlumberger, Philips) sind fähig, mittels in der Karte oder extern abgespeicherter Algorithmen Ver- und Entschlüsselungsvorgänge zu vollziehen. Im Labortest befinden sich aber auch bereits Entwicklungen, die den großen Rechenaufwand von "öffentlichen Schlüsseln" (Public Key) meistern. Zur Zeit werden Karten in Feldversuchsanwendungen verwendet, deren Speicherfähigkeit zwischen 4,5 und 16 KBit beträgt. Diese Größenordnung wird sich nach oben verschieben. Sie wird sich am Verhältnis zwischen dem zur Zeit technisch Machbaren - d.h. 128 KBit - 256 KBit auf ca. 20 qmm Fläche beim VLSI-Chip (Very Large Scale Integrated) - und dem Preis von z.Z. etwa 0,2 Pfg/Bit orientieren. Augenblicklich überwiegen die Bestrebungen, die Speicherkapazität zugunsten des Preises nicht zu verändern, da der Kartenpreis (z.B. Bull CP 8) von 13 DM/Stck bei einer Million Auflage den Anwendern noch zu hoch ist.

3.4.2.4.3
Funktionsprinzip

In einer Chipkarte werden Daten gespeichert, gelesen, verändert und Rechenvorgänge ausgeführt. Der integrierte Speicher kann je nach Funktion mit einer Schreib-/Lesesperre versehen werden, die durch eine persönliche Geheimzahl (PIN) initiiert werden kann. Ist das Schreibregister der Karte blockiert oder zerstört (z.B. infolge eines unberechtigten Zugriffsversuchs oder einer Manipulation), sind die Speicherinhalte der Karte nicht mehr veränderbar.

Das Rechenwerk der Karte kann von außen eingegebene Daten und Informationen mit eigenen Speicherinhalten vergleichen bzw. verarbeiten. Die Karte ist damit in der Lage, mit einem Terminal (Kartenleser) oder einem externen Rechner einen sicheren, d.h. verschlüsselten Dialog zu führen. Die Bausteine der Chipkarte sind heute übliche elektronische Halbleiter (RAM, ROM, PROM u.a., vgl. das Verzeichnis der Fachtermini unten 5.4). Sie sind entweder in einer monolithischen Schaltung aufgebracht (Bull CP 8) oder sie befinden sich in getrennten Schaltkreisen, die durch elektrische Verbindungen (BUS) aktiviert werden (Philips).

3.4.2.4.4
Beispiel: Die Chipkarte CP 8 von Bull (Frankreich)

Eine der vom technischen Aufbau und der Betriebssicherheit her interessantesten Chipkarten, die auch zugleich in umfangreichen Feldversuchen im Einsatz ist, ist die CP 8-Karte von Bull.

Die CP 8 enthält einen Mikroprozessor (Mikrocomputer) und Speichermedien. Alle notwendigen elektronischen Bauteile sind auf einem Substrat vereinigt (Monolith). Dies hat u.a. den Vorteil, daß in die Karte zu implantierende Verbindungsleitungen zwischen verschiedenen elektronischen Bauteilen - sie wären leichter Manipulationen ausgesetzt - entfallen.

Der Chip der CP 8-Karte enthält das Rechenwerk und die Speichereinheit, die durch verschiedene Datenpfade verbunden sind (Adressen-BUS, Daten-BUS, Steuer-BUS). Der Mikrocomputer der Karte ist so geschaltet, daß er selbständig seinen Speicherinhalt beschreiben bzw. ändern kann, ohne ein laufendes Programm zu unterbrechen (SPM - Self Programable Micro Computer). Diese Technik, die mit zwei simultan geschalteten Zugängen über zwei Register arbeitet, von denen jeweils eines gesperrt werden kann, bietet die Möglichkeit der Programmausführung in Abhängigkeit von bestimmten internen Zuständen bzw. erlaubt die Selbstzerstörung eines Programms (z.B. bei Manipulation). Externe Zugriffe zum Speicher der Karte sind nur über den Mikroprozessor möglich. Das bedeutet, er führt nicht nur alle Rechenoperationen aus, sondern kontrolliert auch alle Schreib- und Lesefunktionen im Speicher. Die vorgegebene Funktion (Programm) der Karte wird bei der Herstellung oder genauer bei Herstellung des Chips im ROM als Mikroprogramm gespeichert.

Die Zugriffskontrolle des Chips arbeitet mit drei voneinander getrennten Speicherbereichen:

(1) Geheime Zone (Secret Memory):

Sie ist gegen Zugriffe von außen geschützt. Nur der Mikroprozessor allein kann im Rahmen seines Programms auf diese Zone zugreifen. Sie enthält die Geheimzahlen und Parameter, die alle Zugriffe zu den übrigen Speicherbereichen steuern.

(2) Geschütze Zone (Confidential Memory)

Die geschützte Zone - zu ihr gehört auch der Transaktionsspeicher - ist nur über die entsprechenden Geheimzahlen, welche die Lese-und/oder Schreibvorgänge aktivieren, zugänglich. Die Plausibilitätsprüfung der von außen -z.B. über ein Terminal - eingegebenen Geheimzahlen erfolgt im Mikroprozessor der Chipkarte.

(3) Freie Zone (Free Access Memory)

Auf die freie Zone kann ohne Kontrolle von außen zugegriffen werden. Sie enthält in der Regel die Daten, die auch optisch erkennbar auf der Karte aufgedruckt sind. Dies sind z.B. Name, Anschrift des Inhabers, Kartennummer usw.

3.4.2.4.5
Dialog zwischen Karte, Kartenlesegerät und externem Rechner

Die Chipkarte funktioniert nur in Verbindung mit einer intelligenten Kartenlesestation (Terminal), einem Zentralprozessor und den Schnittstellenprogrammen zur Kommunikation zwischen speziellem Programm zur Netzsteuerung (Telepass/Btx) und den Programmen der Anwendercomputer (externe Rechner).

Die elektrische Verbindung des Kartenchips mit dem Terminal wird durch 8 Kontakte im Kartenleser hergestellt. Der Datenaustausch zwischen Karte, Terminal und Host-Rechner erfolgt nach dem System der offenen Netzarchitektur, d.h. er entspricht in etwa dem Aufbau des "ISO-7-Schichten-Modells" (EHKP). Bei den heutigen Versuchsanwendungen sind aber noch nicht alle Protokollebenen enthalten. Die an den Pilotprojekten beteiligten Hersteller fordern rechtzeitige Absprachen über eine Norm, welche die Kompatibilität der verschiedenen Kartenterminals sicherstellen soll.

Aus der Sicht des Datenschutzes stellt sich hier z.B. die Frage, ob mit diesem neuen "technischen Zwang" nicht wieder Rahmenbedingungen geschaffen werden, die unter bestimmten Bedingungen umfassende Datenverknüpfungen erlauben, die dann zu Effekten führen, wie sie die Datenschutzbeauftragten am Beispiel des maschinenlesbaren Bundespersonalausweises aufgezeigt und kritisiert haben (s. Ziff. 3.1).

3.4.2.4.6
Sicherheitsfunktionen

Eine Schwachstelle in offenen Netzen der Datenfernverarbeitung ist der Austausch von unverschlüsselten Authentisierungsmerkmalen (PIN, Passwort, Terminal-Id) über das Netz. Durch passive Beeinträchtigung können diese Merkmale abgehört und von einem anderen Datenendgerät aus unbefugt verwendet werden. Eine denkbare Lösungsmöglichkeit wurde oben bereits geschildert, der Austausch von Listen mit Einweg-Geheimzahlen (s. Ziff. 3.4.2.3.3). Die folgende Lösung ist technisch eleganter:

1. Im Host-Rechner wird eine Zufallszahl E erzeugt und an das Terminal des Teilnehmers übermittelt.

2. Der Teilnehmer wird nun aufgefordert, seine Geheimzahl einzugeben, die das Terminal mit einem in ihm festverdrahteten Algorithmus verschlüsselt (Black Box). Das Ergebnis wird zurück zum Host-Rechner übermittelt.

3. In der Zwischenzeit hat der Host-Rechner, der über den gleichen Algorithmus verfügt und die Geheimzahl des Teilnehmers gespeichert hat, die Rechnung des Terminals nachvollzogen. Ergibt der Vergleich des gesendeten Schlüssels mit der errechneten Zahl eine Übereinstimmung, dann ist der Teilnehmer eindeutig identifiziert. Da der Host ständig neue Zufallszahlen erzeugt, wird auf dem Netz für einen unbefugten Lauscher nie eine verwendbare Identifikation gesendet.

Preiswerte elektronische Miniaturbausteine (Zufallsgenerator), die in einem Chip integriert diese Funktion ausführen, sind bereits im Handel (MUX-Generator z.B. der Fa. RACAL MILCO). Eine Schwachstelle hat jedoch auch diese Lösung. Der Betreiber des Host-Rechners kennt alle Geheimzahlen der Teilnehmer am Rechnerverbund und der Diebstahl einer "Black Box" würde das gesamte Sicherheitssystem sprengen. Interne Manipulationen sind also nicht auszuschließen.

Diese Sicherheitslücke schließt sich durch die Verwendung intelligenter Chipkarten. Die Karte ist Träger der Informationen "Geheimzahl" und "Algorithmus" und führt den Rechenvorgang in ihrem integrierten Mikroprozessor aus. Es werden also keine sicherheitsempfindlichen Daten über das Leitungsnetz gesendet, sondern lediglich ein verschlüsseltes Ergebnis in Form einer numerischen Zeichenfolge. Auch beim Host-Rechner sind diese verarbeiteten Informationen nicht gespeichert, sondern befinden sich in einem gesonderten Geräteteil, der als eine Art intelligentes Terminal dem Rechner vorgeschaltet ist.

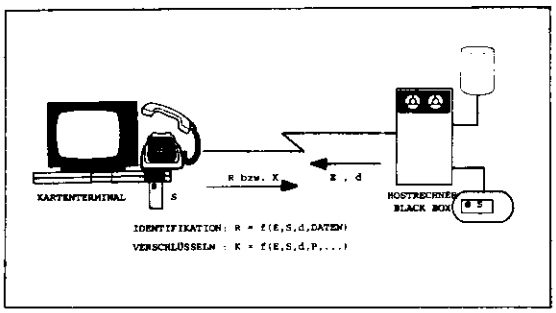
3.4.2.4.7
Beispiel eines Dialogs Karte ./. Host-Rechner

Im geheimen, d.h. zugriffsgeschützten und nicht löschbaren Speicherbereich der Chip-Karte sind folgende Informationen enthalten:

f : Algorithmus des Rechenvorgangs
S : Geheimzahl der Karte
P : sonstige geschützte Parameter

Der Mikroprozessor der Karte kann zwei Rechenvorgänge darstellen:

1. **Identifizierung/Authentisierung**
   R = f (E, S, d, Daten)
2. **Verschlüsselung**
   K = f (E, S, d, P, Daten)



IDENTIFIZIEREN UND SCHLÜSSELN MIT DER CHIP - KARTE

Der Identifizierungsvorgang läuft wie folgt ab: Wird eine Chip-Karte in ein Kartenterminal gesteckt, vergleicht das Terminal die Information seines Datenspeichers mit den Informationen, die der Kartenprozessor nach der Formel 1 liefert. Bei Übereinstimmung fordert es den Host-Rechner auf, eine Zufallszahl E und die Dialognummer d zu senden (Polling). Die Chip-Karte bildet die Funktion f und sendet die Identifikation R bzw. das Schlüsselprodukt K. Im Host-Rechner befindet sich ebenfalls ein Kartenterminal in Form einer "Black Box", das eine Chip-Karte einer höheren Hierarchiestufe enthält, die sog. "Mutterkarte". Hier wird das Produkt R oder K wieder zurückgerechnet und die Daten erst dann an den eigentlichen Rechner übergeben.

3.4.2.4.8
Sicherheitsprinzip der Schaltung

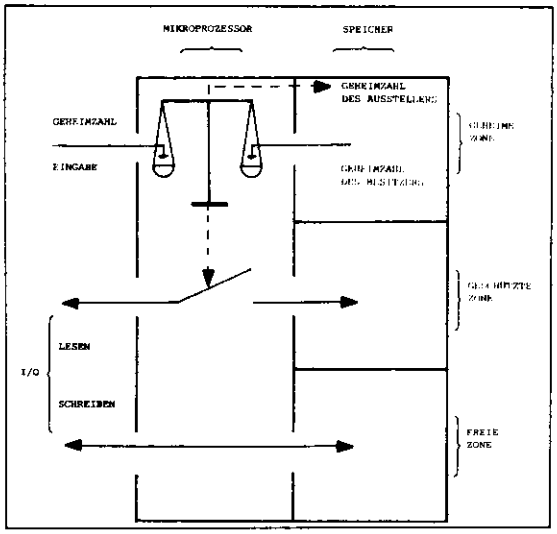
Die Chipkarten sind aufgrund ihrer Konstruktion weitgehend sicher vor Fälschung und Manipulation, d.h.

- Duplizierung
- Veränderung
- Imitation (die Karte wird dem Kartenterminal durch ein Mikrocomputerprogramm vorgetäuscht)
- Simulation (Karte und Kartenterminal werden dem Rechner gegenüber durch das Programm eines Minicomputers "simuliert").

Das Kopieren von Chipschaltkreisen ist nutzlos, da ihre Funktion, d.h. die Schreib-/Lesevorgänge, nicht auslesbar sind. Die Speicherinhalte ihrerseits wären nur unter Inkaufnahme der Zerstörung dieses gesamten Bauteils z.B. durch Röntgenstrahlung änderbar. In mit Kunstharz vergossenen Chips sind auch unter dem Röntgenschirm oder elektronischer Vergrößerung bestenfalls Bitmuster zu erkennen, nicht aber deren Zuordnung. Die Simulation oder Imitation (s.o.) erfordert einen ungeheuren technischen Aufwand, dem zudem durch spezielle Vorrichtungen am Kartenterminal - z.B. mechanische und elektrische Sicherung des Kartenschlitzes - begegnet werden kann (Tamperproofing).

3.4.2.4.9
Zugriffssicherheit zum Speicher der Chipkarte

Zugriffe zu den Speicherbereichen einer Chipkarte sind nur über den integrierten Mikroprozessor möglich. Dieser wird allein von dem bei der Kartenherstellung im ROM abgelegten Programm gesteuert. Die Zugriffssicherung zum Chipkartenspeicher arbeitet mit Informationen, die sich in den geheimen oder geschützten Zonen des Kartenspeichers befinden. Nur nach Eingabe der Geheimzahl - oder bei multifunktionalen Karten mehrerer Geheimzahlen durch den Benutzer - ist es dem Mikroprozessor möglich, auf den geheimen Speicherbereich zuzugreifen.



ZUGRIFFSKONTROLLE ZU DEN SPEICHERBEREICHEN
(BULL CP8 - KARTE)

Der Sicherheitsmechanismus der Karte beruht also im Grunde auf dem Erkennen der Identität des Kartenbenutzers. Da die Geheimzahl des Benutzers und die des Kartenausstellers voneinander getrennt in der geheimen Zone des Kartenspeichers abgelegt sind, ist ein gegenseitiges Auslesen unmöglich. Der Benutzer kennt nicht den Geheimcode des Ausstellers und umgekehrt. Die notwendige Korrelation zwischen beiden Geheimzahlen kann nur der Mikroprozessor in der Karte vornehmen. Die Karte gibt ihr "Geheimnis" also nie preis.

Vor jedem Schreib-/Lesevorgang erfolgt eine Kontrolle des eingegebenen PIN mit der Geheimzahl in der Karte. Diese Kontrolle wird durch Zerstörung (Ausbrennen) eines Bits in einem Zählregister der Karte (Transaktionsspeicher) unlöschbar gespeichert. Die Eingabe eines falschen Benutzer-PIN hat die Selbstblockade der Karte nach dem dritten Versuch zur Folge. Versuch und Blockade werden ebenfalls in einem Register gespeichert. Diese Blockade der Karte kann durch die gleichzeitige Eingabe von Benutzer-PIN und Aussteller-PIN im Terminal des Kartenausstellers aufgehoben werden. Die Eingabe und Kontrolle der Aussteller-Geheimzahl erfolgt sofort bei der maschinellen Ausstellung der Karte. Jeder weitere externe Zugriffsversuch auf diese Geheimzahl führt zur augenblicklichen Zerstörung der Karte. Nach Eingabe der einzelnen Geheimzahlen bei Ausgabe der Karte an den Benutzer werden die entsprechenden Speicherstellen durch Änderung des Adressregisters "verriegelt" (Speicherschutz).

3.4.2.4.10
Funktionsunfähigkeit

Die Funktionsunfähigkeit der Chipkarte ist zugleich ein Element der Sicherheit. Sie kann durch interne und externe Ereignisse ausgelöst werden, und zwar durch:

- Ablauf der Gültigkeitsdauer
- Speicherüberlauf (alle Transaktionen sind verbraucht, d.h. Bits ausgebrannt)
- Selbstblockade der Karte infolge Manipulation.

3.4.2.5
Pilotprojekte mit intelligenten Chip-Karten

Die bekannt gewordenen Pilotprojekte mit intelligenten Chipkarten konzentrieren sich in ihrer Aufgabenstellung auf die speziellen Fähigkeiten dieses Kartentyps, nämlich Logik- und Speicherfunktionen. Erprobt werden die sichere Benutzeridentifikation, Transaktionszählung und bargeldlose Dienste:

- Home-Banking
- Bank(Geld)automaten (ATM)
- Point of Sale (POS)
- Videotex
- Kartentelefon

3.4.2.5.1 In der Bundesrepublik Deutschland

Fast alle Versuche mit Kassenterminals (POS) und Bankanwendungen (ohne Home-Banking) basieren in der Bundesrepublik zur Zeit noch auf der Euroscheckkarte mit Magnetzone nach ISO-Norm. Diese Karte ist fälschungsanfällig, die Datenübertragung zwischen Karte und Terminal, Terminal und Hostrechner muß durch Schlüsselgeräte oder Schlüsselprogramme gesichert werden.

In den meisten größeren Städten sind isolierte Versuchsanwendungen einzelner Banken und Sparkassen mit Geldautomaten installiert. Weitergehende Überlegungen zum Einsatz von (Chip)Karten auf Netzen zur Nutzung der erwähnten Dienste sind vorläufig nur in ersten Ansätzen zu sehen. Die Bundespost als Träger des Bildschirmtextdienstes hat zwei Studien über die Verwendungsmöglichkeiten von Chipkarten im Btx-Netz und anderen Postdiensten in Auftrag gegeben. Diese Studien sind bereits fertiggestellt und abgeliefert (OPTIMA, Frankfurt am Main und SCS, Hamburg). Sie plant in den Jahren 1984/85 Versuche im Raum Bonn/Aachen und in München mit Chipkarten-Telefonen und Btx-Anwendungen. Ab Ende 1984 wird der Deutsche Bankenverband einen bundesweiten POS-Versuch im Online-Verfahren über eine "Autorisierungszentrale" in Frankfurt am Main starten. Dezentrale Prüfungseinrichtungen in den Kassenterminals sind bei diesen Versuchen wegen der Kosten nicht vorgesehen.

Mir ist aber auch bekannt, daß eine Bankengruppe im süddeutschen Raum dabei ist, ein regionales Pilotprojekt mit der intelligenten Chipkarte vorzubereiten. Dabei sollen auch Funktionen der Zugriffs- und Speicherkontrolle getestet werden.

3.4.2.5.2
Im Ausland

Im Ausland laufen zahlreiche POS-Anwendungen und Versuche mit entgeltpflichtigen Diensten privater und öffentlicher Anbieter. Der Schwerpunkt dieser Versuche konzentriert sich ebenfalls auf Identifizierung und Bonitätsprüfung baldgeldlos zahlender Kunden. Die umfangreichsten europäischen Pilotprojekte mit Chipkarten laufen seit 1978 in Frankreich.

(1) **Télétel 3 V**

Nach Festlegung der ersten Normen für den französischen Videotex erfolgte 1978 die Entscheidung der Direction Générale de Télécommunication (DGT), ein Pilotprojekt durchzuführen. Es erhielt den Namen "Télétel 3 V" und findet bei 3000 Familien im Raum Vélizy, Versailles, Val de Bièvres statt. Télétel ist ein Programmpaket, welches hauptsächlich der Identitätsprüfung, Authentisierung und Transaktionsspeicherung dient. Im Rahmen dieses Versuchs werden Home-Banking, POS und andere Bildschirmtext (Videotex)-Anwendungen getestet.

(2) **Kartentelefon**

Die französische Post betreibt augenblicklich Versuche mit Nicht-nachladbaren Chip-Telefonkarten (Wegwerf-Karten bzw. Prepaid Card). Der Benutzer erwirbt die Karte, die über einen entsprechenden Wert ausgestellt ist, bei der Post. Das Kartentelefon bucht je nach Gesprächsdauer die Gesprächseinheiten aus dem Kartenspeicher ab, d.h. der Speicher wird durch Ausbrennen von Bitadressen nach und nach geleert. Das Projekt "Kartentelefon" wurde im Juni 1983 in Lyon und Blois begonnen und im November 1983 auf Marseilles und Paris ausgedehnt. Im Frühjahr 1984 wird noch Lille einbezogen. Bis Ende 1984 sollen 3000 Kartentelefone in Betrieb sein, zu denen 1,5 Millionen Karten im Umlauf sind.

Ab 1984 wird die Chip-Karte in Norwegen im Videotex-Netz erprobt.

Zusammenfassend ist zu sagen, daß die Probleme und deren Lösungsansätze, wie sie sich in ausländischen Pilotprojekten darstellen, auf den Bereich des Bildschirmtextdienstes der Bundespost - evtl. mit entsprechenden Modifikationen - übertragbar sind. Welche Kartentechnik sich letzten Endes durchsetzen wird, ist noch nicht abzusehen.

(Die Darstellungen in diesem Abschnitt 3.4.2 beruhen u.a. auf der Auswertung von Informationsmaterial der Bundespost, der Firmen Bull, Crouzet, Intelmatique France und Siemens sowie der Carl Cranz-Gesellschaft.)

4. Beispiele und Erfahrungen

4.1
Aktenarchive und Zugang für die Forschung - neue Fälle

Die Behinderung der zeitgeschichtlichen Forschung in Hessen durch fehlende archivgesetzliche Bestimmungen (vgl. dazu ausführlich 10. Tätigkeitsbericht, Ziff. 3.2 und 11. Tätigkeitsbericht, Ziff. 2.3) ist auch in diesem Jahr

wieder deutlich zu Tage getreten. Besonders gut läßt sich dies zeigen an dem Forschungsprojekt "Die Heil- und Pflegeanstalt Hadamar von 1933 bis 1945", das zum Ziel hat, die unter dem Nazi-Regime als Euthanasie bezeichnete Tötung "lebensunwerten Lebens" näher zu untersuchen. Gleiches gilt für ein Projekt der Gesamthochschule Kassel, das unter anderem auch die Geschichte der Juden und anderer politisch Verfolgter in einer hessischen Region unter dem Nationalsozialismus zu klären beabsichtigt. Während im ersten Fall alle beteiligten Landesinstitutionen wie auch der Hessische Datenschutzbeauftragte bemüht waren, das Forschungsprojekt im Rahmen des geltenden Rechts zu ermöglichen, wird im zweiten Fall durch den Hessischen Minister des Innern und den Hessischen Sozialminister der Zugang zu Entschädigungsakten unter Berufung auf das Aktengeheimnis und den Datenschutz verweigert.

4.1.1
Forschungsprojekt "Die Heil- und Pflegeanstalt Hadamar von 1933 bis 1945" der Fachhochschule Frankfurt am Main

4.1.1.1
Anonymisierte Dokumentation

Beim Forschungsprojekt der Fachhochschule Frankfurt ging es in einer ersten Phase zunächst darum, Krankenakten und Krankenregister (Hauptkrankenverzeichnisse und Sterberegister), die in einem Keller des Landeskrankenhauses Hadamar lagerten, zu ordnen und nach bestimmten Kriterien zu erschließen. Diese historischen Quellen sollten für eigene Zwecke der Klinik wie auch für externe Forschung zugänglich und verwertbar gemacht werden. Nach dem mir vorliegenden Forschungsdesign wird für jede Krankenakte bis 1945 eine Karteikarte angelegt, die die Akten nach Datenbereichen und Klassifikationen erschließt. Die Karteikarten selbst enthalten keine unmittelbaren Identifikatoren (wie z.B. Name und ursprüngliche Adresse des in die Anstalt eingelieferten Patienten), sondern lediglich eine Code-Nummer, die auch auf die jeweils zugeordnete Krankenakte übertragen wird. Auf diese Weise wird sichergestellt, daß die Karteikarte nur solche Angaben enthält, die unter Berücksichtigung aller Umstände, insbesondere auch der seither vergangenen Zeit von -rechnet man das Kriegsende- mindestens 38 Jahren, eine Reidentifikation einzelner Insassen bzw. Opfer des "Euthanasie-Programms" wenig wahrscheinlich machen. Die Akten werden zudem im Krankenhaus selbst durch eigens zu diesem Zweck eingestellte Hilfskräfte -allerdings nach den Vorgaben des Forschungsprojekts - aufbereitet. Außerhalb des Krankenhauses sollen keine Krankenakten ausgewertet werden. Geplant ist eine automatisierte Verarbeitung derjenigen Daten, die auf den Karteikarten enthalten sind, wobei die Einzelheiten in der Implementationsphase noch festgelegt werden müßten.

Das in den Karteikarten aufbereitete und dann klassifizierte Datenmaterial soll der Ziehung von Stichproben bestimmter Populationen dienen und für quantitative statistische Analysen zum Zwecke der Hypothesenbildung für die zweite Phase des Forschungsprojekts aufbereitet werden.

Da die Erschließung der Krankenakten bzw. der Aufbau einer historischen ärztlichen Dokumentation im Landeskrankenhaus Hadamar mit ärztlichem Hilfspersonal erfolgt, sind weder die ärztliche Schweigepflicht noch der Datenschutz tangiert, wenn zugleich darauf geachtet wird, daß die dabei beschäftigten Personen auf das Datengeheimnis verpflichtet und angemessene Datensicherungsmaßnahmen getroffen sind. In diesem Zusammenhang ist auch die Absicht des ärztlichen Leiters hervorzuheben, die erschlossenen Krankenakten zunächst im zentralen Krankenblattarchiv aufzubewahren, bevor sie dann - wie von mir vorgeschlagen - an das Hessische Staatsarchiv abgegeben werden, auch wenn nach wie vor Zweifel an dem Bestehen einer Rechtsgrundlage für eine Abgabe an das Staatsarchiv bestehen, sofern die Daten der ärztlichen Schweigepflicht unterliegen. Eine Übermittlung von Daten mit Personenbezug an die Hochschule findet in dieser Phase des Forschungsprojekts nicht statt, da die codierten Karteikarten als faktisch anonymisiert anzusehen sind. Ich habe daher auch dem Hessischen Sozialminister mitgeteilt, daß aus der Sicht des Datenschutzes grundsätzlich keine Bedenken bestehen, soweit es diesen Abschnitt des Forschungsvorhabens angeht.

4.1.1.2
Informationsanspruch der Wissenschaft und Akteneinsicht

Zweifellos schwieriger zu beurteilen ist die zweite Phase des Forschungsprojekts, in der eine qualitative Analyse der Krankenakten unter dem allgemeinen Gesichtspunkt der "Euthanasie" geplant ist. Dazu ist es notwendig, den am Forschungsprojekt beteiligten Mitarbeitern Einblick in die Krankenakten zu gewähren. Die Einsicht von Außenstehenden in medizinische Unterlagen stellt immer die Frage nach der Wahrung des ärztlichen Berufsgeheimnisses.

Nun ist zweifellos richtig, daß die ärztliche Schweigepflicht auch den Tod von Patienten überdauert, anders als das Datenschutzgesetz, das nur auf lebende Personen anwendbar ist. Diesem auch verfassungsrechtlich geschützten postmortalen Persönlichkeitsrecht der Insassen bzw. Opfer der Euthanasie steht die grundrechtlich positivierte Wissenschafts- und Forschungsfreiheit gegenüber. Dieses Grundrecht des Art. 5 Abs. 3 GG bedeutet nicht nur eine Absage an staatliche Eingriffe in den Eigenbereich der Wissenschaft, es schließt nach Auffassung des Bundesverfassungsgerichts vielmehr das Einstehen des Staates, der sich als Kulturstaat versteht, für die Idee einer freien Wissenschaft und seine Mitwirkung an deren Verwirklichung ein und verpflichtet ihn, sein Handeln positiv danach

einzurichten (vgl. BVerfGE 35, 114 f.). Einschränkungen der Wissenschaftsfreiheit sind danach nur aus der Verfassung selbst herzuleiten. Die durch die Rücksichtnahme auf kollidierende Verfassungswerte notwendig werdende Grenzziehung oder Inhaltsbestimmung kann nicht generell, sondern nur im Einzelfall durch Güterabwägung vorgenommen werden. Dazu folgende Aspekte:

Forschungsziel ist in diesem Fall die Analyse der sog. Euthanasie der NS-Zeit am Beispiel der Heil- und Pflegeanstalt Hadamar. Die ärztlichen Unterlagen sind mindestens 38 Jahre alt (s.o.) und seither nicht mehr gebraucht worden. Nach Ziff. 5.9 des Gemeinsamen Erlasses der Landesregierung betreffend Aufbewahrungsbestimmungen für Akten und sonstiges Schriftgut der Dienststellen des Landes Hessen vom 10. August 1978 (StAnz. 35/1978, S. 1706) können solche Akten nach 10 Jahren Aufbewahrungszeit im psychiatrischen Landeskrankenhaus an ein staatliches Archiv abgegeben werden. Hätten sich die Akten in einem Staatsarchiv befunden, könnten sie heute nach Maßgabe der Benutzungsordnung für die Hessischen Staatsarchive ausgewertet werden. Gleiches gälte für eine Aufbewahrung der Akten im Bundesarchiv. Aber sie könnten auch dort nur genutzt werden unter Rückgriff auf eine Güterabwägung auf Verfassungsebene. Denn die Benutzungsordnung kann als Verwaltungsvorschrift die gesetzlichen Vorschriften über die ärztliche Schweigepflicht nicht verdrängen.

Diese rechtlichen Schwierigkeiten belegen erneut die gebotene Notwendigkeit einer Archivgesetzgebung. Nur Archivgesetze im Bund und in den Ländern könnten in solchen Fällen sowohl das allgemeine Persönlichkeitsrecht der Betroffenen wie auch die Forschungsfreiheit effektiv und bestimmbar gewährleisten. Andererseits kann und darf die Untätigkeit des parlamentarischen Gesetzgebers die Forschung angesichts ihrer grundrechtlichen Verbürgung nicht verhindern.

Legt man daher der hier vorzunehmenden Güterabwägung die Maßstäbe der "Mephisto"-Entscheidung des Bundesverfassungsgerichts (BVerfGE 30, 194 f.) zugrunde, dann kommt man zu dem Schluß, daß die Menschen, um die es hier geht, in ihrer auch nach dem Tode gewährleisteten Menschenwürde durch das Forschungsprojekt nicht verletzt werden. Im Gegenteil: Die Aufklärung des historischen Geschehens "Euthanasie" kann die Menschenwürde ihrer Opfer nicht beeinträchtigen; sie verhindert vielmehr kollektive Verdrängung und stellt durch die Auseinandersetzung mit der nationalsozialistischen Vergangenheit Achtung vor dem psychisch kranken bzw. dem als solchen etikettierten Menschen erst her.

4.1.1.3
Die Grenzen der ärztlichen Schweigepflicht

In diesem Kontext ist daher fraglich, ob die Normen der ärztlichen Schweigepflicht auch auf solche Fälle zutreffen, in denen gar nicht beabsichtigt ist, den psychisch Kranken zu behandeln, sondern seine physische Vernichtung von vorneherein eingeplant ist. Schließlich ist nach ständiger Rechtsprechung geschütztes Rechtsgut des § 203 Abs. 1 Ziff. 1 StGB das "allgemeine Interesse an einer funktionsfähigen ärztlichen Gesundheitspflege", die ohne ein vertrauensvolles Verhältnis zwischen Arzt und Patient nicht möglich ist. Dieses - für die ärztliche Schweigepflicht konstitutive - Vertrauensverhältnis zwischen Arzt und Patient hat aber in den Fällen der "Euthanasie" nicht oder nur zum Teil bestanden. Entfällt die unmittelbare Anwendung der Vorschriften über die ärztliche Schweigepflicht aus diesem Grunde im Einzelfall, so tritt an deren Stelle das allgemeine Persönlichkeitsrecht (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG) bzw. der postmortale, durch die Verfassung gewährte Persönlichkeitsschutz der Patienten, der nach wie vor auch von den Forschern im Hinblick auf eventuelle Publikationen zu beachten ist. Akten noch lebender Patienten können daher nur mit Einwilligung der Betroffenen ausgewertet werden. Dagegen werden die Handlungen von Ärzten als Amtsträgern und Mittätern im Rahmen der "Euthanasie" durch das allgemeine Persönlichkeitsrecht oder gar das ärztliche Berufsgeheimnis nicht geschützt.

Im Ergebnis halte ich daher bei Wahrung strengster Vertraulichkeit personenbezogener Daten von Betroffenen auch die qualitative Aktenanalyse durch Wissenschaftler für zulässig. Die institutionellen Rahmenbedingungen müssen jedoch sicherstellen, daß sowohl die organisatorischen und technischen Maßnahmen der Datensicherung getroffen sind als auch die Verpflichtung der Beteiligten auf das Datengeheimnis und die ärztliche Schweigepflicht vorgenommen wird. Dazu gehört insbesondere, daß keine Krankenakte außerhalb des Krankenhauses ausgewertet wird. Darüber hinaus habe ich alle Beteiligten auf die strenge Zweckbindung der Auswertung durch die konkrete Zielsetzung des Forschungsprojekts hingewiesen.

4.1.2
Forschungsprojekt "Juden im Nationasozialismus"
Freigabe von Entschädigungsakten

Aufgrund ähnlicher Überlegungen habe ich dem Hessischen Sozialminister mitgeteilt, daß ich eine Freigabe von Entschädigungsakten für das Forschungsprojekt "Juden im Nationalsozialismus" der Gesamthochschule Kassel im Grundsatz für rechtlich möglich halte. Dies allerdings nur deshalb, weil auch hier die Untätigkeit des Gesetzgebers nicht zur Verhinderung verfassungsmäßig verbürgter wissenschaftlicher Forschung führen darf und kann. In diesem Zusammenhang ist auch die mangelnde Initiative des sowohl für Forschungs- wie für Archivfragen zuständigen Hessischen Kultusministers besonders zu bedauern.

Der Konflikt, der gerade für die zeitgeschichtliche Forschung bezeichnend ist, läßt sich auch an diesem Beispiel einfach beschreiben: Diejenigen Akten und personenbezogenen Unterlagen, in die Einsicht durch Institutionen der wissenschaftlichen Forschung begehrt wird, unterliegen einer gesetzlichen Geheimhaltungsbestimmung, im vorliegenden Fall dem § 30 Hessisches Verwaltungsverfahrensgesetz (HVwVfG) in Verbindung mit § 203 StGB. Dem steht ein verfassungsrechtlich zugesicherter Informationsanspruch der Wissenschaft gegenüber, der sich unmittelbar nur aus dem Grundgesetz selbst ableiten läßt. Es verwundert allerdings nicht, daß dieser letzte Gesichtspunkt bei der Konferenz der Entschädigungsreferenten der Länder, die die Aktenfreigabe generell abgelehnt hat, keine Erwähnung gefunden hat. Denn der einfache Gesetzgeber hat zwar die Geheimhaltung, nicht aber den Informationszugang gesetzlich geregelt.

Diese Situation hat schon wiederholt zu negativen Entscheidungen hessischer Behörden zu Lasten historischer Forschung geführt, da eine verfassungskonforme Auslegung bzw. Begrenzung der Geltungsdauer von Geheimhaltungsnormen in der Regel nicht riskiert wird und von den Verwaltungsgerichten im Falle eines Rechtsstreits möglicherweise auch nicht akzeptiert werden würde. All dies befreit aber nicht von der Überlegung, wie lange denn Geheimhaltungsbestimmungen wie z.B. § 30 HVwVfG auch nach dem Tod der Betroffenen Gültigkeit haben sollen. Würde man in dieser Frage dem Beschluß der Konferenz der Entschädigungsreferenten folgen, könnte die Unzugänglichkeit der Aktenbestände unbegrenzt dauern, jedenfalls so lange bis eine gesetzliche Regelung, etwa ein Informationsfreiheitsgesetz oder eine Archivnorm, die Geheimhaltung relativieren und den Datenzugang eröffnen würde. Ein solches Ergebnis wäre nicht verfassungskonform, da es das legitime Informationsinteresse der Wissenschaft nicht hinreichend berücksichtigt. Die einzige Möglichkeit, unter den genannten Umständen einen Aktenzugang zu gewähren, ist der Weg über eine verfassungskonforme Auslegung des Tatbestandsmerkmals der "unbefugten Offenbarung" in § 30 HVwVG. Maßstab ist auch in diesem Fall das Grundrecht des Art. 5 Abs. 3 GG, das nach ständiger Rechtsprechung die Verpflichtung des Staates, für eine freie Wissenschaft einzustehen und sein Handeln positiv danach einzurichten, einschließt (s.o.).

Absolute Verdikte des Zugangs zu Behördenakten sind daher aus meiner Sicht mit der Verfassung unvereinbar. Dabei habe ich stets betont, daß die Einwilligung der Betroffenen für die Einsichtnahme in Akten in jedem Fall dann einzuholen ist, wenn es sich um noch lebende Personen handelt. Eine Stellungnahme des Hessischen Sozialministers bzw. des Hessischen Kultusministers zu diesem Problem liegt bis heute nicht vor.

4.1.3
Projekt "Alltag im Nationalsozialismus"

Die geschilderten Probleme vervielfachen sich im kommunalen Bereich, wo unter der Schirmherrschaft des Bundespräsidenten Schulen und Schüler motiviert werden sollen, sich im Rahmen des Projekts "Alltag im Nationalsozialismus" mit der Geschichte des Nationalsozialismus in der eigenen Umgebung auseinanderzusetzen, und zwar anhand historischer Quellen, statt sich mit Sekundärdarstellungen zu begnügen.

Viele Eingaben weisen auf die zumeist unklare Rechtslage bei kommunalen Archiven hin. Der weitaus größte Teil der kommunalen Körperschaften besitzt weder eine Archivsatzung noch eine Benutzungsordnung. Zugang zu und Einsicht in archivierte Unterlagen hängen daher häufig eher vom Ermessen eines Stadtarchivars, von subjektiven Einstellungen und Erwägungen gegenüber Forscher und Erforschten ab als von rechtlich fundierten Argumenten.

Diese Rechtsunsicherheit führt immer wieder zu aus meiner Sicht unverständlichen und auch ermessensfehlerhaften ablehnenden Entscheidungen, die wenig davon spüren lassen, daß auch und gerade die Geschichte einer Stadt oder Gemeinde eine "öffentliche Angelegenheit" ist, was für den Bürger einen Zugang zu den historischen Quellen einschließt. Auch stellt es einen Widerspruch zu allen Bemühungen dar, den Stellenwert der Geschichte im Gemeinschaftskundeunterricht bzw. des Geschichtsunterrichts zu verbessern, wenn interessierten Schülern die Einsicht in Quellenmaterial verschlossen bleibt.

4.2
Bezug von Sozialhilfe durch Ausländer - Meldung an die Ausländerbehörden

4.2.1
Ausweisungsgefahr bei Sozialhilfebezug - Änderung der Rechtslage

Eine Reihe von Kommunalpolitikern und Ausländerinitiativen hat mich um die Prüfung gebeten, ob die Praxis von Sozialämtern zulässig sei, diejenigen Ausländer an die Ausländerbehörde formular- oder listenmäßig zu melden, die Sozialhilfe beziehen. Sie kritisierten, daß dadurch der Schutz des Sozialgeheimnisses bei Ausländern weniger greife als bei deutschen Leistungsempfängern. Hintergrund dieser Mitteilungen ist die Vorschrift des § 10 Abs. 1 Nr. 10 Ausländergesetz (AuslG), die es erlaubt, einen Ausländer auszuweisen, wenn "er den Lebensunterhalt für sich und seine unterhaltsberechtigten Angehörigen nicht ohne Inanspruchnahme der Sozialhilfe bestreiten kann oder bestreitet". Diese Bestimmung ist in den letzten Jahren zum einen durch die insgesamt verschärfte Ausländerpolitik, zum anderen durch den sprunghaften Anstieg der Ausgaben für die Sozialhilfe bei schlechter Haushaltslage

der Kommunen in das Blickfeld behördlichen Interesses gerückt. Wieviele Betroffene tatsächlich ausschließlich oder auch wegen des Bezugs von Hilfen zum Lebensunterhalt ausgewiesen wurden oder sonstige ausländerrechtliche Maßnahmen (z.B. Nichtverlängerung der Aufenthaltserlaubnis) zu gewärtigen hatten, ist nicht bekannt; doch werden in der Presse sowie durch Ausländerinitiativen immer wieder solche Fälle berichtet.

Mit dem Inkrafttreten des SGB X (2. Kapitel) am 1. Januar 1981 mit seinen Bestimmungen über den Schutz der Sozialdaten wurde klargestellt, daß diese Mitteilungspraxis von den Sozial- an die Ausländerämter nicht zulässig war. In §§ 67 ff. SGB X hat der Gesetzgeber, um das Sozialgeheimnis besser zu schützen, einen abschließenden Katalog zulässiger Übermittlungen von Sozialdaten durch die verschiedensten Stellen der Sozialverwaltung - also auch durch die Sozialämter - aufgestellt (vgl. zur Neuregelung des Sozialdatenschutzes 10. Tätigkeitsbericht, Ziff. 4.1 und 9. Tätigkeitsbericht, Ziff. 3.3). § 71 Ziff. 2 SGB X erklärte in seiner ursprünglichen Fassung die Meldung von Ausländern nur im Falle des § 10 Abs. 1 Nr. 9 Ausländergesetz, nämlich bei Gefährdung der öffentlichen Gesundheit oder Sittlichkeit, für erlaubt, nannte aber die Nr. 10 dieser Vorschrift über die Inanspruchnahme von Sozialhilfe gerade nicht.

Für eine Änderung dieser Rechtslage haben sich vor allem die Kommunen bzw. die kommunalen Spitzenverbände mit Nachdruck eingesetzt. Dies geschah mit dem Argument, daß die im Ausländergesetz vorgesehene Ausweisungsmöglichkeit wegen des Bezuges von Sozialhilfe nicht wahrgenommen werden könne, wenn die Ausländerbehörde davon keine Kenntnis erhalte. Im Zusammenhang mit der Verabschiedung des 3. Kapitels des SGB X wurde dann auch der § 71 SGB X mit Wirkung vom 1. Juli 1983 in diesem Punkt novelliert. Nach der jetzt geltenden Formulierung dieser Vorschrift ist die Offenbarung personenbezogener Daten eines Ausländers zulässig, soweit es nach pflichtgemäßem Ermessen des Sozialamts erforderlich ist, den Ausländerbehörden ausländerrechtlich zulässige Maßnahmen u.a. deshalb zu ermöglichen, weil der Ausländer sozialhilfebedürftig ist. Während der ersten sechs Monate eines Bezugs von Sozialhilfe soll allerdings von einer Mitteilung dieser Tatsache abgesehen werden (§ 71 Abs. 2 SGB X).

4.2.2
Positionen im Gesetzgebungsverfahren

Die parlamentarische Entstehung dieser Bestimmung ist bemerkenswert. Der ursprüngliche Gesetzesbeschluß des Bundestages zum SGB X vom 25. Juni 1982 hatte nämlich eine erweiterte Zulässigkeit der Weitergabe personenbezogener Angaben über Ausländer nicht vorgesehen. Trotz der entgegenstehenden Voten des Innenausschusses und des Ausschusses für Jugend, Familie und Gesundheit hatten es zunächst der federführende Arbeits- und Sozialausschuß sowie schließlich das Plenum des Parlaments abgelehnt, den § 71 SGB X zu erweitern. Dies wurde u.a. mit der Notwendigkeit weiterer gründlicher Überlegungen sowie einschränkender Formulierungen begründet; diskutiert wurde auch, eine solche Regelung einer Novellierung des Ausländergesetzes vorzubehalten. Der Bundesrat rief jedoch dann u.a. wegen dieses Punktes den Vermittlungsausschuß an und verwies darauf, ohne Informationen durch das Sozialamt seien die Ausländerbehörden nicht mehr in der Lage, das Ausländergesetz in diesem Punkte zu vollziehen, womit eine einheitliche und gleichmäßige Anwendung des Ausländergesetzes nicht gewährleistet werden könne. Im Vermittlungsausschuß wurde dann die jetzt Gesetz gewordene Fassung ausgehandelt, die gegenüber dem Formulierungsvorschlag des Bundesrates zwei Einschränkungen enthält: Zum einen muß das Sozialamt sein "pflichtgemäßes Ermessen" betätigen, darf also nicht routinemäßig und ausnahmslos ohne nähere Prüfung jeden seiner ausländischen Klienten an die Ausländerbehörde melden. Zum anderen soll eine möglichen Ausweisung erst bei längerem Bezug von Sozialhilfe drohen; deshalb soll in der Regel während der ersten sechs Monate von einer Mitteilung abgesehen werden.

Im Gesetzgebungsverfahren hatte ich der Hessischen Landesregierung vor dem Durchgang im Bundesrat im Juli 1982 meine Bedenken gegen die in Aussicht stehende Neufassung des § 71 SGB X vorgetragen. Wolle man an der prinzipiellen Absicht des Gesetzgebers bei der Verstärkung des Sozialgeheimnisses festhalten, nämlich die Datenbestände der Sozialverwaltung grundsätzlich gegenüber anderen Verwaltungszweigen abzuschotten, seien Wünsche nach einer Erweiterung der Offenbarungsbefugnisse für Sozialdaten mit äußerster Zurückhaltung zu beurteilen. Die Übermittlung von Ausländerdaten durch die Sozialämter dürfe nicht nur unter ausländerrechtlichen Gesichtspunkten, sondern müsse auch unter dem Blickwinkel der Schutzwürdigkeit der Vertrauensbeziehung auch der ausländischen Mitbürger zu den Sozialämtern betrachtet werden. Ich schlug damals vor, die Mitteilung zumindest von der Voraussetzung abhängig zu machen, daß durch sie schutzwürdige Belange der betroffenen Ausländer nicht beeinträchtigt würden. Meine Stellungnahme hat zusammen mit ähnlichen Interventionen anderer Datenschutzbeauftragter dazu beigetragen, daß die vom Bundesrat zunächst vorgesehene weite Übermittlungsmöglichkeit jedenfalls teilweise eingeschränkt wurde. Auf die allgemeine Tendenz, das Sozialgeheimnis wieder mehr zu öffnen und sich damit von der ursprünglichen gesetzgeberischen Intention zu entfernen, hatte ich im übrigen bereits in meinem 10. Tätigkeitsbericht (vgl. Ziff. 4.1.4) kritisch hingewiesen.

4.2.3
Mitteilungspraxis nach der neuen Rechtslage

Der neue § 71 Abs. 2 SGB X legalisiert zwar grundsätzlich den Datenfluß zwischen Sozialamt und Ausländeramt, was die Mitteilung von Ausländern angeht, die Sozialhilfe beziehen. Allerdings muß ich darauf dringen, daß die bereits genannten Einschränkungen beachtet und früher geübte Übermittlungspraktiken nicht einfach fortgesetzt oder wieder aufgenommen werden. Zum einen bezieht sich § 10 Abs. 1 Nr. 10 Ausländergesetz ausschließlich auf die Hilfe zum Lebensunterhalt, ist also nicht auf andere Leistungen aus der Sozialhilfe gemünzt. Zum zweiten ist eine Meldung über den Hilfebezug in aller Regel erst nach Ablauf von sechs Monaten zulässig; es reicht mithin nicht aus, daß die Gewährung von laufender Sozialhilfe über ein halbes Jahr hinaus "absehbar" ist. Ausnahmen von dieser Regel bedürfen besonderer zusätzlicher Gründe in der Person des Betroffenen.

Das gesetzliche Erfordernis, das "pflichtgemäße Ermessen" zu betätigen, hat für die Sozialämter die Verpflichtung zur Konsequenz, auch nach Ablauf der Sechs-Monats-Frist die Argumente für und gegen eine Weiterleitung von Namen an das Ausländeramt abzuwägen. § 78 SGB X macht deutlich, daß Stellen, die Sozialdaten erhalten haben, diese nur zu dem Zweck verwenden dürfen, zu dem sie ihnen befugt offenbart worden sind. Für Ausländerbehörden besteht daher aufgrund dieser Zweckbindung ein Verwertungsverbot für solche Angaben über nichtdeutsche Sozialhilfeempfänger, die das Sozialamt unter Verstoß gegen die genannten Einschränkungen des § 71 SGB X übermittelt hat.

Ich habe mich in einer hessischen Großstadt ausführlich über die Mitteilungspraxis und die dazu ergangene Verfügung informiert. Dabei bestand Einigkeit darüber, daß eine Meldung an die Ausländerbehörde z.B. dann nicht in Betracht kommt, wenn der Hilfesuchende aus einem Herkunftsland stammt, mit dem ein Sozialhilfeabkommen besteht, und er sich bereits seit mindestens fünf Jahren in der Bundesrepublik Deutschland aufhält. Dies deshalb, weil in diesen Fällen aufgrund der Abkommen allein wegen des Bezuges von Sozialhilfe eine Ausweisung nicht erfolgen kann. Übereinstimmung war weiter darüber gegeben, daß die gesetzliche Neufassung des § 71 SGB X eine sorgfältige Prüfung des Einzelfalles vor der Übermittlung voraussetzt. Soweit Divergenzen über die Auslegung der Sechs-Monats-Frist des Hilfebezuges bestanden, hat mir die betroffene Kommune zugesagt, ihre Rundverfügung entsprechend zu präzisieren und ggfs. mit Beispielen den zuständigen Sachbearbeitern gesetzeskonforme Vorgaben für die Übermittlung zur Verfügung zu stellen; dazu habe ich meine Hilfestellung angeboten.

4.3
Bundesweiter Direktzugriff der Polizei auf Kfz-Halterdaten

4.3.1
Das Zentrale Verkehrsinformationssystem (ZEVIS) des Kraftfahrtbundesamtes

Das Kraftfahrtbundesamt (KBA) verfügt über die Daten von 23 Millionen Kraftfahrzeughaltern, d.h. - läßt man einmal juristische Personen und Kapitalgesellschaften beiseite - etwa jeder dritte Einwohner der Bundesrepublik Deutschland ist mit seinem Namen, seiner Anschrift und seinem Geburtsdatum sowie den Daten seines Kraftfahrzeugs und dessen Versicherung in dieser Datei erfaßt. Hinzu kommen die Daten von Personen, denen die Fahrerlaubnis entzogen oder gesperrt wurde. Um den Zugriff auf diese Daten zu erleichtern, wurde ein "Zentrales Verkehrsinformationssystem" (ZEVIS) eingerichtet, das eine Reihe von Abfragemöglichkeiten bietet.

4.3.2
Der Direktzugriff von Polizeidienststellen der Länder auf ZEVIS

Schon im Februar 1978 beschloß der Arbeitskreis II "Öffentliche Sicherheit und Ordnung" der Arbeitsgemeinschaft der Innenministerien der Bundesländer einen Verbund des Informationssystems der Polizei (INPOL) mit dem System ZEVIS stufenweise einzurichten. Die Polizeidienststellen einzelner Bundesländer - allerdings keine hessischen Dienststellen - erhielten im Rahmen eines Pilotprojekts einen Direktzugriff auf die Dateien des KBA. Nach dem heutigen Ausbaustand soll in ZEVIS etwa die Hälfte des Fahrzeugbestandes der Bundesrepublik Deutschland einschließlich der jeweiligen Halterdaten gespeichert sein. Folgende Zugriffsmöglichkeiten auf das System stehen derzeit zur Verfügung: Durch die Eingabe des Kennzeichens können die angeschlossenen Polizeidienststellen über die direkte Schaltung unmittelbar Fahrzeugdaten und Halterdaten abrufen. Gleiches ist über die Eingabe der Fahrgestellnummer des Kraftfahrzeuges möglich. Schließlich kann über die Eingabe des bekannten Teils eines Kennzeichens versucht werden, ein Fahrzeug und dessen Halter zu identifizieren.

Noch nicht realisiert aber geplant ist die sog. P-Abfrage. Sie würde es jedem zugriffsberechtigten Polizeibeamten erlauben, über die Eingabe von Name oder Anschrift einer Person, die allerdings als Halter in der Datei gespeichert sein muß, die übrigen Personalien zu erfahren. Natürlich können auch die Daten des von dieser Person gehaltenen Kraftfahrzeugs abgerufen werden.

4.3.3
Der Stand in Hessen

Im Gegensatz zu anderen Bundesländern, die die Zugriffsmöglichkeit der Polizei - mit Ausnahme der P-Abfrage -bereits realisiert haben, steht Hessen noch vor der Entscheidung, ob der Direktzugriff auf ZEVIS auch für die Landespolizei eingeführt werden soll.

Gegen eine solche Einführung hätte ich erhebliche Bedenken, die ich dem Hessischen Minister des Innern mitgeteilt habe (s. unten Ziff. 4.3.4).

Bereits in früheren Tätigkeitsberichten (vgl. 9. Tätigkeitsbericht, Ziff. 1.3 und 2.1.1, 10. Tätigkeitsbericht, Ziff. 2.3.1 und 11. Tätigkeitsbericht, Ziff. 3.1.2) habe ich darauf hingewiesen, daß ein Direktzugriff der Polizei auf Dateien der Kraftfahrzeugzulassungsstellen nach der derzeit geltenden Rechtslage nicht zulässig ist. Auch der Landtag hat sich in seinem Beschluß zum 9. Tätigkeitsbericht (Plenarprotokoll 9/58 der Sitzung vom 23. Juni 1981, S. 3620 i.V.m. der Drs. 9/4880) mit dem Direktzugriff der Polizei auf die Daten der Kraftfahrzeugzulassungsstellen beschäftigt. Im Zusammenhang mit der Behandlung meines 11. Berichts hat er in seiner Sitzung vom 21.7.1983 die Landesregierung und den Hessischen Datenschutzbeauftragten aufgefordert zu prüfen, inwieweit tatsächlich und rechtlich die Notwendigkeit zur Regelung des Online-Zugriffs einer speichernden Stelle auf personenbezogene Daten anderer speichernder Stellen besteht (vgl. Drs. 10/1022). Die rechtliche Problematik habe ich bereits - wie erwähnt - in meinen früheren Tätigkeitsberichten erörtert.

4.3.4
Rechtliche Einwände gegen den Direktzugriff

Sowohl der Bundesbeauftragte für den Datenschutz als auch die Landesbeauftragte für den Datenschutz in Baden-Württemberg haben die für Polizeibehörden ihres Kontrollbereichs bereits eingeführte Direktanbindung an ZEVIS als Verstoß gegen bestehende Rechtsvorschriften beanstandet. Ich teile diese Beurteilung.

Da § 26 Abs. 5 der Straßenverkehrszulassungsordnung lediglich die Auskunft durch die Kraftfahrzeugzulassungsstellen regelt, ist die Datenübermittlung vom Kraftfahrtbundesamt an örtliche Polizeidienststellen nach § 10 des Bundesdatenschutzgesetzes in Verbindung mit § 12 des Hessischen Datenschutzgesetzes zu beurteilen. Die Rechtslage ist für beide Fälle weitgehend identisch. Gemäß § 2 Abs. 2 Nr. 2 BDSG bzw. HDSG gilt mit der Einrichtung des Direktzugriffs der gesamte betroffene Datenbestand des Kraftfahrtbundesamtes als an alle zugriffsberechtigten Polizeidienststellen übermittelt. Da die Übermittlung aller betroffener Daten an die Polizei jedoch nicht als "erforderlich" im Sinne der Datenschutzgesetze angesehen werden kann, wäre die Anbindung unzulässig. Dies ergibt sich daraus, daß die Polizei faktisch immer nur die Daten eines Bruchteils des zur Verfügung gestellten Datenbestandes benötigt; diese Untermenge ist im Zeitpunkt der Einrichtung des Direktzugriffs noch nicht absehbar.

Im Unterschied zu der vom Landtag bereits erörterten Anbindung örtlicher Polizeidienststellen an die Dateien örtlicher Kraftfahrzeugzulassungsstellen (s.o.) würde der Direktzugriff auf ZEVIS eine Abfrage sämtlicher Halterdaten aus dem gesamten Bundesgebiet ermöglichen. Erhebliche Zweifel sind angebracht, ob es noch mit dem rechtsstaatlichen Gebot der Verhältnismäßigkeit zu vereinbaren ist, wenn -zig Millionen Datensätze von Bürgern aus allen Teilen der Bundesrepublik von jeder örtlichen Dienststelle der Polizei ohne die präventive Einschaltung einer Kontrollinstanz abgefragt werden können.

Das Bundesdatenschutzgesetz geht mit seiner Übermittlungsdefinition in § 2 Abs. 2 Nr. 2 eindeutig davon aus, daß mit dem Direktzugriff eine erhöhte Gefahr der mißbräuchlichen Abfrage von Daten einzelner Betroffener und damit eine Gefährdung ihrer Rechte verbunden ist. Diese Wertung wurde vom Oberlandesgericht Düsseldorf vor kurzem bestätigt (vgl. Neue Juristische Wochenschrift 1983, 399). Im Zusammenhang mit der rechtlichen Bewertung einer Datenbank, die als Gemeinschaftseinrichtung von mehreren Kreditinstituten geführt wird und von der diese Institute jederzeit Informationen über ihre Kreditnehmer abrufen können, stellte das Gericht fest, die Gefahr für die gespeicherten Personen sei dann am größten, "wenn Gefahr für die gespeicherten Personen sei dann am größten, "wenn die menschliche Verantwortung für den Auskunftsgrund ganz allein im Bereich der abrufenden, also selbst interessierten Stelle liegt" und die Zulässigkeit des Einzelabrufs von keiner weiteren Instanz - etwa der die Datei führenden Stelle - vorher geprüft werde.

4.3.5
Die besondere Gefährdung durch die "P-Abfrage"

Für besonders problematisch halte ich die geplante "P-Abfrage". Wie gesagt: Sie erlaubt nach Eingabe von einzelnen Personalien eines Halters die Abfrage nicht nur seiner Kfz-Daten, sondern auch - und das ist der entscheidende Punkt - die Abfrage aller übrigen in dieser Datei gespeicherten Angaben zu seiner Person, die der Polizei vorher noch nicht bekannt waren. Mir ist nicht ersichtlich, warum für die Ermittlung eines unbekannten Kraftfahrzeuges und sonstiger Personalien eines namentlich bekannten Halters - also gerade der umgekehrte Fall

zur üblichen Halterfeststellung - ein Online-Zugriff erforderlich ist. Durch die Einrichtung der P-Abfrage wäre es jeder Polizeidienststelle möglich, von jedem Kfz-Halter und damit nahezu von jedem dritten Bundesbürger unbekannte Personaldaten abzufragen. Dieses Abfragesystem würde somit für einen beträchtlichen Teil aller Bundesbürger zu einem Ersatz für ein Bundesmelderegister. Der Deutsche Bundestag hat jedoch sowohl bei den Beratungen zum Melderechtsrahmengesetz als auch zum Personalausweisgesetz deutlich gemacht, daß er eine zentrale Speicherung der Daten aller Bundesbürger ablehnt. Diese Haltung kommt in den beiden Gesetzen ebenso deutlich zum Ausdruck wie in den Landesmeldegesetzen.

4.3.6
Ansätze zu einer Novellierung der Rechtsgrundlage

Die heutige Rechtslage hat dazu geführt, daß im Novellierungsentwurf zum Bundesdatenschutzgesetz eine Änderung der Übermittlungsvorschriften angestrebt wird, nach der die Einrichtung von Direktzugriffen vermehrt zulässig sein soll. Umfang und Inhalt der Änderung sind jedoch unter den beteiligten Stellen gerade insoweit umstritten, als dadurch der direkte Zugriff der Polizeibehörden auf Datenbestände anderer öffentlicher Stellen ermöglicht werden soll. Der Bundesminister für Verkehr hat in den vergangenen Monaten deutlich gemacht, daß er durch eine Änderung der derzeitigen straßenverkehrsrechtlichen Vorschriften eine bereichsspezifische Regelung der Übermittlung von Daten aus den Beständen des Kraftfahrtbundesamtes bzw. des Verkehrszentralregisters anstrebt. Allerdings läßt der derzeitige Entwurf zur Erweiterung des Straßenverkehrsgesetzes (StVG) die Befürchtung aufkommen, daß die Bundesregierung den Zweck einer bereichsspezifischen Lösung verkennt: Keinesfalls kann es darum gehen, das StVG um textgleiche Vorschriften aus dem BDSG zu erweitern. Unumgänglich ist vielmehr, eine konkrete, auf die Bedürfnisse der beteiligten Stellen zugeschnittene Lösung zu entwickeln, die im besonderen Maße den schutzwürdigen Belangen der betroffenen Bürger gerecht wird.

Mit dem Hessischen Innenminister stehe ich derzeit noch im Meinungsaustausch über die Rahmenbedingungen dieses Zugriffsverfahrens und die von ihm ausgehenden Gefahren. Er hat mir mitgeteilt, daß die Einführung des Direktzugriffs der hessischen Polizeidienststellen auf das System ZEVIS zur Zeit noch geprüft wird, und zwar auf der Grundlage des Arbeitsentwurf des Bundesministers für Verkehr zur Änderung des Straßenverkehrsgesetzes. Im übrigen hat er darauf hingewiesen, daß in einer Reihe von Fallkonstellationen aus polizeilicher Sicht das geplante System Vorteile bringe und für erforderlich gehalten werde. Diese technischen Vorzüge sind zwar nicht zu bestreiten, sie können jedoch nicht eine umfassende, auch die Gesichtspunkte des Datenschutzes einbeziehende Wertung ersetzen. Auf keinen Fall geht es an, durch bestimmte technische Vorgaben die Entscheidung des Parlaments zu präjudizieren, dem allein die Ausgestaltung jeder Regelung von Online-Verfahren zukommt.

4.4
Die "Schwarzfahrerdateien" städtischer Versorgungsbetriebe

Die städtischen Versorgungsbetriebe, die einen öffentlichen Bus-oder Bahnverkehr betreiben, erfassen regelmäßig die Daten derjenigen Fahrgäste in einer Datei, die beim Fahren ohne gültigen Fahrschein angetroffen werden.

In mehreren Fällen wandten sich Eltern an mich, nachdem ihre Kinder beim "Schwarzfahren" gefaßt worden waren und die städtischen Unternehmen darauf bestanden, deren Daten in ihre "Schwarzfahrerdatei" zu übernehmen. Diese Vorfälle veranlaßten mich zu Nachforschungen und Kontrollen, die die Rechtmäßigkeit der Führung solcher Dateien überhaupt zum Gegenstand hatten.

4.4.1
Zweck und Dauer der Speicherung

Wird ein Fahrgast von einem Kontrolleur ohne einen gültigen Fahrschein angetroffen, so kann von ihm nach § 9 der Verordnung über die allgemeinen Beförderungsbedingungen für den Straßenbahn-und Omnibusverkehr sowie den Linienverkehr mit Kraftfahrzeugen vom 27.2.1970 (BGBl. I S. 230) ein "erhöhtes Beförderungsentgelt" verlangt werden. Zahlt der Fahrgast dieses Entgelt - regelmäßig in Höhe von DM 40,— - sofort, erhält er hierfür eine Quittung. Seine personenbezogenen Daten werden nicht erfaßt. Anders ist es jedoch, wenn die betroffene Person die geforderte Summe nicht zahlen kann oder will. In diesem Fall dürfen die Stadtwerke die erforderlichen Daten des Fahrgastes speichern, um die spätere Zahlung abbuchen zu können oder ggfs. durch Zahlungsaufforderungen, Mahnungen oder auch Vollstreckungshandlungen die Zahlung zu erzwingen.

Mit anderen Worten: Beschränkte man sich auf die zivilrechtliche Seite des Problems, so wäre die Speicherung so lange zulässig, wie die Geldforderung von den Stadtwerken noch geltend gemacht wird und noch nicht bezahlt wurde.

Ein strafrechtlicher Aspekt kommt jedoch hinzu. Das Strafgesetzbuch (§ 265a) stellt das Verhalten des Fahrgastes unter Strafe, der "die Beförderung durch ein Verkehrsmittel... in der Absicht erschleicht, das Entgelt nicht zu entrichten,...". Eine solche "Beförderungserschleichung" wird sich bei kommunalen Verkehrsmitteln regelmäßig auf einen Fahrpreis von unter DM 10,— beziehen. Da diese Summe nur gering ist, wird die Tat nur auf Antrag (§ 265a Abs. 3 i.V.m. § 248a StGB) der Stadtwerke zu verfolgen sein. Der Strafantrag der städtischen Unternehmen kann der Polizei innerhalb von drei Monaten nach Kenntnis von der Tat und der Person des Täters zugeleitet werden (§ 77b StGB). Liegt kein Antrag auf Strafverfolgung vor, darf nach diesem Zeitpunkt die Beförderungserschleichung nicht mehr verfolgt werden. Daraus folgt, daß zum Zweck einer möglichen Strafverfolgung auch nach der Entrichtung des "erhöhten Beförderungsentgeltes" eine Speicherung noch zulässig ist, solange diese Antragsfrist nicht abgelaufen ist.

4.4.2
Folgerungen für die Praxis

In der Praxis werden oft die Daten einzelner Schwarzfahrer über ein bis zwei Jahre nach der Bezahlung des Entgelts oder auch der Entscheidung der Stadtwerke, auf die Geldforderung zu verzichten, gespeichert. Der Verband der öffentlichen Verkehrsunternehmen sieht sogar eine Speicherung der Daten bis zu fünf Jahren nach dem Abschluß des Vorgangs für gerechtfertigt an. Die Stadtwerke können sich jedoch gemäß § 23 des Bundesdatenschutzgesetzes auf die Wahrung ihrer berechtigten Interessen nur solange berufen, wie sie die Daten im Rechtsverkehr verwerten können. Die genannten Fristen setzen hier eine eindeutige Grenze. Dies gilt selbst für die Fälle, in denen der Fahrgast sich vorgenommen hat, für einen unabsehbaren Zeitraum und in unzähligen Fällen "schwarz zu fahren". Die Antragsfrist für das Strafverfahren beginnt jedesmal dann zu laufen, wenn die Stadtwerke von Tatvorgang und Täter der jeweiligen Schwarzfahrt Kenntnis erhalten. Ihr Recht, einen Strafantrag stellen zu können, endet jeweils drei Monate nach diesem Zeitpunkt.

In der Praxis wurde ein Strafantrag bisher regelmäßig allenfalls dann gestellt, wenn die betroffene Person sich mehrmals unter besonders schweren Umständen die Beförderung erschlichen hatte. Ein mehrfaches "Schwarzfahren" kann demgemäß nur dann in einen Strafantrag münden, wenn sich die einzelnen Fahrten innerhalb von drei Monaten ereigneten.

Als Ergebnis bleibt festzuhalten: Die Stadtwerke sind gehalten, jeweils zu prüfen, ob nach zivilrechtlichen oder strafrechtlichen Gesichtspunkten eine Verwertung der Daten noch in Frage kommt. Die nach diesen Maßstäben nicht mehr verwertbaren Daten sind unverzüglich zu löschen. Konkret bedeutet dies, daß die Daten nur so lange aufbewahrt werden dürfen, wie das Unternehmen noch eine Geldforderung gegen den Schwarzfahrer geltend machen kann oder das Recht, einen Strafantrag zu stellen, noch besteht.

4.4.3
Die Speicherung der Daten Minderjähriger

Zu einem eindeutigen Ergebnis führte die Gesetzeslage in den Fällen, in denen auch nach dem Zeitpunkt der Zahlung oder dem Verzicht der Stadtwerke auf das erhöhte Beförderungsentgelt - bis dahin war die Speicherung zur Durchsetzung der zivilrechtlichen Forderung notwendig und damit zulässig - die Daten von unter 14 Jahre alten Kindern weiterhin gespeichert wurden. Da sie strafunmündig waren, durften ihre Daten nicht zum Zwecke einer Strafverfolgung in der Schwarzfahrerdatei registriert bleiben. Die betroffenen Stadtwerke löschten sie dementsprechend aufgrund meiner Aufforderung.

Soweit einzelne städtische Unternehmen ihre Schwarzfahrerdateien diesen gesetzlichen Vorgaben noch nicht angepaßt haben, sollten sie ihre Verarbeitungsverfahren unverzüglich überprüfen.

4.4.4
Zur Zuständigkeit des Hessischen Datenschutzbeauftragten für Stadtwerke

Im Zusammenhang mit meinen Nachforschungen äußerten einzelne Stadtwerke die Meinung, sie unterstünden als öffentliche Wirtschaftsunternehmen der Kontrolle des Hessischen Datenschutzbeauftragten nicht. Sie wiesen auf den Wortlaut des § 23 Hessisches Datenschutzgesetz (HDSG) hin, nachdem nur die in "§ 3 Abs. 1 genannten Behörden und Stellen..." der Kontrolle des Datenschutzbeauftragten unterworfen seien, nicht aber die in § 3 Abs. 2 HDSG erwähnte Gruppe der "öffentlich-rechtlichen Unternehmen, die am Wettbewerb teilnehmen". Diese Ansicht vertritt auch der bundesweite Verband öffentlicher Verkehrsbetriebe.

Sie entspricht jedoch nicht dem Sinn des Gesetzes. Soweit die Stadtwerke nicht in einer selbständigen privatrechtlichen Rechtsform - etwa als AG oder GmbH - geführt werden, sondern als ein "Eigenbetrieb der Gemeinden", sind sie grundsätzlich "öffentliche Stellen der Gemeinden" i. S. des § 3 Abs. 1 HDSG. § 3 Abs. 2 HDSG bestätigt als Ausnahmeregelung, daß grundsätzlich für alle öffentlich-rechtlichen Unternehmen alle Vorschriften des Datenschutzgesetzes zur Anwendung kommen. Nur für einige Bereiche, wie die Datenverarbeitung für eigene Zwecke und im Auftrag, treten an die Stelle der Vorschriften dieses Gesetzes Regelungen des Bundesdatenschutz-

gesetzes. Daß sowohl die Kontrollkompetenz des Hessischen Datenschutzbeauftragten als auch die Pflicht dieser Stellen zur Meldung ihrer Dateien an mein Dateienregister nach §§ 23 und 25 HDSG regelmäßig für alle öffentlich-rechtlichen Unternehmen gelten, zeigt sich auch darin, daß § 3 Abs. 2 Nr. 2 Satz 2 HDSG von der Anwendbarkeit der §§ 20 - 31 HDSG ausdrücklich nur Kreditinstitute, Versicherungsunternehmen, deren Zusammenschlüsse und Verbände von diesem Kontrollsystem ausnimmt und diese Art Unternehmen der Aufsicht der Regierungspräsidenten unterstellt. Daraus ergibt sich im Gegenschluß, daß die städtischen Versorgungsunternehmen als öffentlich-rechtliche Unternehmen, die am Wettbewerb teilnehmen und dieser Gruppe nicht zugeordnet werden können, im Kontrollbereich des Hessischen Datenschutzbeauftragten verbleiben. Der Hessische Minister des Innern teilt diese Rechtsansicht.

4.5
Mitteilung veralteter Polizeiinformationen an den Arbeitgeber - berufliche Nachteile für den Betroffenen

4.5.1
Unzulässige Auskunftserteilung durch die Polizei - Konsequenzen

Ein Arbeitnehmer hatte infolge einer Auskunft der Polizei an seinen Arbeitgeber eine bessere Stelle, auf die er sich beworben hatte, nicht erhalten. Bei der Überprüfung des Sachverhalts stellte sich folgendes heraus:

Die Polizei hatte dem Arbeitgeber - einer amerikanischen Dienststelle - mitgeteilt, daß der Betroffene einmal erkennungsdienstlich behandelt worden war. Die Auskunft umfaßte auch eine Darstellung des Vorfalls, der fünf Jahre zurücklag. Der Betroffene war damals verdächtigt worden, einen Zigarettenautomaten aufgebrochen zu haben. Aufgrund der polizeilichen Ermittlungen hatte sich dieser Verdacht allerdings als unzutreffend herausgestellt.

Von diesem Zeitpunkt an war sowohl die Speicherung der Informationen bei der Polizei als auch ihre Weiterleitung an die alliierte Dienststelle aus mehreren Gründen rechtswidrig. Die Polizei hätte die erkennungsdienstlichen Unterlagen nach Abschluß des Ermittlungsverfahrens vernichten müssen, weil keine konkreten Anhaltspunkte dafür vorlagen, daß der Betroffene in Zukunft straffällig wird (s. hierzu bereits BVerwGE 26, 169). Zu diesem Zeitpunkt durften auch die übrigen Daten aus dem Ermittlungsverfahren nicht mehr gespeichert werden. Nr. 5.4.1 der Richtlinien für die Führung kriminalpolizeilicher Sammlungen (KpS-Richtlinien) legt ausdrücklich fest, daß Unterlagen stets auszusondern sind, wenn ihre Kenntnis für die Aufgabenerfüllung der Dienststelle nicht mehr erforderlich ist. Und außerdem: Die bloße Tatsache einer erkennungsdienstlichen Behandlung hätte keinsfalls an die US-Dienststelle mitgeteilt werden dürfen. Eine erkennungsdienstliche Behandlung dient lediglich der Identifizierung einer Person. Sie besitzt aus der Sicht des Empfängers keine weitere Aussagekraft. In diesen Fällen besteht jedoch die Gefahr, daß der Empfänger den falschen Schluß zieht, die Polizei verfüge über belastendes Material gegen den Betroffenen.

Die geschilderte Praxis zeigt erneut, daß Vorschriften allein nicht ausreichen, um den Datenschutz zu gewährleisten. Es bedarf deshalb verstärkter Anstrengungen, um die in den Richtlinien festgelegten Löschungsfristen auch tatsächlich durchzusetzen. Solange während einer Übergangszeit die polizeilichen Datenbestände nicht vollständig bereinigt sind, muß durch klare organisatorische Vorkehrungen und Dienstanweisungen sichergestellt werden, daß die Betroffenen hierdurch keine Nachteile erleiden.

Der Hessische Minister des Innern teilt meine Ansicht, daß die Auskunft im konkreten Fall unzulässig war. Er sieht jedoch keinen Anlaß für generelle organisatorische Vorkehrungen, die Vorfälle dieser Art für die Zukunft ausschließen könnten.

Dieser Fall beweist auch, daß das von mir mehrfach hervorgehobene Problem der Auskunftserteilung aus dem polizeilichen Informationssystem einerseits und dem Bundeszentralregister andererseits dringend gelöst werden muß (s. hierzu 11. Tätigkeitsbericht, Ziff. 3.2.3). Die differenzierten Schutzvorschriften des Bundeszentralregisters werden durch Datenübermittlungen an Dritte aus dem polizeilichen Informationssystem unterlaufen, das vergleichbare Regelungen nicht kennt.

Zur Veranschaulichung folgender Vergleich: Hätte sich der Verdacht gegen den Betroffenen bestätigt und wäre er rechtskräftig verurteilt worden, so wäre diese Verurteilung zwar im Bundeszentralregister gespeichert worden. In ein von der Registerbehörde ausgestelltes Führungszeugnis hätte sie jedoch nicht aufgenommen werden dürfen (vgl. § 30 Nr. 5 BZRG). Amerikanische Dienststellen erhalten nach § 39 BZRG keine über das Führungszeugnis hinausgehenden Informationen. Gelöscht worden wäre die Eintragung spätestens nach drei Jahren (vgl. § 32 Abs. 1 Nr. 1 BZRG). Der betroffene Arbeitnehmer wurde im Ergebnis somit schlechter gestellt als eine Person, bei der sich der Verdacht, einen Automatendiebstahl begangen zu haben, bestätigt hat und die deshalb rechtskräftig verurteilt wurde.

4.5.2
Polizeiliche Mitteilungen an amerikanische Dienststellen

Die Auskunft wurde im konkreten Fall dem "Safety Security Field Service" der amerikanischen Streitkräfte erteilt. Es stellt sich deshalb die Frage, in welchem Umfang deutsche Behöden an alliierte Dienststellen personenbezogene Daten übermitteln dürfen.

Der Hessische Innenminister verweist hierzu auf Art. 3 des Zusatzabkommens zu dem Abkommen zwischen den Parteien des Nordatlantikvertrages über die Rechtsstellung ihrer Truppen hinsichtlich der in der Bundesrepublik Deutschland stationierten Truppen (NATO-Truppenstatut) vom 3. August 1959 (BGBl. 1961 II S. 1183), der nach seiner Ansicht als vorrangige Vorschrift den Datenaustausch zwischen deutschen und alliierten Stellen regelt. Die Vorschrift lautet:

"1. In Übereinstimmung mit den im Rahmen des Nordatlantik-Vertrages bestehenden Verpflichtungen der Parteien zur gegenseitigen Unterstützung arbeiten die deutschen Behörden und die Behörden der Truppen eng zusammen, um die Durchführung des NATO-Truppenstatutes und dieses Abkommens sicherzustellen.

2. Die in Abs. 1 vorgesehene Zusammenarbeit erstreckt sich insbesondere

   a) auf die Förderung und Wahrung der Sicherheit sowie den Schutz des Vermögens der Bundesrepublik, der Entsendestaaten und der Truppen, namentlich auf die Sammlung, den Austausch und den Schutz aller Nachrichten, die für diese Zwecke von Bedeutung sind...".

Dieser Art. 3 des Zusatzabkommens liefert allein jedoch keine Rechtsgrundlage für die Mitteilung personenbezogener Informationen an alliierte Dienststellen. Vielmehr ist er nur im Rahmen des § 16 HDSG zu berücksichtigen. Abs. 1 Satz 1 des § 16 HDSG verlangt für Datenübermittlungen von deutschen Verwaltungsbehörden an Personen und Stellen "außerhalb des öffentlichen Bereichs" u.a., daß der Empfänger der Angaben "ein berechtigtes Interesse an der Kenntnis der zu übermittelnden Daten glaubhaft macht und dadurch (d.h. durch die Übermittlung) schutzwürdige Belange des Betroffenen nicht beeinträchtigt werden." § 16 Abs. 1 Satz 3 sieht ausdrücklich den Fall vor, daß Daten an nicht-deutsche, über- und zwischenstaatliche Behörden und Stellen weitergegeben werden und schreibt auch in diesen Fällen die Anwendbarkeit des Abs. 1 Satz 1, mithin die Prüfung der berechtigten Interessen und der schutzwürdigen Belange (s.o.), vor. Dies geschieht allerdings mit der Modifizierung, nach der für diese Übermittlungen geltende Vereinbarungen und Verträge Anwendung finden. Doch könnten nur vertragliche Bestimmungen, die Zweck und Umfang der Datenübermittlungen - in diesem Fall von deutschen Behörden an NATO-Stellen - konkret festlegen, die Pflicht zur Abwägung zwischen berechtigten Interessen und schutzwürdigen Belangen des Satz 1 einschränken. Eine allgemein formulierte Zusammenarbeitsverpflichtung reicht hierfür nicht aus. Weder die Vertragspartner des Abkommens noch der Bundesgesetzgeber wollten über Art. 3 den alliierten und deutschen Behörden die Befugnis einräumen, deutsche Rechtsvorschriften zu umgehen.

Somit waren zwar im Rahmen des § 16 Abs. 1 Satz 1 HDSG die in Art. 3 Abs. 2 des Zusatzabkommens genannten Zwecke der "Förderung und Wahrung der Sicherheit sowie der Schutz des Vermögens der Bundesrepublik, der Entsendestaaten und der Truppen..." als "berechtigte Interessen" des Datenempfängers zu berücksichtigen. Dieses Interesse konnte jedoch nicht zur Mitteilung von Informationen berechtigen, die nach den deutschen Rechtsvorschriften längst hätten gelöscht sein müssen. Durch die Übermittlung nicht rechtmäßig gespeicherter Daten werden in jedem Fall auch die schutzwürdigen Belange des Betroffenen beeinträchtigt.

5. Materialien

5.1
Zum Personalausweis (Ziff. 3.1)

Beschluß der Konferenz der Datenschutzbeauftragten der Länder und des Bundes am 13. September 1983

Datenschutzrechtliche Anforderungen an den fälschungssicheren und maschinenlesbaren Personalausweis bzw. Paß

Die Datenschutzbeauftragten in Bund und Ländern weisen darauf hin, daß sie bereits im November 1979 datenschutzrechtliche Anforderungen an die Einführung des fälschungssicheren und maschinenlesbaren Personalausweises gestellt haben. In das Bundespersonalausweisgesetz sind daraufhin entscheidende datenschutzrechtliche Regelungen aufgenommen worden.

Die Datenschutzbeauftragten betonten jedoch seinerzeit, daß ein maschinenlesbarer Personalausweis nur in Verbindung mit einem datenschutzgerechten Melderecht und bereichsspezifischen Datenschutzregelungen für den Sicherheitsbereich hinnehmbar ist. Anknüpfend an diese Forderungen nahm der Deutsche Bundestag bei der Verabschiedung des Personalausweisgesetzes am 17. Januar 1980 den nachstehenden Entschließungsantrag an (vgl. BT-Drs. 8/3498):

"Der Deutsche Bundestag ist der Auffassung, daß angesichts der raschen Fortentwicklung der automatischen Datenverarbeitung und deren Einsatz in der öffentlichen Verwaltung über die Verabschiedung des Gesetzes zur Änderung des Gesetzes über Personalausweise hinaus weitere Maßnahmen erforderlich sind, um einen ausreichenden Schutz der Persönlichkeitsrechte der Bürger gegen mißbräuchliche Verwendung ihrer persönlichen Daten zu gewährleisten.

Die Bundesregierung wird deshalb ersucht,

1. den Entwurf eines datenschutzgerechten Melderechtsrahmengesetzes einzubringen und
2. die Arbeiten zur Entwicklung bereichsspezifischer Datenschutzregelungen für die Sicherheitsbehörden nachdrücklich fortzusetzen."

Die Anwendung moderner Informationstechnologien hat inzwischen zunehmend zur Kombination und Integration neuer und vorhandener Informationssysteme geführt. Die Entwicklung der Informationstechnologie ist gekennzeichnet durch die Verknüpfung von Daten, Text, Sprache, Schriftzügen und Bildern, die eine umfangreiche Darstellung und Überprüfung von Personen möglich machen können. Die Einführung des maschinenlesbaren Personalausweises bzw. Passes muß im Zusammenhang mit dieser Entwicklung gesehen werden. Die Aussage, daß ein maschinenlesbarer Personalausweis unter Datenschutzgesichtspunkten hinnehmbar ist, kann nur dann aufrechterhalten werden, wenn die bereits 1979 erhobenen Forderungen in ausreichendem Maße erfüllt werden und auch im übrigen bei der Ausführung des Personalausweisgesetzes den Datenschutzbelangen Rechnung getragen wird. Das bedeutet, daß weitere Regelungen getroffen werden müssen, um inzwischen zutage getretene Unklarheiten und Mißverständnisse auszuräumen und eine datenschutzgerechte Anwendung des Gesetzes sicherzustellen.

A) Zum Personalausweisgesetz

1. Soweit bei polizeilichen Personenkontrollen Anfragen in polizeilichen Informationssystemen vorgenommen werden, dürfen diese Anfragen nicht personenbezogen protokolliert werden, damit insbesondere keine Bewegungsbilder entstehen können. Da solche Protokollierungen, die als "Einrichtung von Dateien" anzusehen sind, nicht Zwecken der Grenzkontrolle und der Fahndung im Sinne des § 3 Abs. 5 Satz 2 Personalausweisgesetz dienen, sind sie nach § 3 Abs. 5 Satz 1 Personalausweisgesetz unzulässig. Im übrigen läßt sich aus der Entstehungsgeschichte dieser Vorschrift ableiten, daß der Gesetzgeber eine Verwendung des Ausweises zur automatischen Einrichtung von Dateien grundsätzlich nicht gestatten wollte.

2. Die Datenschutzbeauftragten gehen davon aus, daß die Nutzung des Personalausweises durch die Polizei nach § 3 Abs. 5 Satz 2 Personalausweisgesetz nicht auch die Verwendung der Seriennummer einschließt; hierfür ist § 3 Abs. 4 Personalausweisgesetz die Spezialvorschrift.

3. Die unterschiedliche Formulierung in § 3 Abs. 5 Satz 1 und § 4 Satz 2 Personalausweisgesetz gibt zu Mißverständnissen Anlaß. Die Regelung in § 4 muß deshalb der in § 3 angeglichen werden.

4. Die internationale Lesbarkeit des Personalausweises erfordert für deutsche Staatsangehörige die gleiche Schutzintensität auch im grenzüberschreitenden Reiseverkehr. Die Konferenz bittet daher die Bundesregierung, sich dafür einzusetzen, daß die datenschutzrechtlichen Anforderungen an die innerstaatliche Verwendung des Ausweises auch im internationalen Bereich umgesetzt werden.

B) Zu den Ausführungsvorschriften der Länder

1. Im Ausführungsgesetz oder in den Verwaltungsvorschriften muß festgelegt werden, daß ein Personenfeststellungsverfahren nur durchzuführen ist, wenn Zweifel an der Identität des Ausweisbewerbers nicht ausgeräumt werden können, und daß in diesem Verfahren erkennungsdienstliche Maßnahmen nur als letztes Mittel zulässig sind. Eine Weiterleitung dieser Unterlagen an das Bundeskriminalamt darf nur für den Vergleich mit anderen Unterlagen zugelassen werden.

2. Im Ausführungsgesetz muß bestimmt werden, daß die erkennungsdienstlichen Unterlagen zu vernichten sind, sobald die Identität festgestellt ist.

3. In das Personalausweisregister dürfen nur die im Personalausweis enthaltenen personenbezogenen Daten (§ 1 Abs. 2 Personalausweisgesetz) sowie Vermerke über Anordnungen nach § 2 Abs. 2 Personalausweisgesetz aufgenommen werden. Von der Aufnahme der Angabe "unveränderliche Kennzeichen" (§ 11 Abs. 2 Nr. 6 des Formulierungsvorschlags) muß abgesehen werden.

4. Der Zweck des Personalausweisregisters ist im Ausführungsgesetz selbst festzulegen. Hierbei ist zu berücksichtigen, daß es nicht Aufgabe dieses Registers sein kann, eine weitere umfassende Identifizierungsdatei neben dem Melderegister zu eröffnen, zumal dadurch weitere Daten (Lichtbild und Unterschrift) mit den Meldedaten verknüpft werden können. Datenübermittlungen an andere öffentliche Stellen und an Private sind auszuschließen. Eine Ausnahme darf nur für Übermittlungen an die Polizei zugelassen werden, wenn es im Einzelfall für deren Aufgabenerfüllung erforderlich ist.

5. Spätestens fünf Jahre nach Ablauf der Gültigkeit des Personalausweises sind die Daten im Personalausweisregister ohne Einschränkung zu löschen.

   Für die Ausstellung eines vorläufigen Personalausweises reicht eine kürzere Aufbewahrungsdauer aus. Entsprechend § 10 Abs. 4 des Entwurfs des Niedersächsischen Ausweisgesetzes sollten die Daten höchstens bis zu einem Jahr nach Ablauf des Jahres der Gültigkeitsdauer aufbewahrt werden.

6. Für Daten der Personen, die im Fall der Entmündigung, wegen Geisteskrankheit oder im Fall dauernder Anstaltsunterbringung von der Ausweispflicht befreit worden sind, ist wegen der damit gegebenen Sonderstellung eine strenge Verwendungsbeschränkung vorzusehen.

7. In den Verwaltungsvorschriften zum Ausführungsgesetz der Länder müssen das Verfahren bei Mitteilungen über den Verlust des Personalausweises geregelt und das Formular festgelegt werden.

C) Bereichsspezifische Datenschutzregelungen

1. Soweit die Regelungen in den Meldegesetzen der Länder dem Melderechtsrahmengesetz entsprechen, sind die datenschutzrechtlichen Anforderungen erfüllt. Die Speicherung der Seriennummer, die in einigen Landesmeldegesetzen in den Datenkatalog aufgenommen wurde, widerspricht dem in § 3 Abs. 4 Satz 1 Personalausweisgesetz festgelegten Nutzungsverbot, erhöht die mit der Maschinenlesbarkeit des Personalausweises verbundenen Gefahren und ist überdies im Hinblick auf die Fälschungssicherheit des Ausweises überflüssig.

2. Durch die Maschinenlesbarkeit des Ausweises werden die nachfolgend aufgeführten datenschutzrechtlichen Probleme verschärft, deren Lösung die Datenschutzbeauftragten von Bund und Ländern bereits früher gefordert haben, die aber durch die bisher erlassenen polizeilichen Richtlinien (insbesondere KpS-und Dateienrichtlinien sowie die Regelung über die Amtshilfe zwischen Bundesgrenzschutz und Nachrichtendiensten) noch nicht erreicht ist:

   2.1 Im Polizeirecht des Bundes und der Länder und im Strafverfahrensrecht sind gesetzliche Grundlagen für die Informationsverarbeitung der Polizei, insbesondere für die polizeiliche Beobachtung und die Identitätsfeststellung zu schaffen. Ziel dieser Regelung muß es auch sein, den Umfang der Personenkontrollen im Hinblick auf die Nutzung des maschinenlesbaren Ausweises zu begrenzen.

   2.2 Zulässigkeit und Grenzen des Informationsaustausches zwischen Polizei und den Nachrichtendiensten sind gesetzlich zu regeln.

   2.3 Der Beschluß der Innenministerkonferenz vom 2. September 1977, der vorsieht, daß alle Personen, die der Polizei bei der Erfüllung ihrer Aufgaben bekannt werden, durch Abfrage in der Personenfahndungsdatei überprüft werden, muß aufgehoben werden. Die vorhandenen Rechtsgrundlagen lassen eine derart umfassende Überprüfung nicht zu. Das gleiche gilt für einen routinemäßigen Abgleich mit den Fahndungsdateien im Rahmen von Verkehrskontrollen.

   2.4 Eine Rechtsgrundlage für den Anschluß der Länderpolizeien an die zollrechtliche Überwachung ist nicht ersichtlich. Dieser Anschluß ist zu lösen.

3. Für die Praxis der Polizeikontrollen, insbesondere unter Verwendung des maschinenlesbaren Personalausweises, sind Richtlinien zu erlassen, die den Grundsatz der Verhältnismäßigkeit konkretisieren.

D) Zum Entwurf eines Paßgesetzes

Die gleichen datenschutzrechtlichen Forderungen gelten für die mit dem Entwurf eines Paßgesetzes vorgesehene Einführung eines maschinenlesbaren Passes.

Darüber hinaus behält sich die Konferenz weitere Forderungen zum Paßgesetz vor.

5.2
Zur Volkszählung (Ziff. 1.1.1 und 1.2)

5.2.1
Zwischenbericht des Hessischen Datenschutzbeauftragten zur Volkszählung 1983 vom 14. März 1983 (Drucks. 10/573 - vom Abdruck wird abgesehen)

5.2.2
Beschluß der Konferenz der Datenschutzbeauftragten der Länder und des Bundes am 22. März 1983 zur Volkszählung '83

I.
Die Konferenz beobachtet die wachsende Unruhe in der Bevölkerung über die bevorstehende Volkszählung '83. Die Datenschutzbeauftragten haben Verständnis für die Sorgen der Bürger. Die anhängigen Verfassungsbeschwerden geben Gelegenheit, die Verfassungsmäßigkeit der Volkszählung zu prüfen.
Das Volkszählungsgesetz weist einige Unklarheiten und Schwachstellen auf. Die Konferenz erinnert deshalb an die schon 1979 von Datenschutzbeauftragten im Laufe des Gesetzgebungsverfahrens vorgebrachten Bedenken. Diese richteten sich vornehmlich gegen die Durchbrechung des Prinzips der Trennung von Statistik und Verwaltungsvollzug, insbesondere

- gegen die Verbindung einer statistischen Erhebung mit der Aktualisierung der Melderegister
- gegen die Übermittlung nicht anonymisierter Volkszählungsdaten durch die Statistischen Landesämter an Dritte
- gegen die unklare Reichweite des Benachteiligungsverbotes.

Die Konferenz stellt fest, daß die Volkszählungserhebungsbogen den Bestimmungen des Volkszählungsgesetzes, des Bundesstatistikgesetzes und der Datenschutzgesetze nicht in allen Punkten entsprechen, und zwar weil

- nicht darauf hingewiesen wird, daß jeder Auskunftspflichtige einen eigenen Haushalts- und Wohnungsbogen ausfüllen kann, damit er nicht anderen Auskunftspflichtigen seine personenbezogenen Daten offenbaren muß
- der Hinweis auf das Verbot von Maßnahmen gegen den Auskunftspflichtigen mißverständlich ist, da nicht jeglicher Nachteil für den Betroffenen ausgeschlossen werden kann
- der Namensteil von den sonstigen Daten nicht abgetrennt werden kann
- nicht auf die Freiwilligkeit derjenigen Angaben hingewiesen wird, zu deren Beantwortung keine Verpflichtung besteht.

II.
Die Datenschutzbeauftragten haben sich seit langem bei den für die Durchführung der Volkszählung zuständigen öffentlichen Stellen für die Gewährleistung datenschutzrechtlicher Anforderungen eingesetzt. Die Konferenz begrüßt, daß entsprechende Maßnahmen in einem Teil der Länder bereits vorgesehen sind. Soweit die nachstehenden Anforderungen nicht bereits berücksichtigt sind, fordert die Konferenz:

- Zähler dürfen nicht in unmittelbarer Nähe ihres Wohngebietes eingesetzt werden,
- auf den Einsatz von Zählern, bei denen im Hinblick auf ihre dienstliche Tätigkeit Interessenkonflikte nicht auszuschließen sind, sollte verzichtet werden,
- der Bürger muß auf sein Recht hingewiesen werden, den Volkszählungsbogen der Erhebungsstelle im verschlossenen Umschlag direkt zuzuleiten oder abzugeben, wenn er nicht wünscht, daß der Zähler von den Angaben Kenntnis erhält,
- die Bürger sind darüber aufzuklären, daß niemand verpflichtet ist, seine Daten einem anderen Auskunftspflichtigen zu offenbaren; daher ist jedem Auskunftspflichtigen, sofern er dies verlangt, ein eigener Bogen auszuhändigen,
- die Bürger müssen darauf hingewiesen werden, daß die Beantwortung der nachstehend genannten Fragen freiwillig ist

  Telefonnummer,

  Fragen an Diplomaten und Angehörige ausländischer Streitkräfte, soweit sie über die diesbezügliche Zugehörigkeit hinausgehen,

  Gründe für die Nichtzahlung von Löhnen und Gehältern (Arbeitsstättenbogen)

- den Meldebehörden dürfen nur die zum Melderegistervergleich erforderlichen Daten zur Verfügung gestellt werden; es ist unzulässig, den Meldebehörden den kompletten Erhebungsbogen zugänglich zu machen,
- eine Berichtigung des Melderegisters darf erst nach einem förmlichen melderechtlichen Verfahren erfolgen, in dem der Bürger Gelegenheit zur Äußerung erhält,
- die Bürger müssen darüber aufgeklärt werden, daß das Verbot von Maßnahmen gegen den Betroffenen beim Melderegistervergleich kein striktes Verwertungsverbot darstellt, das jegliche Benachteiligung des Betroffenen nach Berichtigung des Melderegisters ausschließt,
- außer für den Melderegistervergleich dürfen die Gemeinden Einzelangaben aus den Erhebungsbogen nicht für eigene Zwecke verwenden,
- eine Datenübermittlung im Rahmen des § 9 Abs. 2-4 VZG darf nur im Rahmen des Erforderlichen stattfinden. In aller Regel dürfen nur statistische Ergebnisse übermittelt werden. Eine Übermittlung von Einzelangaben, insbesondere von Straße und Hausnummer, ist ausgeschlossen, wenn die Übermittlung aggregierter Daten ausreicht.
- Im Rahmen von § 9 Abs. 2 VZG dürfen Einzelangaben nur für statistische und planerische Zwecke übermittelt werden. Deshalb läßt das VZG nicht zu, daß z.B. Polizei, Verfassungsschutz, Sozialbehörden und Finanzämter Einzelangaben erhalten.
- Im Rahmen von § 9 Abs. 3 VZG dürfen den Gemeinden Einzelangaben nur für eine bestimmte statistische Aufbereitung zur Verfügung gestellt werden. Die Übermittlung muß auf die für die jeweilige statistische Aufbereitung erforderlichen Angaben beschränkt werden: dazu gehört in keinem Fall der Name.
- Die Statistischen Landesämter haben in jedem Einzelfall zu prüfen, ob die angeforderten Daten zur Erfüllung des angegebenen und zulässigen Zwecks erforderlich sind.
- Der zuständige Datenschutzbeauftragte ist über alle Übermittlungen von Einzelangaben aus der Volkszählung durch die Statistischen Ämter des Bundes und der Länder zu unterrichten.
- Die Erhebungsunterlagen sind nach Übernahme der Daten auf elektronische Datenträger, spätestens jedoch Ende 1984 zu vernichten. Gleichzeitig sind Kennummer und Zählerlistennummer zu löschen.

III.
Die Datenschutzbeauftragten werden verstärkte Kontrollen bei der Ausführung des VZG durchführen. Sie werden dabei insbesondere

- die Erhebung der Daten,
- das Verfahren des Melderegistervergleichs,
- die Aufbewahrung, Auswertung und Vernichtung der Erhebungsunterlagen bei den Statistischen Landesämtern sowie die Übermittlung statistischer Einzelangaben und ihre Verwendung beim Empfänger

prüfen und die Öffentlichkeit über die Ergebnisse der Prüfungen unterrichten.

IV.
Wird diesen Forderungen der Datenschutzbeauftragten Rechnung getragen, so sind nach ihrer Überzeugung die Sorgen der Bürger im wesentlichen unbegründet.

Bremerhaven, 22. März 1983

5.2.3
Stellungnahme des Hessischen Datenschutzbeauftragten vom 25. März 1983 zu den Anträgen auf Erlaß einer einstweiligen Anordnung gegen das Volkszählungsgesetz '83

I. Zur Zulässigkeit der Verfassungsbeschwerden

Die Verfassungsbeschwerden richten sich unmittelbar gegen ein Gesetz. Ständiger Rechtsprechung des Bundesverfassungsgerichts zufolge ist Voraussetzung für die Zulässigkeit einer Verfassungsbeschwerde gegen eine Rechtsnorm, daß der Beschwerdeführer selbst, gegenwärtig und unmittelbar durch das Gesetz betroffen ist (zuletzt BVerfGE 60, 370).

Durch die im Gesetz über eine Volks-, Berufs-, Wohnungs- und Arbeitsstättenzählung (Volkszählungsgesetz 1983 -VZG) normierte Auskunftsverpflichtung des Bürgers wird in das allgemeine Persönlichkeitsrecht im Sinne von Artikel 2 Abs. 1 in Verbindung mit Artikel 1 Abs. 1 GG eingegriffen. Dieser Auskunftsverpflichtung unterliegen alle volljährigen oder einen eigenen Haushalt führenden minderjährigen Personen (§ 5 Abs. 1 Nr. 1 VZG). Inhalt und Reichweite der Auskunftsverpflichtung werden durch das VZG abschließend festgelegt. Die Auskunftsverpflichtung des Bürgers ergibt sich damit unmittelbar aus dem Gesetz. Das Gesetz geht allerdings davon aus, daß eine besondere Aufforderung des Bürgers zur Auskunftserteilung erfolgt. Gegen diese Aufforderung kann der Bürger Widerspruch einlegen, der freilich keine aufschiebende Wirkung hat (§ 5 Abs. 2 VZG). Das Bundesverfassungsgericht hat in diesem Zusammenhang auf die Gesichtspunkte des Rechtsschutzbedürfnisses sowie der Subsidiarität hingewiesen. Beide fallen vor allem dann ins Gewicht, wenn das Gesetz der Verwaltung einen Auslegungsspielraum läßt. Fehlt ein solcher Spielraum, so kann ausnahmsweise ein Rechtsschutzbedürfnis für die unmittelbare Anfechtung eines Gesetzes bereits vor Erlaß des Vollziehungsaktes zu bejahen sein (ständige Rechtsprechung, z.B. BVerfGE 59, 18; 43, 386; 60, 379). Im konkreten Fall besteht für die Verwaltung kein Auslegungs- und Entscheidungsspielraum, da das VZG Inhalt und Reichweite der Auskunftsverpflichtung abschließend regelt. Zudem sind die zentralen rechtlichen Bedenken gegen das VZG verfassungsrechtlicher Art. Das Bundesverfassungsgericht müßte sich daher voraussichtlich auch in den Fällen, in denen zunächst ein Verwaltungsgericht angerufen würde, im Wege der konkreten Normenkontrolle mit dem VZG befassen.

II. Zu Fragen der materiellen Verfassungsmäßigkeit - Die Verknüpfung von Statistik und Verwaltungsvollzug

1. Das Trennungsprinzip - Strukturmerkmal der amtlichen Statistik

Die Volkszählung ist das "Kernstück der statistischen Bestandsaufnahme" - so heißt es in der amtlichen Begründung des Gesetzes. Sie soll die "unentbehrlichen Grundlagen" für gesellschafts- und wirtschaftspolitische Entscheidungen des Bundes, der Länder und Gemeinden schaffen. Gegenstand der Volkszählung sind Struktur und Stand der Bevölkerung, ihre Arbeitsstätten und Wohnungen. Zahlreiche Rechtsvorschriften nehmen auf die Ergebnisse der Volkszählung Bezug. Die Wahlkreiseinteilung, der kommunale Finanzausgleich sowie die Schulentwicklungs- und Verkehrsplanung basieren auf den Daten der Volkszählung. Neben Staat, Parteien und Tarifpartnern ist auch die Wissenschaft auf anonymisierte aktuelle Mikrodaten angewiesen. Die Daten aus der Volkszählung bilden schließlich die statistische Grundgesamtheit für repräsentative Befragungen auf Stichprobenbasis. Nicht zuletzt deshalb hat die Europäische Gemeinschaft in der Richtlinie Nr. 73/403 die Notwendigkeit von Volkszählungen bestätigt. Sie kommt gleichermaßen in einer Empfehlung der Vereinten Nationen zum Ausdruck.

Ein Strukturmerkmal der Statistikgesetze ist die strikte Trennung statistischer Zwecke und administrativer Ziele. Eine amtliche Statistik ist genau genommen nur möglich, solange an dieser Trennung festgehalten wird. Sie beruht auf dem Gedanken, daß Informationen, die von einem Bürger für statistische Zwecke gegeben werden, prinzipiell gegenüber der Verwaltung abgeschottet und damit auch sanktionslos bleiben. Selbst wenn der Bürger im Rahmen einer statistischen Erhebung Angaben macht, die auf ein gesetzwidriges Verhalten schließen lassen, braucht er keinerlei Konsequenzen zu befürchten. Die funktionale Trennung von Administration und Statistik, die im Statistikgesetz durch Geheimhaltung und Anonymisierung ihren Ausdruck findet (vgl. § 11 Bundesstatistikgesetz -BStatG -), garantiert, daß z. B. niemand, der für die Statistik des produzierenden Gewerbes andere Angaben zum Umsatz macht als gegenüber dem Finanzamt, mit einem auf die statistischen Einzelangaben gegründeten Steuerstrafverfahren rechnen muß. Dieser Grundsatz leuchtet umso mehr ein, als sonst der Bürger unter Strafandrohung (vgl. § 10 BStatG) verpflichtet wäre, Angaben zu machen, mit denen er sich selbst u.U. einer strafbaren Handlung bezichtigte.

Zudem: Nur die strikte Abschottung der Statistik und die Geheimhaltung der statistischen Einzelangaben sichern die Auskunftsbereitschaft des Bürgers. Erst wenn er darauf vertrauen kann, daß statistische Information sedimentäre Information bleibt und sich nicht als Grundlage für Verwaltungsmaßnahmen gegen ihn richten kann, ist die amtliche Statistik überhaupt funktionsfähig.

2. Trennungsgrundsatz, Nachteilsverbot und Rechtsstaatsprinzip

Im Volkszählungsgesetz ist diese Trennung von Statistik einerseits und Verwaltungsvollzug andererseits aufgehoben. Zulässig ist zunächst nach § 9 Abs. 1 VZG der Abgleich einiger ausgewählter Daten (Name, Anschrift, Geschlecht, Geburtsdatum, Familienstand, Religionszugehörigkeit, Nutzung der Wohnung als Haupt- oder Nebenwohnung) mit den Melderegistern der Gemeinden.

Dieser Abgleich erfolgt zu zwei verschiedenen Zwecken: Zum einen soll er der sich aus dem Melderecht (vgl. z.B. § 43 des Hessischen Meldegesetzes vom 14. Juni 1982) ergebenden Verpflichtung der Gemeinden dienen, "auf der Grundlage der Erhebung der nächsten Volkszählung innerhalb von zwei Jahren nach dem Stichtag der Volkszählung" (a.a.O.) die Hauptwohnung von Bürgern mit mehreren Wohnungen festzustellen. Zum anderen sollen die im Melderegister enthaltenen Daten vervollständigt bzw. aktualisiert werden. So sollen die Gemeinden z.B. mit Hilfe der durch die Volkszählung erhobenen Daten von ihnen noch nicht bekannte Änderungen im Familienstand oder

der Religionszugehörigkeit erfahren, vor allem aber auch den Aufenthalt bisher nicht gemeldeter Personen in ihrem Bereich. Über das Melderegister werden die bei der Volkszählung erhobenen Daten an zahlreiche weitere Behörden und Privatpersonen gelangen. Gemäß § 1 Abs. 2 Nr. 1 und 2 Melderechtsrahmengesetz ist die Übermittlung von Daten aus dem Melderegister an Behörden und Privatpersonen nach Maßgabe dieses Gesetzes oder anderer Rechtsvorschriften zulässig. Tatsächlich bildet das Melderegister eine zentrale Informationsgrundlage für viele Bereiche der Verwaltung, so z.B. auch die Ausländerbehörden, die Polizeibehörden und die Sozialbehörden, ferner auch für die Rechtspflege und die Religionsgesellschaften (vgl. § 19 Melderechtsrahmengesetz). Zu berücksichtigen ist hierbei auch, daß den Meldebehörden über ihre klassische Aufgabe hinaus - den Nachweis von Identität und Wohnung der Einwohner - durch Bundesrecht eine Reihe zusätzlicher Aufgaben übertragen wurden, so z.B. die Mitwirkung bei der Ausstellung von Lohnsteuerkarten und Pässen, bei der Wehr- oder Zivildienstüberwachung und bei der Vorbereitung von Wahlen zum Deutschen Bundestag sowie zum Europäischen Parlament.

Der Grundsatz der Trennung von Statistik und Verwaltung wird durch den Abgleich mit dem Melderegister durchbrochen. Das Gesetz sieht ferner in § 9 Abs. 2-4 VZG auch die Übermittlung von personenbezogenen Einzelangaben an oberste Bundes- und Landesbehörden, an Gemeinden und Gemeindeverbände sowie wissenschaftliche Institutionen vor.

Die verfassungsrechtliche Beurteilung knüpft an folgende Gesichtspunkte an:

Die im VZG normierte Verpflichtung des Bürgers zur Auskunftserteilung ist ein Eingriff in das allgemeine Persönlichkeitsrecht i.S. von Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG. Als grundrechtseinschränkendes Gesetz muß das Volkszählungsgesetz selbst im Einklang mit der verfassungsmäßigen Ordnung stehen. Zur verfassungsmäßigen Ordnung zählt auch das in Art. 20 Abs. 3 GG verankerte Rechtsstaatsprinzip. Das Rechtsstaatsprinzip stellt bestimmte allgemeine Anforderungen an Gesetze, die vom Bundesverfassungsgericht in einer Reihe von Entscheidungen konkretisiert wurden. Ein Gesetz darf nicht in sich widerspruchsvoll sein, es muß eine innere Folgerichtigkeit aufweisen. Gesetze müssen den rechtsstaatlichen Grundsätzen der Normenklarheit und Justiziabilität entsprechen. Die mit dem Gesetz verfolgten Zwecke müssen für den Bürger klar erkennbar sein; er muß die Gesetze verstehen und die sich für ihn möglicherweise ergebenden Konsequenzen erkennen können. Gesetze müssen deshalb in ihren Voraussetzungen und in ihrem Inhalt so formuliert sein, daß die Betroffenen die Rechtslage erkennen und ihr Verhalten danach einrichten können (vgl. u.a. BVerfGE 1, 45 f.; 17, 318; 21, 79; 47, 247). Diesen Anforderungen genügt das VZG nicht.

Dies zeigt sich an den Vorschriften des § 9 Abs. 1 S. 2, Abs. 2 S. 3 und Abs. 3 S. 3 VZG über das Nachteilsverbot. Danach dürfen aus den statistischen Angaben gewonnene Erkenntnisse nicht zu Maßnahmen gegen den einzelnen Auskunftspflichtigen verwendet werden. Vom Bürger wird diese Vorschrift regelmäßig als umfassende Zusicherung verstanden, daß ihm aus der Beantwortung des Fragebogens weder unmittelbare noch mittelbare Nachteile erwachsen können. Für diese Interpretation der Vorschrift spricht auch, daß sie fast wortgleich aus § 11 Abs. 3 S. 3 BStatG übernommen wurde, einer Bestimmung also, die nach einhelliger Meinung weder unmittelbare noch mittelbare Nachteile für den Auskunftspflichtigen zuläßt. Hinzuweisen ist auch auf die amtliche Begründung zum VZG, nach der § 9 Abs. 1 S. 2 VZG den Gemeinden ausdrücklich untersagt, "Erkenntnisse aus den statistischen Einzelangaben unmittelbar oder mittelbar gegen den Auskunftspflichtigen oder sonst Betroffenen zu verwenden" (BT-Drucks. 9/451, S. 11).

Ein so umfassend verstandenes Nachteilsverbot kann jedoch wegen der im VZG vorgenommenen Verknüpfung von Statistik und Verwaltungsvollzug weder rechtlich noch faktisch realisiert werden. Rechtlich nicht, weil die Behörden, denen die Daten übermittelt werden sollen (so z. B. die Meldeämter), ihren gesetzlichen Verpflichtungen nachkommen müssen. Das VZG als eine Rechtsvorschrift des Bundes, die eine Bundesstatistik anordnet, kann weder Landesgesetze noch Bundesgesetze, die andere Materien regeln (wie z.B. das Ausländergesetz oder die Strafprozeßordnung), abändern oder gar derogieren. So dürfte z.B. von der Ausweisung eines Ausländers, der sich illegal in der Bundesrepublik aufhält, nicht deshalb abgesehen werden, weil sein Aufenthalt durch die Volkszählung bekannt wurde. Ebenso wenig etwa dürften von den Meldeämtern zum Zwecke der Festnahme oder Aufenthaltsermittlung vorhandene Suchvermerke deshalb ignoriert werden, weil die Wohnung eines Betroffenen durch die Volkszählung aufgedeckt wurde. Faktisch kann ein derartiges Nachteilsverbot deshalb nicht realisiert werden, weil sich die aus der Volkszählung gewonnenen Angaben nach der Übermittlung an andere Behörden dort mit anderen Daten vermischen. Die melderechtlichen Vorschriften der Länder sehen in der Regel keine Speicherung des Grundes einer Änderung im Melderegister vor. Soweit die Register - was bereits in weit überwiegendem Umfang der Fall ist - automatisiert geführt werden, ist die Speicherung und Verarbeitung dieses Merkmals in der Praxis nicht vorgesehen und faktisch kaum möglich. Demzufolge wird eine besondere Verarbeitung dieser Angaben, die Nachteile für die Betroffenen ausschließt, nicht möglich sein. Damit ist die Tragweite des Nachteilsverbots im Sinne von § 9 Abs. 1 S. 2 VZG insgesamt unklar. Der Bürger kann die sich für ihn möglicherweise ergebenden Folgen nicht erkennen; er wird sich vielmehr im Regelfall eine falsche Vorstellung von der Tragweite der gesetzlichen Zusicherung machen. Im übrigen ist auch der Adressatenkreis des Benachteiligungsverbotes nicht klar. Die Verantwortlichkeit für seine Einhaltung wird nicht eindeutig festgelegt.

3. Trennungsprinzip und Anonymisierungsgebot

Die Verknüpfung statistischer und administrativer Ziele führt zu einer Übermittlung nichtanonymisierter Daten an die Verwaltung. Dies gilt zunächst für § 9 Abs. 1 VZG und den damit verbundenen Melderegisterabgleich. Dies gilt aber auch für § 9 Abs. 2 bis 4 VZG. Danach können "Einzelangaben ohne Namen" zu bestimmten Zwecken an eine Reihe im Gesetz bezeichneter Stellen weitergegeben werden. Solange von den nach dem VZG zu erhebenden personenbezogenen Daten lediglich der Name weggelassen wird, ist beispielsweise mit dem in einer Gemeinde vorhandenen Zusatzwissen eine Identifizierung des Betroffenen möglich. Das Bundesverfassungsgericht hat sich mit der Bedeutung der Anonymisierung im Mikrozensusbeschluß auseinandergesetzt. Das Gericht hat in dieser Entscheidung zwei Kriterien für die verfassungsrechtliche Zulässigkeit von Statistiken aufgestellt. Einmal darf die Statistik nicht den Bereich menschlichen Verhaltens erfassen, der von Natur aus Geheimnischarakter hat. Wie auch immer man den Begriff der Intimsphäre versteht, den das Bundesverfassungsgericht auch als "unantastbaren Bereich privater Lebensgestaltung" definiert, ist das gesetzliche Frageprogramm des VZG als solches wohl kaum bedenklich. Der im VZG vorgesehene Datenkatalog ist im Vergleich zum VZG 1970 und zum Mikrozensusgesetz entscheidend eingeschränkt.

Aber auch dort, wo dieser Bereich nicht tangiert wird, ist eine statistische Erhebung nur verfassungskonform, wenn diese Angaben durch die Anonymität ihrer Auswertung den Persönlichkeitsbezug verlieren und die Anonymität ausreichend gesichert ist. Diese Voraussetzungen sind beim Mikrozensus in seiner bisherigen Ausgestaltung gegeben, weil eine Übermittlung zu Verwaltungszwecken nicht vorgesehen ist. Das Gericht stellte ausdrücklich fest, daß statistische Ämter auch ihrer vorgesetzten Dienststelle keine Einzelangaben auf dem Dienstweg weiterleiten dürfen.
Der Verzicht auf den Personenbezug der statistischen Auswertung begrenzt also die administrative Verwertung der Daten. Das Prinzip der funktionalen Trennung von Statistik und Verwaltungsvollzug ist nicht nur von der Sache geboten, sondern eine Konkretisierung des allgemeinen Persönlichkeitsrechts i.S.v. Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG im Bereich der amtlichen Statistik. Es ist praktischer Grundrechtsschutz durch organisatorische Struktur. § 9 Abs. 1-4 VZG steht mithin nicht im Einklang mit diesem aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 abgeleiteten Prinzip.

Hinsichtlich der Folgen wäre eine Unterscheidung der Fälle des § 9 Abs. 1 einerseits und der Fälle des § 9 Abs. 2-4 VZG andererseits möglich. Soweit § 9 Abs. 2-4 VZG betroffen ist, könnte - anders als beim Melderegisterabgleich nach § 9 Abs. 1 VZG - über eine verfassungskonforme Auslegung eine Anonymisierung sichergestellt werden. Die Übermittlung dürfte sich in diesem Fall jedoch nur auf faktisch anonymisierte Angaben erstrecken.

Diese Feststellungen berücksichtigen ihrerseits noch nicht die automatisierte Verarbeitung personenbezogener Daten bei der amtlichen Statistik und in der öffentlichen Verwaltung. Selbst an und für sich harmlos erscheinende Daten aus der Volkszählung können, verknüpft mit anderen Daten, Gefahren erzeugen, die mit den Kategorien des Mikrozensusbeschlusses nicht mehr adäquat zu beschreiben sind. Die Möglichkeit, durch Vernetzung und Verknüpfung von Daten aus den verschiedensten Zusammenhängen den Menschen in seiner ganzen Persönlichkeit zu registrieren und zu katalogisieren, läßt auch Daten von an sich geringer Sensitivität in anderem Licht erscheinen. Der Verlust des Kontextes, in dem die Daten erhoben und verarbeitet werden, bringt gerade in diesen Fällen Gefahren für den Einzelnen mit sich. Nicht die Informationen an sich, sondern ihre dysfunktionale Weitergabe, auf die der Betroffene keinen Einfluß hat, zerstört die Privatsphäre. Diesen Gesichtspunkt auch in die verfassungsrechtliche Prüfung des VZG zu integrieren,wäre aus meiner Sicht eine notwendige Reaktion des Gerichts auf die Gefahren moderner Informationstechnologien.

III. Zur einstweiligen Anordnung

1.

Der Hauptsacheantrag ist, wie die Darlegungen zur verfassungsrechtlichen Problematik der Übermittlungsbestimmungen des § 9 VZG deutlich gemacht haben (vgl. oben II), nicht offensichtlich unbegründet. Es besteht auch ein Interesse, daß nicht vor der Entscheidung des Bundesverfassungsgerichts vollendete Tatsachen geschaffen werden. Die Durchführung der Volkszählung, so wie das Gesetz sie vorsieht, würde einer nachträglichen verfassungsgerichtlichen Entscheidung die Wirkung nehmen, die in der Verhinderung einer verfassungswidrigen Maßnahme liegt (BVerfGE 7, 370). Ist der Melderegisterabgleich erfolgt oder haben andere Übermittlungen von Daten aus der Volkszählung (§ 9 Abs. 2-4 VZG) bereits stattgefunden, bevor das Bundesverfassungsgericht in der Hauptsache entschieden hätte, dann könnte eine bloße Feststellung, daß das Volkszählungsgesetz ganz oder teilweise verfassungswidrig ist, die Wirkungen dieser Datenübermittlungen nicht mehr verhindern.

Ein Rechtsschutzbedürfnis der Beschwerdeführer besteht jedenfalls dann, wenn die Verfassungswidrigkeit eines Gesetzes geltend gemacht wird, das die Grundlage für eine nur einmalige und nicht wiederholbare Maßnahme abgibt. Die Beschwerdeführer sind verpflichtet, Auskunft über ihre Daten zum Stichtag der Volkszählung zu geben. Im Gegensatz zu den statistischen Auswertungsverfahren entfalten die Übermittlungsbestimmungen des § 9 VZG sofortige und unmittelbare Wirkung. Insbesondere die Berichtigung der Melderegister anhand der erhobenen Daten steht in einem engen zeitlichen Zusammenhang mit der Befragung selbst. Bedenken gegen die Zulässigkeit einer einstweiligen Anordnung bestehen insofern nicht.

2.
Eine einstweilige Anordnung ist begründet, wenn sie zur Abwehr schwerer Nachteile oder aus einem anderen wichtigen Grund zum gemeinen Wohl dringend geboten ist (§ 32 Abs. 1 BVerfGG).

Das VZG verpflichtet - wie bereits erwähnt - den Bürger dazu, zu einem bestimmten Stichtag eine Reihe seiner personenbezogenen Daten bereitzustellen. Nach dem Erhebungsplan sollen zwischen dem 22. und 26. April 1983 die Erhebungsbögen durch die Zähler an die Bevölkerung ausgeteilt werden. Zwischen dem 28. April und dem 11. Mai 1983 sind die ausgefüllten Erhebungsbögen von den Zählern einzusammeln. Spätestens zum letztgenannten Zeitpunkt muß der Bürger seine Mitwirkungspflicht erfüllt haben. Danach hat der Bürger keinen Einfluß mehr auf die Verwendung seiner Daten. Dies gilt sowohl für die weitere Aufbereitung zu statistischen Zwecken als auch für den Abgleich mit den örtlichen Melderegistern und die sich daran anschließenden Datenübermittlungen an andere Stellen der öffentlichen Verwaltung. Über die allgemeine Melderegisterauskunft gelangen Angaben aus der Volkszählung auch an private Unternehmen, Einrichtungen und Personen.

Insbesondere der Melderegisterabgleich steht in einem unmittelbaren zeitlichen Zusammenhang mit dem Einsammeln der Erhebungsbögen. Für diese Berichtigung des Melderegisters steht den Gemeinden der Zeitraum vom 11. Mai bis spätestens 10. Juni 1983 zur Verfügung; danach sind die Erhebungsbögen an die Statistischen Landesämter weiterzuleiten. Die Nutzung der für die Volkszählung erhobenen Daten zu administrativen Zwecken nach § 9 Abs. 1 VZG schließt sich insofern direkt an die Phase der Erhebung an. Ohne den Erlaß einer einstweiligen Anordnung wird es deshalb in jedem Fall zu Übermittlungen noch vor der Endentscheidung des Gerichts kommen. Von besonderer Bedeutung ist hierbei, daß nach der Aktualisierung der Melderegister eine Überprüfung der Tatsache, ob bestimmte Änderungen aufgrund des Verfahrens nach § 9 Abs. 1 VZG erfolgt sind, nicht mehr möglich ist. Nicht nur bei den Meldeämtern selbst, sondern auch bei allen weiteren Empfängern dieser geänderten Angaben kann damit der Nachweis, daß ein bestimmtes Datum aufgrund des Verfahrens nach § 9 Abs. 1 VZG in den Verwaltungsvollzug gelangt ist, nicht geführt werden. Auch die mittelbaren Folgen der Verarbeitung dieser Daten in den übrigen Teilen der öffentlichen Verwaltung wären nicht mehr rückgängig zu machen. Aus diesen Überlegungen ergibt sich, daß eine uneingeschränkte Durchführung des Gesetzes nicht revidierbare Folgen für die betroffenen Bürger hat.

Andererseits: Käme es zu einer auf § 9 Abs. 1-4 VZG bezogenen einstweiligen Anordnung, so hätte dies sicherlich Auswirkungen auf die Gemeinden und die öffentlichen Stellen, die Daten aus dem Melderegister beziehen. In erster Linie ist an die sich aus dem Melderecht ergebende Verpflichtung der Gemeinden zu denken, die Hauptwohnung von Bürgern mit mehreren Wohnsitzen festzustellen. Die Gemeinden sind an einer Aktualität der Daten interessiert. Eine Verzögerung des Abgleichs könnte diese Aktualität in Frage stellen. Allerdings könnte eine Korrektur des Status der Wohnung in jedem Fall erst nach einer vorherigen besonderen Anhörung des Bürgers erfolgen, so daß zwischenzeitliche Änderungen berücksichtigt werden können. Entsprechendes - allerdings ohne die letztgenannte Möglichkeit - gilt auch für die Berichtigung der übrigen Angaben im Melderegister.

Dieser Nachteil muß gegen die sich für den Bürger ergebenden nicht revidierbaren sowie möglicherweise schweren Konsequenzen abgewogen werden.

Hinzu kommen zwei Aspekte: Die auch nur einmalige Verletzung fundamentaler Verfassungsprinzipien durch den nicht mehr rückgängig zu machenden, also eine vollendete Tatsache schaffenden Vollzug eines Maßnahmegesetzes muß als schwerer Nachteil für das gemeine Wohl angesehen werden. Die einstweilige Anordnung kann gerade deshalb nötig werden, weil dem Gericht die zur gewissenhaften und umfassenden Prüfung der für die Entscheidung der Hauptsache erheblichen Rechtsfragen die erforderliche Zeit fehlt (BVerfGE 7, 367).

Alle diese Gesichtspunkte sprechen für den Erlaß einer einstweiligen Anordnung, die sich allerdings auf die Aussetzung des Vollzugs des § 9 Abs. 1-4 VZG beschränken könnte.

Über den verfassungsrechtlich gebotenen Schutz des Bürgers hinaus hätte eine solche Anordnung folgende Konsequenz: Die Volkszählung könnte als rein statistische Erhebung termingerecht im vorgesehenen Umfang durchgeführt werden. Die bisher investierten Haushaltsmittel wären nicht verloren, ein nicht zuletzt im Hinblick auf die angespannte Lage der öffentlichen Haushalte wichtiger Gesichtspunkt. Vor allem aber: Die Befürchtungen und Ängste der Bevölkerung, die auf der möglichen Nutzung der statistischen Angaben zu Verwaltungszwecken beruhen, könnten dann ausgeräumt werden. Auch könnte mit einer erheblich größeren Auskunftsbereitschaft der Bevölkerung gerechnet werden. Damit würde sich auch die Chance, die für eine staatliche Planung unerläßlichen zuverlässigen Angaben zu bekommen, beträchtlich erhöhen.

IV.

Da sich die Verfassungsbeschwerde gegen ein Gesetz richtet, sehe ich von einer verfassungsrechtlichen Stellungnahme zu Fragen, die die Durchführung des Gesetzes betreffen, ab.

gez. Prof. Dr. Simitis

5.2.4
Stellungnahme des Hessischen Datenschutzbeauftragten vom 12. Juli 1983 zu den Verfassungsbeschwerden gegen das Volkszählungsgesetz '83

I.
Vorbemerkung

Die nachfolgenden Überlegungen knüpfen an die dem Bundesverfassungsgericht am 25. März 1983 vorgelegte schriftliche, in der mündlichen Verhandlung vom 12. April 1983 ergänzte Stellungnahme an. Sie gehen deshalb davon aus, daß § 9 Abs. 1 bis 4 VZG verfassungswidrig ist sowie davon, daß im übrigen schwerwiegende verfassungsrechtliche Bedenken gegen das VZG bestehen, und versuchen, diese bereits eingenommene Position anhand der vom Bundesverfassungsgericht gestellten Fragen näher zu substantiieren. Dabei werden allerdings nicht sämtliche vom Gericht angeschnittenen Problemkomplexe behandelt, sondern vor allem die Fragenbereiche, an denen sich ganz besonders nachweisen läßt, welche Konsequenzen sich aus der auch und gerade unter verfassungsrechtlichen Aspekten wichtigen Entwicklung des Datenschutzes für die Statistikgesetzgebung ergeben.

II.
Zur Zweckbindung

1.
Grundvoraussetzung eines wirksamen Datenschutzes ist eine möglichst strikte Zweckbindung der Datenverarbeitung. Ganz gleich, ob die personenbezogenen Angaben von öffentlichen oder privaten Instanzen verarbeitet werden, für die jeweils Betroffenen lassen sich die Verarbeitungsziele ebenso wie die Verarbeitungsfolgen erst in dem Augenblick verläßlich ausmachen und abschätzen, in dem Gewißheit über den Verarbeitungszweck besteht. Die Zweckbindung sichert freilich nicht nur die Transparenz der Verarbeitung, sie ist zugleich notwendige Vorbedingung einer Einschränkung der Verarbeitung. Solange die Zulässigkeit der Verarbeitung auch und vor allem an der Erforderlichkeit der Daten für den konkreten, jederzeit erkennbaren und nachprüfbaren Zweck gemessen wird, bleibt der Umfang der jeweils in Anspruch genommenen Angaben zwangsläufig beschränkt. Zugänglich ist immer nur eine Auswahl der verarbeitbaren Daten, und zwar stets in dem Maße, in dem sich ihre Beziehung zum Verarbeitungszweck begründen läßt.

Deshalb stellen die Datenschutzgesetze den Grundsatz der Erforderlichkeit in den Mittelpunkt ihrer Anforderungen. Jeder Versuch, Daten auf Vorrat zu speichern, um etwa künftige, nicht näher definierte Aufgaben zu erfüllen, verstößt daher gegen die bestehenden gesetzlichen Regelungen, ohne Rücksicht im übrigen darauf, ob sich die öffentliche Verwaltung oder ein privates Unternehmen für die Angaben interessiert (1). Die gleichen Überlegungen haben die meisten Landesdatenschutzgesetze veranlaßt, sich bei der Übermittlung personenbezogener Daten aus dem öffentlichen Bereich an nicht-öffentliche Stellen unmißverständlich für eine Verpflichtung des Empfängers auszusprechen, die übermittelten Daten nur für den Zweck zu verwenden, zu dessen Erfüllung sie ihm übermittelt wurden (2). Konsequenterweise hat die Forderung nach einer entsprechend eindeutigen Aussage von Anfang an im Vordergrund aller Reformbestrebungen des BDSG gestanden (3). Deshalb sind ferner die Bemühungen gescheitert, die Meldebehörden in ein Datendepot mit einer Vielzahl von Angaben für die unterschiedlichsten Zwecke der öffentlichen Verwaltung umzugestalten (4). Der Gesetzgeber hat sich statt dessen im Melderechtsrahmengesetz auf eine am Meldezweck orientierte Verarbeitung festgelegt (§ 1 MRRG). Aus dem gleichen Grund setzen sich schließlich, wie sich am Melderechtsrahmengesetz ebenso wie an den Vorschriften des SGB zum Sozialgeheimnis erweist, mehr und mehr die Bestrebungen durch, die öffentliche Verwaltung, jedenfalls soweit es um den Datenschutz geht, eben nicht als Einheit anzusehen, sondern strikt funktional aufzugliedern, die Verarbeitung also von der jeweiligen Aufgabe her zu betrachten und grundsätzlich auf sie zu begrenzen (5).

Die verschiedenen Ausprägungen der Zweckbindung konkretisieren freilich weit mehr als nur einen der tragenden Grundsätze der Datenschutzgesetzgebung. Jede von ihnen ist vielmehr Ausdruck der sich aus dem Grundgesetz ergebenden, den Datenschutz rechtfertigenden und erzwingenden Anforderungen. Eine demokratisch strukturierte Gesellschaft und eine rechtsstaatlich operierende Verwaltung sind mit einer beliebigen, jeder Kontrolle entzogenen Verarbeitung personenbezogener Daten unvereinbar. Wo es an klar definierten Verarbeitungsvoraussetzungen fehlt, die auch und vor allem die Zweckbindung sicherstellen, droht der einzelne unter den Bedingungen einer automatischen Verarbeitung der seine Person betreffenden Angaben zu einem letztlich uneingeschränkt manipulierbaren Informationsobjekt zu werden. Die Verarbeitungsregelung schafft, so gesehen, erst die Voraussetzungen, um die im Grundgesetz garantierten Freiheitsrechte realisieren zu können (6). Solange die sich ständig verfeinernden Verarbeitungsinstrumente ohne weiteres genutzt werden können, um ein minutiöses persönliches Profil des einzelnen aufzuzeichnen und steuernd in seine "soziale Biographie" einzugreifen, bleibt die in der Verfassung zugesicherte Autonomie Fiktion (7). Insoweit ist der Datenschutz Barriere gegen alle Versuche, "den Menschen zwangsweise in seiner ganzen Persönlichkeit zu registrieren und zu katalogisieren" (8) und damit Garant des Rechtes, "allein gelassen zu werden" (9). Anders aber als noch etwa die Mikrozensus-Entscheidung (10) vermuten läßt, liegt die Voraussetzung dafür nicht in einer wie auch immer formulierten Umschreibung "unzu-

gänglicher" Bereiche, sondern, wie sich gerade an der Datenschutzgesetzgebung und den mit ihrer Hilfe gewonnenen Erfahrungen erweist, in der gesetzlichen Festlegung von Verfahren, die zur Offenlegung der Verarbeitungsziele zwingen und damit den jeweiligen Verarbeitungskontext in den Mittelpunkt aller Überlegungen zur Zulässigkeit des Verarbeitungsprozesses stellen.

2.
Statistische Erhebungen, wie sie etwa das VZG vorsieht, widersprechen eindeutig den in den Datenschutzgesetzen festgeschriebenen Erwartungen. Sie werden nicht von der Zweckbindung beherrscht, sondern von der Absicht, die einmal erhobenen Daten für eine Vielzahl nicht näher definierbarer Zwecke zur Verfügung zu stellen. Konsequenterweise bezeichnet die Gesetzesbegründung die Volkszählung als "Kernstück der statistischen Bestandsaufnahme" (10a) und sieht in den mit ihrer Hilfe ermittelten Angaben den Ausgangspunkt für die Fortschreibung der laufenden Entwicklung sowie die Auswahlgrundlage für Repräsentativerhebungen. Die Volkszählung verfolgt, anders ausgedrückt, ein eminent methodisches Ziel: Sie soll eine gesicherte Datenbasis für weitere statistische Untersuchungen ebenso wie für den politischen Planungsprozeß vermitteln, und zwar durch eine verläßliche Feststellung der Bevölkerungszahl und ihrer Sozialstruktur. Volkszählungen liefern, verkürzt formuliert, die für jeweils ein Jahrzehnt notwendige "Referenzdatei".

Damit entfällt von vornherein die Möglichkeit einer zumindest relativ präzisen Zweckumschreibung, wie sie für die meisten gesetzlichen Regelungen über Einzelstatistiken kennzeichnend ist. Ganz gleich, ob man das Hochschulstatistik- oder das Berufsbildungsförderungsgesetz nimmt - um es bei diesen beiden Beispielen zu belassen -, mit dem ausdrücklich angegebenen Ziel der statistischen Erhebung werden zugleich die allgemeinen Grenzen des gesetzlich angeordneten Erhebungsprogramms festgelegt, wenn auch keineswegs eindeutig determiniert. Denn zur Feststellung etwa von Ausbildungsverläufen und ihrer Bewertung kann man die unterschiedlichsten Daten für aussagefähig halten, ohne dabei den generellen Rahmen der Zweckbindung der konkreten Einzelstatistik zu verlassen. Demgegenüber ist die Volkszählung ihrer ganzen Struktur und Intention nach Datensammlung auf Vorrat. Sie beschränkt sich darauf, aggregiertes Wissen zu vermitteln, auf das zu den verschiedensten Zeiten sowie für die verschiedensten Ziele zurückgegriffen werden kann. Nur solange diese Multifunktionalität gesichert ist, erfüllt sie auch ihre Aufgabe. Eben deshalb kommt der automatischen Verarbeitung bei allgemeinen statistischen Erhebungen wie der Volkszählung eine ganz besondere Bedeutung zu. Genaugenommen ermöglicht sie es erst, die Chance der Multifunktionalität voll zu nutzen. Dank der automatischen Datenverarbeitung verwandelt sich die amtliche Statistik in eine jederzeit mit den Datenbeständen aller Einzelstatistiken verknüpfbare Datenbasis, die ständig nach den jeweils für relevant gehaltenen Gesichtspunkten ausgewertet werden kann. Die Segmentierung der Bundesstatistiken und ihrer Erhebungsprogramme wird so in einem tendenziell universellen Datenbankkonzept aufgehoben.

Kein Wunder, wenn sich daher die amtliche Statistik als immer attraktiver für die unterschiedlichsten Informationserwartungen erweist. Von der mikroanalytischen Simulation, mit deren Hilfe die Folgen einzelner Politikentscheidungen im sozialen Bereich nicht zuletzt für den einzelnen Haushalt und seine Mitglieder sichtbar gemacht werden können, bis hin zu einer sich auf Sozialindikatoren gründenden Sozialberichterstattung - die amtliche Statistik stellt eine in ihrer Art und ihrem Umfang einzigartige Datenbasis zur Verfügung (11).

III.
Sicherung durch Methodenwahl

1.
Beides, die mangelnde Anbindung an einen bestimmten, jederzeit erkennbaren und nachvollziehbaren Zweck sowie die multifunktionale Verwendbarkeit der Daten, begünstigt just die Tendenzen, die durch die Datenschutzgesetze aufgefangen und eingeschränkt werden sollten. Gerade weil es von vornherein an zweckorientierten Schranken fehlt, die den Datensatz eingrenzen, sind Volkszählungen tendenziell Vehikel für jene schon im Mikrozensus-Beschluß (12) angesprochene lückenlose "Registrierung" und "Katalogisierung" des einzelnen. Vokabeln wie "Totalerhebung", die im Zusammenhang mit Volkszählungen wie selbstverständlich benutzt werden, sind bezeichnend dafür. Sie geben die Reichweite der Erhebung deutlich an und lassen damit zugleich ihre möglichen Konsequenzen erkennen.

Wie immer man jedoch Zweifel und Kritik an statistischen Erhebungen einschätzt, sie dürfen nicht dazu führen, die Bedeutung der Statistik für eine rationale, den im Grundgesetz festgeschriebenen Zielen verpflichtete staatliche Politik zu übersehen. Wenn die ökonomische und soziale Entwicklung nicht als unabänderliches Schicksal hingenommen, sondern als permanente Aufgabe verstanden werden soll, dann gibt es keine Alternative zu einer umfassenden, kontinuierlichen sowie ständig aktualisierten Information über die wirtschaftlichen, ökologischen und sozialen Zusammenhänge. Erst die Kenntnis der je relevanten Daten und die Möglichkeit, die durch sie vermittelten Informationen mit Hilfe all der Chancen, die eine automatische Datenverarbeitung bietet, voll zu nutzen, schafft die für die staatliche Politik unentbehrliche Reflexions- und Handlungsgrundlage (13). Nur so läßt sich, mit anderen Worten, die für eine hochindustrialisierte Gesellschaft kennzeichnende, ständige Zunahme der

Umweltkomplexität aufschlüsseln und für gezielte staatliche Maßnahmen aufbereiten. Kurzum, jeder Versuch, eine auf ebenso detaillierten wie exakten statistischen Erhebungen aufbauende Informationsverarbeitung zu negieren, läuft zwangsläufig darauf hinaus, die unabdingbaren Voraussetzungen sozialstaatlicher Politik in Frage zu stellen und damit zugleich "pathologische Lernprozesse" (K.W. Deutsch) der öffentlichen Verwaltung zu vervielfachen.

Der bloße Hinweis auf die noch so evidente Notwendigkeit statistischer Erhebungen reicht allerdings nicht aus. Sowohl der Gesetzgeber als auch die öffentliche Verwaltung bleiben, so sehr sie im übrigen auf die jeweilige Information angewiesen sein mögen, verpflichtet, ihre Informationserwartungen und die Art und Weise der Verwirklichung dieser Erwartungen an den möglichen Konsequenzen für die Struktur der staatlichen Organisation und Tätigkeit sowie für die jeweils Betroffenen zu messen. Die statistische Methode wird damit zum Prüfstein der Verfassungsmäßigkeit der statistischen Erhebung. Konkret: Der Staat ist bei der Methodenwahl gebunden. Er muß sich für den für die Betroffenen schonendsten Erhebungsweg entscheiden und zugleich jederzeit in der Lage sein, nachzuweisen, warum gerade dieser eine Weg unter Verhältnismäßigkeitsgesichtspunkten den Vorzug vor anderen konkurrierenden Befragungsmethoden verdient.

So gesehen ist es gleichgültig, ob eine bestimmte Methode immer schon im Zusammenhang mit Volkszählungen verwendet worden ist. Vielmehr kommt es darauf an, sich vor jeder neuen Entscheidung für eine noch so oft durchgeführte Erhebung eingehend mit dem Stand der Methodendiskussion auseinanderzusetzen, um festzustellen, ob und in welchem Umfang die tradierten Methoden der Informationserhebung und Informationsverarbeitung beibehalten werden können. Ganz in diesem Sinne hat der Deutsche Bundestag in einem Beschluß vom 15. Dezember 1982 zum "Gesetz über die Durchführung einer Repräsentativstatistik der Bevölkerung und des Erwerbslebens" (Mikrozensusgesetz) die Bundesregierung ersucht, darzulegen,

"1. in welchem Umfang auf Erhebungen nach dem Mikrozensusgesetz wegen Reduzierung oder Wegfalls der sachlichen Notwendigkeit dieser Erhebung verzichtet werden kann,

2. in welchem Umfang Erhebungen nach dem Mikrozensusgesetz durch weniger kostenintensive und gleichwertige oder bessere Umfragemethoden ersetzt werden können. Dabei sollen auch die neuesten Erkenntnisse der empirischen Sozialforschung und die Erfahrungen mit statistischen Erhebungen im Ausland bewertet und, sofern sie auf anderen Systemen beruhen, ihre Geeignetheit für die Bundesrepublik Deutschland geprüft werden." (14)

Genau daran hat es beim Volkszählungsgesetz gefehlt. Zu keinem Zeitpunkt hat sich der Gesetzgeber die Frage gestellt, ob es wirklich noch angeht, nach den bisher angewandten Methoden zu verfahren. Gewiß, verglichen mit früheren Erhebungen enthält die gesetzliche Regelung eine ganze Reihe von Modifikationen, wie sich schon allein am Fragenkatalog erweist. Soweit es allerdings um die Erhebungsmethode selbst geht, scheinen nicht die geringsten Zweifel bestanden zu haben. Alternativen zur "Totalerhebung" werden nirgendwo erwähnt, geschweige denn ausführlich diskutiert. Für den Gesetzgeber war die Volkszählung offensichtlich nicht mehr als eine periodisch wiederkehrende Erhebung, die sich deshalb nach den bislang widerspruchslos hingenommenen Voraussetzungen zu richten hatte. Damit mag zwar die Kontinuität gewahrt worden sein, die verfassungsrechtliche Verpflichtung zur konstanten Überprüfung der Erhebungsmethode blieb dagegen unbeachtet.

2.
Gründe, die es nahegelegt hätten, gerade die Erhebungsmethode zu überprüfen, gab es genug. Schon deshalb, weil längst national wie international Zweifel an der Verläßlichkeit von Vollerhebungen geäußert worden waren. Die oft sehr viel sorgfältigere und detailliertere Planung von Repräsentativerhebungen ermöglicht auch genauere Ergebnisse. Abgesehen davon sind Repräsentativerhebungen in der Regel billiger und nehmen, soweit es um die Durchführung sowie die statistische Auswertung geht, sehr viel weniger Zeit in Anspruch. Um so schneller kann auch über die Ergebnisse verfügt werden. Hinzu kommen Zweifel, die sich auf den wachsenden staatlichen Datenbestand gründen. In der Tat, je umfassender die schon vorliegenden Informationen sind, desto weniger will der Sinn einer Vollerhebung einleuchten. Weitaus verständlicher erscheint es vielmehr, die ohnenhin bereits gespeicherten Daten statistisch auszuwerten. Schließlich spricht, spätestens seit der ausdrücklichen gesetzlichen Anerkennung des Datenschutzes, das mit einer Vollerhebung verbundene, erhöhte Reidentifikationsrisiko für einen Methodenwechsel. Anders als Repräsentativerhebungen zielen Erhebungen wie die Volkszählung auf eine Abbildung der Gesamtbevölkerung. Je genauer jedoch die Abbildung demographischer und wirtschaftlicher Merkmale gerät, desto leichter fällt es letztlich, die jeweils Befragten oder den einzelnen Haushalt zu reidentifizieren. Demgegenüber schließen sowohl die bereits vorausgesetzten Erhebungsfehler als auch die Tatsache, daß zumeist unbekannt ist, ob jemand einer statistischen Stichprobenpopulation angehört, eine Reidentifikation bei Repräsentativerhebungen schon dann weitgehend aus, wenn nur Name und Adresse unbekannt sind. Verständlicherweise sind es zunächst die Bedenken gegen die Zuverlässigkeit von "Vollerhebungen", die zu der Forderung nach einem Übergang zu anderen Erhebungsmethoden geführt haben. So setzte in den Vereinigten Staaten schon Mitte

der vierziger Jahre eine intensive Diskussion mit dem Ziel ein, die Voraussetzungen zu schaffen, endgültig auf "Vollerhebungen" zu verzichten (15). Spätestens seit den siebziger Jahren rücken freilich Datenschutzgesichtspunkte mehr und mehr in den Vordergrund (16). Symptomatisch dafür ist die parlamentarische Auseinandersetzung in den Vereinigten Staaten über die für 1970 geplante Volkszählung (17). Sie läßt nicht nur die Akzentverschiebung deutlich erkennen, sondern weist auch alle Merkmale auf, die seither die Überlegungen zur Volkszählung weit über die Vereinigten Staaten hinaus beherrschen. Den Abgeordneten und Senatoren erschien es einerseits wichtig, das Erhebungsprogramm einer genauen Kontrolle zu unterziehen. So unterschiedlich dabei die Einschätzung der Manipulationsmöglichkeit des einzelnen durch die Datensammlung gewesen sein mag, Konsens bestand weitgehend über die Notwendigkeit einer Reduktion des Fragenkatalogs und einer Rechtfertigung der jeweils gewünschten Informationen. Darüber hinaus aber verfolgte die parlamentarische Diskussion das Ziel, die Erforderlichkeit einer Vollerhebung zu überprüfen, und zwar mit Rücksicht auf die inzwischen manifest gewordenen Erwartungen, den Datenschutz sicherzustellen.

Durchaus vergleichbar ist die Entwicklung in Schweden verlaufen (18). Wiederum haben also Datenschutzgesichtspunkte dazu geführt, die Methodenfrage zu stellen. Konsequenterweise wurde deshalb das Statistische Zentralamt beauftragt, die für 1985 vorgesehene Volkszählung auf eine völlig neue Grundlage zu stellen, konkret, sich ausschließlich der in den bereits vorhandenen, mittlerweile weit ausgebauten Registern aufgenommenen Daten zu bedienen.

Hinzuweisen ist schließlich auf die Diskussion in der Schweiz. Datenschutzrechtliche Vorkehrungen wurden erstmals in der Verordnung zur Durchführung der Volkszählung von 1980 berücksichtigt (19). Zu den seither insbesondere auch im Rahmen der vom Bundesamt für Statistik eingesetzten Studienkommission erörterten Verbesserungsmöglichkeiten gehört auch der Verzicht auf die "Vollerhebung".

Kurzum, ganz gleich, welches der angeführten Länder man nimmt, eines bestätigt sich immer wieder: Der Gesetzgeber sieht sich durchweg mit der Forderung konfrontiert, sich mit "Vollerhebungen" nicht mehr abzufinden oder sie gar als den methodisch einzig möglichen Weg auszugeben, sondern im Interesse der von ihm selbst betonten und akzeptierten Notwendigkeit, die Verarbeitung personenbezogener Daten einzuschränken und strikten Bedingungen zu unterwerfen, auch einen Methodenwechsel von der "Voll-" zur "Repräsentativerhebung" zu vollziehen.

So deutlich die Forderung aber auch formuliert worden ist, so wenig hat sie sich bislang durchgesetzt. Im Gegenteil, in allen drei Ländern wird nach wie vor an der "Vollerhebung" festgehalten. Doch wäre es viel zu vordergründig, sich mit dieser Feststellung zufriedenzugeben. Denn für jedes von ihnen gilt wohl gleichermaßen: Die "Vollerhebung" wird nur noch vorläufig akzeptiert, ihre Hinnahme also mit der Erwartung verknüpft, die schon eingeleiteten methodischen Untersuchungen fortzusetzen und zu intensivieren, um so schnell wie möglich von der "Vollerhebung" abzugehen. Sie mag mit anderen Worten immer noch als unentbehrlich ausgegeben werden, sie ist es aber lediglich auf Zeit. Zu den zentralen Aufgaben des Gesetzgebers gehört es, so gesehen, sich ständig zu vergewissern, ob nicht der Zeitpunkt des Methodenwechsels erreicht ist.

Damit nicht genug. Sowohl in den Vereinigten Staaten als auch in Schweden wird mittlerweile akzeptiert, daß es gegenwärtig schon durchaus möglich ist, die traditionelle "Vollerhebung" durch eine Kombination von "Vollerhebung" und "Repräsentativerhebungen" zu ersetzen. Danach würde es genügen, bestimmte demographische Grunddaten bei allen Auskunftspflichtigen zu erheben; 20 v.H. der Gesamtpopulation müßten zusätzliche wichtige Fragen, etwa nach der Ausbildung und dem Beruf, beantworten und weitere 5 v.H. auf einen sehr viel umfangreicheren Fragenkatalog eingehen. Die 1970 in den Vereinigten Staaten durchgeführte, auf einer solchen Kombination beruhenden Volkszählung hat gezeigt, daß nicht nur die Ergebnisse verläßlich sind, sondern auch die Auskunftsbereitschaft der Bevölkerung beträchtlich erhöht wird. Zudem bietet ein solches Vorgehen die Chance, die deskriptiven Verfahren der amtlichen Statistik mit den zielgruppen- oder objektgerichteten Untersuchungsmethoden der empirischen Sozialforschung zu verbinden und damit nicht zuletzt Informationen über aktuelle Probleme zu erhalten. Schließlich kann auf diese Weise die Informationsermittlung mehr und mehr auf eine freiwillige Basis umgestellt werden.

Für den Gesetzgeber in der Bundesrepublik folgt daraus: Eine "Vollerhebung" mag in der Tat gegenwärtig noch erforderlich sein. Sie ist aber nur unter der Bedingung der Verbindung einer die gesamte Bevölkerung verpflichtenden Zählung der demographischen Basisdaten mit freiwilligen Repräsentativerhebungen für verschiedene Informationsziele hinnehmbar. Der Gesetzgeber muß also, um dem Verhältnismäßigkeitsgrundsatz Rechnung zu tragen, im Rahmen der Volkszählung eine Erhebung anstreben, die das Gewicht der Informationsermittlung zunehmend auf Repräsentativerhebungen verlegt, kurzum, in der Kombination von Voll- und Repräsentativerhebung und nicht in der Exklusivität der Vollerhebung den allein zulässigen Weg sehen.

Je konsequenter dieser Weg verfolgt wird, desto besser dürfte es gelingen, die im Rahmen der "Vollerhebung" ermittelten Daten auf die jeweils erforderliche demographische Mindestgrundlage zu beschränken. Anders ausgedrückt: Die Verbindung von Voll- und Repräsentativerhebung zwingt von vornherein zu einer Reduktion der über die Vollerhebung ermittelten Angaben. In Betracht kommen nur die als Referenzangaben wirklich unerläßlichen Basisdaten. Obgleich es also nach wie vor bei einer Datenerhebung auf Vorrat bleibt, wird zugleich, in Kenntnis der Notwendigkeit statistischer Erhebungen, aber auch der Gefahren allzu breit angelegter Informationsermittlungen, das Erhebungsprogramm begrenzt.

IV.
Sicherung durch Verfahren

1. Funktionale Trennung von Statistik und Verwaltung
So wichtig eine am Verhältnismäßigkeitsgrundsatz ausgerichtete Methodenwahl auch ist, sie reicht für sich genommen nicht aus. Vielmehr bedarf es einer Reihe zusätzlicher, sich unmittelbar auf das Verarbeitungsverfahren beziehender Vorkehrungen. Ganz in diesem Sinn begnügt sich der Mikrozensus-Beschluß keineswegs mit allgemeinen Überlegungen zur "absoluten" Grenze der Informationsermittlung, sondern weist ausdrücklich auf die gesetzlich anerkannte Notwendigkeit hin, die Anonymität der durchaus zulässigerweise erhobenen Angaben zu garantieren (21). Die Grundrechtsverwirklichung hängt mithin nicht nur von der Methodenwahl, sondern ebenso von einer bestimmten organisatorischen Struktur der statistischen Erhebung ab. Methodenwahl und präzise definierter Verfahrensablauf sind untrennbar miteinander verbundene, sich gegenseitig ergänzende Sicherungselemente. Auch wenn deshalb die Regelung des Verfahrensablaufs unstreitig Aufgabe des einfachen Gesetzgebers ist, muß er sich dabei nach den Grundsätzen richten, die eine Grundrechtsverträglichkeit staatlicher Informationsverarbeitung gewährleisten. Die Dispositionsfreiheit des Gesetzgebers ist insofern von vornherein durch bestimmte, die Verfassung unmittelbar konkretisierende Regelungsanforderungen begrenzt.

Dazu zählt vor allem anderen die strikte funktionale Trennung von Statistik und Verwaltung. Weil die Datenerhebung ohne eine direkte Anbindung an einen konkreten Verwertungszweck, auf Vorrat also, erfolgt, ist die Informationsermittlung eine "Einbahnstraße", die ausschließlich zu den statistischen Ämtern führt. Die Erhebung ist mit anderen Worten nur solange tolerierbar, wie die Daten "amtshilfefest" bleiben. Konsequenterweise zählt das "Statistikgeheimnis" zu den selbstverständlichen Voraussetzungen statistischer Regelung. Ebenso folgerichtig ist das Verbot, gegen einzelne Auskunftspflichtige Maßnahmen zu treffen, die sich auf ihre zu statistischen Zwecken gemachten Angaben gründen (§ 11 BStatG). Erst die von der Verfassung geforderte und gesetzlich abgesicherte Abschottung der Statistik öffnet den Zugang des Staates zu der für seine Planungsaufgaben erforderlichen Information. Nur auf dem Hintergrund dieser Abschottung kann und darf daher vom Bürger erwartet werden, die von ihm verlangten Auskünfte zu erteilen. Ganz in diesem Sinn hat sich das Census Bureau in den Vereinigten Staaten mit Erfolg allen Versuchen widersetzt, der amerikanischen Regierung nach dem Ausbruch des Zweiten Weltkrieges die Namen aller Amerikaner japanischer Abstammung mitzuteilen (22).

1.1 Der Melderegisterabgleich
Vordergründig genügt das VZG dieser verfassungsrechtlich fundierten Anforderung durchaus. § 9 Abs. 1 Satz 2 VZG enthält ein ausdrückliches, dem § 11 Abs. 3 Satz 3 BStatG nachgebildetes Nachteilsverbot. Auf den ersten Blick also verhält sich das Gesetz genauso wie schon zuvor das Bundesstatistikgesetz. Die Volkszählung bleibt allem Anschein nach an die Bedingung gebunden, Statistik und Verwaltung deutlich voneinander zu trennen.

Wie wenig freilich in Wirklichkeit diesem Grundsatz Rechnung getragen wird, zeigt sich vor allem an dem im VZG (§ 9 Abs. 1) vorgesehenen Melderegisterabgleich. Um jedes Mißverständnis auszuschließen: Wenn im Zusammenhang mit dem Abgleich von möglichen Nachteilen gesprochen wird, so im Hinblick auf die Konsequenzen der durch den Abgleich angestrebten, ja ihn überhaupt rechtfertigenden Berichtigung der im Melderegister enthaltenen Daten. Eines läßt sich mit Sicherheit nicht bestreiten: Dem Gesetzgeber erschien die Volkszählung als willkommener Anlaß, um eines der wichtigsten Informationsinstrumente der öffentlichen Verwaltung, das Melderegister, zu berichtigen. Gerade weil die Volkszählung eine alle Bürger einbeziehende Erhebung ist, sollte sie als Korrekturgrundlage eines Registers dienen, in dem sich ebenfalls alle Bürger wiederfinden. Die Implikationen lassen sich nicht vollständig aufzählen, da die Korrektur die unterschiedlichsten Wirkungen haben kann. Die Verwaltungspraxis weist aber eine Reihe typisierter Abläufe auf, die es ermöglichen, bestimmte Folgen unschwer auszumachen.

Hauptzweck des Melderegisters ist die Feststellung und der Nachweis der Identität sowie der Wohnung des jeweiligen Einwohners (§ 1 Abs. 1 MRRG). Das Melderegister vermittelt so eine für sehr unterschiedliche Aufgaben wichtige Grundinformation. Regelmäßige, vom MRRG ausdrücklich sanktionierte und an bestimmte gesetzlich ebenfalls festgelegte Bedingungen gebundene Datenübermittlungen an andere öffentliche Stellen, aber auch die Erteilung einer Vielzahl von Einzelauskünften an Privatpersonen und nichtöffentliche Institutionen sind die zwangsläufige Folge. Ebenso regelmäßig wird sich deshalb die empfangende Stelle veranlaßt sehen, zu prüfen, ob die möglicherweise erforderliche Korrektur der ihr bislang zur Verfügung stehenden Angaben zu bestimmten, für den Betroffenen unter Umständen nachteiligen Maßnahmen führen muß.

Regelmäßig erhalten beispielsweise die Kreiswehrersatzbehörden die Zuzugs- und Wegzugsmeldung jedes der Wehrüberwachung unterliegenden Bürgers (§ 24 Abs. 9 Wehrpflichtgesetz). Die "Umdatierung" des Hauptwohnsitzes von Berlin in das Bundesgebiet auf Grund der über die Volkszählung ermittelten Angaben kann somit dazu führen, daß der Betroffene zum Wehrdienst einzuziehen ist.

Weiter: Der Zu- und Wegzug aller Ausländer wird den Ausländerbehörden und damit mittelbar dem Ausländerzentralregister mitgeteilt. Ausländer, die keine Aufenthaltsgenehmigung besitzen oder gegen die ein belastender Verwaltungsakt nicht vollzogen werden konnte, weil ihre Anschrift bislang nicht bekannt war, müssen mit ihrer Ausweisung bzw. mit dem Vollzug des Verwaltungsaktes rechnen.

Schließlich: Bislang erfolgte in Hessen in größeren zeitlichen Abständen ein Abgleich der Fahndungsdaten der Polizei mit den bei den Kommunalen Rechenzentren befindlichen Meldedaten der Gemeinden, in denen etwa 95 v.H. der hessischen Einwohner in automatisierten Verfahren erfaßt sind. Ebenso wie diese Routineaktionen erfahrungsgemäß dazu führen, Straftäter zu ergreifen, würden auch die aufgrund der Volkszählung aktualisierten Datenbestände polizeiliche Maßnahmen gegenüber den Betroffenen zur Folge haben, jedenfalls solange, wie man sich nicht bereit findet, die gegen solche Fahndungsmethoden bestehenden rechtlichen Bedenken zu teilen.

Andere öffentliche Stellen erhalten zwar nicht regelmäßig Änderungsmitteilungen aus dem Melderegister, sie haben jedoch im Einzelfall einen uneingeschränkten Zugang zu den Meldedaten, soweit diese zu ihrer Aufgabenerfüllung erforderlich sind. Vor allem die Festlegung des Wohnsitzes ist im Verwaltungsvollzug von besonderer Bedeutung. Eine Korrektur kann sich etwa auf die Gewährung von wohnsitzgebundenen Sozialleistungen auswirken.

Zudem: Eine Gemeinde kann beispielsweise die Benutzung der von ihr angebotenen Kindergarten-, Schul- oder Altenheimplätze von der Begründung der Hauptwohnung in ihrem Gemeindegebiet abhängig machen. Wiederum wirkt sich dann eine Änderung des Melderegisters auf den Betroffenen aus.

Hinzuweisen ist aber auch auf den steuerlichen Bereich. Wird etwa aufgrund der Volkszählung festgestellt, daß Ehepartner entgegen ihren Angaben in der Steuererklärung Hauptwohnungen an unterschiedlichen Orten begründet haben, so ist davon auzugehen, daß sie "dauernd getrennt leben" - mit der Konsequenz einer Änderung der Steuerklasse zu ihren Lasten.

Die jeweiligen Daten des Melderegisters sind schließlich Handlungsgrundlage für Gläubiger und Kreditauskunfteien. Ihre Aktionsmöglichkeit richtet sich nicht zuletzt nach der Zuverlässigkeit der Meldedaten. Das Melderegister vermittelt, anders ausgedrückt, den von ihnen angestrebten Zugang zum jeweils Betroffenen, mit all den Folgen, die sich daraus für ihn ergeben können. Sicher, der Einwand liegt auf der Hand, die Korrektur des Melderegisters führe fast durchweg dazu, rechtswidrige Situationen zu beseitigen. Jeder gegen den Gesetzgeber gerichtete Vorwurf mute deshalb merkwürdig an, ja sei völlig fehl am Platz, eine gerade im Zusammenhang mit dem Volkszählungsgesetz immer wieder geäußerte Meinung. Wer allerdings so argumentiert, verkennt die verfassungsrechtliche Ausgangslage. Sie ist, um noch einmal daran zu erinnern, durch die funktionale Trennung von Statistik und Verwaltung gekennzeichnet. Ob die Konsequenzen der administrativen Verwertung statistischer Angaben den Betroffenen zum Vor- oder zum Nachteil gereichen, spielt weiter keine Rolle. Was einzig interessiert, ist die strikte Abschottung der Statistik. Insofern kommt es auf eine wie immer geartete Bewertung der Nachteile gar nicht erst an. Unter verfassungsrechtlichen Gesichtspunkten zählt lediglich die Durchlässigkeit der Statistik. Sie muß ausgeschlossen und nicht, wie es das Volkszählungsgesetz in § 9 Abs. 1 tut, begünstigt werden.

1.1.1
Die nachteiligen Konsequenzen des Melderegisterabgleichs lassen sich weder technisch noch rechtlich verhindern. Technisch deshalb nicht, weil die Datenverarbeitung im Meldebereich mittlerweile fast vollständig automatisiert worden ist. Sie beruht daher auf einem eindeutig vorgegebenen einheitlichen Datensatz. Wollte man den Grund der Änderung einer Angabe gesondert vermerken, so müßte ein Sonderprogramm - mit weiteren Programmen für die Empfängerbereiche - ausgearbeitet werden. Jeder Versuch, den Änderungsgrund aufzuzeichnen, droht deshalb bereits an dem kaum zu bewältigenden technischen Aufwand zu scheitern. Rechtliche Grenzen kommen hinzu. Die Korrektur der Meldedaten hat nun einmal unstreitig auch und gerade das Ziel, der öffentlichen Verwaltung zu ermöglichen, die mit ihrem Aufgabenbereich verbundenen Vollzugsmaßnahmen wirksam vorbereiten und treffen zu können. Genau dieses Ziel steht aber in offenkundigem Widerspruch zu den verfassungsrechtlichen Grundvoraussetzungen statistischer Erhebungen. Der Widerspruch läßt sich aber jedenfalls dann nicht auflösen, wenn etwa die Daten den Strafverfolgungsbehörden übermittelt worden sind. Straftäter, deren Aufenthalt mit Hilfe der Korrektur der Melderegister den Strafverfolgungsbehörden bekannt wird, müssen verfolgt werden. Anderenfalls hätte § 9 Abs. 1 Satz 2 Volkszählungsgesetz den Charakter eines Amnestiegesetzes - ein wohl kaum ernsthaft vertretbares Ergebnis. Nichts anderes gilt für Ausländer, die sich ohne Aufenthaltserlaubnis in der Bundesrepublik aufhalten, oder für Steuerpflichtige sowie Bezieher von Sozialleistungen, deren bislang gespeicherte Angaben korrigiert werden müßten. Die nachteiligen Konsequenzen der Korrektur des Melderegisters lassen sich rechtlich nicht vermeiden, sie sind im Gegenteil rechtlich geboten.

Auch der in der öffentlichen Diskussion über das Volkszählungsgesetz immer wieder formulierte Vorschlag, wenigstens auf die Rückforderung von Geldleistungen zu verzichten, die aufgrund der vor dem Stichtag der Volkszählung eingetragenen Daten geleistet wurden, hilft nicht weiter. Derartige Unterscheidungen lassen sich mit dem Rechtsstaatsgebot nicht vereinbaren.

Kurzum, das Volkszählungsgesetz mag mit Formulierungen wie der des § 9 Abs. 1 Satz 2 äußerlich der Trennung von Statistik und Verwaltung entsprochen haben. In Wirklichkeit bleibt das Nachteilsverbot auf den Randbereich der unmittelbar mit dem Melderegister zusammenhängenden Ordnungswidrigkeitsverfahren beschränkt und spielt darüber hinaus höchstens dort eine Rolle, wo das Opportunitätsprinzip eine flexible Handhabung des Verfahrensrechts ermöglicht. Das Volkszählungsgesetz verstößt damit gegen die verfassungsrechtlichen Grundbedingungen statistischer Erhebungen.

1.1.2
Die durch den Wortlaut des § 9 Abs. 1 Satz 2 bewirkte Verschleierung der möglichen Folgen der Volkszählung für die auskunftspflichtigen Einzelnen wird durch die ständigen Hinweise auf die Notwendigkeit der Statistik für die gesamtstaatliche, landesweite und gemeindliche Planung nur noch verstärkt. Die wiederholten Versicherungen, kaum ein anderes Geheimnis biete einen größeren Schutz als das Statistikgeheimnis, akzentuieren noch einmal den Eindruck, von nachteiligen Konsequenzen könne und dürfe gar nicht erst die Rede sein. Um so nachhaltiger stellt sich die Frage, wie sich eine solche Regelung mit dem zu den zentralen Voraussetzungen rechtsstaatlicher Gesetzgebung zählenden Gebot der Normenklarheit verträgt (23).

Gerade dann, wenn, wie bei statistischen Erhebungen, die funktionale Trennung von Statistik und Verwaltung zu den verfassungsrechtlich fundierten, vom Gesetzgeber durch die Normierung des Statistikgeheimnisses (§ 11 BStatG) ausdrücklich bestätigten Grundbedingungen staatlicher Aktivität gehört, kommt der Normenklarheit und damit der Vorhersehbarkeit der Verwendung der mit Hilfe der Volkszählung erhobenen Daten ganz besondere Bedeutung zu. Dem Bürger wird durch den sowohl bei der Formulierung als auch bei den Vorbereitungen zur Durchführung des Gesetzes nachdrücklich in den Vordergrund gestellten und als allein ausschlaggebend bezeichneten statistischen Zusammenhang förmlich suggeriert, daß seine Beteiligung an der Volkszählung einzig den Zweck verfolgt, die für eine auch auf seine Interessen bedachte staatliche Politik notwendigen statistischen Informationen zu gewinnen. Gefordert wird also nicht seine Mitwirkung an Entscheidungen, die sich erkennbar auf ihn beziehen, sondern an Maßnahmen, die losgelöst von seiner Person eine generelle, sich auf alle Bürger beziehende Information zum Gegenstand haben. § 9 Abs. 1 VZG zeigt aber: Während der Bürger Informationen in der Erwartung vermittelt, sich an einer statistischen Erhebung zu beteiligen, liefert er gleichzeitig Daten, die für ein konkretes gegen ihn gerichtetes Verwaltungsverfahren genutzt werden können. Die Verschleierung wiegt um so schwerer, als die Aufgabe des Melderegisters, eine Vielzahl öffentlicher und privater Stellen mit Informationen zu versorgen, es dem Bürger unmöglich macht, den Verwendungszusammenhang rechtzeitig zu erkennen und in seiner Tragweite abzuschätzen. Die multifunktionale Verwendung der Meldedaten erlaubt es bestenfalls einem mit allen Details des Melderechts und der Arbeitsweise der Meldebehörden vertrauten Verwaltungsfachmann, einen relativ genauen Überblick über die jeweiligen Informationsströme zu haben. Entgegen der Vorstellung, die beim Bürger geweckt und genährt wird, gerät also die Information in einen Verwaltungsbereich, der sich seiner ganzen Struktur nach einer Vorhersehbarkeit der Konsequenzen der Informationsvermittlung widersetzt.

Selbst wenn die Korrektur des Melderegisters von einem besonderen, die Anhörung des Betroffenen garantierenden Verfahren abhängig gemacht werden sollte, ändert sich nichts daran, daß die Behörde dank der mit Hilfe der statistischen Erhebung gewonnenen Angaben über Daten verfügt, die sie sonst gar nicht haben würde. Die Anhörung mag insofern dem Betroffenen die Chance einräumen, selbst Stellung zu den unterschiedlichsten Daten zu beziehen; sie behebt aber nicht den Mangel, eine zu statistischen Zwecken konzipierte und im Hinblick auf diese Zwecke dem Bürger präsentierte Erhebung in einer für ihn nicht vorausschaubaren, mit der Gefahr einschneidender Nachteile behafteten Weise zu nutzen. Der Gesetzgeber verletzt daher das Gebot der Normenklarheit. Er kann es nur einhalten, wenn er von vornherein uneingeschränkt auf jede administrative Verwendung verzichten würde. Solange er diese Konsequenz nicht eindeutig zieht, bleibt dem Betroffenen nur übrig, sich entweder selbst zu bezichtigen und sich damit den Folgen des Verwaltungsvollzugs auszuliefern, ohne sie auch nur annähernd zu überschauen oder die vom Gesetzgeber angestrebte, für die Funktionsfähigkeit der Statistik unerläßliche, korrekte Beteiligung zu umgehen. Nur die konsequente Abschottung vermag also letztlich die Auskunftsbereitschaft der Bürger und damit die für eine staatliche Planung notwendige Präzision des statistischen Materials zu gewährleisten.

2. Anonymisierung
Neben der Trennung von Statistik und Verwaltung ist die Anonymisierung der jeweiligen Angaben die zweite entscheidende Voraussetzung für einen verfassungskonformen Ablauf statistischer Erhebungen. Der personenbezogene Teil ist lediglich Hilfsmittel für den Informationszugang und die Informationskontrolle. Mit dem Abschluß der Erhebung verliert deshalb der Personenbezug, jedenfalls unter statistischen Aspekten, jede Bedeutung. Grundlage der für die staatliche Planung erforderlichen statistischen Analysen ist allein der um die personenbezogenen Elemente verkürzte Datenbestand. Die Anonymisierung reduziert infolgedessen den Informationsgehalt der

Daten auf das statistisch Notwendige. In eben dieser Indifferenz gegenüber dem Personenbezug liegt auch die Absicherung gegen alle Versuche, die statistische Erhebung doch noch zu nutzen, um mit Hilfe der ermittelten Daten steuernd auf den einzelnen einzuwirken. Die Anonymisierung wahrt den statistischen Wert der Information und schließt zugleich einen Rückgriff auf den einzelnen aus. Ganz gleich, zu welchen Zwecken der Empfänger die übermittelten Daten benutzt, die Anonymisierung versperrt den Rückweg zum Betroffenen.

Anders das VZG. Für die Übermittlung genügt es schon, den Namen (§ 9 Abs. 2 und 3) oder den Namen und die Adresse (§ 9 Abs. 4) wegzulassen. Beides erfüllt nicht einmal annähernd die Bedingungen einer Anonymisierung. Spätestens seit der Diskussion über den Anwendungsbereich der Datenschutzgesetze steht fest, wie wenig es auf den Namen oder die Adresse bei der Identifizierung einer Person ankommt. Nicht von ungefähr qualifiziert das BDSG (§ 2 Abs. 1) auch und gerade die Daten einer "bestimmbaren" Person als personenbezogen. Das BDSG erkennt damit ausdrücklich an, daß die Reindividualisierung nicht nur von der Art der jeweils vorliegenden Angaben, sondern ebenso vom Zusatzwissen des Übermittlungsadressaten abhängt (24). Inwieweit also Daten personenbezogen sind, richtet sich nicht zuletzt nach der Organisation des Informationssystems (25). Gerade dort aber, wo - wie es das VZG vorsieht - die Daten an Behörden und Kommunen übermittelt werden sollen, ist die Existenz des zur Reindividualisierung notwendigen Zusatzwissens jedenfalls wahrscheinlich. Sie ist um so höher, je präziser die Anfrage auf kleinere Einheiten eingegrenzt wird, zumal wenn, wie das VZG (§ 9 Abs. 2 und 3) es zuläßt, die Adressen mitübermittelt werden. Kurzum, das VZG nimmt die Bestimmbarkeit der durch die Übermittlung jeweils Betroffenen offen in Kauf. Die mangelnde Anonymisierung stellt erneut die funktionale Trennung von Statistik und Verwaltung in Frage und setzt den einzelnen der Gefahr unmittelbar auf seine Person bezogener, möglicherweise mit Nachteilen verbundener Verwaltungsmaßnahmen aus. Sie ist dann besonders evident, wenn das Gesetz, wie in § 9 Abs. 2, statt die Verwendungsschranken präzise anzugeben, nicht mehr tut, als allgemein auf die Zuständigkeit des Übermittlungsadressaten zu verweisen. Zwar dürften die Informationswünsche der obersten Bundes- und Landesbehörden zumeist mit den für ihren Bereich typischen Planungsaufgaben zusammenhängen, individuelle Maßnahmen also in aller Regel nicht in Betracht kommen. Manche dieser Behörden verfügen aber über Abteilungen, die wie beispielsweise die Landesverfassungsschutzämter, durchaus an personenbezogenen Auswertungen interessiert sind und zudem das notwendige, eine Reindividualisierung erlaubende Zusatzwissen haben. Das VZG verbietet weder die Reindividualisierung noch eine anschließende personenbezogene Verarbeitung. Wohl findet sich in § 9 Abs. 2 Satz 3 eine Verweisung auf das Nachteilsverbot des § 9 Abs. 1 Satz 2, doch die Bemerkungen zu den Konsequenzen der Berichtigung des Melderegisters zeigen, wie gering, ja nichtssagend der Schutz ist, den diese Bestimmung bietet. Abgesehen davon weckt § 9 Abs. 2 VZG auch deshalb Bedenken, weil der Betroffene die Zahl und die Aufgabenstellung der in Frage kommenden Behörden kaum zu überblicken und daher auch nicht die Verarbeitungskonsequenzen verläßlich einzuschätzen vermag.

Nicht viel anders ist die Situation in den Übermittlungsfällen des § 9 Abs. 3 Satz 2 VZG. Danach können den Gemeinden und Gemeindeverbänden für eigene statistische Aufbereitungen Einzelangaben über alle nach der Volkszählung erfaßten Tatbestände zur Verfügung gestellt werden. Die gesetzliche Regelung ist das Ergebnis einer von den kommunalen Spitzenverbänden im Laufe des Gesetzgebungsverfahrens nachdrücklich formulierten Forderung. Sie wollten sicherstellen, daß "sämtliche Daten den Städten für eigene statistische Auswertungen zur Verfügung stehen". Im Unterschied zu der jetzigen Fassung enthielt der Gesetzentwurf allerdings zunächst einen klaren Satzungsvorbehalt. Übermittlungen sollten nur dann zulässig sein, "wenn durch Satzung die Voraussetzungen geschaffen sind und erhalten bleiben, die eine ausschließliche statistische Nutzung der Daten" gewährleisten.

Der Vorbehalt ist alles andere als überflüssig. Kaum eine Kommune bzw. ein Gemeindevorstand verfügt über eine Satzung oder eine innerbehördliche Anordnung, der eindeutig zu entnehmen ist, zu welchen Zwecken Statistiken zu erstellen sind, wie also mit den für statistische Ziele angeforderten Angaben umgegangen werden darf. Ohne eine entsprechende Regelung vermag letztlich kein Statistisches Landesamt festzustellen, welche Daten überhaupt für die jeweilige statistische Aufgabe in Betracht kommen. § 9 Abs. 3 Satz 2 VZG ermöglicht es, genaugenommen, Bürgermeistern, Dezernenten, Amtsleitern oder anderen verantwortliche Funktionen wahrnehmenden Amtsträgern, unter eigener Verantwortung sowie ohne Kontrolle des Kommunalparlaments von den Statistischen Landesämtern personenbezogene Daten anzufordern, um eine eigene Statistik anzufertigen.

Sicher, auf den ersten Blick enthält das Gesetz durchaus eine Verwendungsschranke. Anders als § 9 Abs. 2 VZG gibt sich der Gesetzgeber in § 9 Abs. 3 Satz 2 VZG nicht damit zufrieden, auf die Zuständigkeit zu verweisen, sondern verknüpft die Übermittlung ausdrücklich mit einer Nutzung für "statistische Aufbereitungen". Nur: Von einer deutlichen, für den Betroffenen erkennbaren und auch kontrollierbaren Zweckbindung kann bei bestem Willen nicht die Rede sein. "Statistische Aufbereitungen" ist eine viel zu vage Formulierung, die ohne jede Schwierigkeit herangezogen werden kann, um die verschiedensten Aktivitäten zu decken. Die Etikettierung "statistisch" reicht zudem noch lange nicht aus, um die Übermittlung zu rechtfertigen. Auch Statistiken können die Vorstufe zu einschneidenden, den einzelnen diskriminierenden und benachteiligenden Maßnahmen sein, und zwar nicht zuletzt dann, wenn sich die Angaben wie im kommunalen Bereich auf kleinere Personengruppen beziehen. Deshalb muß gerade dann, wenn statistische Auswertungen zur Debatte stehen, Klarheit über ihren Ausgangs-

punkt, ihre Durchführung und ihre möglichen Implikationen bestehen. Wollte man anders verfahren, so würde man gegen die schon in der Mikrozensus-Entscheidung (26) festgehaltenen verfassungsrechtlichen Anforderungen verstoßen. Die Volkszählung mag bestimmte, für alle weiteren statistischen und planerischen Maßnahmen notwendige Grunddaten zur Verfügung stellen, und insofern zwangsläufig zu einer Verarbeitung auf Vorrat führen, sie darf dennoch nicht dazu benutzt werden, um beliebige "statistische Aufbereitungen" vorzunehmen. Genau das, was bei der Volkszählung selbst nicht möglich ist, wird mit jedem Zugriff auf das mit ihrer Hilfe ermittelte Material um so erforderlicher: die exakte Beschreibung der mit allen weiteren statistischen Erhebungen verfolgten Ziele, besonders dann, wenn - wie bei der Übermittlung an die Kommunen - der Mikrobereich tangiert wird. Der Rückgriff auf die Daten muß daher solange ausgeschlossen bleiben, wie es an in der Satzung festgehaltenen klaren Verarbeitungszielen und Verarbeitungsmaßstäben fehlt.

In beiden Fällen, sowohl also bei der Übermittlung an die obersten Bundes- und Landesbehörden (§ 9 Abs. 2 VZG) als auch bei der Weitergabe zu "statistischen Aufbereitungen" im Rahmen der kommunalen Aufgaben (§ 9 Abs. 3 Satz 2) erweist sich mithin, wie unverzichtbar die Anonymisierung ist. Längst steht allerdings fest, daß auch eine Anonymisierung keinen absoluten Schutz, mathematisch-statistisch gesprochen "ein Risiko von genau Null", bieten kann (27). Spätestens seit den von Block und Olsson durchgeführten Identifikationsexperimenten (28) hat sich gezeigt, daß es auch bei einem scheinbar einwandfrei anonymisierten statistischen Material durchaus gelingen kann, die Datensätze zu entschlüsseln. Aber auch die Erfahrungen der Datenschutzbeauftragten geben deutlich zu erkennen, wie wenig es angeht, die Anonymisierung als unüberwindbare Barriere anzusehen (29), vor allem dort, wo - wie bei statistischen Angaben für kleinräumige Planungen - das für die Deanonymisierung erforderliche Zusatzwissen zumeist vorhanden sein dürfte.

Die Zweifel an der Anonymisierung rechtfertigen es trotzdem nicht, auf die Übermittlung etwa an die Gemeinden vollends zu verzichten. Gerade die wachsende Kritik an der Annahme, die Anonymisierung könne einen absoluten Schutz gewährleisten, hat dazu geführt, die Erwartungen einzuschränken und sich mehr und mehr mit einer "faktischen Anonymisierung" zufriedenzugeben, die dann vorliegt, "wenn der Betroffene nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Personal identifiziert werden kann" (30). Das, freilich minimale, Restrisiko für den jeweils Betroffenen ist offenkundig, kann aber als zumutbarer Preis für einen Kompromiß angesehen werden, der einerseits in Kenntnis der Bedeutung auch und gerade kleinräumiger Planung den Zugang zu den erforderlichen Angaben garantiert und andererseits auf die spezifische Situation der Betroffenen sowie auf die Gefahren der Verarbeitung personenbezogener Daten Rücksicht nimmt. So wenig sich also die Grenzen der Anonymisierung übersehen lassen, so sehr kommt es darauf an, die Grundbedingungen staatlicher Planung aufrechtzuerhalten. Die am Verhältnismäßigkeitsgrundsatz orientierte "faktische Anonymisierung" bietet einen akzeptablen, verfassungskonformen Ausweg. Ich hatte deshalb bereits im Rahmen der Anhörung vor dem Innenausschuß des Deutschen Bundestages zum VZG 1981 vorgeschlagen, die faktische Anonymisierung als Anknüpfungspunkt für die Übermittlungstatbestände des § 9 Abs. 2 - 4 VZG zu wählen.

Doch auch bei einer Gewährleistung der Anonymisierung überzeugt die Regelung des § 9 Abs. 2 - 4 VZG nicht so recht. Nach der von den Übermittlungsadressaten im Laufe der parlamentarischen Vorarbeiten übereinstimmend bekundeten Auffassung richtet sich ihr Interesse ausschließlich auf anonymisierte und aggregierte Angaben im Sinne von § 11 Abs. 5 und 6 BStatG. Dann aber bedarf es keiner zusätzlichen, wesentlich komplizierteren und detaillierteren Regelung. Dem Statistischen Bundesamt und den Statistischen Landesämtern muß es vielmehr überlassen bleiben, innerhalb der durch § 11 Abs. 5 und 6 BStatG festgelegten Grenzen zu operieren. Nur so kann auch von vornherein jeder Versuch unterbunden werden, statistische und administrative Zwecke zu vermischen, durch Formulierungen also, wie sie etwa § 9 Abs. 2 VZG enthält, doch noch den Weg in die administrative Nutzung zu eröffnen. Wenn die Volkszählung wirklich zu nicht mehr dienen soll, als die für alle weiteren statistischen Untersuchungen und die mit ihnen verknüpften Planungsaufgaben notwendige Referenzbasis aufzubauen, dann kann und darf eine Übermittlung der mit ihrer Hilfe ermittelten Daten nur in dem Maße hingenommen werden, in dem sie zu statistischen Zwecken erfolgt und sich dabei strikt an die für die Verarbeitung statistischer Daten maßgeblichen Grundsätze, insbesondere also an eine (faktische) Anonymisierung der Angaben, hält.

3. Gesetzliche Regelung der Durchführung

Die verfassungsrechtlichen Anforderungen an die organisatorische Struktur der Volkszählung bedingen schließlich eine gesetzliche Regelung aller für die Durchführung der Erhebung maßgeblichen Vorkehrungen. Gegenstand dieser Regelung muß deshalb über eine klare Normierung der Auskunftsverpflichtung hinaus die exakte Festlegung der anzugebenden Daten sowie die präzise Umschreibung der zur Abschottung der erhobenen Angaben erforderlichen Maßnahmen sein.

3.1 Auskunftsverpflichtung
§ 5 VZG nennt als Auskunftspflichtige alle Volljährigen oder einen eigenen Haushalt führenden Minderjährigen. Adressat der Auskunftsverpflichtung ist damit jeder einzelne Bürger. Die Entscheidung des Gesetzgebers ist allerdings nicht zwingend, schon deshalb, weil der Haushalt die zentrale Grundgröße sowohl für volkswirtschaftliche Gesamtrechnungen als auch für die etwa im Zusammenhang mit den staatlichen Planungsaufgaben notwendigen sozialwissenschaftlichen Untersuchungen ist. Zudem: Im Interesse einer zuverlässigen Erhebung muß von vornherein alles getan werden, um beispielsweise zu vermeiden, daß die nach § 5 Abs. 1 Nr. 3 VZG zu erhebenden wohnungsstatistischen Angaben nicht gleich mehrfach, also bei jedem in einem Haushalt lebenden Volljährigen ermittelt werden. Verständlicherweise knüpft daher der Fragebogen an den Haushalt an. Damit wird allerdings ein zusätzliches, im Gesetz nicht vorgesehenes Datum erfragt. Unabhängig davon bleibt unklar, wer etwa von den in einem Haushalt lebenden Ehegatten oder Wohngemeinschaftsmitgliedern zur Auskunft verpflichtet ist. Allem Anschein zuwider steht mithin keineswegs eindeutig fest, wer genau den Fragebogen erhalten und ausfüllen muß. Der gesetzlichen Regelung fehlt es insofern schon bei dieser für die Durchführung der Erhebung zentralen Voraussetzung an der notwendigen Präzision.

3.2 Fragebogen
An der Verpflichtung des Gesetzgebers, die zu offenbarenden Daten anzugeben, hat auch bislang kein Zweifel bestanden. Der Streit konzentrierte sich vielmehr auf die jeweils konkret verlangten Angaben. Nur: Anders als es die bisherige und auch die gegenwärtige Regelung (§§ 2 ff. VZG) vermuten läßt, reicht die Auflistung der an den Bürger zu richtenden Fragen nicht aus. Wie sich gerade an den Erfahrungen mit der Vorbereitung des VZG zeigt, kann die Konkretisierung der Befragung durch die Ausgestaltung des Fragebogens durchaus zu einer Erweiterung des gesetzlich festgeschriebenen Fragenkatalogs führen. So hat die Zusammenfassung aller in einem Haushalt lebenden Auskunftspflichtigen in einem Fragebogen zur Folge, daß der einzelne Bürger, entgegen der Regelung der §§ 2 ff. VZG, auch darüber Auskunft erteilt, ob er einer Wohngemeinschaft angehört. Darüber hinaus vermittelt der Fragebogen gesetzlich ebenfalls nicht geregelte Informationen darüber, inwieweit sich jemand zum Zeitpunkt der Erhebung in einer psychiatrischen Anstalt oder in einem Gefängnis befindet. Kurzum, der Fragenkatalog und die Ausgestaltung des Fragebogens lassen sich nicht voneinander trennen. Beides bildet vielmehr einen einheitlichen Komplex, der insgesamt in die gesetzliche Regelung einbezogen werden muß. Dem Gesetzgeber kann es also nicht gleichgültig sein, wie die von ihm akzeptierte statistische Erhebung konkret umgesetzt werden, vor allem also, wie der für die Durchführung der Erhebung unerläßliche Fragebogen ausgestaltet sein soll. Nur solange es nicht der Verwaltung überlassen bleibt, die jeweils notwendigen Entscheidungen zu treffen, sondern die gesetzliche Regelung auch auf den Fragebogen eingeht und seine Ausgestaltung festlegt, kann wirklich vermieden werden, daß auf dem Umweg über die scheinbar harmlose und deshalb keiner weiteren Überlegung bedürftige Ausgestaltung des Fragebogens just die verfassungsrechtlich zwingende, vom Gesetzgeber vorzunehmende Eingrenzung der zu erhebenden Daten umgangen wird.

Wie sehr es darauf ankommt, erweist sich gerade dann, wenn, wie bei der für 1983 beabsichtigten Volkszählung, über die Ausgestaltung des Fragebogens Daten einbezogen werden, die auch nicht in den gesetzlichen Fragenkatalog hätten aufgenommen werden dürfen. Von keinem Auskunftsverpflichteten kann etwa im Rahmen der Volkszählung verlangt werden, anzugeben, ob er Insasse einer psychiatrischen Anstalt ist. Jeder in diese Richtung zielende Versuch läuft auf eine verfassungswidrige Sondererfassung einer bestimmten Bevölkerungsgruppe hinaus. Eine Befragung der Insassen psychiatrischer Anstalten oder auch von Gefängnissen darf infolgedessen nur in einer Form erfolgen, die klar vermeidet, die jeweils Betroffenen dazu zu zwingen, ihren Anstaltsaufenthalt offenzulegen. Die Erhebung muß sich deshalb im Zweifelsfall darauf beschränken, nicht mehr als die reine Zahl der Insassen einer bestimmten Anstalt zu erfassen.

3.3 Datensicherung - Zählorganisation
Statistikgeheimnis und Nachteilsverbot sind die gleichsam klassischen und mittlerweile selbstverständlichen gesetzlichen Vorkehrungen, die den Zugriff auf den personenbezogenen Teil der für statistische Zwecke ermittelten Daten versperren. Der Gesetzgeber darf sich aber, jedenfalls bei einer Volkszählung, nicht damit zufriedengeben und es im übrigen der Verwaltung freistellen, selbst darüber zu entscheiden, ob und welche zusätzlichen Maßnahmen möglicherweise erforderlich sind. Vielmehr muß er für ein umfassendes, den gesamten Erhebungs- und Verarbeitungsprozeß einbeziehendes System von Sicherungsvorkehrungen sorgen. Nur unter dieser Bedingung kann der Gesetzgeber seiner doppelten Aufgabe gerecht werden, einerseits die notwendige Erhebungsgrundlage zu schaffen, andererseits aber auch den Erhebungs- und Verarbeitungsgefahren wirksam vorzubeugen. Die Sicherungsvorkehrungen sind insofern kein nebensächlicher, dem administrativen Ermessen überlassener Teil der Erhebungsregelung. Sie zählen im Gegenteil zu den zwingenden Voraussetzungen einer verfassungskonformen gesetzlichen Regelung.

Konkret folgt daraus zunächst die Verpflichtung des Gesetzgebers, die Trennung der formalen Identifikatoren von den übrigen Daten anzuordnen, und zwar für sämtliche Phasen der Durchführung der Volkszählung. Die bloße Sollvorschrift des § 11 Abs. 7 BStatG reicht nicht aus. Für den Fragebogen beispielsweise hat dies zur Konsequenz, daß Name, Geburtsdatum und Anschrift auf eine abtrennbare Seite einzutragen sind und an keiner anderen Stelle wiederkehren dürfen.

Ferner: Der Gesetzgeber muß genau angeben, wann das personenbezogene Material zu vernichten ist. Sicherlich gilt es dabei den Besonderheiten des Erhebungs- und Verarbeitungsprozesses Rechnung zu tragen. So dürfte es wohl notwendig sein, die personenbezogenen Angaben zu erhalten, bis beispielsweise die Plausibilitätsprüfungen durchgeführt und die Stichproben für den Mikrozensus gezogen sind. Dennoch muß der Gesetzgeber darauf bedacht sein, einen möglichst kurzfristigen Termin festzulegen. Gerade weil die personenbezogenen Daten nur vorübergehend benötigt werden und die Verarbeitungsgefahren vor allem mit der Chance verbunden sind, auf diese Angaben zurückzugreifen, kommt es darauf an, den Verarbeitungsprozeß, zeitlich jedenfalls, so zu gestalten, daß sowohl die Fragebögen als auch alle anderen personenbezogenen Daten nur für eine kurze, gesetzlich zwingend eingegrenzte Zeit bei den Statistischen Ämtern bleiben und spätestens mit der Erreichung dieses Zeitpunktes vernichtet werden.

Schließlich: Der gerade für Volkszählungen typische Erhebungsumfang erhöht den Personalbedarf und verändert erfahrungsgemäß die Aufbewahrungs- und Verarbeitungsbedingungen der Daten. Faktoren wie die Bestellung einer Vielzahl von Personen als Zähler oder die verstreute Lagerung der Erhebungsunterlagen bei den Gemeinden steigern das Gefährdungspotential. Der Gesetzgeber muß unter diesen Umständen zunächst prüfen, ob es nicht unter Verhältnismäßigkeitsgesichtspunkten geboten ist, sich grundsätzlich mit einer brieflichen Beantwortung des Fragebogens zu begnügen. Soweit sich die Bestellung von Zählern wirklich als erforderlich erweisen sollte, sind wenigstens die Grundsätze der Zählorganisation zu regeln. Zwar kann kein Gesetz auf sämtliche organisatorischen Fragen eingehen, schon deshalb, weil sie nicht durchweg einer allgemeinen Regelung zugänglich sind. Der Gesetzgeber ist dennoch in der Lage und verpflichtet, den für die Zählorganisation verbindlichen Rahmen vorzugeben, und zwar indem er spezifische, auf die einzelnen Zähl- und Verarbeitungsphasen bezogene Ziele festlegt. Dazu gehören etwa:

- eine sorgfältige Auswahl der Zähler unter Vermeidung von Fällen der Interessen- oder Pflichtenkollision (z.B. kein Einsatz im eigenen Wohnbereich, keine Bestellung von Kriminal- oder Finanzbeamten);
- die gezielte Beschränkung der Kenntnisnahme der Daten durch die eingesetzten Zähler und die Mitarbeiter der Zählungsdienststellen;
- eine gründliche Belehrung dieses Personenkreises über das Statistikgeheimnis, die damit zusammenhängende Abschottung der erhobenen Daten und die sich daraus ergebenden Konsequenzen;
- spezifische, auf den großen Umfang des Erhebungsmaterials zugeschnittene Datensicherungsmaßnahmen und die Gewährleistung ihrer Kontrolle.

Anmerkungen

1) Statt aller **Ordemann/Schomerus**, BDSG (3. Aufl. 1982) Anm.1.3; Simitis/**Dammann**/Mallmann/Reh, BDSG (3. Aufl. 1981) § 9 Rdnr. 21; **Bull**, ZRP 1975, 12.

2) § 11 Abs. 4 LDSG BW; Art. 18 Abs. 5 BayDSG; § 16 Abs. 2 HDSG; § 13 Abs. 2 DSG NW; § 7 Abs. 3 LDatG RP; § 16 Abs. 6 SDSG.

3) Vgl. etwa das Protokoll der internen Anhörung zu den Gesetzentwürfen zur Änderung des Bundesdatenschutzgesetzes vom 21. und 22. April 1980, Deutscher Bundestag Innenausschuß -724-2451, Punkt 5; sowie den 10. Tätigkeisbericht des Hessischen Datenschutzbeauftragten 1981, 19 f.

4) Vgl. **Simitis**, in Festschrift für Mallmann (1978) 262 ff.; **Fuckner**, NJW 1981, 1016 ff.

5) Vgl. den 10. Tätigkeitsbericht des Hessischen Datenschutzbeauftragten 1981, 66 ff.; **Fuckner**, NJW 1981, 1018; **Simitis**, in Festschrift für Coing (1982) 519 f.

6) Vgl. **Schmidt**, JZ 1974, 245 f.; **Gallwas**, Der Staat 1979, 514; **Heußner**, in Festschrift für Wannagat (1981) 179; **Simitis**, in Festschrift für Coing 513 f.

7) Vgl. **Benda**, in Festschrift für **Geiger** (1974) 23 ff.; **Benda**/Maihofer/Vogel, Handbuch des Verfassungsrechts (1983) 123.

8) BVerfGE 27,6.

9) Justice **Brandeis**, in Olmstead v. United States, 277 U.S. 438, 478 (1938); BVerfGE 27, 6; 35, 220; **Benda**/Maihofer/Vogel, Handbuch 123.

10) BVerfGE 27,1.

10a) BT-Drucks. 9/451, Begr. A I

11) Statt aller **Zapf**, in Beilage zu Wirtschaft und Statistik H.8 1974, 3 ff.

12) BVerfGE 27,6.

13) Vgl. auch BVerfGE 27, 7, 9; **Benda**/Maihofer/Vogel, Handbuch 120; sowie Rickenbacker v. U.S., 309 F. 2d 462 (1962).

14) BR-Drucks. 9/83; BT-Drucks. 9/2261, S. 3.

15) Dazu insb. **Hansen/Hurwitz**, Sampling methods applied to census work, U.S.Bureau of the Census (o.J.); U.S.Bureau of the Census, The Accuracy of census statistics with and without sampling, Technical paper Nr. 2, 1960; U.S.Bureau of the Census, Sampling applications in censuses of population and housing, Technical paper Nr. 13, 1965; **Waksberg**, The role of sampling in population censuses - its effect on timeliness and accuracy, U.S. Bureau of the Census 1967.

16) Vgl. insb. die Übersicht bei **Dalenius**, Information privacy and statistics, U.S. Bureau of the Census, Technical Working paper No. 41; **Flaherty**, Privacy and government data banks (1979) 261 ff.; **Rapaport**, Legal and technical means for protection of data in statistics production, United Nations Economic and Social Council, Statistical Commission and Economic Commission for Europe, Conference of European Statisticians, 1983, 31st Plenary Session Item 5.

17) The Decennial Census, Report of the Decennial Census Review Committee to the Secretary of Commerce (1971) insb. VI; **Eckler**, The Bureau of the Census (1972) 195 ff.; aber auch U.S. Senate, Committee on the Judiciary, Federal Data Banks and Constitutional Rights, 93rd. Congress, 2nd. Session (1974) I, XV ff.

18) SCB, The National Central Bureau of Statistics and the General Public (1977) insb. 3 ff., 50 ff.; SCB, Public attitudes toward the 1970 Census (1970) 4 ff.; **Dalenius/Klevmarken**, Proceedings of a symposium on personal integrity and the need for data in the social sciences (1976) insb. 18 ff., 82 ff.

19) Verordnung des Bundesrates vom 6. Februar 1980 über die Eidgenössische Volkszählung 1980, Systematische Sammlung des Bundesrechts 431.112.1.

20) Vgl. insb. U.S.Bureau of The Census, Sampling applications aaO.; **Waksberg**, The role of sampling aaO.; **Hansen/Tepping**, Progress and problems in survey methods illustrated by the work of the United States Bureau of the Census, U.S. Bureau of the Census (1968); **Waksberg/Hanson/Bounpane**, Estimations and presentation of sampling errors for sample data from the 1970 U.S. Census (o.J.); SCB, Untersuchungen über alternative Methoden für künftige Volkszählungen und Wohnungsberechnungen 3.7.2.; aber auch **Dalenius**, Access to information through censuses and surveys (1982).

21) BVerfGE 27, 7.

22) Dazu insb. Hearing on the 1970 Census and Legislation related thereto, Subcommittee on Census and Statistics of the House Committee on Post Office and Civil Service, 91st Congress 1st. Sess. Serial No. 91-8 (1969). Auch die französische Datenschutzkommission betont in ihrer Stellungnahme zur Volkszählung 1982 besonders die Notwendigkeit einer klaren Trennung von Statistik und Verwaltung, Commission nationale de l'informatique et des libertés, 2ème rapport d'activité (1982) 21 ff.

23) BVerfGE 27, 8; 45, 420; 48, 221 f.; 50, 378; 53, 311 f.

24) Simitis/**Dammann**/Mallmann/Reh, BDSG § 2 Rdnrn. 20 ff. 26 ff. mit weiteren Angaben.

25) Vgl. auch **Steinmüller**, in **Kaase/Kruppe/Pflanz/Scheuch/Simitis**, Datenzugang und Datenschutz - Konsequenzen für die Forschung (1980) 115 ff.

26) BVerfGE 27, 1.

27) Statt aller **Schlörer**, in **Kaase u.a.** Datenzugang 119.

28) Statistikal Tidskrift 1976, 135 ff.

29) Vgl. etwa den 5. Tätigkeitsbericht des Hessischen Datenschutzbeauftragten, Drucks. 8/2475, 4.6.

30) So die in der Erklärung der European Science Foundation zum Datenschutz und zu der Verwendung personenbezogener Daten für Forschungszwecke vom 12. November 1980, 1.6., wiedergegeben im 9. Tätigkeitsbericht des Hessischen Datenschutzbeauftragten 1980, 75 ff., enthaltene Definition.

Wiesbaden, den 12. Juli 1983

gez. Prof. Dr. Simitis

5.3 Zur Novellierung des Bundesdatenschutzgesetzes (Ziff. 1.1.4)

Erklärung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder und der Datenschutzkommission Rheinland-Pfalz vom 4. November 1983 zur Novellierung des Bundesdatenschutzgesetzes

I.
Die öffentliche Diskussion zu den Themen Volkszählung, maschinenlesbarer Personalausweis, Personalinformationssysteme wie auch Bildschirmtext und andere Neue Medien zeigt eine zunehmende Sensibilisierung zu Fragen des Datenschutzes. Vor diesem Hintergrund ist in der Öffentlichkeit die Erwartung entstanden, daß eine Novellierung des Bundesdatenschutzgesetzes

- die bisher gewonnenen Erfahrungen sowie die neu aufgetretenen Probleme aufgreift und regelt und
- den Datenschutzinstanzen wirksamere Kontrollinstrumente an die Hand gibt.

Die Datenschutzbeauftragten haben sich mehrfach für eine Novellierung ausgesprochen und sind nach wie vor der Meinung, daß das Bundesdatenschutzgesetz novellierungsbedürftig ist. Sie sehen jedoch im vorliegenden Referentenentwurf keinen geeigneten Beitrag zur Fortentwicklung des Datenschutzes, weil er

1. das geltende Datenschutzrecht teilweise verschlechtert,
2. hinter den bisherigen Entwürfen (CDU-Entwurf von 1980, SPD/FDP-Entwurf von 1980, Referentenentwurf von 1982) zurückbleibt
3. wesentliche Forderungen der Datenschutzbeauftragten (Beschluß der Konferenz vom 21. Juni 1982) unberücksichtigt läßt und
4. den Anforderungen nicht gerecht wird, die sich aus der technischen Entwicklung ergeben.

II.
Die Datenschutzbeauftragten fordern zu folgenden Punkten:

1. Aufgabe des Datenschutzes
Die Umschreibung der Aufgabe des Datenschutzes im Bundesdatenschutzgesetz als Schutz vor Mißbrauch ist irreführend, widerspricht dem Regelungsgehalt des Gesetzes und verkürzt den Schutz des Betroffenen. Im Gesetz ist deshalb klarzustellen: Aufgabe des Datenschutzes ist die Regelung des rechtmäßigen Umgangs mit personenbezogenen Daten und nicht nur die Verhinderung vorwerfbaren Fehlverhaltens. Neben der Speicherung, Veränderung, Löschung und Übermittlung sind deshalb auch die Erhebung und sonstige Nutzung Gegenstand des Datenschutzes.

2. Dateibegriff
Die Entscheidung des Gesetzgebers, bei der Anwendung des Bundesdatenschutzgesetzes von der Verarbeitung personenbezogener Daten in Dateien auszugehen, ist für den Bürger kaum verständlich, führt in der Praxis zu Unzuträglichkeiten und mindert die Wirksamkeit des Datenschutzes. Solange diese Anknüpfung besteht, muß der Dateibegriff wenigstens so definiert werden, daß ein Höchstmaß an Schutz für den Betroffenen erreicht wird. Dazu gehört, daß alle automatisierten Verfahren und alle Akten und Aktensammlungen einbezogen werden, die mit Hilfe automatisierter Verfahren erschlossen werden können.

3. Interne Dateien
Ausnahmeregelungen für interne Dateien sind mit einem konsequenten Schutz der Betroffenen unvereinbar. Deshalb muß das Bundesdatenschutzgesetz grundsätzlich auch auf interne Dateien anwendbar sein.

4. Einwilligung
Da das Gesetz jede Datenverarbeitung zuläßt, wenn die Einwilligung des Betroffenen vorliegt, muß der Gesetzgeber durch besondere Regelungen den Betroffenen davor schützen, daß er durch soziale, wirtschaftliche und psychische Zwänge (etwa als Mieter, Patient oder Arbeitssuchender) in seiner Entscheidungsfreiheit unangemessen eingeschränkt wird.

5. Unterrichtung des Betroffenen
Transparenz der Datenverarbeitung ist eine notwendige Voraussetzung des Datenschutzes. Der Betroffene ist deshalb in jedem Fall über die Tragweite seiner Einwilligung in die Datenverarbeitung sowie über die Rechtsgrundlage der Datenerhebung zu unterrichten, und zwar auch dann, wenn er dies nicht ausdrücklich verlangt. Die Unterrichtung bei der Datenerhebung muß ohne Rücksicht darauf erfolgen, ob die Daten in einer Datei, in Akten oder sonstigen Unterlagen festgehalten werden.

6. Verschuldensunabhängiger Schadensersatzanspruch und Folgenbeseitungsanspruch
Bei unzulässiger oder unrichtiger Datenverarbeitung muß der Betroffene einen verschuldensunabhängigen Schadensersatzanspruch (auch für Nichtvermögensschäden) sowie einen Folgenbeseitigungsanspruch haben.

7. On-line-Anschlüsse
Der direkte Zugriff auf automatisierte Dateien über on-line-Anschlüsse ist für den Bürger mit besonderen Risiken verbunden. Dies gilt vor allem dort, wo Daten aus dem Medizin-, Sozial- und Sicherheitsbereich oder über strafbare Handlungen, Ordnungswidrigkeiten, religiöse und politische Anschauungen zum Abruf bereitgehalten werden. Diesen Risiken trägt der Entwurf nicht hinreichend Rechnung. Die Anforderungen an die Zulässigkeit von on-line-Anschlüssen sind zu erhöhen und präziser zu fassen.

8. Zweckbindung
Die Zweckbindung der Daten ist eine der wichtigsten Voraussetzungen für den Schutz des Bürgers. Sie muß insbesondere in folgenden Bereichen verstärkt werden:

- Die Datenweitergabe innerhalb derselben Behörde muß grundsätzlich den gleichen Einschränkungen unterworfen werden wie die Datenübermittlung an andere öffentliche Stellen.
- Bei der Datenübermittlung an andere öffentliche Stellen muß die Verantwortung der übermittelnden Stelle ungeschmälert bleiben.
- Werden Daten an Stellen außerhalb des öffentlichen Bereichs übermittelt, so darf der Empfänger die Daten nur für den Zweck verwenden, zu dessen Erfüllung sie ihm übermittelt wurden.

9. Auskunftsanspruch
Das Recht des Bürgers auf Auskunft über seine Daten ist ein grundlegendes Datenschutzrecht. Es darf nicht eingeschränkt, sondern muß verstärkt werden. Dieses Auskunftsrecht muß gegenüber allen Behörden bestehen, grundsätzlich auch gegenüber den Sicherheits- und Finanzbehörden. Eine generelle Befreiung von der Begründungspflicht ist abzulehnen. Sie stände weder mit der Verfassung noch mit der Rechtsprechung in Einklang. Die Verweigerung einer Auskunft in Ausnahmefällen muß nachprüfbar sein. Die Erteilung der Auskunft muß stets kostenfrei sein.

10. Kontrolle
Im Interesse des Bürgers ist eine unabhängige und umfassende Datenschutzkontrolle unerläßlich. Die Datenschutzbeauftragten stellen dazu fest:

- Ihre Kontrollbefugnis umfaßt die Einhaltung der Datenschutzgesetze und aller anderen Datenschutzvorschriften, unabhängig davon, ob Daten in Dateien, in Akten oder in sonstiger Form festgehalten werden.
- Sie haben das Recht, uneingeschränkt alle Akten einzusehen, die mit der Verarbeitung personenbezogener Daten in Zusammenhang stehen.
- Besondere Geheimhaltungsvorschriften können ihnen bei ihrer Tätigkeit nicht entgegengehalten werden.

III.
Eine Novellierung des Bundesdatenschutzgesetzes kann notwendige bereichsspezifische Regelungen nicht ersetzen. Die Datenschutzbeauftragten erinnern an ihre frühere Forderung nach Sonderregelungen insbesondere für den Sicherheitsbereich und für den Arbeitnehmerdatenschutz.

IV.
Unabhängig von den verschiedenen Vorstellungen zur Novellierung des Bundesdatenschutzgesetzes können und dürfen die sich aus der technologischen Entwicklung ergebenden Konsequenzen nicht übersehen werden. Das Vordringen mittlerer und kleinerer Datenverarbeitungssysteme, die automatisierte Textverarbeitung sowie die Einführung bundesweiter Kommunikationssysteme stellen die Eignung des jetzigen Datenschutzkonzepts in Frage. Der Gesetzgeber wird daher nicht umhin können, in naher Zukunft erneut und umfassend zum Datenschutz Stellung zu beziehen.

Bremen, 4. November 1983

5.4
Zum Bildschirmtext (Ziff. 3.4)

Verzeichnis der Fachausdrücke - Bildschirmtext -

ATM - AUTOMATIC TELLER MACHINE
Terminal (s. dort) für Bankanwendungen wie z.B. Auszahlung von Bargeld, Überweisungen usw.

AUTHENTISIERUNG
Feststellung der Glaubwürdigkeit (z.B. des Absenders von Daten) bei Datenfernverarbeitung

AUTORISIERUNG
Bevollmächtigung (des Benutzers eines Datenfernverarbeitungssystems)

BACK-UP FUNKTION/PROZESSOR
Reservefunktion oder Reserverechner für Datenfernverarbeitungssysteme mit hoher Verfügbarkeit (z.B. Systeme der Polizei). Fällt in einem Backup-System ein Rechner aus, so kann der zweite Rechner dessen Funktionen sofort - d.h. ohne Unterbrechung - übernehmen.

BILDSCHIRMTEXT (Btx)/INTERACTIVE VIDEOTEX
Neuer Dienst der Bundespost. Er bietet die Möglichkeit, über das Fernsprechnetz Informationen (Texte und Grafiken in verschiedenen Farben), die in einem Rechner der Bundespost von verschiedenen Anbietern abgespeichert worden sind, auf den Fernsehschirm abzurufen, Mitteilungen abzusenden, Nachrichten zu empfangen oder im sog. Rechnerverbund, Programme und Daten eines Informationsanbieters abzurufen. Benötigt werden: Ein Farbfernsehgerät mit Fernbedienung, Beistell- oder Einbaudecoder (s. dort), ein Modem (s. dort) und ein Fernsprechanschluß.

BIT
Englisches Kunstwort aus Binary Digit. Kleinste Darstellungseinheit für Binärdaten, zugleich Maßeinheit für das Speichervolumen elektr. Speichermedien wie Band, Platte, Arbeitsspeicher von Computern; Kbit = 1024 Bit.

BTX - Bildschirmtext
(s. dort)

BUS
Elektrische Leitung für Steuerbefehle und Daten in Computern oder Komponenten von Datenverarbeitungsmaschinen; über sie werden alle Informationen innerhalb des Systems ausgetauscht. Meist sind die Schaltungen für Datenadressen (Adreßbus), Steuerdaten (Steuerbus) und Daten (Datenbus) getrennt realisiert.

CEPT - Conference Européene des Administrations des Postes et des Télécommunications
Europäische Konferenz der Post- und Fernmeldeverwaltungen, gegründet 1959 in Montreux/Schweiz, mit dem Ziel, Personal und Informationen auszutauschen und die Verwaltungs- und Betriebsdienste zu harmonisieren.

CHIPKARTE / CHIP-IN-A-CARD
Plastikkarte mit integrierter elektronischer Schaltung (Mikrocomputer). Die Chipkarte kann von außen zugeführte Daten mit intern gespeicherten (geheimen) Informationen nach einem ebenfalls intern gespeicherten (geheimen) Programm verarbeiten und damit unzulässige Zugriffe "abwehren".

DATEX-P (DATA EXCHANGE-PACKET SWITCHED)
Ein öffentliches Netz der Bundespost zum Datenaustausch - Datenfernverarbeitung - mit sog. Paketvermittlung. D.h. jedes "Datenpaket" trägt die Empfängeradresse im Datensatz mit sich und wird vom Vermittlungscomputer "zugestellt". Im Gegensatz dazu: DATEX-L, ein Netz mit gleicher Aufgabenstellung, das aber ähnlich dem Telefonnetz **leitungsvermittelt** geschaltet ist.

DES - FEDERAL INFORMATION PROCESSING DATA ENCRYPTION STANDARD
Eine Norm des US-National Bureau of Standards zur verschlüsselten Datenübertragung. Wird u.a. im gesamten US-Bankverkehr angewendet.

EEPROM
Electrical EPROM (s. dort) mit Permanentspeicher, der beschrieben und gelöscht werden kann; Speicherinhalte bleiben auch bei Spannungsverlust erhalten.

EHKP - Einheitliche Höhere Kommunikationsprotokolle
Dieser Verwaltungsstandard wurde als Vorläufer einer ISO-Norm (s.dort) festgelegt. Er ermöglicht den systemneutralen Aufbau von Datennetzen (Verbund von DV-Anlagen unterschiedlicher Hersteller) auf der Grundlage des Modells "Kommunikation offener Systeme" (ISO-7-Schichtenmodell 7498).

EPROM
Eraseable PROM - Programmierbarer Lesespeicher, der durch Bestrahlung mit ultraviolettem Licht gelöscht werden kann.

GATEWAY
Bezeichnung für einen Computer, der als Vermittlungsstelle zu einem anderen Rechner oder Datenverarbeitungsnetz eingesetzt ist.

GEHEIMZAHL, Persönliche
s. P.I.N.

GESCHLOSSENE BENUTZERGRUPPE
Durch den Betreiber eines Datenverarbeitungssystems bestimmte Benutzergruppe, der er den Zugang zu Informationen und Rechenleistungen seines Computers über das Btx-Netz erlaubt. Die Autorisation der Benutzer wird durch die Eingabe eines persönlichen Kennwortes am Terminal geprüft.

HALBLEITER
Material für elektronische Bauelemente (z.B. Germanium und Silizium); Ausgangsbasis für Transistoren, integrierte Schaltungen und Halbleiterspeicher (mikroelektronische Speicher).

HOST/HOSTRECHNER
Datenverarbeitungsanlage, die im Wege des Direktzugriffs einem externen Benutzer Zugriff auf Daten und Programme erlaubt.

INHOUSE - ANWENDUNG/BETRIEB
Btx-Betrieb auf privaten Leitungswegen. Dient dem Informationsaustausch innerhalb eines Unternehmens oder einer Institution und ist gegenüber herkömmlichen DV-Anlagen wesentlich preiswerter, da er die vorhandene Fernsprechnebenanlage und Standard-Fernsehgeräte verwendet.

INTEGRIERTE SCHALTUNG
Mikroelektronische Schaltung, deren Bauelemente auf einer Platte (Substrat) in einem gemeinsamen Herstellungsprozeß aufgebracht werden. Enthält diese Schaltung Logikfunktionen (Mikroprozessor) **und** Speicherelemente, spricht man auch von einem sog. Monolith.

INTERAKTIVE DATENFERNVERARBEITUNG
Dialogbetrieb zwischen einem Terminal (s. dort) und einem Computer. In einem Frage-Antwort"spiel" zwischen Benutzer und Rechnerprogramm wird eine Aufgabe gelöst.

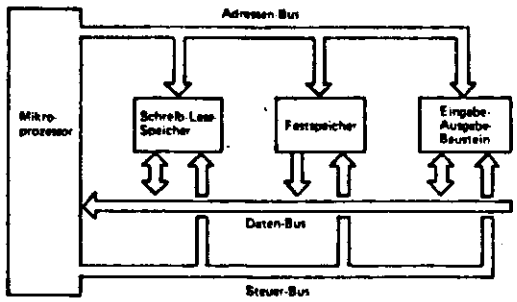
ISO - INTERNATIONAL STANDARDS ORGANISATION
Internationaler Verband der Normungsgremien.

KRYPTOGRAPHIE
Geheimschrift, Verschlüsselungsverfahren z.B. in der Datenfernverarbeitung.

MEMORY CARD
s. Chipkarte

MENU/MENUSYSTEM
Bedienerführung in einem Programm zur Datenfernverarbeitung am Bildschirm (Inhaltsverzeichnis bzw. Bedienungshinweise).

MIKROCOMPUTER/MICROCOMPUTER
Minicomputer (s. dort) auf der Basis höchstintegrierter Schaltungen (VLSI - s. dort) ohne eigene Bedienungselemente. Seine Bestandteile sind: Mikroprozessor, Programmspeicher, Datenspeicher und eine Ein-/Ausgabeeinrichtung als Schnittstelle zu externen Geräten. Microcomputer für bestimmte (begrenzte) Anwendungen werden bereits auf einem Chip (s. dort) von der Größe eines Zehnpfennigstückes untergebracht.



MIKROPROZESSOR/MICROPROCESSOR
Auf kleinstem Raum realisierte logische Verarbeitungseinheit ähnlich der Zentraleinheit (CPU) eines Computers. Der Mikroprozessor ist stets aufgabenneutral angelegt und somit ein reines Werkzeug. Die erforderlichen Informationen (Daten und Programm) erhält er aus den angeschlossenen Speichern (s. Mikrocomputer).

MINICOMPUTER
Rechnergeneration (1960 Fa. Digital Equipment USA) die durch die Verwendung von hochintegrierten Bauteilen (s. VLSI) große Rechnerleistung bei kleinerer Abmessung und sehr günstigem Preis/Leistungsverhältnis bietet.

MODEM (**Mo**dulator/**Dem**odulator)
Gerät zur Datenübertragung auf dem Fernsprechnetz. Ein Modem wandelt die Gleichstromimpulse einer Datenendeinrichtung (z.B. Terminal) in Wechselstromimpulse um, deren Kenngröße die binäre Null oder die binäre Eins darstellen. Diesen Vorgang bezeichnet man als Modulation bzw. Demodulation.

MONOLITHISCHE SCHALTUNG; MONOLITH
(s. integrierte Schaltung)

ÖFFENTLICHER SCHLÜSSEL
Schlüsselalgorithmus auf der Basis großer Primzahlen. Seine Besonderheit liegt darin, daß jeder Teilnehmer seinen geheimen Schlüssel und einen gemeinsamen (öffentlichen) Schlüssel benutzt. Ein bekannter öffentlicher Schlüssel ist der sog. RSA-Schlüssel, benannt nach den Mathematikern Rivest, Shamir und Adlmann.

PERONALCOMPUTER
aus dem Englischen "personal" d.h. persönlicher Computer; besonders preiswerter Minicomputer (s. dort).

P.I.N. - Personal Identifier Number
persönliche Geheimzahl zur Identifizierung gegenüber dem Computer in einem Datenfernverarbeitungssystem.

POLLING
Technisches Verfahren in der Datenübertragung; unter Verwendung einer standardisierten Übertragungsprozedur "fragt" der Computer bei einem Datenendgerät an, ob es sendebereit ist.

POS-POINT OF SALE SYSTEM/EFTS-ELECTRONIC FUNDS TRANSFER SYSTEM
Vertriebssystem des Handels, bei dem bei bargeldloser Zahlung (Euroscheck, Kreditkarte o.ä.) ein (automatisiertes) Kassenterminal die Kreditwürdigkeit des Kunden prüft. Dies kann durch Direktzugriff auf einen Bankcomputer (online) oder durch Abfrage eines integrierten Speichers (offline) geschehen.

PROM - PROGRAMMABLE ROM
Weiterentwicklung des Lesespeichers (ROM) der im Gegensatz zu einem ROM auch noch **nach** der Herstellung durch Zugriff von außen mit einem Programm geladen werden kann.

PUBLIC KEY
s. öffentlicher Schlüssel

RAM - RANDOM ACCES MEMORY
Lese- und Schreibspeicher mit **direktem** Zugriff auf ein Wort bzw. Byte. Informationen in einem RAM sind **nicht** permanent gespeichert, d.h. ohne Spannungsquelle (Batterie o.ä.) geht die Information verloren. RAM's werden als Arbeitsspeicher in Mikroprozessoren (s. dort) eingesetzt.

REMOTE JOB ENTRY
Aufruf einer Programmfolge in einem Computer zur Lösung eines Problems (job) von einem entfernten (externen) Terminal.

ROM - READ ONLY MEMORY
Halbleiterspeicher der nur gelesen werden kann. Er wird bei der Herstellung mit einem Programm geladen (kodiert). ROM's sind in der Regel Programmspeicher für Mikroprozessoren.

RSA-Funktion
s. öffentlicher Schlüssel

SCHLÜSSELALGORITHMUS
Rechenschema (Regeln), mit dessen Hilfe Daten ver- bzw. entschlüsselt werden.

SCHLÜSSELMANAGEMENT
Schlüsselverteilung und Schlüsselbehandlung (z.B. Auswechseln der Schlüssel, Vernichtung von Schlüsseln) in Datenfernverarbeitungssystemen mit kryptographischen Verfahren; in der Regel ein Mengen- und Sicherheitsproblem.

SMART CARD
s. Chipkarte

STAPELVERARBEITUNG/STAPELBETRIEB - BATCH PROCESSING
Verarbeitungsform in der Datenverarbeitung, bei der alle mit den gleichen Programmen zu bearbeitenden Geschäftsvorgänge (Daten) zuerst (auf einem Datenträger) gesammelt und dann in einem Schub verarbeitet werden.

SWIFT/SWIFTNET - SOCIETY FOR WORLDWIDE INTERBANK FINANCIAL TELECOMMUNICATION
Internationaler Zusammenschluß von Banken zum Zweck des beleglosen grenzüberschreitenden Zahlungsverkehrs. SWIFT betreibt ein eigenes rechnergesteuertes Datennetz mit Rechenzentren in Leiden/Holland und Brüssel/Belgien.

TAMPERPROOF/TAMPERPROOFING
engl.: Sicherheit gegen Manipulation/Sichern gegen Manipulation (z. B. eines Terminals oder eines Chipkartenlesers).

TéLéTEL - Téléphone et Téléviseur
neuer Dienst der französischen Post PTT. In einem Großversuch werden Dienste wie HOME-BANKING oder POS-Verfahren (s. dort) angeboten; Vorläufer des Bildschirmtextes.

TERMINAL
Datenendgerät in einem System zur Datenübertragung, z.B. Bildschirm mit Schreibmaschinentastatur.

TERMINAL-ID
Kennummer eines Terminals (s. dort) gegenüber dem Computer; dient zur einwandfreien Zuordnung eines Datenendgerätes, z.B. bei Zugriffen auf geschützte Datenbanken bzw. Datenbankbereiche.

VIDEOTEX
Bildschirmtext (s. dort) im Ausland

VLSI - VERY LARGE SCALE INTEGRATED CHIP
Mikroelektronischer Speicher (Chip) mit z.Z. 65.536 Bit (64 KBit) bzw. 131.072 Bit (128 KBit) Speicherkapazität, der als Massenprodukt in großen Stückzahlen hauptsächlich in den USA und Japan, aber auch in der Bundesrepublik (IBM u. Siemens) gefertigt wird. 256 KBit Chips werden bereits in kleinen Serien produziert; IBM hat in den USA einen Chip mit 512 KBit als Labormuster hergestellt und getestet.

ZUFALLSZAHL/RANDOMNUMBER
Nach den Regeln der Wahrscheinlichkeitsrechnung gefundene Zahl. Wird eine Zufallszahl in einer ADV-Anlage mit einem Programm erzeugt (Zufallszahlengenerator), erhält man keine **echten** Zufallszahlen, da sie sich zwangsläufig nach einem bestimmten Zyklus wiederholen müssen. Wird dieser Zyklus ausreichend groß gewählt, dann sind diese Dubletten für die durchzuführenden Aufgaben meist ohne Bedeutung.