12. Wahlperiode

Drucksache **12/4040**

HESSISCHER LANDTAG

02. 02. 89

Siebzehnter Tätigkeitsbericht des Hessischen Datenschutzbeauftragten

Professor Dr. Spiros Simitis

vorgelegt zum 31. Dezember 1988
gemäß § 30 des Hessischen Datenschutzgesetzes vom 11. November 1986

Eingegangen am 2. Februar 1989 · Ausgegeben am 28. Februar 1989

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

12/4040

INHALTSVERZEICHNIS

KERNPUNKTE DES 17. TÄTIGKEITSBERICHTS

1. Der Gesetzentwurf zur Novellierung des Bundesdatenschutzgesetzes, den das Bundeskabinett am 20. Dezember 1988 verabschiedet hat, ist ebenso wie die früheren Änderungsvorschläge inakzeptabel, weil Zulässigkeit und Kontrolle der Datenverarbeitung nicht entsprechend den Vorgaben des Bundesverfassungsgerichts geregelt werden sollen (Ziff. 1.1.1.1 und 2.2.1).
2. Der am 20. Dezember 1988 vom Bundeskabinett verabschiedete Entwurf eines Bundesverfassungsschutzgesetzes ist verfassungswidrig (Ziff. 1.1.1.2 und 2.1.2).
3. Die Patientendaten in Krankenhäusern sind gegenwärtig völlig unzureichend gesetzlich geschützt. Meine Regelungsvorschläge für die Verarbeitung von Patientendaten hat das Sozialministerium in seinem im Dezember 1988 vorgelegten Gesetzentwurf zur Neuordnung des Krankenhauswesens in Hessen (Hessisches Krankenhausgesetz 1989) unverändert übernommen (Ziff. 1.1.2.2 und 5.1).
4. Solange über die möglichen sozialen und rechtlichen Folgen einer Nutzung der Genomanalyse keine Klarheit besteht, ist aus der Sicht des Datenschutzes der Aufbau genetischer Datensammlungen nicht akzeptabel (Ziff. 1.1.3 und 5.2).
5. Die drei dem Landtag vorliegenden Gesetzentwürfe zur Novellierung des Hessischen Gesetzes über die öffentliche Sicherheit und Ordnung (HSOG) bieten eine ausreichende Grundlage für eine verfassungskonforme Regelung der polizeilichen Datenverarbeitung. Allerdings sind noch in vielen Punkten Präzisierungen und Eingrenzungen erforderlich (Ziff. 3.1).
6. Die Datenspeicherungen, die die Polizei in der sogenannten „L-Gruppe" (Personenbeschreibung) des Hessischen Polizeiinformationssystems (HEPOLIS) vornimmt, berücksichtigen nicht ausreichend die Grundsätze des Datenschutzes (Ziff. 3.3).
7. Für die Zentralen Namensdateien der Staatsanwaltschaften gibt es keine ausreichende Rechtsgrundlage. Sollte der Bundesgesetzgeber diese nicht bis Ende 1990 geschaffen haben, dürfen nach einer Entscheidung des Oberlandesgerichts Frankfurt die Dateien nicht weiter geführt werden (Ziff. 4.1).
8. Das Hessische Sozialministerium hat den Entwurf eines für alle klinischen Krebsregister in Hessen einheitlichen Datenschutzkonzepts vorgelegt. Der Entwurf, über den noch einmal unter Beteiligung der betroffenen Stellen verhandelt werden soll, berücksichtigt meine Vorschläge (Ziff. 5.3).
9. Aids-Tests dürfen grundsätzlich nur mit Einwilligung der Betroffenen durchgeführt werden. Die Anforderungen der Datenschutzgesetze an eine rechtswirksame Einwilligung werden oft nicht eingehalten (Ziff. 5.4.2).
10. Für den Entwurf eines Gesetzes zur Einführung eines Sozialversicherungsausweises gilt die gleiche Kritik wie für das Gesundheits-Reformgesetz. Es ist keine ausreichende Prüfung von Maßnahmen zur Bekämpfung der Schwarzarbeit vorausgegangen, die das informationelle Selbstbestimmungsrecht weniger einschränken (Ziff. 6.2).
11. Die Jugendämter sind gesetzlich verpflichtet, dem Hessischen Datenschutzbeauftragten Einsicht in Jugendhilfeakten zu gewähren (Ziff. 6.3).
12. Entsprechend meiner Forderung ist in Hessen die Beseitigung der Erhebungsunterlagen aus der Volkszählung 1987 so beschleunigt worden, daß der Großteil der Papiere im Jahr 1988 vernichtet worden ist (Ziff. 7.1).
13. Mit der Immatrikulationsverordnung vom 26. Mai 1988 wird den hessischen Universitäten, Kunst- und Fachhochschulen erstmalig detailliert vorgeschrieben, welche Studentendaten sie für welche Verwaltungszwecke verarbeiten dürfen und welche sonstigen Bedingungen dabei eingehalten werden müssen (Ziff. 8.1).
14. Bei Heranziehung von Anliegern zu Straßenbeiträgen dürfen Gemeinden nicht die gesamten Abrechnungsunterlagen öffentlich zur Einsichtnahme auslegen (Ziff. 10.1).
15. Die Straßenverkehrsbehörde darf Gemeinden nicht über Fahrerlaubnisentziehungen und Fahrverbote unterrichten (Ziff. 10.4).
16. Private Stellen sind nicht verpflichtet, dem Finanzamt regelmäßig Empfänger von Honorarzahlungen mitzuteilen (Ziff. 11.3).
17. Es verstößt gegen das Steuergeheimnis, wenn das Finanzamt allen Banken und Sparkassen am Wohnort eines Steuerschuldners Pfändungsverfügungen zustellt, ohne zu wissen, ob tatsächlich eine Bankverbindung zu den jeweiligen Kreditinstituten besteht (Ziff. 11.5).
18. Die angebotene Datenschutzsoft- und -hardware für Arbeitsplatzcomputer hat sich deutlich verbessert. Ihr Funktionsumfang hat sich demjenigen für Großrechner angenähert (Ziff. 12.1).
19. Bei Prüfungen stellt sich immer wieder heraus, daß die vom Hessischen Datenschutzgesetz geforderten Datensicherheitsmaßnahmen bei der Aufbewahrung von Akten nicht oder nicht in ausreichendem Maße getroffen worden sind (Ziff. 12.2).

1. Zur Situation

1.1
Gesetzgebung

Fünf Jahre ist es mittlerweile her, seit das Bundesverfassungsgericht in seiner Entscheidung zum Volkszählungsgesetz von 1983 die Bedingungen umschrieben hat, denen eine verfassungskonforme Verarbeitung personenbezogener Daten genügen muß, fünf Jahre, in denen der Gesetzgeber allen Anlaß und auch genug Zeit gehabt hätte, die notwendigen Maßnahmen zu treffen. Schließlich war er vom Gericht unmißverständlich angesprochen worden. Niemand sonst kann ebenso generell wie verbindlich Verarbeitungsvorgaben formulieren, die etwa neben einer genauen Information des Betroffenen und einer strikten Zweckbindung die höchstmögliche Transparenz sowie eine uneingeschränkte Kontrollierbarkeit vorschreiben. Niemand anders ist zudem so unmittelbar von der verfassungsrechtlichen Verpflichtung betroffen, die Funktionsvoraussetzungen der informationellen Selbstbestimmung sicherzustellen.

Die Reaktion war und ist enttäuschend. Legislative Entscheidungen wie die des hessischen Gesetzgebers zur Novellierung des Datenschutzgesetzes sind immer noch die Ausnahme. Überhaupt waren es die Landesgesetzgeber, die am ehesten den Erwartungen des Bundesverfassungsgerichts Rechnung getragen haben. Auf der Bundesebene zog man es statt dessen weitgehend vor, sich lange und intensiv zu unterhalten über die Schwierigkeit der Aufgabe und die Unmöglichkeit, sie innerhalb einer bestimmten absehbaren Frist zu erfüllen. Inzwischen hat sich durch den Beschluß des OLG Frankfurt vom 14. Juli 1988, in dem das Gericht vom Bundesgesetzgeber verlangt, bis 1990 für die Zentralen Namensdateien der Staatsanwaltschaften eine ausreichende Rechtsgrundlage zu schaffen (vgl. Ziff. 4.1 dieses Berichts), freilich genau das bestätigt, was schon im 15. Tätigkeitsbericht klar angegeben war: Die Reaktionsfrist des Gesetzgebers ist beschränkt. Die Bedeutung des Regelungsgegenstandes läßt keine Wahl: Der Gesetzgeber ist gleichsam zweifach gebunden, inhaltlich ebenso wie zeitlich. Insoweit besteht auch kein Unterschied zwischen Bundes- und Landesgesetzgeber. Verschieden kann allenfalls der Zeitpunkt sein, bis zu dem der jeweilige Gesetzgeber die ihm obliegende Regelungspflicht zu erfüllen hat.

1.1.1
Regelungsaufgaben des Bundesgesetzgebers

Die Rechtsprechung hat klar zu erkennen gegeben: Für den Bundesgesetzgeber läuft die Frist zur Schaffung verfassungskonformer Rechtsgrundlagen für die Verarbeitung personenbezogener Daten mit dem Ende der gegenwärtigen Legislaturperiode ab. Wie schwer diese Feststellung wiegt, zeigt sich, sobald man nicht nur die Kürze der noch verbleibenden Zeit bedenkt, sondern auch die Tragweite der Aufgabe. Allzu leicht neigt man dazu, nicht zuletzt unter dem Eindruck der öffentlichen Diskussion, sie lediglich auf die Reform des Bundesdatenschutzgesetzes und die für eine Verarbeitung personenbezogener Daten im Sicherheitsbereich erforderlichen gesetzlichen Grundlagen zu beziehen. Die Liste ist freilich sehr viel länger und enthält etwa mit der Strafprozeß- sowie der Abgabenordnung Regelungen von durchaus vergleichbarer Bedeutung, die zudem keineswegs geringere Ansprüche an die Vorbereitung der Gesetzestexte stellen. Kurzum, mit der Novellierung des Bundesdatenschutzgesetzes allein ist es nicht getan, die zeitliche Bindung gilt genauso für alle anderen im Hinblick auf die Verarbeitung personenbezogener Daten erforderlichen Regelungen. Dies um so mehr, als das Bundesverfassungsgericht es nicht bei der Forderung nach gesetzlichen Vorschriften belassen, vielmehr ausdrücklich auf den jeweiligen Verarbeitungszusammenhang abgestellte Bestimmungen verlangt hat, zumindest für all die Fälle, in denen der Betroffene gezwungen wird, Informationen zu seiner Person bereitzustellen. Noch so überzeugend novellierte allgemeine Datenschutzgesetze können, so gesehen, bestenfalls eine Notlösung sein, mit deren Hilfe sich die Zeit bis zur Verabschiedung der eine Verarbeitung letztlich allein legitimierenden bereichsspezifischen Regelungen überbrücken läßt. Nach wie vor sind aber für nahezu alle wichtigen Verarbeitungsbereiche keine Entscheidungen gefallen und auch die Zahl der Entwürfe, die über erste Überlegungen hinausgehen, ist bedenklich gering. Nach wie vor fehlt es überdies an verläßlichen Aussagen über Art und Anzahl der erforderlichen Regelungen, die einzuhaltende Reihenfolge sowie den vorgesehenen Zeitplan. Kaum verwunderlich, wenn die kurze verbleibende Frist von zwei Jahren noch bedrohlicher wirkt. Ebensowenig überraschen freilich die sich mehrenden Zweifel daran, ob es der Bundesgesetzgeber überhaupt schaffen kann, seiner Verpflichtung nachzukommen.

1.1.1.1
Novellierung des Bundesdatenschutzgesetzes – ein drohender Rückschritt

Die Zweifel werden erst recht verständlich, sobald man sich die bislang vorliegenden Gesetzentwürfe genauer anschaut. Um mit dem Bundesdatenschutzgesetz zu beginnen: So schwer konnte es nicht sein, Lösungen zu finden, die bei allen Meinungsverschiedenheiten im Detail durchaus den Erwartungen des Bundesverfassungsgerichts entsprochen hätten. Schließlich hat die Diskussion über die notwendigen Korrekturen schon kurz nach der Verabschiedung des BDSG eingesetzt. Zudem liegen mittlerweile drei Landesdatenschutzgesetze vor, deren ausdrückliches Ziel es gewesen ist, die im Hinblick auf die Entscheidung des Bundesverfassungsgerichts erforderlichen Änderungen vorzunehmen. Und doch schlägt der am 20. Dezember 1988 vom Bundeskabinett verabschiedete Gesetzentwurf einen Weg ein, der letztlich nicht dazu führt, den Datenschutz zu verbessern, sondern weit eher dazu verhilft, ihn zu unterlaufen (vgl. auch Ziff. 2.1.1).

1.1.1.1.1
Einschränkung der Kontrollbefugnisse des Datenschutzbeauftragten

Allein schon die Bestimmungen zur Kontrollbefugnis des Bundesdatenschutzbeauftragten reichen aus, um zu zeigen, wie sehr die Verfasser des Entwurfs Schranken dort aufzurichten versuchen, wo sie gerade behoben werden müßten. Die

Wirksamkeit des Datenschutzes hängt, so viel läßt sich nicht ernsthaft bestreiten, gerade von einer ebenso kontinuierlichen wie uneingeschränkten Kontrolle der verschiedenen Verarbeitungsvorgänge ab. Ganz in diesem Sinn hatte das Bundesverfassungsgericht die Existenz sowie die Tätigkeit unabhängiger Datenschutzbeauftragter als eine der Grundvoraussetzungen eines präventiven Rechtsschutzes bezeichnet. Und eben deshalb begnügt sich das Hessische Datenschutzgesetz nicht mit Vorschriften, die eine institutionelle Unabhängigkeit des Datenschutzbeauftragten garantieren, sondern gewährleistet den jederzeitigen und uneingeschränkten Zugang des Datenschutzbeauftragten zu allen für die Ausübung seiner Tätigkeit erforderlichen Unterlagen.

Anders der Entwurf: Auffällig ist schon, daß er nahezu nichts an den bislang, etwa im Sicherheitsbereich, bestehenden Zugangsbarrieren ändert. Neu hinzu kommen weitere Erschwerungen. Dazu gehört beispielsweise jene Regelung, die bei personenbezogenen Daten, die dem Steuer- oder dem Arztgeheimnis unterliegen, in Personalakten oder in den im Hinblick auf eine Sicherheitsüberprüfung angelegten Akten enthalten sind, eine Kontrolle nur zuläßt, sofern der Betroffene nicht „widersprochen" hat. Was hier noch etwas verklausuliert formuliert wird, bringt der Entwurf zur Reform der Abgabenordnung klar zum Ausdruck: Die von den Finanzbehörden verarbeiteten personenbezogenen Daten dürfen dem Datenschutzbeauftragten nur „offenbart" werden, wenn der Betroffene „eingewilligt oder sich nach vorheriger schriftlicher Benachrichtigung" nicht dagegen ausgesprochen hat. Auf den ersten Blick eine durchaus den Interessen der Betroffenen entsprechende Vorschrift: Weil es um ihre Daten geht, sollen sie auch selbst darüber befinden, ob der Datenschutzbeauftragte kontrollieren darf. In Wirklichkeit jedoch eine Bestimmung, die den Betroffenen benutzt, um eine nicht um seiner selbst willen konzipierte, sondern gegen ihn gerichtete Vorkehrung durchzusetzen.

Es ist kein Zufall, daß kein einziges Gesetz bislang eine vergleichbare Vorschrift kennt. Der Gesetzgeber wußte nur zu gut: Eine Datenschutzkontrolle kann lediglich dann Erfolg haben, wenn sie sich auf die gesamte Tätigkeit einer bestimmten Behörde oder eines einzelnen Verwaltungszweigs erstreckt. Anders ausgedrückt: Erst eine umfassende, alle oder jedenfalls einen ausschließlich vom Datenschutzbeauftragten festgelegten Ausschnitt der Unterlagen betreffende Überprüfung läßt erkennen, nach welchen Gesichtspunkten die Daten jeweils erhoben und verarbeitet, und damit, ob die gesetzlichen Anforderungen beachtet werden und wenn nicht, wo genau Korrekturen vorzunehmen sind. Ein Blick in die Tätigkeitsberichte der Datenschutzbeauftragten genügt, um sich davon zu überzeugen.

Ganz gleich, ob es um Krankenhäuser, Statistikämter, Polizeibehörden oder kommunale Dienststellen ging, die Chance einer gerade an den Auswirkungen der Verarbeitung auf die Betroffenen ausgerichteten Überprüfung bestand nur so lange, wie es auch möglich war, die Art sowie den Umfang der kontrollierten Unterlagen lediglich vom Kontrollzweck her zu bestimmen. Eine Regelung, wie sie die Entwürfe zum Bundesdatenschutzgesetz und zur Abgabenordnung vorsehen, kommt deshalb einer Preisgabe der auch und vor allem um des Betroffenen willen unerläßlichen Überprüfung der Verarbeitung personenbezogener Daten gleich.

1.1.1.1.2
Akten werden vom Datenschutz freigestellt

Nicht minder weitreichend sind die Konsequenzen der Weigerung, die gesetzlich abgesicherten Verarbeitungsbedingungen auf Akten anzuwenden. Der Datenschutz ist ohne Zweifel zunächst eine Reaktion auf die automatisierte Verarbeitung personenbezogener Angaben gewesen. Längst hat sich aber gezeigt, daß sich die ursprünglich vorgenommene Trennung zwischen Dateien einerseits und Akten andererseits nicht aufrechterhalten läßt. Schon deshalb, weil in der Regel beide Verarbeitungsformen miteinander verbunden werden. Auch dort aber, wo sich einzelne Daten lediglich in Akten finden, folgt daraus noch keineswegs, daß derartige Angaben von höchst zweitrangiger Bedeutung sind. Die Erfahrung zeigt im Gegenteil nur zu gut, daß in einer Vielzahl von Fällen die aus der Perspektive des Betroffenen wichtigsten Informationen zu seiner Person in Akten enthalten sind. Wenn deshalb dem verfassungsrechtlichen Gebot, die informationelle Selbstbestimmung zu gewährleisten, wirklich entsprochen werden soll, dann darf der Schutz gegen die Verarbeitungsgefahren nicht von der Verarbeitungsform abhängen. Ein Datenschutzgesetz, das die Akten ausklammert, verfehlt daher seine Aufgabe.

Gewiß, der Entwurf ist mit einer Novellierung des Verwaltungsverfahrensgesetzes verbunden, die auch auf die Verarbeitung personenbezogener Daten in Akten eingeht. Diese Konzession darf jedoch, von der Kritik an den Einzelheiten der vorgeschlagenen Regelung einmal abgesehen, nicht darüber hinwegtäuschen, daß damit eine durch nichts gerechtfertigte Einschränkung vorgenommen wird. Weite Teile des öffentlichen Bereichs bleiben wegen des beschränkten Anwendungsbereichs des Verwaltungsverfahrensgesetzes von den verfassungsrechtlich gebotenen Verarbeitungsvorkehrungen ebenso ausgeschlossen wie der gesamte private Bereich.

Auch die immer wieder betonte „Ausdehnung" der Prüfungsbefugnisse des Bundesdatenschutzbeauftragten auf die mit einer Kontrolle der Verarbeitung personenbezogener Angaben in Dateien zusammenhängenden Akten macht die verfassungsrechtlich unvertretbare Freistellung der Akten vom Datenschutz nicht akzeptabler. Zunächst: Der Entwurf baut damit die Kontrollrechte keineswegs aus, er korrigiert lediglich eine im Bundesbereich ebenso wie in manchen Bundesländern verbreitete falsche Interpretation des geltenden Rechts. Eine solche sicherlich begrüßenswerte Klarstellung hat zudem lediglich eine partielle Einbeziehung der Akten zur Folge.

Beides, die Einschränkung der Kontrollbefugnisse des Bundesdatenschutzbeauftragten und die unterschiedliche Behandlung von Dateien und Akten, hätte freilich durchaus vermieden werden können. An Vorgaben für eine verfassungskonforme Regelung fehlt es nicht. So bezieht das Hessische Datenschutzgesetz ausdrücklich die Akten ein,

ohne dabei die sich aus der Eigenart der jeweiligen Verarbeitungsform ergebenden Konsequenzen für die Verarbeitungsanforderungen außer acht zu lassen. Genauso verfahren übrigens die anderen nach dem HDSG verabschiedeten Datenschutzgesetze. Der Entwurf fällt insofern eindeutig hinter den inzwischen erreichten Stand der Datenschutzgesetzgebung zurück. So haben die Datenschutzbeauftragten wiederholt auf die Notwendigkeit hingewiesen, die Novellierung zum Anlaß zu nehmen, um Kontrollhindernisse ebenso abzubauen wie von einer Verknüpfung des Datenschutzes mit einer bestimmten Verarbeitungsform abzusehen.

1.1.1.2
Novellierung des Bundesverfassungsschutzgesetzes

Noch schärfer fällt der Widerspruch zwischen den verfassungsrechtlichen Anforderungen und den geplanten Regelungen beim Entwurf für ein neues Bundesverfassungsschutzgesetz aus (vgl. auch Ziff. 2.1.2). Einfach deshalb, weil diese Vorschläge nicht einmal den elementarsten Erwartungen des Bundesverfassungsgerichts genügen. Am Anfang aller Bemühungen, verfassungskonforme Verarbeitungsvorkehrungen zu formulieren, muß, so die unmißverständliche Feststellung des Gerichts, eine klare Umschreibung der Aufgaben der jeweiligen speichernden Stelle stehen, verbunden mit einer ebenso klaren Zuordnung der Verarbeitungsbefugnisse. Anders ausgedrückt: Daß eine bestimmte Behörde meint, bestimmte personenbezogene Daten für ihre Ziele zu brauchen, reicht in keinem Fall. Die Legalität der Verarbeitung läßt sich vielmehr erst beurteilen, wenn feststeht, welche Aufgaben diese Behörde im einzelnen zu erfüllen hat und mit welchen Verarbeitungsbefugnissen sie konkret ausgestattet ist. Genau dies versäumt der Entwurf, den das Bundeskabinett am 20. Dezember 1988 verabschiedet hat. Er beläßt es nicht nur bei den bisherigen überaus allgemeinen Formulierungen, sondern sieht auch von einer aufgabenorientierten Differenzierung bei der Verarbeitung ab. Was immer deshalb der Verfassungsschutz an personenbezogenen Daten erhebt, läßt sich tendenziell für jede seiner durchaus unterschiedlichen Aufgaben verarbeiten.

Mindestens ebenso bedenklich ist die pauschale Weigerung, einen Informationsanspruch des Betroffenen anzuerkennen. Wohlgemerkt, Situationen, in denen es bei vielen datenverarbeitenden Stellen durchaus angebracht, ja notwendig erscheint, von einer Auskunft abzusehen, gibt es ohne Zweifel. Genausowenig kann bestritten werden, daß der Tätigkeitsbereich des Verfassungsschutzes zu den Verarbeitungskomplexen gehört, bei denen sich in einer Reihe von Fällen durchaus überzeugende Gründe für eine Auskunftsverweigerung anführen lassen. Trotzdem geht es nicht an, daraus die Berechtigung zu folgern, den Verfassungsschutz generell von einer Auskunftsverpflichtung freizustellen, schon mit Rücksicht auf die verschiedenen ihm obliegenden Aufgaben. So muß beispielsweise bei einer Sicherheitsüberprüfung der Betroffene das Recht haben, darüber informiert zu werden, welche Daten zu seiner Person vorliegen. Auch hier gilt daher der durch die Erfahrung der letzten Jahre immer wieder bestätigte Grundsatz: Allgemeine Ausnahmen von der Auskunftsverpflichtung zugunsten einzelner datenverarbeitender Stellen darf es nicht geben. Die Auskunftsverweigerung muß eine von vornherein klar begrenzte Ausnahme bleiben. Wo sich jedoch eine Verweigerung nicht vermeiden läßt, ist der Betroffene grundsätzlich über die Ablehnungsgründe zu informieren. In diese Richtung weisen etwa die dem Hessischen Landtag vorliegenden Vorschläge zur polizeilichen Datenverarbeitung.

Beides zusammen, die mangelnde Präzision bei der Aufgabenbeschreibung sowie die fehlende Differenzierung bei den Verarbeitungsbefugnissen und die pauschale Ablehnung eines Auskunftsanspruchs, zwingt zu dem Schluß: Eine Verarbeitungsregelung, wie sie der von der Bundesregierung vorgelegte Entwurf eines Bundesverfassungsschutzgesetzes enthält, ist verfassungswidrig.

Noch einmal: Dem Bundesgesetzgeber steht für die Vorlage mindestens eines Teiles der immer noch ausstehenden Entwürfe sowie für die Korrektur der inzwischen veröffentlichten Regelungsvorschläge nur eine beschränkte Zeit zur Verfügung. Deshalb kann es nicht, wie zuweilen behauptet, gleichgültig sein, ob es noch in dieser Legislaturperiode zu einer Regelung kommt. Mit ihrem Ende läuft auch die Frist ab, innerhalb derer eine den verfassungsrechtlichen Anforderungen nicht entsprechende Verarbeitung hingenommen werden darf. Mit ihrem Ende ist daher auch der Zeitpunkt erreicht, von dem an die Verarbeitung beanstandet werden muß, und zwar auch und gerade dort, wo aus dem Landesbereich personenbezogene Daten in die Verbunddateien eingespeichert werden.

1.1.2
Landesgesetzgebung

Anders stellt sich die Lage auf der Landesebene dar. Schon deshalb, weil der hessische Gesetzgeber mit der Reform des Datenschutzgesetzes die Grundlage für eine verfassungskonforme Verarbeitung personenbezogener Angaben geschaffen hat. Auch bei den hier wie anderswo notwendigen bereichsspezifischen Regelungen sind die Voraussetzungen für eine rechtzeitige Verabschiedung wenigstens für einen Teil der wichtigsten Regelungen günstig.

1.1.2.1
Novellierung des HSOG

Bezeichnenderweise ist die Vorbereitungszeit für die Vorschriften zur polizeilichen Datenverarbeitung durch den Entwurf der Koalitionsfraktionen gezielt verkürzt worden. Der Landtag konnte so noch im Laufe des Jahres 1988 seine Beratungen aufnehmen und dürfte sie, wenn der vorgesehene Zeitplan eingehalten wird, im Frühsommer 1989 abschließen. Die verfassungsrechtlich tolerierbare Entscheidungsfrist wäre damit eingehalten. Aber auch inhaltlich spricht viel dafür, daß die Bedingungen für eine den vom Bundesverfassungsgericht formulierten und vom Hessischen Datenschutzgesetz aufgegriffenen sowie weiter präzisierten Anforderungen entsprechende Regelung gegeben sind. Die

drei mittlerweile dem Landtag vorliegenden Entwürfe bieten eine ausreichende Grundlage, um alle aus der Perspektive eines wirksamen Datenschutzes wichtigen Aspekte einzubeziehen. Sicher gibt es Punkte, die eingehend erörtert werden müssen (s. Ziff. 3.1). Mit der wichtigste ist die Frage, ob und unter welchen Umständen sich die polizeiliche Datenverarbeitung auf die Vorbeugung von Straftaten erstrecken darf. So unterschiedlich aber die Reaktionen darauf sind, so deutlich ist die Abkehr von jener ansonsten in der Diskussion immer wieder auftauchenden Vorstellung einer „Gefahrenvorsorge", die den Weg zu einer verfassungsrechtlich unzulässigen Verarbeitung auf Vorrat eröffnet. Zu den weiteren unter Datenschutzgesichtspunkten besonders wichtigen Problembereichen gehören die Erhebung personenbezogener Angaben im Zusammenhang mit öffentlichen Veranstaltungen und Versammlungen, die Identitätsfeststellung sowie die polizeiliche Beobachtung.

1.1.2.2
Novellierung des Hessischen Krankenhausgesetzes

Ein zweiter, in früheren Tätigkeitsberichten ebenfalls angemahnter Regelungskomplex von durchaus vergleichbarer Bedeutung ist die Verarbeitung personenbezogener Daten in Krankenhäusern (vgl. Ziff. 5.1). Die hohe Sensitivität von Patientendaten, der verstärkte Ausbau klinischer Register, das evidente verfassungsrechtliche Defizit der für den nichtöffentlichen Bereich geltenden Vorschriften des Bundesdatenschutzgesetzes sowie die Unübersichtlichkeit der gegenwärtig anwendbaren Vorschriften lassen keine weitere Verzögerung zu. Der Gesetzgeber hat allen Anlaß, Patienten den Schutz zu garantieren, den die Betroffenen in anderen, gerade aus ihrer Perspektive sehr viel weniger empfindlichen Bereichen genießen. Immerhin, die Vorarbeiten im Sozialministerium scheinen mittlerweile abgeschlossen zu sein. Insofern besteht die Chance einer Verabschiedung der gesetzlichen Regelung vor Ablauf der Legislaturperiode. Nur unter dieser Voraussetzung kann eine rechtswidrige und damit auch zu beanstandende Verarbeitung vermieden werden.

1.1.2.3
Datenschutz beim Umweltschutz

Trotzdem läßt sich nicht leugnen, daß es durchaus Bereiche gibt, in denen eine gesetzliche Regelung zwar dringend erforderlich ist, entsprechende Vorlagen aber noch fehlen. Zu erinnern ist beispielsweise an die im Zusammenhang mit der Verabschiedung des Datenschutzgesetzes formulierte Aufforderung des Landtags an die Landesregierung, die Voraussetzungen für eine Regelung der Verarbeitungsprobleme beim Umweltschutz zu schaffen (vgl. Landtags-Drucks. 11/6819, Ziff. A.3 i.V.m. Plenarprotokoll 11/94, S. 5496). Generalklauseln, wie sie vor allem die Erhebungsvorschrift des Hessischen Datenschutzgesetzes (§ 12) enthält, sind nur vor dem Hintergrund mangelnder bereichsspezifischer Bestimmungen auch und gerade bei der Inanspruchnahme personenbezogener Daten für Zwecke des Umweltschutzes erklärlich. Sie stellen deshalb nur einen kurzfristig hinnehmbaren Ausweg dar. Mit ihrer Verwendung hat sich, anders ausgedrückt, der Gesetzgeber zugleich verpflichtet, die mit ihnen einhergehende Unsicherheit bei der Gesetzesanwendung möglichst schnell zu beheben, und zwar mit Hilfe einer gezielten bereichsspezifischen Regelung just jener Problembereiche, die den Gesetzgeber seinerzeit dazu zwangen, sich mit ebenso allgemeinen wie unpräzisen Formulierungen abzufinden.

Ohne Zweifel läßt sich auf personenbezogene Angaben in einer Vielzahl von Fällen nicht verzichten, solange jedenfalls die Umweltschutzmaßnahmen nicht genauso abstrakte wie folgenlose Appelle bleiben sollen. Ebensowenig ist aber zu bestreiten, daß die Verarbeitung hier wie sonst an feste, vom Gesetzgeber definierte Regeln gebunden sein muß. Jede weitere Verzögerung belastet daher nicht nur den Umweltschutz mit durchaus lösbaren Problemen, sondern gefährdet auch die Glaubwürdigkeit des Datenschutzes, vor allem durch den konstanten Rückgriff auf Generalklauseln, die nach der Vorstellung des Gesetzgebers eben kein Ersatz für die verfassungsrechtlich notwendigen und daher unaufschiebbaren bereichsspezifischen gesetzlichen Regelungen sein dürfen.

1.1.2.4
Novellierung des Gesetzes über das Landesamt für Verfassungsschutz

Noch dringlicher sind freilich gesetzliche Bestimmungen zur Verarbeitung personenbezogener Daten durch das Landesamt für Verfassungsschutz. Ihre Notwendigkeit steht längst fest und ist auch vom Landtag wiederholt bekräftigt worden (vgl. 14. Tätigkeitsbericht, Ziff. 13.1.2). Die gesetzliche Regelung wurde dennoch immer wieder aufgeschoben, nicht zuletzt mit Rücksicht auf die nach wie vor ausstehende Entscheidung des Bundesgesetzgebers. Argumente für eine Abstimmung der bundes- und landesgesetzlichen Vorschriften lassen sich sicher anführen. Die Situation hat sich allerdings, seit diese Überlegung zum ersten Mal vorgebracht wurde, von Grund auf geändert. Was zur polizeilichen Datenverarbeitung gesagt wurde, gilt genauso für den Verfassungsschutz: Der Gesetzgeber ist nicht nur verpflichtet, die Verarbeitungsvoraussetzungen selbst festzulegen, er muß es auch innerhalb einer ganz bestimmten Frist tun. Eine Verarbeitung ohne eine verfassungskonforme gesetzliche Grundlage darf daher allenfalls zeitlich begrenzt in Kauf genommen werden, und zwar ohne Rücksicht auf eine noch so wünschenswert erscheinende Koordination mit dem Bundesgesetzgeber. Eine derartige Abstimmung mag für den Inhalt der Regelung von Bedeutung sein, sie rechtfertigt es jedoch nicht, eine rechtlich nicht haltbare Verarbeitung hinzunehmen. Der Landesgesetzgeber kann sich, anders ausgedrückt, nicht hinter den Bundesgesetzgeber zurückziehen, er muß vielmehr vor dem Ablauf der Frist selbst handeln und so für die Beendigung eines, um es noch einmal zu sagen, lediglich für eine kurze Zeit tolerablen Zustandes sorgen. Gerade der Verlauf der Vorarbeiten auf Bundesebene unterstreicht aber die Dringlichkeit einer Intervention des Landesgesetzgebers. Weder kann von einer unmittelbar bevorstehenden Verabschiedung eines Bundesverfassungsschutzgesetzes die Rede sein, noch genügen die bislang bekanntgewordenen Vorschläge den verfassungsrechtlichen

Anforderungen. Mehr denn je kommt es unter diesen Umständen darauf an, dem Landtag den Entwurf einer gesetzlichen Regelung noch 1989 zuzuleiten, wenn eine Überschreitung der hinnehmbaren Übergangsfrist und damit die Rechtswidrigkeit der Verarbeitung vermieden werden soll.

1.1.2.5
Novellierungsbedürftigkeit des HDSG – das Beispiel „wissenschaftliche Forschung"

So wichtig, ja unerläßlich die Vorbereitung und die Verabschiedung bereichsspezifischer Regelungen ist, so wenig darf darüber die Auseinandersetzung mit dem Datenschutzgesetz vernachlässigt werden, auch und gerade unter dem Blickwinkel seiner Revisionsbedürftigkeit. Sicherlich, eine zunächst befremdliche Feststellung: Schließlich sind seit der Novellierung des Gesetzes nur zwei Jahre vergangen. Zweierlei gilt es freilich nicht zu vergessen: Genauso wie seine beiden Vorgänger ist auch das Dritte Hessische Datenschutzgesetz vor dem Hintergrund eines bestimmten Entwicklungsstandes der Verarbeitungstechnik und den nicht zuletzt dadurch vorgezeichneten Verarbeitungsmodalitäten im Rahmen der öffentlichen Verwaltung entstanden. Der Gesetzgeber hat sich insofern für eine zwar notwendige, aber in weiten Teilen vorläufige Regelung entschieden. Sowohl die sich ständig weiter verfeinernde Verarbeitungstechnik als auch der sich kontinuierlich modifizierende Umgang der öffentlichen Stellen mit personenbezogenen Daten zwingen ihn daher, sich immer wieder von neuem die Frage zu stellen, ob die gesetzliche Regelung noch ihrer Aufgabe genügt, die informationelle Selbstbestimmung durch gezielte, verbindlich vorgeschriebene Verarbeitungsvorkehrungen sicherzustellen. Hinzu kommen die Folgen einer seinerzeit durchaus angestrebten und absehbaren, aber noch keineswegs realisierten, zunehmend bereichsspezifischen Verarbeitungsregelung. Je konkreter sich ihre Konturen abzeichnen, desto mehr engt sie den Anwendungsbereich des Datenschutzgesetzes ein und führt zwangsläufig dazu, seine Anwendungsvoraussetzungen im Hinblick auf die in den einzelnen Verarbeitungsbereichen gewonnenen Erfahrungen zu überprüfen.

So viel sollte aber damit deutlich sein: Gemeint sind keineswegs Korrekturen, wie sie etwa mittlerweile im Zusammenhang mit der Benachrichtigungspflicht nach § 18 Abs. 2 HDSG vorgenommen worden sind (vgl. Ziff. 15.2). Im Vordergrund standen dabei lediglich praktische Schwierigkeiten bei der Anwendung der Benachrichtigungspflicht auf „Alt-Dateien". Genaugenommen ging es also nur um eine bessere Übergangslösung, nicht jedoch um eine Revision der nach wie vor richtigen Entscheidung des Gesetzgebers für eine neue und bessere Form der Kommunikation mit den Betroffenen. Die Forderung nach einer konstanten Überprüfung der gesetzlichen Regelung auf ihre Vereinbarkeit mit ihren eigenen Zielen bezieht sich demgegenüber auf die Notwendigkeit, der Wirksamkeit des gesetzlich sanktionierten Verarbeitungskonzepts nachzugehen sowie die jeweils erforderlichen Änderungen vorzunehmen.

Einer der Bereiche, in denen sich Zweifel an der Möglichkeit abzeichnen, die Verarbeitungsprobleme mit Hilfe der im Datenschutzgesetz formulierten Verarbeitungsvoraussetzungen adäquat zu lösen, ist die Verwendung personenbezogener Angaben im Rahmen der wissenschaftlichen Forschung. Das Gesetz enthält zwar eine eigens auf die Forschung zugeschnittene Bestimmung, die inzwischen weit über Hessen hinaus breite Anerkennung gefunden hat. § 33 beschränkt sich allerdings auf einen ganz bestimmten Verarbeitungsaspekt: die Übermittlung. Der Grund läßt sich unschwer ausmachen. Für die wissenschaftliche Forschung kommt es entscheidend darauf an, den Zugang zu den jeweils benötigten Informationen sicherzustellen. Verständlicherweise sind deshalb Schwierigkeiten bislang zumeist im Zusammenhang mit der Weitergabe bereits durch einzelne öffentliche Stellen verarbeiteter Angaben entstanden. § 33 greift dabei die Regelung des alten Datenschutzgesetzes auf und versucht vor dem Hintergrund der Erfahrungen mit den verschiedensten Projekten die Übermittlungsvoraussetzungen in einer Weise zu revidieren, die, ohne die informationelle Selbstbestimmung der Betroffenen zu gefährden, den Datentransfer erleichtert.

Sobald es jedoch nicht um eine Übermittlung anderswo schon erhobener Daten, sondern um eine im Rahmen eines bestimmten Projekts vorzunehmende Erhebung geht, hilft das Gesetz nicht weiter. Sicher, an einer Regelung fehlt es nicht. Es bleibt beim allgemeinen, in § 12 Abs. 1 festgehaltenen Grundsatz: Die Daten sind beim Betroffenen mit seiner Kenntnis zu erheben. Ob es also zu einer Verarbeitung überhaupt kommen darf, richtet sich nach der Bereitschaft des Betroffenen, sich mit der Verwendung der Angaben zu seiner Person einverstanden zu erklären. Just die Gründe, die den Gesetzgeber bei der Übermittlung bewogen haben, unter bestimmten Bedingungen von einer Einwilligung abzusehen, lassen sich aber unter Umständen auch bei der Erhebung geltend machen. Nicht von ungefähr hat sich deshalb der nordrhein- westfälische Gesetzgeber zwar an der hessischen Regelung orientiert, im Unterschied jedoch zu § 33 sämtliche Verarbeitungsaspekte einbezogen (§ 28 Abs. 2 DSG NW), wenngleich nur im Hinblick auf die von „öffentlichen Stellen" durchgeführten Forschungsprojekte.

Kurzum, die gegenwärtige Regelung reicht nicht aus. So angebracht freilich eine Korrektur erscheint, sie läßt sich nicht über eine Interpretation der Vorschriften des Datenschutzgesetzes erreichen. Keine der in § 12 Abs. 3 aufgezählten Ausnahmen vom Einwilligungserfordernis kann herangezogen werden, ohne gegen das Gesetz zu verstoßen. Auch eine ergänzende, außerhalb des Datenschutzgesetzes angesiedelte Regelung hilft nicht weiter. Durchweg geht es um Verarbeitungsprobleme, die sich bei jeder wissenschaftlichen Untersuchung stellen können. Ganz zu Recht hat es deshalb der Gesetzgeber bei der Übermittlung abgelehnt, nur die universitäre oder die von „öffentlichen Stellen" betriebene Forschung anzusprechen. Art. 5 Grundgesetz verbietet derlei Differenzierungen und verpflichtet dazu, Lösungen zu suchen, die sich nicht lediglich an der oft zufälligen äußeren Organisationsform der Forschung orientieren. Insofern ist es etwa mit einer entsprechenden Ergänzung der Hochschulgesetzgebung nicht getan. Eine Alternative zu einer Korrektur des Datenschutzgesetzes mit dem Ziel, dies zu klären, ob und unter welchen Bedingungen die bisherige Regelung des § 33 auf sämtliche Verarbeitungsaspekte ausgedehnt werden kann, gibt es daher nicht.

1.1.3
Genomanalyse

Der wichtigste Ansatzpunkt für eine Weiterentwicklung der bisherigen Verarbeitungsvorkehrungen ist freilich nach wie vor die auf den technologischen Wandel zurückzuführende Veränderung des Verarbeitungsspektrums. Mit das aktuellste Beispiel dafür sind die bereits im 15. Tätigkeitsbericht (Ziff. 1.4.2) angesprochenen Auswirkungen der Gentechnologie. Eines hat sich seither mit Sicherheit geändert: An der Notwendigkeit, sich mit der Gentechnologie gerade unter Datenschutzaspekten auseinanderzusetzen, läßt sich nicht mehr zweifeln. Die dem Landtag vorliegende, von allen Fraktionen getragene Resolution zur Genomanalyse verlangt ausdrücklich eine strikte Beachtung des Datenschutzes (s. unten Ziff. 5.2.1). Dieser Erwartung läßt sich allerdings nur wirklich Rechnung tragen, wenn Möglichkeiten und Grenzen einer Verarbeitung der mit Hilfe von Genomanalysen gewonnenen Daten noch vor der Einführung derartiger Verfahren geklärt werden. Ganz gleich also, ob Patienten, Arbeitnehmer oder Tatverdächtige betroffen sind, die Entscheidung über die Zulässigkeit einer genetischen Untersuchung darf nur in Kenntnis der Konsequenzen einer Verwendung der Ergebnisse ergehen und muß daher auch eine Aussage zur Nutzung dieser Ergebnisse enthalten. Nur unter dieser Voraussetzung besteht immerhin die Chance, eine rechtliche Regelung zu formulieren, die nicht hoffnungslos hinterherhinkt, sondern rechtzeitig und präventiv eingreift, nur so kann es daher gelingen, die informationelle Selbstbestimmung in Anbetracht der gentechnologischen Entwicklung aufrechtzuerhalten.

Erwartung und Realität drohen jedoch mehr und mehr auseinanderzufallen, wie allein schon das Beispiel der „genetischen Fingerabdrücke" zeigt. Weder besteht Klarheit darüber, ob eine Genomanalyse zulässig ist, von wem sie gegebenenfalls durchgeführt werden darf und wie konkret mit den Ergebnissen umgegangen werden muß, noch gibt es eine einschlägige gesetzliche Regelung. Nicht einmal dort, wo es einen konkreten Anlaß durchaus gibt, etwa im Rahmen der Entwürfe zur Reform der Strafprozeßordnung oder der Polizeigesetze, liegen Vorschläge vor. Und doch wird die Genomanalyse offensichtlich wie selbstverständlich zum polizeilichen Instrumentarium gerechnet. Dafür sprechen nicht nur die intensiven organisatorischen Vorbereitungen, sondern auch und erst recht die Feststellung (unten Ziff. 5.2.2.3), genetische Analysen sollten in Zukunft grundsätzlich Vorrang haben vor den herkömmlichen Untersuchungsmethoden.

Sicher, manche der bislang bekanntgewordenen Fälle sind erst durch den ausdrücklichen Wunsch des Tatverdächtigen ausgelöst worden, sich einer Genomanalyse zu unterziehen. Ebensowenig läßt sich bestreiten, daß Verfahren, wie sie bislang angewandt worden sind, lediglich auf eine Identitätsfeststellung abzielen. Trotzdem geht es nicht an, im „genetischen Fingerabdruck" nur eine andere, gleichsam modernere Form des Fingerabdrucks zu sehen, die dann konsequenterweise durchaus nach den ansonsten ebenfalls zu beachtenden Vorschriften behandelt werden kann. Der Schluß von einem bestimmten Testverfahren auf die Genomanalysen überhaupt ist zu vorschnell. Nicht von ungefähr hat die Enquete- Kommission des Deutschen Bundestages zu den Chancen und Risiken der Gentechnologie auf die mit einer solchen Analyse möglicherweise verbundenen „Überschußinformationen" hingewiesen, die nicht zuletzt Aussagen zur Persönlichkeit des Betroffenen erlauben könnten. Um genau diese Möglichkeit geht es aber in erster Linie: Sie verdeutlicht den qualitativen Unterschied zwischen der Genomanalyse und allen anderen bisher praktizierten Untersuchungsmethoden und läßt die Gefahren unschwer erkennen, denen der Betroffene bei einer Verwendung der Ergebnisse ausgesetzt ist. Just diesen Unterschied gilt es zunächst aufzugreifen, um dann auf die Folgen durch präzise gesetzliche Regelungen etwa im strafprozessualen oder im polizeilichen Bereich zu reagieren. Die Diskussion über die polizeiliche Datenverarbeitung bietet die Gelegenheit dazu. Der Gesetzgeber sollte sie nutzen und damit zugleich die vom Landtag zur Gentechnologie getroffenen Feststellungen in rechtlich verbindliche Handlungsanleitungen von unmittelbarer praktischer Bedeutung umsetzen.

1.1.4
Datenschutz und presserechtlicher Auskunftsanspruch

Zuweilen geht es freilich um Probleme, die den Datenschutz gleichsam von Anfang an begleitet haben. Die jüngst wieder aufgeworfene Frage nach dem Verhältnis der Datenschutzgesetzgebung zum Presserecht ist beispielhaft dafür. Ausgelöst wurde die vor allem im Innenausssschuß des Landtags geführte Diskussion durch den Aids-Test einer afrikanischen Asylbewerberin und die darauf folgende Information der Presse durch die Behörden (unten Ziff. 5.4.2.2.1).

So viel dürfte wohl unstreitig sein: Jede Mitteilung personenbezogener Daten an Außenstehende ist eine Übermittlung im Sinne des Datenschutzgesetzes und unterliegt deshalb den strengen, dort näher präzisierten Bedingungen (§ 14 ff.). Das Hessische Pressegesetz räumt allerdings der Presse ausdrücklich ein Auskunftsrecht ein (§ 3 Abs. 1) und nennt zugleich die Fälle, in denen Behörden die Auskunft verweigern dürfen. Danach können etwa Auskünfte über persönliche Angelegenheiten dann unterbleiben, wenn kein berechtigtes Interesse an einer öffentlichen Bekanntgabe besteht. Kurzum, den auf eine Minimierung der Verbreitung personenbezogener Informationen bedachten Bestimmungen des Datenschutzgesetzes steht der auf eine möglichst weitgehende Offenlegung und deshalb nur wenige, teilweise recht unscharf formulierte Ausnahmen zulassende presserechtliche Auskunftsanspruch gegenüber.

Der Gesetzgeber war sich des möglichen Konflikts durchaus bewußt. Konsequenterweise war deshalb im Rahmen der Beratungen über die Novellierung des Datenschutzgesetzes im Zusammenhang mit den Vorschriften zur Verarbeitung personenbezogener Daten durch den Hessischen Rundfunk auch die Frage eingehend erörtert worden, inwieweit Sonderbestimmungen zur Verwendung personenbezogener Informationen durch die Presse in das neue Gesetz

aufgenommen werden sollten. Sehr bald setzte sich aber die Meinung durch, daß das Datenschutzgesetz der falsche Ort dafür wäre. Legislativer Ansatzpunkt könne und dürfe, so die einhellige Ansicht, nur das Pressegesetz sein. Ob eine Regelung erforderlich ist und wie sie im einzelnen aussehen müßte, läßt sich in der Tat nur in Kenntnis der spezifischen verfassungsrechtlichen Voraussetzungen journalistischer Arbeit sowie der konkreten Bedingungen, unter denen sie sich vollzieht, korrekt beurteilen. Aus genau diesem Grund hatte seinerzeit der Bundesgesetzgeber und hatten ihm folgend die Landesgesetzgeber sich in den allgemeinen Datenschutzgesetzen auf eine Vorschrift beschränkt, die den journalistischen Bereich gezielt ausklammert und lediglich die administrativ-organisatorische Verwendung personenbezogener Daten einbezieht (§ 1 Abs. 3 BDSG).

Die Entstehungsgeschichte der Novellierung gibt mithin deutlich zu erkennen: Aus der Sicht des Gesetzgebers kommt lediglich eine strikt bereichsspezifische, im Pressegesetz angesiedelte Regelung in Betracht. Wohlgemerkt, der Gesetzgeber hat keineswegs in den gegenwärtig geltenden presserechtlichen Vorschriften die von ihm in Erwägung gezogene bereichsspezifische Regelung gesehen, sondern neue, das geltende Recht korrigierende und ergänzende Vorschriften gemeint. Nur solche Bestimmungen können in der Tat in Kenntnis der besonderen, unter anderem im Datenschutzgesetz festgehaltenen Anforderungen des Datenschutzes konzipiert und deshalb als eine gezielt bereichsspezifische Reaktion des Gesetzgebers ausgegeben werden.

Genau dies gilt es auch und gerade bei der Interpretation des § 3 Abs. 1 Hessisches Pressegesetz zu beachten. Anders ausgedrückt: Weil es sich um eine Vorschrift handelt, die ohne Rücksicht auf die speziellen, in den Datenschutzgesetzen angesprochenen Gefahren der Verarbeitung personenbezogener Daten und die damit verbundene Forderung nach einer Gewährleistung der informationellen Selbstbestimmung entstanden ist, läßt sie sich zwar als Spezialvorschrift qualifizieren, nicht jedoch, und ausschließlich darauf kommt es an, als bereichsspezifische Regelung im Sinne eines konsequent durchgeführten, den verfassungsrechtlichen Anforderungen entsprechenden Datenschutzes. § 3 Abs. 1 Pressegesetz rechtfertigt es also nicht, sich über die Übermittlungsvorschriften des Datenschutzgesetzes hinwegzusetzen. Der Auskunftsanspruch muß im Gegenteil vor dem Hintergrund dieser Bestimmungen gesehen und unter Berücksichtigung der von ihnen aufgestellten Bedingungen beurteilt werden. Jede andere Interpretation muß zwangsläufig dazu führen, eine Weitergabe personenbezogener Daten verbunden mit einer Veröffentlichung selbst dort zu akzeptieren, wo sich der Gesetzgeber unmißverständlich für eine ausschließlich auf eine bestimmte verarbeitende Stelle beschränkte Verwendung ausgesprochen hat. Der Gesetzgeber würde, so gesehen, dem Betroffenen zwar versichern, nur eine wirklich eng begrenzte Verarbeitung seiner Daten zu tolerieren, zugleich aber die schärfste mögliche Form einer Verbreitung, die Veröffentlichung, in Kauf nehmen. Daran ändern auch die in § 3 Abs. 1 vorgesehenen Ausnahmen nichts. Allein schon die überaus abstrakte Formulierung und der damit einhergehende weite Interpretationsspielraum genügen, um die Notwendigkeit einer Berücksichtigung der Verarbeitungsanforderungen des Datenschutzgesetzes zu unterstreichen.

Der Gesetzgeber muß sich unter diesen Umständen zunächst fragen, unter welchen Voraussetzungen eine Übermittlung personenbezogener Angaben in Anbetracht der eindeutig restriktiven Haltung der Datenschutzgesetze in Betracht kommt. Eine pauschale Antwort kann es darauf nicht geben. Vielmehr gilt es, die einzelnen an sehr verschiedenen Stellen angesiedelten Übermittlungsverbote genau zu betrachten, den je spezifischen Regelungszweck also ebenso zu berücksichtigen, wie etwa den jeweiligen Verarbeitungskontext oder die Art der zur Debatte stehenden Daten. Kurzum, Regelungen, wie sie beispielsweise im Sozialgesetzbuch enthalten sind, legen eine sorgfältige Differenzierung nahe. Nicht von ungefähr hat sich der Gesetzgeber in § 35 SGB I für eine strikte Geheimhaltung entschieden und in § 69 Abs. 1 Nr. 3 SGB X lediglich unter eng begrenzten Voraussetzungen eine öffentliche Bekanntgabe von Sozialdaten (öffentliche Richtigstellung) erlaubt. Der Datenschutz, genauer noch, die im Interesse der informationellen Selbstbestimmung unerläßliche Zweckbindung der Verarbeitung verbieten es, bei den bislang üblichen Generalklauseln zu verharren und gebieten es, sich für eine möglichst exakte, den unterschiedlichen Verarbeitungszusammenhängen Rechnung tragende Regelung zu entscheiden.

Davon zu trennen ist die weitere, sehr viel kompliziertere Frage, die auch im Zusammenhang mit dem Staatsvertrag über den Bildschirmtext eine wichtige Rolle gespielt hat, inwieweit es zusätzlicher, die Verarbeitung im journalistischen Bereich betreffender gesetzlicher Vorkehrungen bedarf. Das Datenschutzgesetz enthält immerhin eine in diese Richtung weisende, allerdings auf den Hessischen Rundfunk beschränkte Regelung. § 37 Abs. 1 HDSG ergänzt das traditionelle Gegendarstellungsrecht um die Verpflichtung des Rundfunks, die Äußerung der Betroffenen zu den gespeicherten Daten zu nehmen und sie zudem so lange wie die Angaben selbst aufzubewahren. Das Gesetz greift damit einen bereits im Zusammenhang mit der Novellierung des Bundesdatenschutzgesetzes geäußerten Vorschlag auf. Bezeichnenderweise hat es aber davon abgesehen, einer Reihe weiterer Anregungen zu folgen, darunter die Anregung, dem Betroffenen ein Auskunftsrecht noch vor der Publikation der sich auf ihn beziehenden Informationen einzuräumen. Der Grund liegt auf der Hand: So sehr es darauf ankommt, Mittel und Wege zu finden, die der informationellen Selbstbestimmung Rechnung tragen, so wenig darf dabei der Datenschutz zum Vehikel einer verfassungsrechtlich unzulässigen Zensur werden. Wiederum erweist sich aber, wie wichtig es, bei aller Notwendigkeit, Datenschutzvorkehrungen zu formulieren, ist, die in Betracht kommenden Regelungen durchweg in Kenntnis der Eigenart und der Bedeutung journalistischer Arbeit zu entwickeln.

1.2
Datenschutz im nicht-öffentlichen Bereich

Der hessische Gesetzgeber hat als erster den für die Verarbeitung personenbezogener Daten im nicht-öffentlichen Bereich zuständigen Aufsichtsbehörden vorgeschrieben, einen Bericht über ihre Tätigkeit vorzulegen (§ 30 Abs. 2 Satz 2 HDSG). Wie richtig und wichtig diese Entscheidung war, zeigt der jetzt vorliegende erste Bericht (Drucks. 12/3069). Er

korrigiert zunächst den falschen Eindruck, den die bisherige gesetzliche Regelung durch die ausschließlich dem öffentlichen Bereich vorbehaltene Berichtspflicht förmlich provoziert hat: Datenschutzprobleme entstehen keineswegs nur dort, wo die Polizei, die Sozialbehörden oder die kommunalen Dienststellen personenbezogene Angaben verarbeiten. Die informationelle Selbstbestimmung steht mindestens genauso auf dem Spiel, wenn Auskunfteien, Kreditschutzorganisationen oder Adressenvermittler, um nur einige der im Bericht genannten Beispiele zu nennen, auf personenbezogene Angaben zurückgreifen. Eine Diskussion über die im Interesse eines wirksamen Datenschutzes erforderlichen Vorkehrungen muß deshalb immer und zugleich eine Auseinandersetzung mit den Verarbeitungsproblemen im nicht- öffentlichen Bereich sein. Wo dieser Bereich ausgespart oder nur nebenbei zur Kenntnis genommen wird, kann daher von einer verfassungskonformen, die informationelle Selbstbestimmung konsequent gewährleistenden Datenschutzregelung keine Rede mehr sein.

Der Bericht unterstreicht, zweitens, die Parallelität der Probleme. Sowohl bei Patientendaten als auch bei Arbeitnehmerdaten oder bei der Registrierung von Angaben zu Telefongesprächen, um es wiederum bei einigen wenigen Beispielen zu belassen, stellen sich im Prinzip genau die Fragen, die auch bei einer Verarbeitung durch öffentliche Stellen beachtet werden müssen und die deshalb nicht nur von den Tätigkeitsberichten der vergangenen Jahre, sondern genauso im Rahmen der Beratungen über das Datenschutzgesetz sowie der Vorbereitung bestimmter bereichsspezifischer Regelungen aufgegriffen worden sind. Daran erweist sich aber auch, wie sehr es darauf ankommt, die jeweils in Betracht zu ziehenden Datenschutzmaßnahmen aufeinander abzustimmen. Dies um so mehr, als es Bereiche gibt, für die, wie etwa für die privatrechtlich organisierten Kreditinstitute einerseits und die Sparkassen andererseits, eine geteilte Überwachungszuständigkeit besteht. Genauso wichtig erscheint eine Abstimmung schließlich in den Fällen, in denen sich die Kompetenzen überlappen, weil beispielsweise bestimmte Angaben aus dem öffentlichen Bereich an den nicht-öffentlichen übermittelt werden, mit der Folge, daß dem Hessischen Datenschutzbeauftragten die Aufgabe zufällt, die Zulässigkeit der Übermittlung zu bewerten, während es der Aufsichtsbehörde obliegt, die Rechtmäßigkeit der Speicherung zu kontrollieren. Ein Vergleich der beiderseitigen Erfahrungen und Reaktionen zeigt schnell: Gravierende Divergenzen hat es erfreulicherweise nicht gegeben. Zu den eher sekundären Punkten, bei denen die Meinungen wohl auseinandergehen, zählen die Anforderungen an die Fernwartung (Ziff. 8.4 des Berichts der Landesregierung). Sie müßten meiner Überzeugung nach schärfer gefaßt werden.

Der Bericht bestätigt, drittens, die seit Jahren vorgebrachte Kritik an den mangelnden rechtlichen Möglichkeiten der Aufsichtsbehörden, die Konsequenzen aus ihrer Kontrolle zu ziehen. Kein Betroffener kann beispielsweise verstehen, wieso eine datenverarbeitende Stelle eindeutig rechtswidrige Speicherungen trotz aller Vorhaltungen der Aufsichtsbehörde aufrechtzuerhalten vermag (vgl. etwa a.a.O. Ziff. 7.1.1). Genauso wenig ist einzusehen, warum die Aufsichtsbehörde selbst dann die Beschwerde eines Betroffenen abwarten muß, um zu kontrollieren, wenn die Medien ausführlich über mögliche Verstöße gegen den Datenschutz berichtet haben (Ziff. 3.2).

Der Bericht gibt, viertens, klar zu erkennen, wie dringend erforderlich eine Korrektur des Bundesdatenschutzgesetzes ist, aber auch wie wenig die bislang vorgeschlagenen Korrekturen die bei der Kontrolle der Verarbeitung personenbezogener Daten im nicht-öffentlichen Bereich sichtbar gewordenen Mängel zu beseitigen vermögen. So muß die immer noch, wenn auch eingeschränkt beibehaltene Anlaßaufsicht bei einer Verarbeitung, die lediglich eigenen Zwecken dient, endgültig aufgegeben werden. Nur wenn die Aufsichtsbehörde von sich aus entscheiden kann, ob, wann, in welchem Umfang und mit welchen Zielen kontrolliert werden soll, besteht die Chance, einen verläßlichen Überblick über die Einhaltung der gesetzlichen Verarbeitungsanforderungen zu gewinnen, und damit auch für die konkret notwendigen Veränderungen zu sorgen. So darf es nicht bei einer Verknüpfung der Anwendung der Datenschutzvorschriften mit einer Verarbeitung personenbezogener Angaben in Dateien bleiben. Der Bericht illustriert, wie anachronistisch und sinnwidrig die Konsequenzen eines solchen „Zwei-Klassen-Datenschutzes" sind (Ziff. 7.1). So gilt es schließlich, wie sich vor allem am Beispiel der durch die Auskunfteien durchgeführten Befragungen erweist, die Erhebung personenbezogener Daten in die gesetzliche Regelung einzubeziehen.

Der Bericht verdeutlicht, fünftens, wie sehr es an der Zeit ist, der im öffentlichen Bereich mittlerweile von niemandem mehr bestrittenen Notwendigkeit einer differenzierten Verarbeitungsregelung auch im nicht-öffentlichen Bereich Rechnung zu tragen, den Schwerpunkt also mehr und mehr von den allgemeinen Datenschutzvorschriften auf gesetzlich verankerte bereichsspezifische Bestimmungen zu verschieben. Vor allem die Beispiele aus der Verarbeitungspraxis der Banken, Kreditkartenunternehmen und Kreditschutzorganisationen demonstrieren nicht nur, wie verfehlt die hartnäckig wiederholten Behauptungen über die Unanwendbarkeit zentraler, vom Bundesverfassungsgericht eindringlich betonter Datenschutzgrundsätze, wie etwa der Zweckbindung, im nicht- öffentlichen Bereich sind, sondern auch und gerade die Unmöglichkeit, wirklich wirksame Verarbeitungsvorkehrungen zu formulieren, ohne sich am je spezifischen Verarbeitungskontext zu orientieren. Ganz gleich, ob man die Erhebungsmodalitäten, die Art und den Umfang der konkret verarbeiteten Angaben, die Verarbeitungstechnik oder den Informationsaustausch nimmt, überall sind die Besonderheiten dermaßen evident, daß es wohl kaum einen anderen Bereich gibt, sieht man einmal von der Verarbeitung von Arbeitnehmerdaten ab, bei dem sich die Entscheidung für eine eindeutig bereichsspezifische Regelung so nachhaltig aufdrängt.

1.3
Datenaustausch mit dem Ausland

Zu den wichtigsten Faktoren für die weitere Entwicklung des Datenschutzes zählt der grenzüberschreitende Austausch personenbezogener Daten. Darauf haben schon die früheren Tätigkeitsberichte hingewiesen. Was freilich bislang als eine typische Begleiterscheinung privater unternehmerischer Tätigkeit angesehen wurde, gewinnt aus einem durchaus

naheliegenden Grund auch im öffentlichen Bereich zunehmend an Bedeutung. Je mehr die Grenzkontrollen entfallen, desto nachdrücklicher richtet sich die Aufmerksamkeit auf eine kontinuierliche gegenseitige Information. Vor diesem Hintergrund ist beispielsweise 1986 das „Schengener Übereinkommen" entstanden (GMbl. 1986, 79). Die Bundesrepublik, die Benelux-Staaten und Frankreich verpflichten sich darin nicht nur zu einem „schrittweisen Abbau der Kontrollen an den gemeinsamen Grenzen", sondern auch zu einer verstärkten Zusammenarbeit der Zoll- und Polizeibehörden, auch und gerade mit Hilfe einer Übermittlung der Informationen, die „im Kampf gegen die Kriminalität von Interesse sein könnten" (Art. 9). Konsequenterweise sieht Art. 18 die Ausarbeitung von Vereinbarungen zur Kooperation bei der „präventiven Verbrechensbekämpfung und der Fahndung" vor.

In der Bundesrepublik ist seither wenig über die weiteren Schritte zur Verwirklichung dieser Abmachung bekannt geworden, sieht man einmal von einigen sehr allgemein gehaltenen Erklärungen über die Zweckmäßigkeit einer internationalen Zusammenarbeit ab. Auch wiederholte Anfragen zum Stand der Kooperation haben nicht mehr erbracht als vage Hinweise auf erste, noch überaus generelle Überlegungen. Weitaus konkreter gestalten sich dagegen die Informationen in den anderen Vertragsstaaten, vor allem in Belgien. Danach ist inzwischen etwa die Einrichtung einer internationalen Datenbank beschlossen worden. Sie soll ihren Sitz in Belgien haben und bereits 1989 mit einer ersten „probeweisen" Verarbeitung polizeilicher Daten beginnen.

Daran ist mindestens zweierlei bemerkenswert. Zunächst: Das „Schengener Übereinkommen" stellt den internationalen Datenaustausch ausdrücklich unter den Vorbehalt des „jeweiligen innerstaatlichen Rechts" (Art. 9 Abs. 1 Satz 2). Dazu zählen, zumindest in der Bundesrepublik, mit Sicherheit die Datenschutzgesetze. Bei Übermittlungen personenbezogener Daten gilt jedenfalls nach dem Hessischen Datenschutzgesetz (§ 17), daß sie grundsätzlich nur zulässig sind, wenn im Empfängerstaat gleichwertige Datenschutzregelungen gelten. Belgien zählt aber zu den Ländern, die kein Datenschutzgesetz haben. Alle Bemühungen, etwa vor dem Hintergrund der Datenschutz-Konvention des Europarates die Verarbeitung personenbezogener Daten gesetzlich zu regeln, haben dort bisher zu keinem Ergebnis geführt. Um so erstaunlicher ist es deshalb, sollte die Information zutreffen, daß sich Vertragsstaaten wie die Bundesrepublik und Frankreich, die schon lange über entsprechende Regelungen verfügen, mit der Verarbeitung in einem der Vertragsstaaten einverstanden erklären, die keine Gewähr für einen gesetzlich abgesicherten Verarbeitungsverlauf bieten können.

Genauso bedenklich ist, die Richtigkeit der Informationen wiederum vorausgesetzt, die Vorgehensweise. Weder die Zulässigkeit der Übermittlungen noch die unter Datenschutzgesichtspunkten wichtigen Verarbeitungsdetails dürfen während des „Probebetriebes" oder gar nach seinem Abschluß geprüft werden. Auch eine „probeweise" Weitergabe personenbezogener Daten ist eine Übermittlung im Sinne der gesetzlichen Regelung. Kein Gesetz erteilt, anders ausgedrückt, einen Dispens vom Datenschutz für „Probeläufe". Konsequenterweise darf es keine Übermittlung geben, solange ihre Zulässigkeit nicht einwandfrei feststeht. Und ebensowenig geht es an, Daten weiterzugeben, wenn die einzelnen Verarbeitungsbedingungen nicht genau geklärt sind. Gemeint sind damit keineswegs nur die Anforderungen an den Verarbeitungsverlauf, sondern genauso die Kontrollvoraussetzungen. Die Erfahrung zeigt nur zu gut, daß jede Internationalisierung der Verarbeitung, jedenfalls im öffentlichen Bereich, Bestrebungen nach sich zieht, die bestehenden Kontrollmechanismen auszuschalten. Für die Bundesrepublik kann es jedoch keinen „gleichwertigen" Datenschutz ohne die Garantie einer wirklich unabhängigen Kontrolle geben.

Spätestens bei den Überlegungen zu den Verarbeitungsvoraussetzungen macht sich freilich einmal mehr jener Mangel bemerkbar, der zunehmend alle Bemühungen um eine Internationalisierung des Datenschutzes gerade im Rahmen der Europäischen Gemeinschaft belastet: die tiefe Diskrepanz zwischen den Reaktionen auf die Verarbeitung personenbezogener Daten. Nach wie vor haben vier der zwölf Mitgliedsländer (Belgien, Italien, Spanien und Portugal) keine gesetzliche Regelung. In weiteren zwei (Griechenland und den Niederlanden) verzögert sich die Verabschiedung der einschlägigen Gesetze immer wieder. Aber auch dort, wo, wie in den sechs übrigen Mitgliedsstaaten, der Gesetzgeber bereits eingegriffen hat, sind die Unterschiede beträchtlich, wie schon allein ein Vergleich zwischen der dänischen und der irischen oder der französischen und der britischen Regelung zeigt. Wie schwer die Diskrepanz wiegt, wird erst richtig deutlich, wenn man die sich ansonsten intensivierenden Bestrebungen um eine Vereinheitlichung bedenkt. Je weiter sie fortschreitet, desto weniger läßt sich ein Austausch personenbezogener Daten vermeiden. Solange es jedoch an gemeinsamen, den Datenschutz wirklich gewährleistenden Vorkehrungen fehlt, ist der Konflikt unausweichlich. Für die Bundesrepublik steht jedenfalls fest: Der Datenschutz ist untrennbar mit den in der Verfassung festgeschriebenen Grundsätzen rechtlicher Ordnung verbunden. Eine Angleichung, die sich am geringsten gemeinsamen Nenner orientiert, kann es deshalb nicht geben. Um so wichtiger ist es, so schnell wie möglich Konsens über die Verarbeitungskriterien zu erzielen.

1.4
Behinderungen bei Datenschutzkontrollen

Die Wirksamkeit des Datenschutzes hängt entscheidend davon ab, inwieweit die öffentlichen Stellen, die personenbezogene Angaben verarbeiten, mit dem Hessischen Datenschutzbeauftragten kooperieren. Nur soweit Kooperationsbereitschaft wirklich besteht, läßt sich sowohl eine den gesetzlichen Erwartungen entsprechende Verarbeitungskontrolle durchführen, als auch und vor allem im Vorfeld der Verarbeitung eine Verständigung über ihren Verlauf erzielen. Beides hat sich im vergangenen Jahr einmal mehr bestätigt. Beispielhaft dafür sind die Reaktionen auf die im Zusammenhang mit einer Prüfung der Aufbewahrungsfristen vorgenommene Kontrolle von Polizeidienststellen oder die weitaus umfassendere Überprüfung der Landwirtschaftsämter. Gemeinsam wurden die Verarbeitungsdefizite festgestellt, gemeinsam aber auch über die notwendigen Korrekturen beraten. Gewiß, Meinungsverschiedenheiten hat es im einen

oder anderen Fall durchaus gegeben und nicht immer haben sich die Vorschläge des Datenschutzbeauftragten in allen Einzelheiten durchgesetzt. Durchweg ist es aber gelungen, Lösungen zu finden, die eine datenschutzkonforme Verarbeitung gewährleisten.

Es gibt aber Fälle, wenngleich eher selten, in denen sich öffentliche Stellen der Kontrolle zu entziehen suchen. Das Jugendamt der Stadt Frankfurt ist eines der Beispiele dafür (vgl. Ziff. 6.3). Weder eine generelle Überprüfung noch eine Einzelfallkontrolle lassen sich ohne Einsicht in die jeweils einschlägigen Jugendakten durchführen. Konsequenterweise sind bei Prüfungen von Jugendämtern bisher stets auch die Akten herangezogen worden, fast durchweg ohne jede Schwierigkeit. Wo aber Probleme aufgetaucht sind, konnten sie sehr schnell gelöst werden. Anders in Frankfurt: Das Jugendamt hat, trotz wiederholter Aufforderung und entgegen der im Sozialgesetzbuch eindeutig bestätigten Prüfungskompetenz des Datenschutzbeauftragten (§ 79 Abs. 3 SGB X), zunächst die Akteneinsicht verweigert und später für sich in Anspruch genommen, selbst darüber zu bestimmen, ob jeweils eine Einsicht erforderlich ist. Eine Kontrolle, bei der es dem Kontrollierten überlassen bleibt, festzulegen, wie die Überprüfung abzulaufen hat, verfehlt ihren Sinn und verstößt gegen die gesetzliche Regelung. Es ist deshalb ausschließlich Sache des Hessischen Datenschutzbeauftragten, die Kontrollbedingungen näher zu umschreiben und in diesem Zusammenhang auch festzustellen, ob und in welchem Umfang Akten konsultiert werden müssen. Reaktionen wie die des Jugendamts der Stadt Frankfurt stellen daher den gesetzlich geforderten Datenschutz unmittelbar in Frage. Die inzwischen begonnenen Gespräche mit den verantwortlichen Magistratsmitgliedern der Stadt Frankfurt werden hoffentlich dazu führen, die Kontrollpraxis beim Jugendamt den ansonsten üblichen und ohne weiteres akzeptierten Überprüfungen anzugleichen.

1.5
Revision der Informationsstrukturen

Ein konsequent praktizierter Datenschutz zwingt dazu, manche bislang für selbstverständlich gehaltene Informationserwartung zu überprüfen oder gar preiszugeben. Beispiele dafür enthält fast jeder Tätigkeitsbericht. Auch im diesjährigen Bericht finden sich zwei für die Notwendigkeit einer Veränderung der Informationsstrukturen besonders typische Fälle. Einer davon sind die von zahlreichen Kommunen bei der Bearbeitung von Anträgen auf Sozialleistungen verwendeten Formulare (vgl. Ziff. 6.4). Zweierlei läßt sich sicherlich nicht vermeiden. Wer Sozialleistungen beansprucht, muß auch bereit sein, die für eine korrekte Beurteilung seines Antrags erforderlichen Daten offenzulegen. Der Umfang der Leistungen sowie die Zahl der Anträge formalisieren und typisieren zudem zwangsläufig das Antragsverfahren. Verständlicherweise sieht deshalb das Sozialgesetzbuch eine Mitwirkungspflicht des Antragstellers vor. Ebensowenig überrascht die schematische Zusammenfassung der Fragen in eigens dafür ausgearbeiteten Formularen. An genau diesem Punkt machen sich freilich immer wieder Schwierigkeiten bemerkbar. Der Grund: Die Mitwirkungspflicht wird leicht zum Anlaß genommen, um die Grenze der wirklich notwendigen und deshalb allein gerechtfertigten Informationen zu überschreiten. Je mehr Angaben erhoben werden, desto besser kann es, so heißt es immer wieder, gelingen, nicht nur den Antrag möglichst genau zu bearbeiten, sondern auch denkbaren Mißbräuchen vorzubeugen. Die Aufforderung, sich pauschal mit der Erteilung von Auskünften durch den jeweils behandelnden Arzt oder der Bank, bei der ein Konto unterhalten wird, einverstanden zu erklären, erscheint dann mehr oder minder selbstverständlich.

Verkannt wird dabei nicht nur die besondere Lage des Betroffenen, die eine Einwilligung weitgehend zur Fiktion werden läßt. Unbeachtet bleibt vielmehr vor allem die gesetzliche Verpflichtung der die Angaben erhebenden Stelle, ihre Informationserwartungen so gering wie nur möglich zu halten und dabei ausschließlich die für den konkreten Verarbeitungszweck benötigten Angaben zu verlangen. Eben deshalb mußten die pauschalen „Einwilligungen" beanstandet werden und aus genau dem gleichen Grund gilt es jetzt sicherzustellen, daß nur Formulare, die diesen Anforderungen genügen, verwendet werden. Um kein Mißverständnis aufkommen zu lassen: Pauschale Einverständniserklärungen dürfen nicht etwa noch so lange abverlangt werden, bis der Vorrat an den bisher benutzten Formularen erschöpft ist. Die Aufforderung, derartige Erklärungen abzugeben, war von Anfang an unzulässig. Sie darf daher nicht wiederholt werden, ganz gleich, ob mit Hilfe alter oder neuer Formulare.

Das zweite Beispiel sind die von der Polizei bei der Personenbeschreibung benutzten Merkmale (vgl. Ziff. 3.3). Wiederum kann es keinen Zweifel geben, daß es sich dabei im Prinzip durchaus um Angaben handelt, die für die Erfüllung der polizeilichen Aufgaben erforderlich sind. Und einmal mehr ist nicht in Abrede zu stellen, daß Umfang und Art der konkret in Betracht kommenden Aufgabe zu einer Typisierung der verarbeiteten Daten zwingen. So wenig freilich die Notwendigkeit möglichst schematisierter Merkmale bestritten werden kann, so sehr gilt es dabei, zum einen bei jeder einzelnen Angabe zu fragen, ob sie tatsächlich benötigt wird, und zum anderen stets die Konsequenzen einer automatisierten Verarbeitung typisierter Angaben für den Betroffenen zu bedenken. Konkret: Automatisierte Informationssysteme bergen hier wie sonst mindestens zwei Gefahren in sich: Eine kaum zu kontrollierende Ausweitung der Zugriffsmöglichkeiten und eine vorschnelle Etikettierung der Betroffenen. Beide Gefahren zeichnen sich bei der Personenbeschreibung, so wie sie gegenwärtig praktiziert wird, deutlich ab. Das System ist auf den Zugriff aller hessischen Polizeidienststellen hin konzipiert, gibt also jeder von ihnen die Möglichkeit, die gesamte Beschreibung zur Kenntnis zu nehmen. Je mehr Hinweise aber aufgenommen werden, die etwa in den Grenzbereich zwischen körperlichen und psychischen Merkmalen fallen, oder je unpräziser die Beschreibungen geraten, desto problematischer erweist sich der Verbreitungsgrad. In dem Maße zudem, in dem die ohnehin recht zahlreichen Merkmale durch Freitextfelder ergänzt werden, wächst die Gefahr einer kaum noch korrigierbaren Etikettierung. Mag sein, daß die meisten Merkmale eine lang geübte Praxis widerspiegeln. Die Konsequenzen einer Automatisierung dürfen jedoch in keinem Fall übergangen werden. Vor ihrem Hintergrund und unter ständiger Berücksichtigung der verfassungsrecht-

lich begründeten, im Datenschutzgesetz ausdrücklich bestätigten Verpflichtung, nur Daten aufzunehmen, die ebenso erforderlich wie genau sind, gilt es, die bisher verwendeten Merkmale von Grund auf zu überprüfen.

1.6
Datenschutztechnologie

Die gestiegene Leistungsfähigkeit der Prozessoren sowie die steigende Speicherkapazität peripherer Direktzugriffsspeicher verändern erneut die Verarbeitungsbedingungen. Schon ist von „Arbeitsplatzcomputern" die Rede, die zunehmend die bisherige individuelle Datenverarbeitung mit Hilfe der „persönlichen Computer" verdrängen. Ebenso klar zeichnet sich bei den mittlerweile verwendeten Betriebssystemen neben der sukzessiven auch eine gleichzeitige Nutzung durch mehrere Benutzer ab. Der Schlüssel für die Zukunft des Datenschutzes liegt mehr denn je in der Entwicklung einer besonderen Datenschutztechnologie. Normative Anforderungen mögen zwar nach wie vor unentbehrlich sein, um den verfassungsrechtlich zulässigen Rahmen einer Verarbeitung personenbezogener Daten zu bestimmen. Ob und in welchem Umfang sich allerdings die Verarbeitung in diesen Rahmen einfügen läßt, hängt in zunehmendem Maße von einer Integration der Datenschutzvorkehrungen in die Verarbeitungstechnologie selbst ab. Software allein kommt dafür ebenso in Betracht wie eine Kombination von Soft- und Hardware. Der 15. Tätigkeitsbericht (Ziff. 9) war darauf schon ausführlich eingegangen, der 17. greift die dort angestellten Überlegungen auf, zeichnet die seither eingetretenen Entwicklungen nach und setzt sich mit den sich neu bietenden Möglichkeiten eines technisierten Datenschutzes auseinander (s. Ziff. 12.1).

2. Entwicklung der Datenschutzgesetzgebung im Jahre 1988

2.1
Bundesgesetze

2.1.1
Novellierung des Bundesdatenschutzgesetzes

Die überfällige Novellierung des Bundesdatenschutzgesetzes (BDSG) ist – was die parlamentarische Behandlung angeht – 1988 noch nicht vorangekommen. Der Referentenentwurf des Bundesinnenministeriums vom 5. November 1987 wurde Anfang 1988 den Verbänden und den Landesregierungen zur Stellungnahme zugeleitet. Dieser Entwurf wurde dann in einigen Punkten überarbeitet und am 20. Dezember als Regierungsentwurf durch das Bundeskabinett verabschiedet (Bundesrats-Drucks. 618/88 vom 30. 12. 1988).

Die Kritik, die die Datenschutzbeauftragten der Länder und des Bundes zu dem in der letzten Legislaturperiode vorgelegten Entwurf der Koalitionsfraktionen bzw. der Bundesregierung (vgl. Bundestags-Drucks. 10/4737) geäußert haben, besteht nahezu im gleichen Umfang gegenüber dem neuen Regierungsentwurf fort. Bereits in ihrer Entschließung vom 6. Juni 1988 zum Referentenentwurf 1987 (abgedruckt in diesem Bericht, Ziff. 16.2) hatte die Konferenz der Datenschutzbeauftragten ohne Abstriche auf den – zum Entwurf der letzten Wahlperiode gefaßten – Beschluß vom 14. März 1986 (abgedruckt im 15. Tätigkeitsbericht, Ziff. 12.2) verweisen können.

Ich habe mich zur Notwendigkeit einer grundlegenden Neufassung des BDSG und zu den dabei nach meiner Auffassung aus dem Volkszählungsurteil des Bundesverfassungsgerichts vom Dezember 1983 zu ziehenden Konsequenzen zu wiederholten Malen in meinen Tätigkeitsberichten geäußert (vgl. 15. Tätigkeitsbericht, Ziff. 2.3; 16. Tätigkeitsbericht, Ziff. 1.2.3 und 2.1). Die 1987 bzw. 1988 in Kraft getretenen neuen Datenschutzgesetze der Länder Hessen, Nordrhein-Westfalen und Bremen haben diese Anforderungen des Bundesverfassungsgerichts zu großen Teilen bereits umgesetzt (vgl. unten Ziff. 2.2).

Um Wiederholungen zu vermeiden, seien die Mängel des BDSG-Entwurfs an dieser Stelle nur noch einmal in Stichworten genannt:

- Die Datenerhebung wird nicht ausdrücklich geregelt.
- Es ist verfehlt, den Anwendungsbereich des BDSG auf Dateien zu beschränken und die Datenverarbeitung in Akten im Verwaltungsverfahrensgesetz – und dort auch nur teilweise – zu regeln.
- Die Verarbeitungsvorschriften für den nicht-öffentlichen Bereich sind nach wie vor zu pauschal formuliert.
- Die Kontrollbefugnis des Bundesbeauftragten für den Datenschutz wird eingeschränkt statt ausgeweitet. Kontrolleinschränkungen sollen auch den Landesbeauftragten auferlegt werden.

Ich kann nur hoffen, daß dieser inakzeptable Entwurf im Laufe der Beratungen im Bundestag noch einmal grundlegend überarbeitet wird.

Ein Sonderthema der BDSG-Novellierung, die Stellung des Datenschutzbeauftragten, ist durch einen Gesetzentwurf der Grünen vom April 1988 (Bundestags-Drucks. 11/2175) thematisiert worden. Diese Initiative sieht die Wahl des Bundesbeauftragten für den Datenschutz mit $^2/_3$-Mehrheit durch den Bundestag und die Einrichtung der Institution des Bundesbeauftragten als unabhängige oberste Bundesbehörde mit eigenem Einzelplan im Bundeshaushalt vor. Der

Vorschlag der Grünen ist nach Diskussion im Plenum am 19. Mai 1988 an den Innenausschuß verwiesen, dort aber noch nicht behandelt worden.

Dieser Gesetzentwurf greift Regelungsmodelle auf, die in manchen Bundesländern – wie etwa in Hessen – bereits bestehen und sich bewährt haben, in anderen Ländern derzeit im Rahmen der Novellierungsdiskussion zu den Landesdatenschutzgesetzen erörtert werden. In Rheinland-Pfalz liegt seit dem Januar 1988 der Entwurf der Landesregierung für ein Gesetz zur Bestellung eines Landesbeauftragten für den Datenschutz vor (Landtags- Drucks. 11/730 vom 14. 01. 1988). Darin ist vorgesehen, die derzeit amtierende Datenschutzkommission – die einzige ihrer Art in der Bundesrepublik – zu ersetzen durch einen vom Landtag auf Vorschlag der Landesregierung zu wählenden Datenschutzbeauftragten. Dieser soll organisatorisch dem Ministerium des Innern zugeordnet werden.

Am konsequentesten ist das Modell eines parlamentarisch verantwortlichen Datenschutzbeauftragten in Schleswig-Holstein realisiert worden. Das am 6. Dezember 1988 vom Schleswig- Holsteinischen Landtag verabschiedete Gesetz zur Änderung des Landesdatenschutzgesetzes (Landtags-Drucks. 12/36) zielt auf eine völlige Unabhängigkeit des Datenschutzbeauftragten von der Regierung ab und geht in diesem Punkt noch weiter als das Hessische Datenschutzgesetz. Nicht nur soll der Datenschutzbeauftragte künftig bei der Präsidentin bzw. dem Präsidenten des Landtags angesiedelt werden; vielmehr steht auch das Vorschlagsrecht nicht der Landesregierung, sondern den Fraktionen des Landtags zu (insoweit anders § 21 Abs. 1 HDSG). Ich halte dies für eine vorbildliche Lösung, die die Distanz des Datenschutzbeauftragten zu der von ihm zu kontrollierenden Exekutive noch einmal unterstreicht.

Beide Regelungen sehen eine vergleichsweise lange Amtszeit des Datenschutzbeauftragten vor (Rheinland-Pfalz 8 Jahre, Schleswig-Holstein 6 Jahre). Es gibt sicherlich gute Gründe dafür, die Wahl des Datenschutzbeauftragten terminlich unabhängig von der Konstitution der Landtage zu machen. Eine derart lange Amtsperiode kann aber die Auswahl des oder der Beauftragten in erheblichem Umfang präjudizieren. Ungeachtet dieser oder anderer Einwände im Detail ist für mich in erster Linie wichtig, daß der durch die genannten Gesetzesaktivitäten in Bund und Ländern beschriebene Regelungstrend sich bundesweit fortsetzt.

2.1.2
Bundesverfassungsschutzgesetz

Am 20. Dezember 1988 hat das Bundeskabinett den Entwurf eines Gesetzes über die Zusammenarbeit des Bundes und der Länder in Angelegenheiten des Verfassungsschutzes und über das Bundesamt für Verfassungsschutz (Bundesverfassungsschutzgesetz – BVerfSchG –) verabschiedet (Bundesrats-Drucks. 618/88). Der Entwurf weicht nur in wenigen Punkten ab von dem im 15. Tätigkeitsbericht (Ziff. 6.3.4) kritisierten Regierungsentwurf vom Januar 1986 (Bundestags-Drucks. 10/4737). Im folgenden wird deshalb nur auf einige besonders gravierende Mängel hingewiesen.

2.1.2.1
Aufgaben und Befugnisse der Verfassungsschutzbehörden

Nach wie vor fehlt es an der vom Bundesverfassungsgericht geforderten genauen Festlegung der Aufgaben und Befugnisse der Verfassungsschutzämter. Es genügt nicht, die Haupttätigkeitsbereiche, d. h. Abwehr des politischen Extremismus, Bekämpfung von Spionage und Terrorismus sowie Mitwirkung bei Sicherheitsüberprüfungen, mit nebulösen Generalklauseln zu umschreiben.

Der Versuch, bei der Regelung des Einsatzes von „nachrichtendienstlichen Mitteln" – d. h. z. B. Einschleusung von Vertrauensleuten, Abhörmaßnahmen, Observationen auch mit fototechnischen Mitteln – mehr Transparenz zu schaffen, ist im Ansatz steckengeblieben. Zwar besteht nunmehr die Verpflichtung, die verschiedenen nachrichtendienstlichen Mittel in einer Dienstvorschrift zu benennen. Damit ist aber nicht viel gewonnen, solange die rechtlichen Grenzen der Anwendung solcher Mittel nicht festgelegt werden. Zumindest müßte sichergestellt sein, daß sich der Einsatz nur gegen konkret verdächtige Personen richtet und nicht gegen Dritte, die keinen Anlaß zur Beobachtung gegeben haben.

2.1.2.2
Informationsaustausch

Der Informationsaustausch sollte ursprünglich zum größten Teil in einem sogenannten Zusammenarbeitsgesetz (ZAG), später in einem Verfassungsschutzmitteilungsgesetz geregelt werden. Dieser Gedanke wurde mittlerweile aufgegeben. Statt dessen sollen nun die Übermittlungsvorschriften in das Bundesverfassungsschutzgesetz aufgenommen werden. Das ist sicherlich eine Verbesserung. Da aber bereits die Aufgaben nicht klar definiert werden, verwundert es kaum, daß auch bei den Regelungen des Informationsaustauschs zwischen Verfassungsschutzbehörden und anderen öffentlichen Stellen, insbesondere Sicherheitsbehörden, ähnlich großzügig verfahren wird.

Besonders gefährlich ist dies jedoch, wenn es um das Verhältnis von Verfassungsschutzbehörden zur Polizei geht. Die historischen Erfahrungen erinnern nur zur Genüge daran, wie notwendig eine scharfe Trennung des geheimdienstlichen vom polizeilichen Bereich ist. Sollte der Entwurf Gesetz werden, besteht die Gefahr, daß die institutionelle Trennung beider Bereiche durch eine extensive informationelle Zusammenarbeit unterlaufen wird.

2.1.2.3
Beschränkung auf Dateien

Wie schon im alten Regierungsentwurf sind auch im neuen die Datenverarbeitungsbestimmungen auf die Verarbeitung personenbezogener Daten in Dateien beschränkt. Da aber die Verfassungsschutzämter noch immer den größten Teil der Daten in Akten verarbeiten, bleibt bei dieser Restriktion die Datenverarbeitung weiterhin weitgehend ungeregelt.

2.1.2.4
Auskunftsanspruch des Bürgers

Obgleich unverzichtbar, enthält auch der neue Entwurf keine Regelung zum Recht des Betroffenen, von den Verfassungsschutzämtern Auskunft über die zu seiner Person gespeicherten Daten zu erhalten. Eine differenzierte Regelung muß einmal auf die in unterschiedlichem Maße der Geheimhaltung unterliegenden Aufgaben der Verfassungsschutzbehörden abstellen, zum anderen aber auch die verschiedenen Interessen des Betroffenen an einer Auskunft berücksichtigen, wie z. B. Schwierigkeiten bei der Arbeitssuche, Herabsetzung der Person in der Öffentlichkeit, gesundheitliche oder psychische Belastung. Die derzeitige Praxis der Verfassungsschutzbehörden, die bis auf wenige Ausnahmefälle mit dem Hinweis auf die Ausforschungsgefahr generell jede Auskunft verweigern, wird auch von den Gerichten nicht mehr akzeptiert.

2.2
Neue Landesdatenschutzgesetze

Dem Stillstand der BDSG-Novellierung (vgl. oben Ziff. 2.1.1) steht eine lebhafte Rechtsentwicklung auf Länderebene gegenüber. Am 1. Oktober 1987 ist das Gesetz zur Änderung des Bremischen Datenschutzgesetzes in Kraft getreten (GBl. der Freien Hansestadt Bremen 1987, S. 235). Das Nordrhein-Westfälische „Gesetz zur Fortentwicklung des Datenschutzes" gilt seit dem 23. April 1988 (GVBl. NRW 1988, S. 160). Beide folgen in zentralen Punkten dem Regelungsmodell des Hessischen Datenschutzgesetzes vom 11. November 1986, weichen in Einzelfragen allerdings auch davon ab.

Als wichtigste Gemeinsamkeiten aller drei neuen Landesdatenschutzgesetze der letzten beiden Jahre lassen sich feststellen

- die Einbeziehung der Akten in den Schutzbereich des Gesetzes,
- der Vorrang der Datenerhebung beim Betroffenen mit dessen Kenntnis,
- die Zweckbindung der Datenverwendung mit abschließenden Katalogen zugelassener Ausnahmen,
- spezielle Regelungen für den automatisierten Direktabruf von Daten sowie
- Sonderregelungen für Forschung und Arbeitnehmerdaten.

Hinzu kommt die Ausweitung der Kontrollbefugnisse des Datenschutzbeauftragten. Sie ergibt sich zum einen gleichsam „automatisch" aus der Einbeziehung der Akten in den Anwendungsbereich der Gesetze. Auf der anderen Seite wird der Notwendigkeit Rechnung getragen, den Datenschutzbeauftragten frühzeitig und umfassend mit den Planungen und Konsequenzen von Automationsverfahren zu befassen. Dem entspricht die Pflicht zur Unterrichtung des Datenschutzbeauftragten schon im Stadium der Konzeption automatisierter Informationssysteme (§ 20 Abs. 4 BremDSG, § 22 Abs. 3 GFD/NRW). Dem hessischen Beispiel (§ 24 Abs. 2 HDSG) folgt § 22 Abs. 2 GFD/NRW auch insofern, als dem Datenschutzbeauftragten die neue Aufgabe der Beobachtung des „Informationsgleichgewichts" zwischen Exekutive und Legislative bzw. dessen Verschiebung durch die automatisierte Datenverarbeitung übertragen wird. Parallelen zwischen den neuen Landesdatenschutzgesetzen gibt es auch bei der Statuierung neuer Unterrichtungspflichten bei Verarbeitungsformen von besonderer „Sensitivität" oder besonders schwierigen Abwägungsprozessen, etwa bei der Datenverarbeitung zu wissenschaftlichen Zwecken (vgl. § 33 Abs. 1 HDSG und § 28 Abs. 2 GFD/NRW).

Divergenzen gibt es besonders in einem Punkt, der Benachrichtigung. Bremen und Nordrhein-Westfalen haben die Information des Betroffenen über die erstmalige Einspeicherung seiner Daten in eine automatisierte Datei (§ 18 Abs. 2 HDSG) nicht übernommen. Der hessische Gesetzgeber hatte jedoch in dieser Unterrichtung ein zentrales Instrument der Transparenz der Datenverarbeitung für den Bürger gesehen (vgl. dazu in diesem Bericht Ziff. 15.2).

In allen drei Ländern war das wesentliche Motiv der Novellierung die Anpassung an die Vorgaben des Volkszählungsurteils des Bundesverfassungsgerichts vom 15. Dezember 1983. Zu Recht wurde es abgelehnt, den „Übergangsbonus" durch legislative Untätigkeit allzusehr zu strapazieren. Die Konkretisierung des Schutzes des informationellen Selbstbestimmungsrechts in den drei Gesetzen setzt Standards auch über die Landesgrenzen hinaus: Die verfassungskonforme Interpretation etwa der Zulässigkeitsbestimmungen für die Speicherung und Übermittlung in den noch nicht novellierten Gesetzen einschließlich des BDSG verlangt beispielsweise, daß die grundsätzliche Zweckbindung der Datenverwendung beachtet wird und Zweckänderungen nur in den – von den neuen Gesetzen beispielhaft konkretisierten – Ausnahmefällen überwiegender Allgemeininteressen zugelassen werden. Mit anderen Worten: Es

wird ein verfassungsrechtliches Mindestniveau fixiert, das weder bei den anstehenden Gesetzesnovellierungen in Bund und Ländern noch bei der Interpretation der Generalklauseln in vorhandenen Normen unberücksichtigt bleiben darf.

3. Polizei

3.1
Novellierung des HSOG

3.1.1
Gesetzentwürfe zur polizeilichen Datenverarbeitung

Für die polizeiliche Datenverarbeitung in Hessen fehlt es an einer verfassungskonformen gesetzlichen Grundlage. Spätestens seit dem Volkszählungsurteil des Bundesverfassungsgerichts vom Dezember 1983 ist dies auch allgemein anerkannt. Sicherlich war dem Gesetzgeber eine Übergangsfrist für eine Regelung einzuräumen. Nachdem mittlerweile aber 5 Jahre seit dem Volkszählungsurteil vergangen sind, ist diese Frist nunmehr abgelaufen. Daß die Übergangsfrist 1988 enden würde, darauf habe ich bereits in meinem 16. Tätigkeitsbericht (Ziff. 1.2.1) hingewiesen, und dies sehen anscheinend auch die Fraktionen des Landtags so oder ähnlich.

Denn im September 1988 haben die Koalitionsfraktionen von CDU und FDP mit Hinweis auf die Dringlichkeit einen Entwurf für ein Gesetz zur Änderung des Hessischen Gesetzes über die öffentliche Sicherheit und Ordnung (HSOG) (Drucks. 12/3092) im Landtag eingebracht. Der Entwurf weicht in einer Reihe von Punkten von dem sog. Vorentwurf zur Änderung des Musterentwurfs eines einheitlichen Polizeigesetzes des Bundes und der Länder (Stand: 12. März 1986) ab, der gemäß Beschluß der Innenministerkonferenz vom 25. November 1977 erstellt wurde. Zweifellos ist der Vorschlag eine geeignete Grundlage für die Diskussion der einzelnen Befugnisse der Polizei, personenbezogene Daten zu verarbeiten. Um es jedoch gleich vorwegzunehmen: Der Entwurf müßte noch in vielen Punkten präzisiert und eingegrenzt werden.

Die SPD-Fraktion (Drucks. 12/3108) und die Fraktion der GRÜNEN (Drucks. 12/3109) haben gleichfalls im Herbst 1988 eigene Gesetzentwürfe vorgelegt. Ausgangspunkt für beide Regelungsvorschläge ist der „Entwurf des Hessischen Ministers des Innern eines Gesetzes zur Änderung des Hessischen Gesetzes über die öffentliche Sicherheit und Ordnung (Stand: 30. September 1985)". Wesentlicher Unterschied der beiden Entwürfe: Der Gesetzentwurf der Fraktion der GRÜNEN will der Polizei nicht die Aufgabe der vorbeugenden Verbrechensbekämpfung zugestehen.

Die folgenden Überlegungen beschränken sich auf die wichtigsten Kritikpunkte der drei Gesetzentwürfe.

3.1.2
Vorbeugende Bekämpfung von Straftaten

Die größten datenschutzrechtlichen Probleme bereitet zweifelsohne die polizeiliche Datenverarbeitung zum Zwecke der vorbeugenden Bekämpfung von Straftaten. Die Entwürfe der Koalition und der SPD sehen ausdrücklich auch die vorbeugende Straftatenbekämpfung als polizeiliche Aufgabe an (§ 44 Abs. 1 Nr. 3 Koalitionsentwurf, § 44 Abs. 1 Nr. 2 SPD-Entwurf). Allein die GRÜNEN beschränken den Katalog polizeilicher Aufgaben auf die sog. konkrete Gefahrenabwehr (§ 1 Abs. 1 und § 1 a des GRÜNEN-Entwurfs). Inkonsequent ist dann allerdings § 44 d Abs. 1 Satz 2 dieses Entwurfs, der eine wesentliche Maßnahme im Rahmen der „Vorbeugung", nämlich die präventive Speicherung von personenbezogenen Daten, die aus Strafermittlungsverfahren gewonnen wurden, im Hinblick auf künftige, aber noch nicht konkret erkennbare Strafverfolgungsmaßnahmen, zuläßt.

Zweifellos ist die Polizei schon seit Jahrzehnten auf dem Gebiet der vorbeugenden Straftatenbekämpfung tätig, beschäftigt sich also längst nicht mehr ausschließlich mit Gefahrenabwehr. Bei der Gefahrenabwehr, eine Aufgabe, die bereits das Preußische Allgemeine Landrecht der Polizei zugewiesen hat, geht es genaugenommen lediglich um die Abwehr unmittelbar bevorstehender Gefahren. Wäre dies allerdings die einzige Aufgabe der Polizei, dürfte sie immer nur dann einschreiten, wenn die Gefahr eines Schadens konkret abzusehen wäre. Strikt befolgt würde dies für die polizeiliche Datenverarbeitung z. B. bedeuten, daß Strafakten nach Abschluß des Verfahrens regelmäßig vernichtet werden müßten, da ja eine unmittelbare zu erwartende weitere Straftat des Strafentlassenen bzw. der Person, die die Geldstrafe bezahlt hat, nicht mehr zu erwarten ist. Eine Verwendung der Strafermittlungsakten zur Aufklärung weiterer Straftaten wäre unzulässig.

Darüber hinaus haben sich in bestimmten Deliktsbereichen Verhaltensmuster und Organisationsformen entwickelt, die eine längerfristige Beobachtung und Verwertung personenbezogener Daten erforderlich machen, da nur so Ermittlungserfolge erzielt werden können. Das gilt etwa für die sog. organisierte Kriminalität, vor allem im Drogenhandel. Auf die vorbeugende Straftatenbekämpfung durch die Polizei kann deshalb sieherlich nicht gänzlich verzichtet werden. Wie gesagt: Auch der Entwurf der GRÜNEN sieht offensichtlich polizeiliche Verarbeitungsbefugnisse vor, die nur als Vorbeugung bezeichnet werden können, selbst wenn er eine polizeiliche Aufgabe „vorbeugende Straftatenbekämpfung" ausdrücklich ablehnt.

Damit ist jedoch nicht gesagt, daß die vorgelegten Entwürfe bereits eine befriedigende Lösung anbieten. Insbesondere fehlt es an einer genauen Festlegung, bei welchen Delikten die Polizei vorbeugend tätig werden darf.

3.1.3
Identitätsfeststellung

§ 16 des geltenden HSOG verleiht der Polizei die Befugnis, „die Identität einer Person festzustellen, wenn dies zur Erfüllung ihrer Aufgaben erforderlich ist". Die Entwürfe von SPD und GRÜNEN sehen für diese Bestimmung keine Konkretisierung oder Erweiterung vor. Demgegenüber enthält der Koalitionsentwurf in § 16 Abs. 2 bis 7 einen Katalog von Situationen, in denen über den Erforderlichkeitsgrundsatz hinaus Identitätskontrollen zugelassen werden. Dies gilt z. B. wenn „die Person sich an einem Ort aufhält, von dem aufgrund tatsächlicher Anhaltspunkte erfahrungsgemäß anzunehmen ist, daß dort Personen Straftaten mit erheblicher Bedeutung verabreden, vorbereiten oder verüben, und diese Maßnahme zur Verhütung solcher Straftaten geeignet erscheint...".

Ziel dieser Vorschrift ist es offensichtlich, Identitätskontrollen auch einer Vielzahl von Personen an den genannten Orten zuzulassen. Freilich wären dies nach dem Wortlaut des Vorschlags nicht nur einschlägige Bars, Etablissements im „Milieu", sondern auch Kaufhäuser, Bahnhöfe, Restaurants, Flughäfen oder auch Fußballstadien; selbst Fußgängerzonen könnten als solche Orte qualifiziert werden. Die Polizei könnte jeden, der sich dort aufhält, kontrollieren, ohne daß dies für eine konkrete Gefahrenabwehr erforderlich wäre. Der Willkür wären Tür und Tor geöffnet. Es ist deshalb erforderlich, genau festzulegen, an welchen Orten und bei welchen Straftaten solche Kontrollen zulässig sein sollen.

Auch die Befugnis zu Identitätskontrollen an Orten, „an denen sich Straftäter verbergen", umreißt den betroffenen Personenkreis nicht eindeutig. Gemeint sind wohl verurteilte Straftäter. Klar ist dies indessen nicht. Aus diesem Grund halte ich es für erforderlich, daß der Personenkreis eingegrenzt wird auf „zur Strafvollstreckung gesuchte Straftäter".

Zu unbestimmt wird der Polizei gestattet, in bestimmten „Verkehrs- oder Versorgungsanlagen" oder „einem anderen besonders gefährdeten Objekt" Kontrollen durchzuführen, wenn eine Person sich „in dessen unmittelbarer Nähe aufhält und tatsächliche Anhaltspunkte die Annahme rechtfertigen, daß in oder an Objekten dieser Art Straftaten begangen werden sollen, ...". Hier sollten zumindest auch Anhaltspunkte für eine konkrete Gefährdung durch die zu überprüfende Person als Voraussetzungen für Identitätskontrollen verlangt werden.

Auch die vorgesehene Möglichkeit, Kontrollstellen für bestimmte Zwecke einzurichten, um bestimmte Straftaten zu verhindern, ist zu großzügig. Es handelt sich dabei um eine Parallelvorschrift zu § 111 Strafprozeßordnung, der zu einer auch von Gerichten kritisierten umfassenden Überprüfungspraxis geführt hat. Die Kritik, die zu § 111 StPO, einer Norm für die Straftatenaufklärung, geäußert worden ist, gilt um so mehr für eine ähnlich lautende präventivpolizeiliche Vorschrift, bei der es um die Verhinderung einer Straftat geht. Es stellt sich die Frage, ob eine solche Vorschrift im HSOG überhaupt erforderlich ist.

3.1.4
Datenerhebung mit Einwilligung des Betroffenen

Alle Entwürfe lassen prinzipiell eine Datenerhebung nicht nur aufgrund einer Rechtsvorschrift, sondern auch mit Einwilligung der Betroffenen zu (vgl. § 44 a Abs. 1 Nr. 1 des Koalitionsentwurfs, § 44 a Abs. 3 und 4 des Entwurfs der GRÜNEN und § 44 a Abs. 2 und 3 des SPD-Entwurfs). Das stößt insofern auf Bedenken, als im Zusammenhang mit polizeilichem Handeln Situationen vorstellbar sind, in denen zwar förmlich eine Einwilligung der Betroffenen eingeholt werden könnte, aufgrund der Eingriffssituation eine echte Freiwilligkeit jedoch kaum gegeben sein dürfte. In der Vergangenheit spielte dieses Problem insbesondere bei Prostituiertendateien oder Dateien über Personen aus kriminalitätsnahen Milieus eine Rolle. Erhebungen im Eingriffsbereich müssen deshalb auf gesetzliche Befugnisse gestützt werden. Lediglich im Zusammenhang mit polizeilichen Hilfs- und Rettungsmaßnahmen sollten Erhebungen aufgrund einer förmlichen Einwilligung der Betroffenen zugelassen werden. Eine zweckgebundene Verwertung dieser Dateien wäre zudem sicherzustellen.

3.1.5
Datenerhebung aus allgemein zugänglichen Quellen

Der Koalitionsentwurf erlaubt auch die Erhebung personenbezogener Daten aus allgemein zugänglichen Quellen und zwar ohne Einschränkung durch den Erforderlichkeitsgrundsatz (§ 44 a Abs. 1 Nr. 3). Das ist zumindest mißverständlich. In den Fällen, in denen der Polizei die Erhebung personenbezogener Daten gestattet ist, dürfen diese Daten selbstverständlich auch aus allgemein zugänglichen Quellen entnommen werden. Ohne die ausdrückliche Einschränkung durch den Erforderlichkeitsgrundsatz bestünde aber die Möglichkeit, allgemein zugängliche Quellen umfassend auszuwerten, entsprechende Vorratsdateien anzulegen, um diesen Datenbestand dann losgelöst von seinem ursprünglichen Verwendungszusammenhang zu den verschiedensten Zwecken zu nutzen. Zu Recht hat das Bundesverfassungsgericht im Volkszählungsurteil von 1983 betont, daß es nicht abstrakt auf die Daten selbst oder ihre Herkunft ankommen kann, sondern immer auf den Verwendungszusammenhang. Deshalb ist diese Vorschrift im besten Fall überflüssig, sonst aber bedenklich.

3.1.6
Datenerhebung und -weiterverarbeitung bei öffentlichen Veranstaltungen und Versammlungen

Von besonderer datenschutzrechtlicher Bedeutung ist die polizeiliche Datenerhebung und -weiterverarbeitung bei öffentlichen Veranstaltungen und Versammlungen. Die Entwürfe greifen dieses Thema ganz unterschiedlich auf. GRÜNE und SPD (jeweils § 44 b Abs. 6) erlauben der Polizei nur dann, in öffentlichen Versammlungen personenbezogene Daten zu erheben, wenn „tatsächliche Anhaltspunkte" vorliegen, daß aus oder wegen der Versammlung bestimmte festgelegte Straftaten begangen werden.

Ganz anders dagegen § 44 b des Koalitionsentwurfs: Diese Sondervorschrift gilt lediglich den sogenannten Nichtstörern, d. h. Personen, die nicht für die Störung oder bevorstehende Straftat unmittelbar verantwortlich gemacht werden können, und gestattet, auch deren Daten zu erheben. Ziel der Bestimmungen ist es, eine Grundlage für Massenkontrollen oder gezielte Einzelkontrollen nicht direkt Beteiligter zu schaffen, um damit entweder die Betroffenen präventiv zu kontrollieren oder sie von rechtswidrigen Maßnahmen abzuhalten.

Solche Massenkontrollen sind aber auf keinen Fall – wie es der Koalitionsentwurf vorsieht – schon bei „tatsächlichen Anhaltspunkten" für „nicht geringfügige Ordnungswidrigkeiten" gerechtfertigt. Allenfalls bei Anhaltspunkten für Straftaten, besser noch bei Anhaltspunkten für bestimmte Straftaten, die in einem Katalog zu definieren wären, können so umfassende Maßnahmen in Betracht kommen.

Auch die im Koalitionsentwurf vorgesehene Aufbewahrungsfrist von zwei Monaten erscheint mir als zu lang; bereits einen Monat nach dem Ereignis dürfte erkennbar sein, ob die Daten zur Verfolgung einer Straftat, Ordnungswidrigkeit oder zur Strafvollstreckung benötigt werden.

Die Daten dürften auch wohl kaum in personenbezogener Form für Schulungs- und statistische Zwecke benötigt werden. § 44 b Abs. 2 Satz 3 des Koalitionsentwurfs, der diese Weiterverwendung zuläßt, sollte daher gestrichen werden.

Alle Entwürfe erlauben auch Bild- und Tonaufzeichnungen. Hier ist insbesondere die bereits früher ausführlich diskutierte Frage zu entscheiden, ob generell der gesamte Verlauf der Versammlung aufgezeichnet werden darf, oder es nicht ausreicht, daß die Geräte erst dann eingeschaltet werden dürfen, wenn sich die Gefährdung konkretisiert hat.

3.1.7
Datenerhebung durch Observation und Einsatz technischer Mittel

Mit der Datenerhebung durch Observation und dem Einsatz technischer Mittel sind Erhebungsmethoden angesprochen, die das Recht des Betroffenen auf informationelle Selbstbestimmung in besonderem Maße beeinträchtigen.

Sowohl die Observation als auch der Einsatz technischer Mittel setzen entweder eine Täuschung oder die Unkenntnis des Betroffenen über die Erhebung selbst (verdeckte Erhebung) voraus und greifen damit erheblich tiefer in die Privatsphäre ein als die offene Registrierung von Daten. Je nach Art der Maßnahme kann dabei auch das Grundrecht auf Unverletzlichkeit der Wohnung berührt sein.

Weder der Entwurf der GRÜNEN noch der SPD enthalten Regelungen über den allgemeinen Einsatz von Observationen oder technischen Mitteln. Lediglich die Datenerhebung in oder aus Wohnungen und hierbei der Einsatz optischer und akustischer Hilfsmittel wird jeweils in § 44 b Abs. 7 der Entwürfe angesprochen. Den Einsatz solcher Hilfsmittel läßt der SPD-Entwurf zur Abwehr einer gegenwärtigen erheblichen Gefahr für Leib oder Leben einer Person sowie zur Abwehr einer erheblichen Gefahr für Leib oder Leben der bei einem polizeilichen Einsatz in der Wohnung tätigen Person (verdeckter Ermittler oder „V-Person") zu, wenn diese das Hilfsmittel mit sich führt.

Der Entwurf der GRÜNEN sieht ebenfalls eine solche Maßnahme zur Abwehr einer gegenwärtigen erheblichen Gefahr für Leib und Leben einer Person vor, enthält aber im Gegensatz zum SPD-Entwurf keine Möglichkeit, einen verdeckten Ermittler mit einem solchen Hilfsmittel zu schützen.

Der Koalitionsentwurf läßt eine Observation – gemeint ist die planmäßig angelegte Beobachtung einer Person durchgehend länger als 24 Stunden oder an mehr als zwei Tagen – oder den Einsatz technischer Mittel, insbesondere zur Anfertigung von Bildaufnahmen oder Aufzeichnungen sowie zum Abhören oder Aufzeichnen des gesprochenen Wortes, zu, „wenn tatsächliche Anhaltspunkte die Annahme rechtfertigen, daß eine Straftat mit erheblicher Bedeutung begangen werden soll" (§ 44 c des Koalitionsentwurfs). Hinzukommen muß, daß diese Methode als „letztes Mittel" gebraucht wird und nicht außer Verhältnis zur Bedeutung des aufzuklärenden Sachverhalts steht.

Auch hier ist es wiederum der Begriff der „Straftaten mit erheblicher Bedeutung", der Kritik hervorruft. Der besondere Eingriff in die Privatsphäre des Betroffenen, der in einer Observation oder dem Einsatz technischer Mittel liegt, erscheint nur dann als gerechtfertigt, wenn eine besondere Gefährdungssituation gegeben ist. Dies mag zum einen bei Verbrechen der Fall sein. Darüber hinaus sollte der Anwendungsbereich jedoch auf Straftaten beschränkt werden, die gewerbs-, gewohnheits- oder bandenmäßig begangen werden. Nur insoweit und insbesondere im Bereich der sogenannten organisierten Kriminalität sind diese Maßnahmen angezeigt.

Ebenso auf Kritik stößt die vorgesehene Möglichkeit, „andere Personen" als Erhebungsobjekte einzubeziehen, „wenn tatsächliche Anhaltspunkte die Annahme rechtfertigen, daß sie (mit dem Täter bzw. Störer) in einer Weise in Verbindung stehen, die erwarten läßt, daß die Maßnahme zur Verhütung einer Straftat beitragen wird" (§ 44 c Abs. 3 des Koalitionsentwurfs). Diese Formulierung läßt Bewertungen zu, die sich allein am gewünschten Ergebnis orientieren. Sie ist völlig ungeeignet, den betroffenen Personenkreis einzugrenzen.

Alle einschränkenden Voraussetzungen sollen nach dem Koalitionsentwurf entfallen, „wenn dies zur Abwehr einer Gefahr für Leib oder Leben einer zur Verhütung einer Straftat mit erheblicher Bedeutung eingesetzten Person geschieht, die das technische Mittel mit sich führt" (§ 44 c Abs. 6 des Koalitionsentwurfs). Damit ist der gleiche Gedanke angesprochen, der sich auch im SPD-Entwurf wiederfindet. Nur: Die Formulierung ist recht unklar, da sie nicht erkennen läßt, unter welchen positiven Voraussetzungen eine solche Maßnahme zulässig ist. Der Schluß liegt nahe: immer. Gesetzestechnisch erscheint diese Regelung in jedem Fall als mißglückt.

3.1.8
Polizeiliche Beobachtung

Wie schon die Observation unter Einsatz technischer Mittel, gehört auch die polizeiliche Beobachtung zu den Befugnissen, die zu einem verstärkten Eingriff in den Persönlichkeitsbereich des Betroffenen führen. Wenn auch der Betroffene dabei nicht systematisch in das Blickfeld der ermittelnden Behörde gerät, sondern lediglich an Kontrollstellen allgemeiner Art (Grenzen, Kontrollstellen nach § 111 StPO oder etwa Identitätskontrollen) seine Bewegungen registriert und als mehr oder weniger zufällig zusammengetragene Einzelbeobachtungen einer ermittelnden Behörde zugeleitet werden, so können diese Teilbeobachtungen doch zu einem Bewegungsbild über den Betroffenen zusammengefügt werden. Wie bereits im Zusammenhang mit der Observation und dem Einsatz technischer Mittel sollte die Voraussetzung, daß die Gesamtwürdigung der Person und ihrer bisherigen Straftaten erwarten läßt, daß sie auch künftig Straftaten mit erheblicher Bedeutung begehen wird, präzisiert werden. Auch hier ist ein konkreter Katalog bestimmter Delikte bzw. modi operandi (Begehungsweisen) notwendig, um den Anwendungsbereich einzugrenzen (§ 44 d des Koalitionsentwurfs).

Ebenso unklar ist der Status des Betroffenen. Gemäß Abs. 2 Nr. 1 müßte er bisher „Straftaten mit erheblicher Bedeutung" begangen haben. Dies setzt nicht unbedingt voraus, daß er bereits rechtskräftig verurteilt wurde – eine rechtsstaatlich aber notwendige Voraussetzung. Durch Hinweise etwa auf die Unterstellung unter eine Bewährungshilfe oder eine Führungsaufsicht würde klargestellt, daß es sich um eine bestimmte Phase nach der Entlassung handelt, in der der Betroffene unter verstärkter Aufsicht stehen soll.

3.1.9
Erkennungsdienstliche Maßnahmen

Ein wesentliches Hilfsmittel polizeilicher Tätigkeit auch und gerade im Hinblick auf eine mögliche spätere Aufklärung neuer Straftaten des Betroffenen ist die Durchführung von „erkennungsdienstlichen Maßnahmen". Nach allen drei Entwürfen (§ 44 e des Koalitionsentwurfs, § 44 c der Entwürfe von SPD und GRÜNEN) handelt es sich dabei um Finger- und Handflächenabdrücke, um Lichtbilder sowie um Messungen oder ähnliche Feststellungen äußerer körperlicher Merkmale.

Bereits hier wird jedoch ein Unterschied deutlich. Der Koalitionsentwurf legt fest, daß „insbesondere" diese Maßnahmen als „ED-Maßnahmen" zu qualifizieren sind. Der Katalog dieser Maßnahmen bleibt damit offen. Wie sehr es aber darauf ankommt, Unklarheiten über die zulässigen Maßnahmen gar nicht erst aufkommen zu lassen, zeigt die Diskussion über die Genomanalyse. Sie gibt deutlich zu erkennen, daß ein solches Verfahren über die Täteridentifizierung hinaus zu einer umfassenden Persönlichkeits- oder Gesundheitsanalyse des Betroffenen verwendet werden kann. Der Vorschlag der Koalition schließt dies nicht aus. Er ist deshalb zu unbestimmt. In jedem Fall müßte ein Verbot derart umfassender Analysen in die Bestimmung aufgenommen werden. Bei der Prüfung der Frage, ob eine Verwendung der Genomanalyse zur Identifikation von Störern bzw. Tätern überhaupt in Betracht kommen kann, gilt es, sich zunächst eingehend mit den Bedingungen auseinanderzusetzen, unter denen eine solche Analyse durchgeführt werden kann. Gleiches gilt für die nicht minder entscheidende Frage, inwieweit es möglich ist, die Analyse strikt auf die Identifizierung zu beschränken. Für den Bereich der Vorbeugung sollte die Genomanalyse ausdrücklich untersagt werden.

3.1.10
Datenspeicherung, -veränderung und sonstige Datenverwendung

Alle Entwürfe lassen die Speicherung der erhobenen Daten grundsätzlich nur zu, soweit dies zur Aufgabenerfüllung erforderlich ist (§ 44 f Koalitionsentwurf, § 44 d der Entwürfe von GRÜNEN und SPD). Allerdings verlangen sowohl SPD wie GRÜNE für eine automatisierte Speicherung die Feststellung, daß die ständige Verfügbarkeit der Daten für die Wahrnehmung der polizeilichen Aufgaben erforderlich ist.

Es erstaunt andererseits, daß die aus meiner Sicht notwendige Zweckbindung von Daten, die der Datenschutzkontrolle, der Datensicherung oder zur Sicherstellung des ordnungsgemäßen Betriebs einer Datenverarbeitungsanlage dienen (sog. Protokolldaten), lediglich in den Entwürfen von SPD und Koalition enthalten ist. Der Entwurf der GRÜNEN verzichtet auf eine solche Zweckbindung.

Für problematisch halte ich, daß nach dem Koalitionsentwurf eine Zweckbindung der personenbezogenen Daten nur für die im Umkreis des Störers bzw. Straftäters festgestellten personenbezogenen Daten gelten soll, nicht aber für Daten, die ihn selbst betreffen (§ 44 f Abs. 3 des Koalitionsentwurfs).

Von großer Bedeutung ist die Weiterspeicherung von Daten, die die Polizei im Rahmen von strafrechtlichen Ermittlungsverfahren gewonnen hat. Sie ist nach allen Entwürfen grundsätzlich zulässig. Der Entwurf der Koalition läßt eine Weiterspeicherung in nicht automatisierter Form ganz allgemein ohne Einschränkung zu. Lediglich die automatisierte Speicherung soll davon abhängig sein, daß eine Begehung weiterer Straftaten durch die betroffene Person zu befürchten ist. Es ist nicht einsehbar, warum hier zwischen automatisierter und nicht automatisierter Speicherung getrennt wird. Für beide Formen sollten die gleichen, schärferen Voraussetzungen gelten (vgl. § 44 f Abs. 4 des Koalitionsentwurfs).

Völlig unzureichend ist die Bestimmung, die der Koalitionsentwurf zur Vorgangsverwaltung enthält (§ 44 f Abs. 8). Sie legt lediglich fest, daß die Vollzugspolizei zu diesem Zweck personenbezogene Daten speichern und verwenden kann. Nicht nur der Erforderlichkeitsgrundsatz, sondern auch detaillierte Voraussetzungen für eine automatisierte Vorgangsverwaltung müssen in diesem Zusammenhang vorgegeben werden. Angesichts der anstehenden Automatisierung bei der hessischen Polizei sind entsprechende konkrete Bestimmungen dringlich.

3.1.11
Besondere Formen des Datenabgleichs

Im Gegensatz zu den Entwürfen der Oppositionsparteien, die eine „Rasterfahndung" zu präventivpolizeilichen Zwecken nicht vorsehen, enthält der Koalitionsentwurf eine entsprechende Befugnis (§ 44 lit. l). Demnach könnte die Vollzugspolizei von öffentlichen oder nicht-öffentlichen Stellen zur Abwehr einer gegenwärtigen Gefahr für den Bestand oder die Sicherheit des Bundes oder des Landes oder für Leib, Leben oder Freiheit einer Person die Übermittlung von personenbezogenen Daten bestimmter Personengruppen aus Dateien zum Zweck des Abgleichs mit anderen Datenbeständen verlangen, wenn Tatsachen die Annahme rechtfertigen, daß dies zur Abwehr der Gefahr erforderlich ist. Vorschriften über ein Berufs- oder besonderes Amtsgeheimnis sollen unberührt bleiben.

Auch wenn es um Rechtsgüter von großer Bedeutung geht, ist doch zu kritisieren, daß eine Rasterfahndung aus polizeirechtlichen Gründen stattfinden soll. Zwar greift die Norm nicht in den Bereich der vorbeugenden Straftatenbekämpfung ein, sondern beschränkt sich auf die Abwehr einer gegenwärtigen Gefahr für die genannten wesentlichen Rechtsgüter. Theoretisch können somit kaum Probleme entstehen. Praktisch gesehen gibt es jedoch bisher keine bekannten Beispiele für eine Rasterfahndung zu präventivpolizeilichen Zwecken. Die Bestimmung sollte deshalb gestrichen werden.

3.1.12
Auskunftsanspruch

Alle Entwürfe gewähren dem Betroffenen einen Auskunftsanspruch über die zu seiner Person gespeicherten Daten (§ 44 o des Koalitionsentwurfs, § 44 i der Entwürfe von GRÜNEN bzw. SPD). Eher im Detail als im wesentlichen Inhalt sind hierbei Unterschiede zu verzeichnen. Lediglich auf eine Einzelheit des Koalitionsentwurfs sollte hingewiesen werden: Die gegenwärtige Fassung, die lediglich ein persönliches Auskunftsrecht des Hessischen Datenschutzbeauftragten vorsieht, wenn die Auskunft dem Betroffenen nicht gewährt wird, ist wohl ein redaktionelles Versehen. § 29 Hessisches Datenschutzgesetz gibt klar zu erkennen, daß bei der Verabschiedung des Datenschutzgesetzes bereits die Probleme im Bereich der Sicherheitsbehörden eingehend diskutiert worden sind. Der Gesetzgeber hatte sich deshalb für eine Lösung entschieden, die eine solche Beschränkung nicht enthält. Konsequenterweise müßten deshalb entweder die HDSG-Regelungen in das HSOG übernommen oder diese Bestimmung des Entwurfs ersatzlos gestrichen werden.

3.2
Novellierung des Gesetzes über das Bundeskriminalamt und die Zusammenarbeit des Bundes und der Länder in kriminalpolizeilichen Angelegenheiten (BKAG)

3.2.1
Ziel der Neufassung des BKA-Gesetzes

Das Bundesinnenministerium hat im August 1988 einen Referentenentwurf für ein neues BKA-Gesetz vorgelegt. Erklärtes Ziel des Gesetzentwurfes ist es, nach den Maßstäben des Urteils des Bundesverfassungsgerichts zum Volkszählungsgesetz 1983 eine bereichsspezifische Rechtsgrundlage für die Datenverarbeitung durch das Bundeskriminalamt zu schaffen. Der Entwurf entspricht damit auch einer Forderung der Datenschutzbeauftragten. Das bestehende Gesetz aus dem Jahre 1973 enthält zwar Vorschriften über die Aufgaben des Bundeskriminalamts als Zentralstelle für die Sammlung und Auswertung von Nachrichten und Unterlagen für die polizeiliche Verbrechensbekämpfung und den elektronischen Datenverbund zwischen Bund und Ländern; es enthält auch eine Rechtsgrundlage für die Unterhaltung erkennungsdienstlicher Einrichtungen. Darüber hinaus fehlt es jedoch an präzisen Bestimmungen über die Speicherung von Daten in Informationssystemen beim BKA, deren Weitergabe an andere Stellen sowie die Berichtigung, Löschung und Auskunftserteilung aus diesen Informationssystemen.

3.2.2
Grundlegende Anforderungen an eine bereichsspezifische Regelung für die Tätigkeit des BKA

Das BKA soll als Zentralstelle für das polizeiliche Auskunfts- und Nachrichtenwesen und für die Kriminalpolizei fungieren (§ 2 Abs. 1 BKAG-E), d. h. in „kriminalpolizeilichen Angelegenheiten zur Bekämpfung der länderübergreifenden und internationalen Kriminalität" (§ 1 Abs. 1 BKAG-E) tätig sein. Aus der Sicht des Datenschutzes ist dies die wichtigste Aufgabe.

Die Aufgabenbeschreibung „Zentralstelle" ist allerdings zu unbestimmt und nicht ausreichend, um eine Abgrenzung der einzelnen Rechte und Befugnisse insbesondere im Verhältnis zu den Länderpolizeien vorzunehmen. Erforderlich ist auch, daß bestimmte Grundbedingungen für die Verarbeitung personenbezogener Daten in den polizeilichen Informationssystemen beim BKA und den Landeskriminalämtern im Gesetz ausdrücklich festgelegt werden. Zu regeln ist insbesondere,

- unter welchen Voraussetzungen welche Arten von Dateien oder Verarbeitungssystemen eingerichtet werden dürfen (z. B. einfache Aktennachweissysteme, die lediglich einen Zugriff auf Kriminalakten ermöglichen sollen; Falldateien, die für bestimmte Deliktsbereiche wie etwa Rauschgift oder Sexualstraftaten deliktstypische Begehungsweisen erkennen lassen; Recherchiersysteme, die eine möglichst umfassende automatisierte Auswertung von Akteninhalten nach jeweils neu zu entwickelnden Rastern erlauben; die Sammlung der erkennungsdienstlichen Unterlagen, die eine schnelle Täteridentifikation aufgrund von körperlichen Merkmalen zulassen; Spurendokumentationssysteme, die bei erheblichen Einzelstraftaten oder bestimmten gravierenden Delikten eine umfassende Sammlung aller Hinweise und Spuren in automatisierten Systemen ermöglichen, um diese dann schrittweise auf ihre Verwertbarkeit für die Aufklärung von Straftaten zu überprüfen)

- inwiefern die einzelnen Teilbereiche der polizeilichen Datenverarbeitung in der Form der Verbundverarbeitung (§ 10 des Entwurfs) und in welchem Umfang als unmittelbare Zentraldatei des BKA erfolgen sollen. Verbundverarbeitung bedeutet, daß neben dem BKA insbesondere auch die Landeskriminalämter Daten unmittelbar eingeben und verändern können

- welche Personenkreise (Verdächtige bzw. Beschuldigte einerseits, Zeugen, Opfer, Hinweisgeber andererseits) in diesen Dateien erfaßt werden dürfen

- welche Aufbewahrungsfristen für die verschiedenen Dateitypen, weiter untergliedert nach den betroffenen Personenkreisen, zu gelten haben

- in welchem Umfang eine Zweckbindung der Daten für die Aufklärung in bestimmten Bereichen oder Fällen bzw. die Weitergabe an Dritte erfolgen soll

- in welchem Umfang die Verbundteilnehmer bzw. die Zentralstelle über die einzelnen Daten verfügen und z. B. Auskunft an Dritte oder auch die Betroffenen geben dürfen.

3.2.3
Einzelregelungen

3.2.3.1
Allgemeine Datenverarbeitungsbefugnisse

Wenn § 2 Abs. 2 Nr. 1 des Entwurfs dem Bundeskriminalamt die Befugnis einräumt, für seine Funktion als Zentralstelle für das polizeiliche Auskunfts- und Nachrichtenwesen und für die Kriminalpolizei sowie zum Zwecke der vorbeugenden Bekämpfung und Verfolgung von Straftaten „alle hierfür erforderlichen Informationen, insbesondere sach- und personenbezogene Auskünfte, Nachrichten und Unterlagen, zu sammeln und auszuwerten", so wird der Gesetzentwurf den Anforderungen an eine bereichsspezifische Datenschutzregelung nicht gerecht. Über den bereits in den allgemeinen Datenschutzgesetzen enthaltenen Erforderlichkeitsgrundsatz hinaus enthält die Bestimmung keinerlei Konkretisierung der Datenverarbeitungsbefugnisse.

Die gleiche Kritik gilt auch für die in § 2 Abs. 2 Nr. 3 enthaltene Befugnis, zentrale erkennungsdienstliche Einrichtungen und Sammlungen zu unterhalten sowie die zu deren Betrieb und Unterhaltung erforderliche Zusammenarbeit in der Polizei zu koordinieren.

Positiv hervorzuheben ist lediglich § 6 Abs. 4 des Entwurfs, nach dem bei Bewertungen in Dateien der Zentralstelle feststellbar sein muß, „bei welcher Stelle die Unterlagen geführt werden, die der Bewertung zugrundeliegen". Dies war insbesondere im Zusammenhang mit den sogenannten personenbezogenen Hinweisen im INPOL-System bisher regelmäßig nicht der Fall.

3.2.3.2
Übermittlungsregelungen

Auch die Übermittlungsregelungen für den innerstaatlichen Bereich (§ 7 des Entwurfs) bleiben zu vage und allein dem allgemeinen Erforderlichkeitsgrundsatz verhaftet. Insbesondere der Austausch zwischen BKA einerseits und den Nachrichtendiensten andererseits wird nicht erwähnt. Erhebliche Kritik verdient § 7 Abs. 6 des Entwurfs, der einen automatisierten Direktzugriff auf die beim BKA geführten Datenbestände anderen als Polizeibehörden eröffnet und hierfür lediglich als formale Voraussetzung die Zustimmung des Bundesministers des Innern und der Innenminister/-senatoren der Länder voraussetzt. Inhaltliche Kriterien sind hierfür überhaupt nicht vorgesehen.

Auch die Datenverarbeitungsbefugnisse für die Zusammenarbeit im internationalen Bereich sind zum Teil recht offen formuliert. So ist die Übermittlung personenbezogener Informationen nach § 8 Abs. 1 Nr. 2 an ausländische Polizei- und Justizbehörden sowie an sonstige für die polizeiliche Verbrechensbekämpfung zuständige öffentliche Stellen anderer Staaten zulässig, soweit dies erforderlich ist „zur vorbeugenden Verbrechensbekämpfung bei Straftaten von erheblicher Bedeutung". Eine eingrenzende Wirkung dürfte diese Formulierung kaum entfalten. Sie bedarf deshalb der Präzisierung. Gleiches gilt für die Übermittlung im automatisierten Verfahren von „personenbezogenen Fahndungsdaten" an zentrale Polizeibehörden anderer Staaten sowie an internationale Datenbestände (§ 8 Abs. 2 des Entwurfs). Was „Fahndungsdaten" sind, ist keineswegs eindeutig. Entweder in der Strafprozeßordnung oder im BKAG müßte deshalb eine entsprechende Konkretisierung vorgenommen werden.

Die Schutzvorschrift zugunsten des Betroffenen („die Übermittlung personenbezogener Informationen unterbleibt, soweit ... der Betroffene ein schutzwürdiges Interesse an dem Ausschluß der Übermittlung hat ...") reicht nicht aus. Der Handlungsspielraum der übermittelnden Behörde (BKA) ist zu groß. Besser wäre es, an für den Betroffenen zu erwartende unverhältnismäßige Nachteile anzuknüpfen.

3.2.3.3
Zusammenarbeit zwischen Bund und Ländern

Dem Entwurf gelingt es nicht, in wesentlichen Umrissen den Gegenstand des polizeilichen Informationssystems und seine Strukturen gesetzlich zu bestimmen. Als positiv zu bewerten ist lediglich die in § 10 Abs. 3 vorgesehene Verantwortung der zur unmittelbaren Eingabe der Daten berechtigten Stelle für deren Rechtmäßigkeit, die Zulässigkeit der Übermittlung und die Richtigkeit und Aktualität der Daten. Die Verantwortlichkeit dieser Stelle wird damit konkretisiert. Allerdings dürfte im Zusammenhang mit der Übermittlung bei Direktzugriffen Dritter mangels der Einwirkungsmöglichkeit durch die eingebende Stelle eine Teilung der Verantwortung richtiger sein.

Recht unbestimmt bleibt die in § 11 Abs. 1 vorgesehene Verpflichtung der Landeskriminalämter, dem BKA die zur Erfüllung seiner Aufgaben als Zentralstelle erforderlichen Informationen zu übermitteln. Gleiches gilt für die Zulässigkeit von Übermittlungen durch andere Behörden, „wenn tatsächliche Anhaltspunkte dafür bestehen, daß die Übermittlung für die Erfüllung der Aufgaben des Bundeskriminalamts nach § 2 erforderlich ist" (§ 11 Abs. 5 des Entwurfs).

3.2.3.4
Berichtigung von Daten

Die Berichtigungspflicht des Bundeskriminalamts sollte nicht nur für personenbezogene Daten in Dateien bestehen, „wenn sich ergibt, daß sie unrichtig sind". Vielmehr ist eine aktive Datenpflege im Sinne einer ständigen Überprüfung der Datenbestände notwendig.

3.2.4
Fazit

Der Referentenentwurf des Bundesinnenministeriums läßt zwar Ansätze für eine bereichsspezifische Durchgliederung der Informationsverarbeitung des BKA und – soweit durch ein Bundesgesetz regelbar – der Landeskriminalämter erkennen. Weder die Informations- noch die Dateienstruktur, wie sie sich in den letzten Jahren im Datenverbund von BKA und Landeskriminalämtern entwickelt haben, noch einzelne Speicherungsvoraussetzungen können jedoch dem Gesetzentwurf in ausreichendem Ausmaß entnommen werden. Ergänzungen und Konkretisierungen sind deshalb nötig. Ohne entsprechende Änderungen und Zusätze würde das Gesetz dem Gebot der Normenklarheit und Bestimmtheit nicht gerecht.

3.3
Prüfung von Datenspeicherungen in der sogenannten „L-Gruppe" (Personenbeschreibung) im Hessischen Polizeiinformationssystem (HEPOLIS)

3.3.1
Konzept der Speicherung von Daten in der „L-Gruppe"

Die in der Datei HEPOLIS (Hessisches Polizeiinformationssystem) zu einer Person gespeicherten Daten sind in verschiedene Datengruppen unterteilt. Zu jeder Person gibt es eine „P-Gruppe" – hier sind die Personalien gespeichert.

Wird nach dem Betroffenen gefahndet, sind zusätzliche Fahndungsdaten in der sogenannten „F-Gruppe" gespeichert. Die „E-Gruppe" enthält Daten über „erkennungsdienstliche Maßnahmen" (z. B. Lichtbilder und Fingerabdrücke). Wenn zu einer Person Daten der „E-Gruppe" vorliegen, können weitere Daten zur Personenbeschreibung in einer sogenannten „L-Gruppe" gespeichert sein. Aber auch dann, wenn der Täter noch unbekannt ist, können Informationen in diese Datengruppe eingegeben werden.

Die hessische Polizei erfaßt im Gegensatz zu ihren Kollegen in anderen Bundesländern bereits seit geraumer Zeit Daten in der „L- Gruppe". Sie hat mir auf meine Bitte hin sämtliche in der zweiten Augusthälfte 1988 erfaßten Personenbeschreibungsdaten zur Überprüfung übermittelt. Das Ergebnis meiner Überprüfung habe ich dem Hessischen Innenministerium mit der Bitte um Stellungnahme zugeleitet. Deren Inhalt bleibt abzuwarten. Aber schon die Konzeption dieser Datengruppe stößt auf nicht unerhebliche Bedenken.

Die „L-Gruppe" umfaßt folgende Datenfelder:

„Gestalt, Größe, scheinbares Alter, äußere Erscheinung, körperliche Merkmale, Tätowierungen, Stimme/Sprachmerkmale, Mundart, Fremdsprache, andere personenbezogene Merkmale und Sondervermerke."

Im Datenfeld „Gestalt" kann eine Schlüsselziffer eingegeben werden, die für „schlank", „dick", „vollbusig", „flachbrüstig", „kräftig" oder „schwächlich" steht. Die Größe wird entweder in Zentimetern oder als „auffallend klein" bzw. „auffallend groß" angegeben. In dem Feld „scheinbares Alter" wird eine Jahresangabe gespeichert. Für die „äußere Erscheinung" sind Schlüssel zu den Merkmalen „asiatisch", „negroid", „nordländisch", „orientalisch", „südländisch" oder „slawisch" vorgesehen. Sie sollen einer groben typenmäßigen Zuordnung dienen. Zu dem Datenfeld „körperliche Merkmale" gibt es zwei Datenkataloge. Zum einen wird die „Lagebeschreibung" (d. h. der betroffene Körperteil) verschlüsselt, zum anderen wird die „Art des körperlichen Merkmales" hinzugefügt. Zur „Lagebezeichnung" gibt es 78 mögliche Schlüsselwerte, die z. B. für „Haar, Wange rechts, Unterlippe, Brust rechts, Genital, Fuß rechts" oder „Zehen links" stehen. Zur „Artbezeichnung körperlicher Merkmale" können 92 mögliche Werte gespeichert werden. Sie stehen z. B. für „Hasenscharte, Mißbildung, Zucken, picklig, pockennarbig, Adlernase" oder „Boxernase".

Bei Tätowierungen wird zunächst der für die „körperlichen Merkmale" vorgesehene Katalog der „Lagebezeichnung" herangezogen. Dann folgt ein Katalog von 54 möglichen Angaben zum Motiv der Tätowierung, z. B. „Blume, Seefahrermotiv, Meerjungfrau, Krone" oder „sexuelles Motiv". Im Datenfeld „Stimme/Sprachmerkmale" sind folgende Angaben möglich: „sehr hoch, sehr tief, belegt/heiser, näselt/nuschelt, stottert/stammelt, lispelt, stumm, laut, leise, schnell, langsam" und „sonstige Merkmale". Das Datenfeld „Mundart" kann 32 mögliche Bezeichnungen enthalten, z. B. „hochdeutsch, rheinisch, hessisch, pommersch, thüringisch, pfälzisch-hessisch" oder „alemannisch". Aus dem Datenfeld „Fremdsprache" werden Schlüsselwerte für die Angabe von Fremdsprachen erkennbar. Unter „anderen personengebundenen Merkmalen" werden solche Angaben gemacht, die nicht in die vorherigen Felder eingetragen werden können. Hierzu gehören z. B. „Besonderheiten der Bekleidung, auffällige Verhaltensweisen, Inschriften von Tätowierungen" sowie „markante mitgeführte Gegenstände". Unter „Sondervermerk" können in freier Form weitere ergänzende Angaben gespeichert werden, z. B. „besondere Liebhabereien, auffällige Schreib- oder Sprechgewohnheiten, Gesichtsform, Frisur usw".

3.3.2
Bewertung des Speicherungskonzepts und der Verwertungspraxis

Sicherlich gibt es ein legitimes Bedürfnis der Polizei, ihr bekannte oder auch unbekannte Täter in den eigenen Informationssystemen so exakt zu beschreiben, daß eine eindeutige Identifikation möglich ist. Bei bekannten Tätern lassen dies freilich schon die erkennungsdienstlichen Maßnahmen zu. Bei unbekannten Tätern fehlen solche exakten Angaben wie Fotos, Fingerabdrücke oder körperliche Messungen. Für beide Fallgruppen gibt es möglicherweise, abgesehen von erkennungsdienstlichen Informationen, ein Bedürfnis, auch über andere äußere und auffallende Merkmale, eine Person schnell zu erkennen. Das Konzept der „L-Gruppe" im polizeilichen Datenverarbeitungssystem INPOL von Bund und Ländern erlaubt mit ihren verschiedenen Merkmalstypen und den dazugehörenden Eigenschaftskatalogen zweifellos eine detaillierte Beschreibung überwiegend objektiv feststellbarer Merkmale. Die zusätzlichen Freitextfelder, aber auch eine Reihe von weniger exakten Merkmalen, dienen der Abrundung des Bildes der betroffenen Person.

Nach dem Übereinkommen, das die Polizeibehörden des Bundes und der Länder zur „L-Gruppe" getroffen haben, wird ein möglichst umfassendes und exaktes Bild der betroffenen Person angestrebt. Abwägungen oder auch Einschränkungen bei der Erfassung von Einzelmerkmalen etwa im Hinblick auf die Eigenart bestimmter Delikte oder die Bedeutung der Einzeltat sind nicht vorgesehen. Aus der Sicht des Datenschutzes entsteht dadurch ein Defizit. Sowohl die mögliche Vollständigkeit der Personenbeschreibung als auch die Feststellung von einzelnen Merkmalen, die den Betroffenen als mit körperlichen oder geistigen Mängeln behaftete Persönlichkeit qualifizieren, können auch und gerade angesichts der Zugriffsmöglichkeiten durch alle hessischen Polizeidienststellen unangemessen in das Recht auf informationelle Selbstbestimmung des einzelnen eingreifen. Die Kritik bezieht sich vor allem auf folgende Punkte:

- Die Merkmale der Personenbeschreibung müssen nachprüfbar sein. Eigenschaften, die nur eingeschränkt objektiv wahrgenommen werden können, scheiden deshalb aus. Auszugehen ist dabei von der Fähigkeit des Polizeibeamten, das Merkmal zu erkennen und in das vorgegebene Raster einzupassen. Es ist z. B. fraglich, ob eine Qualifizierung der

äußeren Erscheinung als „nordländisch" oder „slawisch" möglich oder sinnvoll ist. Ganz abgesehen von der politischen Fragwürdigkeit dürfte auch die Einordnung als „negroid" oder „orientalisch" im Einzelfall schwerfallen. Die Aussagefähigkeit dieses Datenfeldes muß deshalb überprüft werden.

Problematisch ist auch ein Merkmalskatalog, der den mit der Einordnung befaßten Polizeibeamten als Sprachforscher bemüht. Dies gilt insbesondere für die Zuordnung der Mundart. Ob jemand friesisch, ostfriesisch, holsteinisch oder niedersächsisch (gibt es für Niedersachsen überhaupt eine einheitliche Mundart?) spricht, dürfte gerade im Einzelfall umstritten sein. Auch eine westdeutsche oder nordfränkische Mundart dürfte bislang noch kein Sprachforscher entdeckt haben. Wenn nicht der Polizeibeamte der entsprechenden Region, so wird doch eine Vielzahl seiner Kollegen aus dem gerade nicht betroffenen Gebiet durch einen derart detaillierten Schlüssel überfordert sein. Damit ergeben sich aber Zweifel an diesem Katalog. Das Gebot, nur richtige und exakte Daten in einem polizeilichen Informationssystem zu erfassen, steht im Widerspruch zu der Qualität des Mundartenkatalogs.

- Merkmale einer Personenbeschreibung, in die eine subjektive Bewertung weitgehend einfließt, sind insofern problematisch, als der Betroffene nicht richtig bezeichnet wird. Ob „schlank" oder „schwächlich", ob „dick" oder „vollbusig" oder auch nur „kräftig", der Erkenntnisgehalt solcher Merkmale ist anzuzweifeln. Da der Betroffene ein Recht auf eine richtige Erfassung seiner Erscheinungsmerkmale hat, stößt auch diese Differenzierung auf Kritik.

- Von größerer Bedeutung sind Bedenken gegenüber Merkmalen, mit denen eine Wertung verbunden ist. Mit den Eigenschaften „pockennarbig, fliehende Stirn, Basedow-Augen, Boxernase, Knollennase, Rauchergebiß, Kropf, stottert, stammelt, näselt, nuschelt" verbindet der Sprachgebrauch oft auch eine Bewertung der Persönlichkeit des Betroffenen. Diese Merkmale können als abwertend empfunden werden. Ihre Erfassung und Einspeicherung im System ist deshalb nicht unproblematisch. Wann immer auch eine solche Qualifizierung als notwendig erscheint, eine Abwägung zwischen dem für den Betroffenen negativen Bewertungsgehalt einerseits und dem Bedürfnis für die polizeiliche Arbeit andererseits ist unabdingbar. Mit anderen Worten: Die Erfassung solcher Merkmale sollte die Ausnahme sein, da der Betroffene mit dieser Qualifizierung zweifellos belastet wird. Die Schwere des Eingriffs in das Persönlichkeitsrecht des Betroffenen erfordert auch und gerade angesichts der landesweiten Zugriffsmöglichkeiten einen Kriterienkatalog für die Vergabe solcher Merkmale, soweit an ihnen überhaupt festgehalten wird.

Im besonderen Maße problematisch kann auch die Erfassung objektiver Merkmale dann werden, wenn die Details so umfassend zusammengetragen werden, daß daraus ein deutlich negatives Gesamtbild der Persönlichkeit entsteht. Der einzelne empfindet dies schließlich zu Recht als Verletzung seiner persönlichen Würde. Dies gilt insbesondere für die geradezu akribische Systematisierung und Erfassung von Tätowierungen. Nicht nur der jeweilige Körperteil, sondern auch die einzelnen Motive werden durch den umfassenden Katalog so zusammengefügt, daß im Einzelfall geradezu ein Oberflächenbild des Betroffenen vor den Augen des Systembenutzers erscheint. Auch wenn aus der Sicht der Polizei jede Tätowierung wegen ihrer Unveränderbarkeit einen unschätzbaren Gewinn für die Eindeutigkeit der Identifikation verspricht, so muß doch dieses Ziel bestimmte Grenzen beachten. Die Totalerfassung einer Vielzahl von Motiven auf der gesamten Körperoberfläche eines Menschen in Verbindung mit weiteren Merkmalen über Gestalt, äußere Erscheinung und evtl. noch ergänzt um entsprechende Freitextzusätze kann das Bild einer debilen, kriminellen und umfassend negativen Persönlichkeit eines einzelnen zeichnen; der Betroffene wird so unwiderruflich gebrandmarkt.

Maßstab für die Vergabe von Merkmalen der „L-Gruppe" ist insbesondere das verfassungsrechtlich begründete Verhältnismäßigkeitsprinzip. Denkbar wäre es, auch über einen konkreten Hinweis auf bestimmte Deliktsgruppen Einschränkungen vorzunehmen, die die Würde der Betroffenen stärker respektieren. In der Form, wie die Erfassung in der „L-Gruppe" bisher betrieben wird, entspricht sie jedenfalls nicht den Vorgaben des Persönlichkeitsschutzes.

4. Justiz

4.1
Zentrale Namensdateien bei den Staatsanwaltschaften

Die Staatsanwaltschaften führen zu den Strafakten sogenannte Zentrale Namensdateien. Darin sind registriert: Name des Beschuldigten, Geburtsdatum, Anschrift, Aktenzeichen, Delikte und evtl. weitere Bearbeitungshinweise. Auf dieses ihrer Meinung nach unverzichtbare Hilfsmittel werden die Staatsanwaltschaften jedoch möglicherweise bald verzichten müssen. Denn wenn der Bundesgesetzgeber nicht in kurzer Zeit, genauer bis 1990, tätig wird, müssen die Zentralen Namensdateien der Staatsanwaltschaften in Hessen gelöscht werden.

Das folgt aus einem Beschluß des Oberlandesgerichts Frankfurt vom 14. Juli 1988 (Aktenzeichen: 3 VAs 4/88). Darin stellt das Gericht unmißverständlich klar, daß die Datenspeicherung in den Zentralen Namensdateien ein Eingriff in das informationelle Selbstbestimmungsrecht der Betroffenen ist, für den derzeit die erforderliche Rechtsgrundlage fehlt und der deshalb unzulässig ist.

Eine Absage erteilt der 3. Senat des Oberlandesgerichts insbesondere der Ansicht der Staatsanwaltschaft, als gesetzliche Grundlage reiche § 152 Strafprozeßordnung aus, in dem es heißt: „Zur Erhebung der öffentlichen Klage ist die Staatsanwaltschaft berufen. Sie ist, soweit nicht gesetzlich ein anderes bestimmt ist, verpflichtet, wegen aller verfolgbaren Straftaten einzuschreiten, sofern zureichende tatsächliche Anhaltspunkte vorliegen." Der Vorschrift, so der Beschluß, sei nicht zu entnehmen, unter welchen Voraussetzungen personenbezogene Daten überhaupt gespeichert

werden dürften. Regelungen über eine zweckgebundene Datenverarbeitung fehlten ebenso wie Aufklärungs-, Auskunfts- und Löschungspflichten. Wie eine verfassungskonforme gesetzliche Regelung aussehen könne, ließen dagegen die vorliegenden Arbeitsentwürfe des Bundesjustizministeriums für eine Novellierung der Strafprozeßordnung erkennen.

Das Gericht akzeptiert mit Recht auch nicht das Hessische Datenschutzgesetz als ausreichende gesetzliche Ermächtigung der Staatsanwaltschaften, für Strafverfolgungszwecke personenbezogene Daten zu verarbeiten, sondern verlangt vielmehr präzise bereichsspezifische gesetzliche Bestimmungen.

Bemerkenswert ist außerdem, daß das Oberlandesgericht diese Anforderungen keineswegs nur für die automatisierte Datenverarbeitung gelten läßt, sondern ausdrücklich auch auf die manuelle Verarbeitung personenbezogener Daten bezieht.

Bei unzulässiger Datenverarbeitung läßt das Hessische Datenschutzgesetz der datenverarbeitenden Stelle keine Handlungsalternative: Die Daten müssen gelöscht, neue Daten dürfen nicht erhoben und gespeichert werden (§ 19 Abs. 4). Soweit wollte aber das OLG im Augenblick noch nicht gehen. Unter Berufung auf die Rechtsprechung des Bundesverfassungsgerichts gewährt es mit Rücksicht auf die andernfalls gefährdete Funktionsfähigkeit der Staatsanwaltschaft dem Gesetzgeber eine Frist für die Schaffung einer ausreichenden gesetzlichen Grundlage. Diese Übergangszeit, in der der Betroffene hinnehmen muß, daß seine Daten auch ohne ausreichende Rechtsgrundlage verarbeitet werden, läuft nach Ansicht des Gerichts mit dem Ende der Legislaturperiode des Bundestags, d. h. 1990, aus. Wörtlich heißt es in dem Beschluß: „Eine noch längere Fristsetzung erscheint nach derzeitigen Erkenntnissen unter Berücksichtigung der schon geleisteten gesetzgeberischen Vorarbeiten nicht erforderlich."

Der Beschluß konnte eigentlich nicht überraschen. Er liegt auf der Linie der Entscheidungen, die bereits eine Reihe anderer Gerichte im Zusammenhang mit der Verarbeitung personenbezogener Daten für Strafverfolgungszwecke getroffen haben, etwa zur Speicherung von Kriminalakten bei den Polizeibehörden, der Aufbewahrung erkennungsdienstlicher Unterlagen bei Polizeidienststellen und zur Frage der Mitteilungen in Strafsachen durch die Staatsanwaltschaft an standesrechtliche Aufsichtsbehörden oder den Dienstherrn eines Beamten. Es ist also keineswegs das erste Mal, daß ein Gericht die Datenverarbeitung für Strafverfolgungszwecke wegen Fehlens einer ausreichenden gesetzlichen Regelung für rechtswidrig erklärt. Neu ist dagegen, daß eine derartige Entscheidung rechtskräftig geworden ist, und das hat für Hessen schwerwiegende Konsequenzen: Sollte der Bundestag nicht bis zum Ablauf der Legislaturperiode für die staatsanwaltlichen Zentralen Namensdateien eine ausreichende gesetzliche Grundlage geschaffen haben, ist die Löschung dieser Dateien im Zuständigkeitsbereich des OLG Frankfurt, d. h. bei allen hessischen Staatsanwaltschaften, unausweichlich. Die Weiterführung der Dateien müßte ich formal beanstanden, darüber hinaus hätte jeder, dessen Daten in der Zentralen Namensdatei gespeichert sind, einen Rechtsanspruch auf Löschung und könnte natürlich diesen Anspruch – wenn er nicht erfüllt wird – auch gerichtlich geltend machen. Es braucht nicht viel Phantasie, um sich die Prozeßflut, die hier entstehen könnte, auszumalen.

4.2
Reform der Strafprozeßordnung

4.2.1
Neue Regelungsvorschläge

Die Reform der Strafprozeßordnung ist nach den Maßstäben des Bundesverfassungsgerichtsurteils zur Volkszählung 1983 sicherlich eines der wichtigsten Gesetzesvorhaben des Bundes zur Verwirklichung eines bereichsspezifischen Datenschutzes. Das bestätigen mittlerweile etliche Gerichtsentscheidungen, insbesondere auch der unter Ziff. 4.1 erläuterte Beschluß des Oberlandesgerichts Frankfurt. Bereits 1986 hatte das Bundesjustizministerium einen „Arbeitsentwurf eines Gesetzes zur Regelung der rechtlichen Grundlagen für Fahndungsmaßnahmen, Fahndungshilfsmittel und für die Akteneinsicht im Strafverfahren" vorgelegt, in dem Vorschläge zur Regelung der Rasterfahndung, der Ausschreibung zur Festnahme und dem Erlaß eines Steckbriefs, der polizeilichen Beobachtung, der „planmäßigen Überwachung" (Observation) sowie der Ermittlungen und Auskunftsverlangen der Staatsanwaltschaften gegenüber öffentlichen Behörden enthalten waren (vgl. hierzu auch 15. Tätigkeitsbericht, Ziff. 5.2). Dieser Entwurf ist in der Zwischenzeit mehrfach verändert und ergänzt worden. Neu hinzugekommen sind Vorschläge für die Speicherung, Nutzung und Übermittlung personenbezogener Daten durch die Strafverfolgungsbehörden. Geändert worden sind insbesondere die vorgesehenen Bestimmungen für die Akteneinsicht im Strafverfahren.

4.2.2
Einzelne Vorschläge

4.2.2.1
Rasterfahndung

Auch die neue Fassung enthält eine Bestimmung für Rasterfahndungen. Danach kann die Polizei zur Aufklärung bestimmter schwerwiegender Delikte von privaten oder öffentlichen Institutionen in größerem Umfang Daten solcher Personen anfordern, die „bestimmte, nach Lage des konkreten Falls auf den vermutlichen Täter zutreffende und für die Ermittlungen bedeutsame Prüfungsmerkmale erfüllen". Die Polizei soll maschinell die Daten entweder mit eigenen Datenbeständen abgleichen oder aber rastermäßig bestimmte Datensätze herausfiltern, „um Nichtverdächtige

auszuschließen oder solche Personen festzustellen, die weitere für die Ermittlungen bedeutsame Prüfungsmerkmale erfüllen". Wesentliches Merkmal der Rasterfahndung ist damit die Übermittlung einer Vielzahl von Datensätzen auch Unbeteiligter, um stufenweise den Kreis der möglichen Täter einzuengen.

Nach dem alten Entwurf sollte die Polizei die Rasterfahndung bei den in § 163 d Strafprozeßordnung aufgezählten Straftaten einsetzen dürfen (die Vorschrift regelt die sog. Schleppnetzfahndung). Die Kritik des 15. Tätigkeitsberichts (Ziff. 5.2.2.1) an dieser Regelung gilt in gleichem Maße für den neuen Entwurf. Auch die Neufassung bestimmt nicht ausreichend klar, in welchen Fällen die Polizei die personenbezogenen Daten von tausenden von Bürgern durchforsten darf, um möglicherweise einen Täter zu finden. Es ist außerdem wiederum nicht geprüft worden, ob die erfaßten Straftaten allesamt so schwer sind, daß sie einen solchen Eingriff wie die Rasterfahndung verhältnismäßig erscheinen lassen.

§ 100 a Satz 1 Nr. 3, 4 StPO ist anstelle des § 163 d erwähnt, der selbst allerdings auf diese Bestimmung verweist. Lediglich der in § 163 d enthaltene Hinweis auf § 111 StPO wäre damit gegenstandslos. Um dem zu entgegnen, hat das Bundesjustizministerium jedoch einen neuen Katalog in die Vorschrift eingefügt, der im Ergebnis zu einer noch umfassenderen Liste an Tatbeständen führt als im früheren Entwurf. Mit anderen Worten: Bei genauer Prüfung ergibt sich, daß die auf den ersten Blick zu vermutende Einschränkung in Wirklichkeit eine Ausweitung ist.

Auch die sogenannte Subsidiaritätsregelung, die die Rasterfahndung nur dann zulassen sollte, wenn auf andere Weise eine Ergreifung des Täters oder die Aufklärung der Straftat „aussichtslos oder wesentlich erschwert wäre", wurde aufgeweicht. Schon dann, wenn die Erreichung dieses Ziels mit anderen Maßnahmen „wesentlich erschwert wäre oder diese erheblich weniger Erfolg versprechen", darf die Rasterfahndung angewandt werden. Der immer wieder zu hörende Hinweis, die Rasterfahndung sei gar kein schwerwiegender Eingriff, da der stufenweise Filterungsprozeß dazu führe, daß die meisten Betroffenen trotz der Übermittlung ihrer Datensätze gar nicht beeinträchtigt würden, überzeugt nicht. Schließlich birgt dieses Verfahren gerade die Gefahr, daß Unbeteiligte aufgrund bestimmter, mit der Straftat nur mittelbar und eher abstrakt in Verbindung stehender Merkmale mit Ermittlungsmaßnahmen überzogen werden. Deshalb wäre es richtig, an der früheren Formel festzuhalten, die im übrigen in § 100 a StPO (Überwachung des Fernmeldeverkehrs) ein bewährtes Modell hat.

Positiv ist hingegen der neue Vorschlag, daß die durch die Rasterfahndung gewonnenen Daten lediglich für Zwecke der Strafverfolgung verwendet werden dürfen. Dies soll im übrigen auch für die Daten, die aus der Überwachung des Fernmeldeverkehrs gewonnen werden, gelten. Eine Verbesserung ist sicherlich auch der Vorschlag, daß sogenannte Zufallsfunde im Rahmen der Rasterfahndung zu anderen Zwecken nur verwendet werden dürfen, wenn dies zur Aufklärung einer anderen in § 100 a bezeichneten Straftat oder zu der Ergreifung des Täters einer solchen Tat notwendig ist.

4.2.2.2
Ausschreibung zur Festnahme und Erlaß eines Steckbriefs

Wie der alte Entwurf sieht auch der neue vor, daß nicht nur der Richter, sondern auch Staatsanwaltschaft und Polizei Steckbriefe erlassen können. Diese Maßnahme muß jedoch allein dem Richter vorbehalten bleiben, denn zum einen kann sie dem Betroffenen erhebliche Nachteile bringen, und zum anderen dürfte sie kaum jemals so eilbedürftig sein, daß Polizei oder Staatsanwaltschaft sie treffen müßten. Der Entwurf läßt außerdem offen, bei welchen Delikten ein Steckbrief ausgestellt werden darf. Lediglich für die sogenannte „Öffentlichkeitsfahndung" auch mit Hilfe der Medien verlangt der Entwurf eine „Straftat mit erheblicher, namentlich mit überörtlicher Bedeutung". Freilich bleibt völlig offen, welche Delikte man sich darunter vorzustellen hat.

4.2.2.3
Akteneinsicht der Behörden

Entgegen dem früheren Entwurf erhalten nach der neuen Fassung nicht nur Gerichte, Staatsanwaltschaften und andere Justizbehörden, sondern unter besonderen Voraussetzungen auch andere Behörden Einsicht in Strafverfolgungsakten. Datenschutzrechtlich ist dies zweifellos eine wesentliche Verschlechterung. Bei der Akteneinsicht können in der Regel über den erforderlichen Umfang hinaus auch andere Daten zur Kenntnis genommen werden, was bei einer Auskunft nicht der Fall ist. Sicher, die Auskunft ist für die abgebende Behörde mit mehr Arbeit verbunden. Das Regel-Ausnahmeverhältnis sollte jedoch in jedem Fall umgekehrt sein: Grundsätzlich sollten andere Behörden nur Auskunft und lediglich in besonders begründeten Ausnahmefällen auch Akteneinsicht erhalten.

4.2.2.4
Akteneinsicht des Betroffenen

Die Bürger müssen „wissen können, wer was wann und bei welcher Gelegenheit über sie weiß", so das Bundesverfassungsgericht im Volkszählungsurteil von 1983 (BVerfGE 65, 43). Deshalb ist das Akteneinsichtsrecht, das auch die Neufassung dem Betroffenen gewährt, unverzichtbar. Grundsätzlich muß dieser allerdings einen Rechtsanwalt einschalten, nur wenn für die Behörde damit kein höherer Arbeitsaufwand verbunden ist, kann er selbst unmittelbar Auskünfte erhalten.

4.2.2.5
Nutzung der aus einem Strafverfahren gewonnenen Informationen durch die Polizeibehörden

Auch wenn man darüber diskutieren kann, ob Bundesgesetzgeber oder Landesparlamente hier die Gesetzgebungskompetenz haben, eines dürfte unstreitig sein: Es muß gesetzlich geregelt werden, in welchem Umfang die Polizeibehörden aus dem Strafermittlungsverfahren gewonnene personenbezogene Daten nicht nur für die Aufklärung, sondern auch die Verhütung von Straftaten und die allgemeine Gefahrenabwehr nutzen dürfen.

Das Bundesjustizministerium schlägt in seinem neuesten Entwurf eine Regelung vor, wonach die Polizei personenbezogene Informationen aus einem Strafverfahren „zur Abwehr einer Gefahr für die öffentliche Sicherheit oder Ordnung nach Maßgabe der Polizeigesetze" verwenden darf. Die Regelungskompetenz des Bundesgesetzgebers für eine solche Öffnungsklausel dürfte kaum zweifelhaft sein. Die Klausel würde sicherlich für größere Klarheit sorgen, auch wenn sie nicht genau erkennen läßt, ob damit auch die Verwendung für Zwecke der vorbeugenden Straftatenbekämpfung gemeint ist.

4.2.2.6
Rückmeldung über den Stand des Verfahrens durch die Staatsanwaltschaft an die Polizeibehörde

Ein datenschutzrechtlicher Fortschritt wäre die vom Bundesjustizministerium vorgeschlagene StPO-Vorschrift, die an Stelle der bisherigen Nr. 11 der „Anordnung über Mitteilungen in Strafsachen" (MiStra), einer Verwaltungsvereinbarung der Landesjustizverwaltungen und des Bundesjustizministeriums, treten soll (vgl. hierzu auch 16. Tätigkeitsbericht, Ziff. 11.1). Mit dieser Vorschrift soll gewährleistet werden, daß die Polizeibehörden insbesondere über den Ausgang des Strafverfahrens informiert werden, um ihre Datenspeicherungen an das Ergebnis anzupassen.

4.2.2.7
Speicherung personenbezogener Informationen in Dateien durch Strafverfolgungsbehörden, Gerichte und Vollstreckungsbehörden

Deutlicher noch als früher kommt nun in der neuen Fassung zum Ausdruck, daß auch die Speicherung und Nutzung von Daten in Dateien an den Erforderlichkeitsgrundsatz gebunden ist.

Unklar bleibt hingegen die Konsequenz aus dem Satz: „Die Informationen können in einer zentralen Datei gespeichert werden." Wer diese Datei führen soll, welchen Umfang sie hat und welche Verwendungsmöglichkeiten damit verbunden sind, bleibt völlig offen.

Offen bleibt auch, wie besondere, vor allem in jüngster Zeit verstärkt genutzte Dateiformen, wie etwa die sogenannten Spurendokumentationsdateien (Spudok-Dateien), eingesetzt werden sollen. Diese Dateien, die als Instrumente der „Verdachtsverdichtung" dienen, und in die auch eine Vielzahl zunächst nicht überprüfter Daten aufgenommen werden, um diese dann sukzessive, aber doch mit erheblicher zeitlicher Verzögerung auf ihren Wahrheitsgehalt zu überprüfen, bedürfen einer besonderen Regelung. Darin ist festzuhalten, für welche Deliktsbereiche oder Vorgehensweisen von Straftätern solche Dateien eingesetzt werden können. In der früheren Fassung war wenigstens die sukzessive Überprüfung von Spureninformationen einschließlich der Löschung nicht erforderlicher Informationen vorgeschrieben. Unverständlich ist, daß der neue Entwurf auf diese Vorgaben verzichtet. Ein Regelungsdefizit ist auch für die sogenannten Falldateien festzustellen, die verfahrensübergreifend bestimmte Falltypen betreffen. Mit anderen Worten: Die vorgesehene Vorschrift zur Datenspeicherung in Dateien reicht bei weitem nicht aus, um den verschiedenartigen Informationssystemen gerecht zu werden.

4.2.2.8
Weiterverwendung von Daten aus einem Strafverfahren „zur Vorsorge für künftige Strafverfolgung"

Mit dieser Vorschrift, die eine Speicherung von Hinweisen auf Akten und darüber hinaus von Daten zur Identifizierung von Personen durch die Strafverfolgungsbehörden nach Abschluß von Strafverfahren zuläßt, wird der Konflikt mit den in den Entwürfen zu den Länderpolizeigesetzen enthaltenen Regelungen deutlich. Hier beansprucht der Bundesgesetzgeber eine Kompetenz zur Regelung von Befugnissen, die in den Ländern als „Vorbeugung von Straftaten" in den Entwürfen zu den Polizeigesetzen detailliert geregelt werden.

Gegenüber den Regelungen in den Polizeigesetzentwürfen der Länder ist der Vorschlag des Bundesjustizministeriums zweifellos die bessere Lösung. Er läßt eine weitere Speicherung nur zu, soweit „unter Berücksichtigung der Persönlichkeit des Beschuldigten, der Art oder Ausführung der Tat, sonstiger Erkenntnisse oder kriminalistischer Erfahrungen zu besorgen ist, daß der Beschuldigte eine weitere Straftat begehen wird". Erforderlich ist somit eine Einzelfallüberprüfung einschließlich einer Prognose über das weitere Verhalten des Betroffenen. Dem steht allerdings die bisherige und auch nach den Polizeigesetzentwürfen vorgesehene Praxis entgegen, nach der pauschal und in jedem Fall eine Weiterspeicherung stattfindet.

Der Entwurf überläßt es den Bundesministerien der Justiz bzw. des Innern und den Landesregierungen, für ihren jeweiligen Geschäftsbereich durch Rechtsverordnungen die näheren Einzelheiten über Art und Umfang der Daten, die zur „Vorsorge für die künftige Strafverfolgung gespeichert werden dürfen", zu regeln.

4.2.2.9
Datenübermittlung

Unverständlich ist, warum der Entwurf den Datenaustausch zwischen Strafverfolgungsbehörden, Strafgerichten, Vollstreckungsbehörden und Gnadenbehörden nicht an das Erforderlichkeitsprinzip bindet, sondern lediglich eine allgemeine Übermittlungsbefugnis vorsieht.

5. Gesundheit

5.1
Hessisches Krankenhausgesetz

Nach wie vor fehlen spezielle gesetzliche Vorschriften für die Verarbeitung der Patientendaten in den hessischen Krankenhäusern. An mangelnden Vorschlägen kann es allerdings nicht liegen, denn bereits Ende 1985 habe ich dem Hessischen Sozialministerium ein Regelungskonzept für die Datenverarbeitung im Krankenhaus unterbreitet (vgl. Ziff. 4.1.2 des 15. Tätigkeitsberichts). Mit Inkrafttreten des neuen Hessischen Datenschutzgesetzes am 1. Januar 1987 sind bereichsspezifische Bestimmungen für die Verarbeitung von Patientendaten in Krankenhäusern noch dringlicher geworden: Da die Krankenhäuser als öffentlich-rechtliche Wettbewerbsunternehmen qualifiziert werden, gelten für sie – soweit sie Behandlungsaufgaben wahrnehmen – immer noch die Vorschriften des Bundesdatenschutzgesetzes über den privaten Bereich (vgl. § 3 Abs. 7 HDSG). Das Bundesdatenschutzgesetz ist jedoch bis heute noch nicht an die Vorgaben der Rechtsprechung des Bundesverfassungsgerichts zum informationellen Selbstbestimmungsrecht angepaßt. Damit unterliegen ausgerechnet die besonders sensitiven Patientendaten der Krankenhäuser einem geringeren gesetzlichen Schutz als z. B. die Hundesteuerdaten. Dies kann nicht länger akzeptiert werden. Der verstärkte Ausbau der klinischen Krebsregister erfordert ebenfalls dringend präzise Vorschriften für die Datenverarbeitung in den Krankenhäusern (vgl. auch Ziff. 5.3). Darüber hinaus lassen die vielen Anfragen, die ich aus den Krankenhäusern erhalten habe, erkennen, daß die gegenwärtig notwendige parallele Anwendung von Vorschriften des Bundesdatenschutzgesetzes (soweit die Krankenhäuser Behandlungsaufgaben wahrnehmen) und des Hessischen Datenschutzgesetzes (soweit es um Arbeitnehmerdatenschutz oder um Forschungstätigkeit geht) in der Praxis große Schwierigkeiten bereitet.

Im März 1988 hatte mir das Sozialministerium einen neuen Entwurf für Datenverarbeitungsregelungen im Hessischen Krankenhausgesetz zur Stellungnahme übersandt. Die Vorschriften waren jedoch zum Teil nicht nur zu pauschal, sondern widersprachen auch dem neuen Hessischen Datenschutzgesetz. In meinem Änderungsvorschlag habe ich daraufhin empfohlen, die Krankenhäuser grundsätzlich in den Anwendungsbereich des Hessischen Datenschutzgesetzes aufzunehmen und darüber hinaus folgende Sonderregelungen zu treffen:

- Datenübermittlungen

  Die Übermittlung von Patientendaten an Personen oder Stellen außerhalb des Krankenhauses ohne Einwilligung des Betroffenen ist abweichend von den Bestimmungen des HDSG nur zulässig, wenn sie erforderlich ist zur Erfüllung des Behandlungsvertrages oder für die Durchführung einer Mit- und Nachbehandlung, zur Abwehr einer gegenwärtigen Gefahr für höherrangige Rechtsgüter, zur Unterrichtung von Angehörigen und zur Erfüllung gesetzlicher Behandlungs- und Mitteilungspflichten, zur Durchsetzung von Ansprüchen aus dem Behandlungsvertrag und schließlich für die Sozialleistungsträger zur Feststellung der Leistungspflicht, zur Abrechnung und zur Überprüfung der Wirtschaftlichkeit, soweit letzteres gesetzlich vorgesehen ist.

  Auf eine vom HDSG abweichende präzise Regelung der Übermittlung von Patientendaten kann nicht verzichtet werden, weil die Übermittlung eine der einschneidendsten Gefährdungssituationen für das informationelle Selbstbestimmungsrecht der Patienten darstellt. Hier stellen sich auch in der Praxis die schwierigsten Anwendungsprobleme, so daß klare Vorgaben für die Mitarbeiter des Krankenhauses notwendig sind.

- Interne Datenverarbeitung des Krankenhauses

  Die Regelungen für Datenübermittlungen an Stellen oder Personen außerhalb des Krankenhauses müssen in Krankenhäusern mit Behandlungseinrichtungen verschiedener Fachrichtungen (Fachabteilungen) auch zwischen diesen gelten. Damit wird noch einmal eindeutig klargestellt, was sich bereits aus dem Hessischen Datenschutzgesetz ergibt, daß nämlich in bezug auf die personenbezogenen Patientendaten das Krankenhaus keine informationelle Einheit ist und deshalb eine Fachabteilung nicht beliebig auf Patientendaten einer anderen zugreifen darf.

- Zweckbindung der Patientendaten auch beim Empfänger

  Personen oder Stellen, die Patientendaten erhalten haben, dürfen diese nur zu dem Zweck verwenden, zu dem sie ihnen befugt übermittelt worden sind. Im HDSG ist eine derart strikte Zweckbindung nur für private Datenempfänger vorgesehen (§ 16 Abs. 2). Öffentliche Stellen dagegen dürfen die erhaltenen personenbezogenen Daten für eine Vielzahl anderer Zwecke verwenden (§ 12 Abs. 2 HDSG). Wegen der besonderen Sensitivität müssen jedoch auch Patientendaten, die an öffentliche Stellen übermittelt wurden, einer strikten Zweckbindung unterliegen.

- Auskunftsrecht der Patienten

  Für das Recht des Patienten auf Auskunft und auf Einsicht in seine Krankenakte gilt § 18 HDSG. Die in § 18 Abs. 1 Satz 1 Nr. 3 enthaltene Beschränkung, wonach nur über die Empfänger regelmäßiger Übermittlungen Auskunft zu geben ist, sollte jedoch für die Krankenhäuser nicht übernommen werden. Für den Patienten ist es in vielen Fällen wichtiger, zu erfahren, wer in einem bestimmten Einzelfall Angaben über ihn erhalten hat. Die Einbeziehung aller Datenempfänger in den Auskunftsanspruch entspricht auch der Rechtslage in den anderen Bundesländern mit bereichsspezifischen Datenschutzregelungen für Krankenhäuser (so z. B. Art. 26 Abs. 3 Satz 1 Bayerisches Krankenhausgesetz).

  Das Krankenhaus kann die Auskunft sowie die Einsichtnahme in die Krankenakte durch einen Arzt vermitteln lassen, soweit dies mit Rücksicht auf den Gesundheitszustand des Patienten erforderlich ist. Auskunfts- und Einsichtsrecht des Patienten werden durch dieses Verfahren allerdings nicht beschränkt, diese Regelung trägt vielmehr den Besonderheiten der medizinischen Daten Rechnung.

- Bestellung eines eigenen Datenschutzbeauftragten

  Für jedes Krankenhaus ist ein Beauftragter für den Datenschutz zu bestellen. Obgleich eine solche Verpflichtung bereits nach dem Hessischen Datenschutzgesetz und dem Bundesdatenschutzgesetz für die Krankenhäuser besteht (vgl. hierzu 16. Tätigkeitsbericht, Ziff. 2.2.2), sollte trotzdem – und zwar weil die Rechtslage derzeit unnötig kompliziert ist – diese Klarstellung in das Hessische Krankenhausgesetz aufgenommen werden. Die Bestellungspflicht für jedes Krankenhaus entspricht im übrigen auch der Regelung anderer Krankenhausgesetze (vgl. z. B. § 36 Abs. 8 Rheinland-Pfälzisches Krankenhausgesetz, § 29 Abs. 8 Saarländisches Krankenhausgesetz). Stellung und Aufgaben des internen Datenschutzbeauftragten ergeben sich aus dem Hessischen Datenschutzgesetz (§ 5 Abs. 2).

Im Dezember 1988 hat mir das Sozialministerium einen überarbeiteten Gesetzentwurf zur Neuordnung des Krankenhauswesens in Hessen (Hessisches Krankenhausgesetz 1989) übersandt. Darin sind meine Regelungsvorschläge für die Verarbeitung von Patientendaten unverändert aufgenommen worden.

5.2
Genetische Analysen

5.2.1
Datenschutz muß frühzeitig berücksichtigt werden

Im Jahr 1988 hat sich die Diskussion über die zunehmenden Möglichkeiten humangenetischer Analysen und die damit verbundenen Chancen und Risiken erheblich intensiviert. Veranlaßt durch den Antrag der SPD-Fraktion betreffend Genomanalyse (Drucks. 12/1185) und den Berichtsantrag der SPD-Fraktion betreffend Genomanalyse zur Täter-Identifikation (Drucks. 12/1840) haben sich auch mehrere Landtagsausschüsse mit diesem Themenbereich beschäftigt. Dabei wurde deutlich: Die bereits existierenden oder noch in der Entwicklung befindlichen revolutionären humangenetischen Analyseverfahren stellen den Datenschutz vor eine Vielzahl neuer Probleme. Gleich, ob es sich etwa um die Durchführung genetischer Analysen im Zusammenhang mit Strafermittlungsverfahren, humangenetischer Beratung, pränataler Diagnostik, Neugeborenen- Screening, Versicherungsverträgen oder Arbeitsverhältnissen handelt, in allen Fällen werden äußerst sensitive personenbezogene Daten verarbeitet.

Bereits der 15. Tätigkeitsbericht (Ziff. 1.4.2) weist darauf hin, daß es nicht angeht, zunächst eine Diskussion über die gleichsam technischen Aspekte der Genomanalyse zu führen und sich um die datenschutzrechtlichen Gesichtspunkte erst später Gedanken zu machen. Beides läßt sich nicht voneinander trennen und kann deshalb auch nicht sukzessiv diskutiert werden. Vielmehr müssen die datenschutzrechtlichen Fragen von Anfang an in die Diskussion einbezogen werden. Dabei kann es – entgegen einem immer wieder auftretenden Mißverständnis – keineswegs nur darum gehen, die mit Hilfe der Genomanalyse gewonnenen Daten vor einem Mißbrauch im konkreten Einzelfall zu schützen bzw. sie generell vor dem Zugriff Unbefugter zu sichern. Konsequenter Datenschutz kann nur dann erreicht werden, wenn die Bedingungen, unter denen die sensiblen und interpretationsbedürftigen genetischen Daten erhoben und verwertet werden dürfen, eindeutig geklärt und festgelegt sind. Dies betont auch die Stellungnahme, die ich im August 1988 vor dem Innenausschuß des Landtags zu den datenschutzrechtlichen Fragen der Genomanalyse abgegeben habe (INA 12/41). Zu Recht weist auch die von allen vier Landtagsfraktionen unterstützte Beschlußempfehlung des Sozialpolitischen Ausschusses zum Antrag der Fraktion der SPD betr. Genomanalyse (Drucks. 12/3664), die Anfang 1989 vom Plenum verabschiedet werden soll, auf die Notwendigkeit einer strikten Beachtung des Datenschutzes bei genomanalytischen Verfahren hin. Auch der Bundesrat hat in seiner Stellungnahme zum EG- Forschungsprogramm zur „prädiktiven Medizin" mit dem Schwerpunkt der Analyse des menschlichen Genoms (Ratsdokument 7929/88) betont, daß die Erforschung des menschlichen Genoms Mißbrauchsmöglichkeiten schaffe, die die Menschenwürde tangieren und Eingriffe in das Persönlichkeitsrecht und die Privatsphäre ermöglichen können. Seiner Auffassung zufolge sind die durch Genomanalyse gewonnenen Daten generell mit dem Risiko verbunden, daß „über die Krankheitsfürsorge hinausgehende Persönlichkeitsinformationen anfallen, die dem Zugriff Dritter unterliegen und für andere als medizinische Zwecke verwendet werden". Hervorgehoben wird vom Bundesrat auch die Gefahr einer Eugenik (Bundesrats-Drucks. 407/88). Ähnlich hat sich der Bundestagsausschuß für Forschung und Technologie in seiner Beschlußempfehlung zu diesem Forschungsprogramm geäußert (Bundestags-Drucks. 11/3555).

Zu den datenschutzrechtlichen Fragen ist gegenwärtig nur eine vorläufige und fragmentarische Einschätzung möglich. Soviel läßt sich jedoch bereits sagen: Die rapide zunehmenden Möglichkeiten der Genomanalyse schaffen die Voraussetzungen für die Gewinnung und Verarbeitung neuer besonders sensibler Daten. Hierbei handelt es sich nicht nur um Informationen, die den konkreten aktuellen Gesundheitszustand der Untersuchten betreffen, sondern immer mehr auch um Informationen über evtl. später ausbrechende Krankheiten und über Dispositionen, deren Stellenwert für die langfristige gesundheitliche Entwicklung der Betroffenen häufig nicht eindeutig bestimmt werden kann. Die mit Hilfe der Genomanalyse gewonnenen Daten betreffen vielfach einen Grenzbereich zwischen Krankheit und Gesundheit. Durch diese Daten werden die Betroffenen dauerhaft etikettiert. Die Erhebung, Kenntnis und Verwendung der Daten kann für sie gravierende Konsequenzen haben.

Die fortschreitende Entwicklung der Genomanalyse bringt die Gefahr mit sich, daß weite Personenkreise – überwiegend gesunde Menschen – ausgegrenzt werden, etwa aus dem Arbeitsleben oder aus sozialen Absicherungsmöglichkeiten, wie z. B. Versicherungsverträgen. Der Aufbau besonders sensibler genetischer Datensammlungen zeichnet sich ab. Die Tatsache, daß die Daten vielfach einen Grenzbereich zwischen Krankheit und Gesundheit betreffen und daß gegenwärtig erhebliche Unsicherheiten hinsichtlich des diagnostischen Stellenwerts bestehen, der ihnen beizumessen ist, lassen eine besonders sorgfältige Reflexion darüber als unerläßlich erscheinen, wann und unter welchen Voraussetzungen und zu welchen Zwecken solche Daten verarbeitet werden sollen. Solange – wie bisher – in vielen Fragen, die die Nutzung der neuen Möglichkeiten der Genomanalyse betreffen, kein gesellschaftlicher Konsens besteht, sondern zum Teil tiefgreifende Meinungsverschiedenheiten vorhanden sind, ist es aus der Sicht des Datenschutzes nicht akzeptabel, sensible genetische Datensammlungen aufzubauen. Denn die Erfahrung zeigt, daß es sehr schwer ist, die Datenverwendung zu beschränken, wenn Datensammlungen erst einmal bestehen.

5.2.2
Regelungsdefizite

5.2.2.1
Polizei, Krankenhäuser, Gesundheitsämter

Besonders dringlich sind spezifische Datenschutzvorschriften in den Bereichen, in denen künftig voraussichtlich in zunehmendem Maße genetische Daten verarbeitet werden. Das gilt für die Polizei (s. Ziff. 3.1.9), die Krankenhäuser (s. Ziff. 5.1) und die Gesundheitsämter. Die Gesundheitsämter sind heute noch auf der Grundlage des als Landesrecht fortgeltenden Gesetzes über die Vereinheitlichung des Gesundheitswesens vom 3. Juli 1934 und den drei dazu ergangenen Durchführungsverordnungen aus dem Jahre 1935 tätig. Dort fehlen klare Aufgaben- und Befugnisregelungen. Diese sind jedoch gerade für die Gesundheitsämter wichtig, da deren Aufgaben sehr vielfältig sind. Die Ämter haben z. B. sowohl Beratungsaufgaben unter freiwilliger Mitwirkung der Betroffenen (z. B. Mütterberatung, Behindertenberatung, Beratung psychisch Kranker, Suchtberatung, künftig möglicherweise in zunehmendem Maße genetische Beratung) als auch hoheitliche Pflichtaufgaben (z. B. nach dem Bundesseuchengesetz). Eine gesetzliche Regelung ist hier im übrigen unabhängig von den Gefahren genetischer Analysen erforderlich. Deshalb hat auch die Konferenz der Datenschutzbeauftragten des Bundes und der Länder in ihrer Sitzung am 27./28. März 1984 gesetzliche Regelungen gefordert, die konkret und detailliert die Verarbeitung personenbezogener Daten im öffentlichen Gesundheitsdienst festschreiben. In anderen Bundesländern liegen zum Teil bereits entsprechende Regelungen vor. So enthält etwa das Bayerische Gesetz über den öffentlichen Gesundheitsdienst – GDG – (Gesetz vom 12. Juli 1986, Bayerisches GVBl. 13/1986) eine Vorschrift über die internen Zweckbindungen der in den Gesundheitsämtern verarbeiteten personenbezogenen Daten.

5.2.2.2
Arbeitnehmerdatenschutz

Regelungsdefizite bestehen im Zusammenhang mit der Genomanalyse vor allem auch im Bereich des Arbeitnehmerdatenschutzes. Durch genetische Analysen können medizinische Untersuchungen auch auf mögliche künftige Erkrankungen ausgedehnt werden und individuelle Dispositionen einbeziehen, die zunächst keinen Krankheitswert haben, aber in Kombination mit anderen Faktoren langfristig unter Umständen zur Entstehung einer Krankheit beitragen können. Hierzu gehört etwa eine besondere Krankheitsanfälligkeit des Arbeitnehmers bei Kontakten mit bestimmten Arbeitsstoffen. Die Gefahren für die Arbeitnehmer hat die Enquete-Kommission des Bundestages in ihrem Bericht (Bundestags-Drucks. 10/6775, Abschnitt C 6.2.3.4) ausführlich beschrieben. Zu nennen ist vor allem die Gefahr, daß immer größere Personenkreise dauerhaft aus dem Erwerbsleben ausgeschieden werden bzw. gar nicht erst ins Erwerbsleben gelangen, daß eine Verlagerung vom objektiven zum subjektiven Arbeitsschutz erfolgt, daß die mit gefährlichen Arbeitsstoffen verbundenen Gesundheitsgefahren durch das Heraussuchen sog. angeblich „resistenter" Arbeitnehmer verharmlost werden, und daß trotz des unsicheren Stellenwerts einer einzelnen genetischen Disposition für die langfristige gesundheitliche Entwicklung des Arbeitnehmers diese im Arbeitsleben eine zentrale Rolle zum Nachteil des Arbeitnehmers erlangen kann, etwa im Sinne einer vorsichtshalber vorgenommenen dauerhaften Ausgrenzung des Arbeitnehmers aus dem Erwerbsleben.

5.2.2.2.1
Einschränkung des Fragerechts des Arbeitgebers

Die vom Bundesarbeitsgericht entwickelten Grundsätze zu den Grenzen des Fragerechts des Arbeitgebers sind kein ausreichender Schutz des Arbeitnehmers vor genetischen Analysen. Das Fragerecht des Arbeitgebers sollte daher

gesetzlich geregelt werden. Dies hat die Enquete-Kommission des Bundestages mit Recht vorgeschlagen und darüber hinaus die Strafbarkeit der Verletzung des Fragerechts gefordert.

Gesundheitliche Eignungsuntersuchungen an Arbeitnehmern sollten nur zulässig sein, soweit sie sich auf die gegenwärtige gesundheitliche Eignung des Arbeitnehmers beziehen, d. h. es dürfen keine Untersuchungen durchgeführt werden, die Dispositionen oder evtl. zukünftig ausbrechende Krankheiten diagnostizieren. Genetische Analysen im Rahmen von Einstellungsuntersuchungen sollten grundsätzlich verboten werden. Verhindert werden müssen auch Umgehungsmöglichkeiten. Es darf nicht sein, daß der Arbeitgeber die Vorlage einer vom Arbeitnehmer selbst zu besorgenden ärztlichen Bescheinigung über die Ergebnisse genetischer Tests verlangt. Diese Überlegung hat beispielsweise den nordrhein-westfälischen Gesetzgeber veranlaßt, im Krebsregistergesetz dem Arbeitgeber zu verbieten, vom Arbeitnehmer die Vorlage einer beim Krebsregister eingeholten „Selbstauskunft" zu fordern (Gesetz vom 12. Februar 1985, GVBl. 1985, S. 125 ff., § 7 Abs. 2).

Genetische Analysen sollten im Rahmen von Einstellungsuntersuchungen allenfalls für bestimmte Einzelfälle zugelassen werden, soweit dies für das Arbeitsverhältnis und für die konkrete Tätigkeit relevant ist und ein überwiegendes Interesse des Arbeitnehmers an einer solchen Untersuchung besteht. Entsprechendes gilt für die Durchführung genetischer Analysen im Rahmen arbeitsmedizinischer Vorsorgeuntersuchungen an Arbeitnehmern.

Wegen der besonders hohen Risiken für das informationelle Selbstbestimmungsrecht des Betroffenen dürfen genetische Untersuchungen nicht ohne die schriftliche Einwilligung des Betroffenen durchgeführt werden, wobei zuvor stets umfassend über die Bedeutung, die näheren Umstände und die Erkenntnismöglichkeiten der genetischen Untersuchung informiert werden muß.

5.2.2.2.2
Schweigepflicht des Betriebsarztes

Präzisiert werden müssen die Voraussetzungen für eine wirksame Entbindung des Betriebsarztes von der Schweigepflicht. Deshalb hat auch die Enquete-Kommission eine gesetzliche Regelung gefordert. Der Arbeitnehmer muß insbesondere die Möglichkeit haben, zunächst den Befund und das Ergebnis der Untersuchung zur Kenntnis zu nehmen und dann über die Weitergabe der Informationen an den Arbeitgeber zu entscheiden. Es darf keine pauschale Entbindung von der Schweigepflicht geben, sondern konkrete Einzelerklärungen sind geboten.

Der Betriebsarzt darf dem Arbeitgeber grundsätzlich keine Einzelheiten der genetischen Untersuchung mitteilen. Der Arbeitgeber hat in der Regel nur ein berechtigtes Interesse an dem allgemeinen Ergebnis der Untersuchung. Allerdings bleibt das Problem, daß er, wenn genetische Tests zu Konsequenzen für den Beschäftigten führen sollen, etwa Umsetzung oder Entlassung, mehr wissen will oder sogar muß als das bloße Ergebnis der Untersuchung, um seine Personalentscheidung „gerichtsfest" gegenüber dem betroffenen Arbeitnehmer oder auch dem Betriebsrat begründen zu können. Soweit genetische Analysen künftig zugelassen werden, kann daher nicht davon ausgegangen werden, daß die konkreten Untersuchungsergebnisse in jedem Fall ausschließlich beim Betriebsarzt verbleiben. Dies muß bei der Entscheidung darüber, inwieweit genetische Analysen künftig durchgeführt werden dürfen, berücksichtigt werden.

5.2.2.2.3
Art der Datenverarbeitung

Gelangen genetische Daten zulässigerweise an den Arbeitgeber, sollten sie ebenso wie sonstige Gesundheitsdaten nur in manueller Form aufgezeichnet und nicht in Personalinformationssystemen gespeichert werden. Bei sensitiven Angaben – und dazu gehören in erster Linie Angaben über den Gesundheitszustand der Arbeitnehmer –, potenzieren sich die Risiken der Langzeitspeicherung, des Kontextverlustes bei der Verwendung sowie der Verknüpfbarkeit mit anderen Daten. Konsequenterweise ist daher auch auf meine Anregung in das neue Hessische Datenschutzgesetz die Vorschrift aufgenommen worden, daß „medizinische und psychologische Befunde des Beschäftigten nicht automatisiert verarbeitet werden dürfen" (§ 34 Abs. 6). Diese Vorschrift gilt selbstverständlich auch für genetische Daten. Sie gilt jedoch nur für die öffentlichen Stellen in Hessen.

5.2.2.3
Genetische Analysen in Strafermittlungsverfahren

Fälle, in denen Straftäter mit Hilfe genetischer Analysen identifiziert und Beschuldigte entlastet worden sind, haben in den letzten Jahren erhebliches Aufsehen erregt. In den Medien wurde 1987 von dem ersten Fall einer „genetischen Massenfahndung" berichtet. Im Rahmen der Fahndung nach dem Sexualmörder eines Mädchens haben in Großbritannien mehr als 5.000 Männer aus drei Dörfern in der Umgebung des Tatortes Blut- und Speichelproben für eine genetische Analyse abgegeben. Aus dem Vergleich mit Haut- und Spermaresten, die am Tatort gefunden worden waren, konnte der Täter überführt werden. In den USA führte kürzlich eine Genomanalyse zur Verurteilung eines Sexualtäters zum Tode. Im August 1988 erklärten die Berliner Polizeibehörden, daß mit Hilfe der genetischen Analyse zum ersten Mal in der Bundesrepublik ein des Mordes verdächtiger Mann überführt werden konnte. Die Analyse wurde in diesem Fall von einer britischen Firma vorgenommen. Nach Ansicht des Hessischen Innenministeriums soll im Strafermittlungsverfahren die genetische Analyse künftig grundsätzlich Vorrang haben vor den herkömmlichen Untersuchungsmethoden (Antwort vom 05.10.1988, -M 3-12/1840- auf den Berichtsantrag der SPD-Fraktion betreffend Genomanalyse zur Täteridentifikation (Drucks. 12/1840)).

Bei dieser Entwicklung ist eine spezielle Vorschrift zur Durchführung genetischer Analysen in der Strafprozeßordnung unverzichtbar (vgl. auch Ziff. 4.2 dieses Berichts). Das geltende Recht sieht in § 81a StPO die körperliche Untersuchung des Beschuldigten gegen seinen Willen zur Feststellung von Tatsachen vor, die für das Strafverfahren von Bedeutung sind. Die Vorschrift ermächtigt zu körperlichen Eingriffen, z. B. auch zur Gewinnung von Sperma, Hautteilen, Haarwurzeln oder Blut, aus denen sich auch das für die Genomanalyse erforderliche Zellmaterial gewinnen ließe. Nicht geregelt sind in der StPO Art und Umfang der Untersuchungen, die an den gewonnenen Proben durchgeführt werden dürfen. Dies erklärt sich daraus, daß bisher immer der bei einer körperlichen Untersuchung im Sinne von § 81a StPO notwendige Eingriff in die körperliche Unversehrtheit des Betroffenen im Vordergrund der Betrachtung stand. Diese Situation ändert sich durch die weitreichenden Möglichkeiten der Genomanalyse. Hier ist nicht nur der körperliche Eingriff, mit dem das Zellmaterial gewonnen wird, mit Beeinträchtigungen oder Gefahren für den Betroffenen verbunden, sondern auch die darauf folgende Analyse des Zellmaterials. Je nach der Ausgestaltung der Testverfahren können diese nicht nur die Zuordnung einer Spur zu einem Verdächtigen, sondern auch Einblick in die Persönlichkeit des Betroffenen ermöglichen. Die gewonnenen Daten können automatisiert gespeichert und mit anderen Daten abgeglichen werden. Es handelt sich daher um eine neue und qualitativ andere Untersuchungsmethode, die besondere Gefährdungen für das informationelle Selbstbestimmungsrecht der Betroffenen mit sich bringt. § 81a der Strafprozeßordnung ist daher keine hinreichende Rechtsgrundlage für die Durchführung genetischer Analysen.

Genetische Analysen sollten künftig zur Täteridentifikation nur dann in Betracht kommen, wenn sie auf die Feststellung verfahrensrelevanter Tatsachen beschränkt werden können und keine weitere Ausforschung der genetischen Anlagen des Betroffenen beinhalten. Entsprechend enthält auch der Bericht der Enquete- Kommission des Bundestages die Empfehlung, daß Testverfahren, die einen persönlichkeitsrelevanten Informationsüberschuß erzeugen, als Erkenntnismittel im Strafprozeß ausscheiden sollten (Abschn. c) 6.2.3.6). Erst wenn eindeutig dargelegt ist, daß dies durch die Auswahl der Testverfahren tatsächlich gewährleistet werden kann, ist eine konkrete Diskussion über eine gesetzliche Regelung der Durchführung genetischer Analysen umfassend möglich. In jedem Fall müßten die zulässigen Untersuchungsverfahren ausdrücklich im Gesetz genannt und weitergehende genetische Analysen verboten werden. Auch die interfraktionelle Resolution über die Genomanalyse (s.o.) hat hier einen Regelungsbedarf gesehen.

Gegenwärtig befaßt sich eine aus Mitarbeitern des Bundeskriminalamts und der Landeskriminalämter Berlin und Baden- Württemberg bestehende Arbeitsgruppe mit der Einführung von genetischen Analysemethoden in Deutschland. Ich habe das Hessische Ministerium des Innern gebeten, mich umgehend zu informieren, wenn diese Arbeitsgruppe ihren Bericht vorgelegt hat.

5.2.3
Recht auf Nichtwissen

Zu den völlig neuen datenschutzrechtlichen Problemen, die durch die genetischen Analysen entstehen, gehört in erster Linie das häufig erwähnte sogenannte „Recht auf Nichtwissen". Stand bisher im Zentrum der datenschutzrechtlichen Diskussion das Recht des Bürgers, Kenntnis über die Verarbeitung seiner Daten zu erhalten – in das neue Hessische Datenschutzgesetz wurde auf meine Anregung sogar die Verpflichtung der speichernden Stellen aufgenommen, die Betroffenen in jedem Fall zu benachrichtigen, wenn ihre Daten in einer automatisierten Datei gespeichert werden (§ 18 Abs. 2) –, so wird jetzt sozusagen die entgegengesetzte Frage diskutiert, ob der Bürger unter Umständen ein Recht auf Nichtwissen seiner Daten hat.

Grundgedanke ist, daß jeder Bürger das Recht haben soll, unbelastet von der Kenntnis einer (möglicherweise) später ausbrechenden Krankheit leben zu können. Gefolgert wird daraus, daß bestimmte Daten gar nicht erst erhoben werden sollen bzw., wenn sie in anderen Zusammenhängen erhoben wurden, daß der Betroffene davor geschützt wird, mit ihnen konfrontiert zu werden. Ein Beispiel für die zweite Fallgruppe ist die im Bericht der Enquete-Kommission diskutierte Frage, ob es eine sogenannte „aktive" Beratung geben soll, d. h. ob ein Arzt unter Umständen von sich aus einen potentiellen späteren Patienten aufsuchen und ansprechen soll, wenn er Kenntnis von einer in der Familie vorhandenen Erbkrankheit hat. Dies hat die Kommission verneint (Ziff. 6.2.3.1 des Kommissionsberichts). Das Recht auf Nichtwissen kann aber auch dadurch in Frage gestellt werden, daß etwa genetische Analysen im Hinblick auf langfristige gesundheitliche Entwicklungen im Rahmen von Arbeitsverhältnissen, Lebensversicherungsverträgen oder Krankenversicherungsverträgen zugelassen werden. Bei der Entscheidung darüber, welche Tests zulässig sein sollen, muß auch das Recht auf Nichtwissen der Betroffenen berücksichtigt werden. Soweit die Tests zugelassen werden, ist es kaum denkbar und wünschenswert, daß die Betroffenen von den Untersuchungsergebnissen keine Kenntnis erhalten, denn diese Untersuchungsergebnisse können weitgehende praktische Konsequenzen für sie haben. Ein Recht auf Nichtwissen kann daher nur in der Form sichergestellt werden, daß die genetischen Daten gar nicht erst in diesen Zusammenhängen erhoben werden.

5.3
Klinische Krebsregister

5.3.1
Notwendigkeit eines einheitlichen Datenschutzkonzepts

Klinische Krebsregister, sog. Nachsorgeregister, haben nach einer Definition der Landesregierung die Funktion, die Krebsbehandlung im einzelnen Erkrankungsfall zu verbessern, indem die Vielzahl der im Rahmen der Behandlung

anfallenden Daten automatisiert erfaßt, verarbeitet und im Interesse einer interdisziplinären Zusammenarbeit den verschiedenen behandelnden Ärzten als solide Informationsbasis zugänglich gemacht werden. Darüber hinaus sollen die Register Arzt und Patienten an die Einhaltung von Kontrolluntersuchungen und Nachsorgeterminen erinnern (Drucks. 11/3565).

Die Gefahr dieser Register besteht darin, daß der Bezug zur Behandlung der Patienten verlorengeht und sich die klinischen Krebsregister zu einer verselbständigten Form der Patientendokumentation entwickeln, weil in ihnen nicht nur die Daten von Patienten der registerführenden Klinik, sondern auch solche von Patienten anderer Kliniken und niedergelassener Ärzte verarbeitet werden. Der Behandlungsbezug muß jedoch gewahrt bleiben, denn es handelt sich um Patientendaten, die aufgrund des mit dem Patienten (bzw. zu seinen Gunsten) geschlossenen Behandlungsvertrags erhoben werden und nur in diesem Rahmen verarbeitet werden dürfen. Wenn dies nicht gewährleistet wird, bedarf es einer gesetzlichen Grundlage für die Datenverarbeitung in den klinischen Krebsregistern.

Auch wenn diese rechtliche Einschätzung grundsätzlich nie in Frage gestellt worden ist, wirft die praktische Ausgestaltung der Datenverarbeitung in den Registern jedoch erhebliche Probleme auf. 1986 hatte ich die Verarbeitung personenbezogener Daten in den Tumorregistern der Städtischen Kliniken Darmstadt und des Universitätsklinikums Frankfurt überprüft. Dabei hatte sich gezeigt, daß die rechtliche Verantwortlichkeit für die in den Registern gespeicherten Patientendaten zum Teil nicht eindeutig festgelegt und realisiert war, die Online-Zugriffsmöglichkeiten teilweise nicht strikt auf die behandelnden Ärzte bzw. Kliniken beschränkt waren, die Verfahrensweise bei der Auswertung der Register nicht hinreichend geklärt und festgelegt und keine am Behandlungszeitraum orientierte zeitliche Begrenzung der Datenspeicherung vorgesehen war. Ein einheitliches Datenschutzkonzept für alle klinischen Krebsregister in Hessen, d.h. für die beiden Tumorzentren Rhein-Main und Marburg-Gießen sowie für die onkologischen Schwerpunktkrankenhäuser in Darmstadt, Fulda, Kassel, Limburg und Offenbach, war und ist deshalb unerläßlich. Der Landtags-Unterausschuß Informationsverarbeitung und Datenschutz hat meine Forderung aus dem 15. Tätigkeitsbericht (Ziff. 4.2) aufgegriffen und mit Beschluß vom 21. April 1988 (UID/12/3 zu Drucks. 12/1545) das Sozialministerium aufgefordert, bis Oktober 1988 ein Konzept vorzulegen. Im Juli 1988 ist mir ein erster Entwurf des Sozialministeriums zugegangen.

5.3.2
Anforderungen an das Konzept

Wie von mir gefordert, grenzt der Entwurf den Zweck der Register ein. Mit Hilfe der Register sollen die Behandlung bzw. Nachsorge der Patienten und die hierzu notwendigen Tätigkeiten der verschiedenen medizinischen Fachkliniken koordiniert werden. Ferner soll bei Patienten der kooperativen Nachsorge die Überwachung der Nachsorgetermine und die Arztbriefschreibung unterstützt werden. Die Register sollen aus zwei getrennten Datenbanken bestehen. In der einen werden die Daten der sich im jeweiligen Krankenhaus zur akuten Behandlung und/oder Nachsorge befindenden Tumorpatienten erfaßt, während die andere die Daten der Patienten enthält, die sich über die Kassenärztliche Vereinigung Hessen in kooperativer Nachsorge befinden.

Für die Festlegung der Einzelheiten der Verarbeitung personenbezogener Daten in den Registern habe ich dem Sozialministerium zahlreiche Ergänzungs- und Änderungsvorschläge unterbreitet. Dabei kam es mir besonders darauf an, daß die verschiedenen rechtlichen Fallkonstellationen der Datenspeicherung im Register genau unterschieden werden:

- Im Register sind zum einen die Daten von Patienten des registerführenden Krankenhauses gespeichert. Zwischen dem Krankenhaus und dem Patienten besteht ein Behandlungsvertrag. Dieser Behandlungsvertrag stellt die Rechtsgrundlage für die Verarbeitung der Daten der Patienten im Register dar, soweit der Behandlungszusammenhang gewahrt bleibt. Speichernde Stelle im Sinne von § 23 Bundesdatenschutzgesetz ist das Krankenhaus. Da Krankenhäuser als öffentlich-rechtliche Wettbewerbsunternehmen gelten, unterliegen sie den Bestimmungen des Bundesdatenschutzgesetzes für den privaten Bereich (§ 3 Abs. 7 Hessisches Datenschutzgesetz).

- Zum anderen werden im Register die Daten von Patienten niedergelassener Ärzte im Rahmen der kooperativen Nachsorge gespeichert. In diesem Fall besteht kein Behandlungsvertrag zwischen dem registerführenden Krankenhaus und den Patienten, sondern zwischen dem niedergelassenen Arzt und den Patienten. Speichernde Stelle im Sinne von § 23 BDSG ist der niedergelassene Arzt, das registerführende Krankenhaus verarbeitet die Patientendaten in seinem Auftrag. Zwischen dem niedergelassenen Arzt und dem registerführenden Krankenhaus muß vertraglich geregelt werden, welche Daten zu welchem Zweck im Register verarbeitet werden. Der niedergelassene Arzt darf allerdings die Daten seiner Patienten nur mit deren Einwilligung zur Verarbeitung an das registerführende Krankenhaus weitergeben, denn er unterliegt der ärztlichen Schweigepflicht gem. § 203 StGB. Die Weitergabe der Daten an das registerführende Krankenhaus stellt eine Offenbarung der Patientendaten im Sinne dieser Vorschrift dar, die nur mit einer besonderen Befugnis vorgenommen werden darf. Eine solche Befugnis kann sich hier nur aus einer Einwilligung der Patienten ergeben.

- Schließlich werden im Register auch die Daten von Patienten anderer Krankenhäuser im Rahmen der kooperativen Nachsorge gespeichert. Auch in diesem Fall besteht kein Behandlungsvertrag zwischen dem registerführenden Krankenhaus und den Patienten, ein Vertrag besteht vielmehr zwischen dem anderen Krankenhaus und den Patienten. Das andere Krankenhaus ist speichernde Stelle im Sinne von § 23 BDSG, das registerführende

Krankenhaus verarbeitet die Patientendaten in seinem Auftrag. Im übrigen gilt hier das gleiche wie für die Daten von Patienten niedergelassener Ärzte.

Um den Zusammenhang der Datenspeicherungen mit der Behandlung der Patienten auf Dauer sicherzustellen, habe ich dem Sozialministerium vorgeschlagen, die folgenden Maßnahmen im Datenschutzkonzept festzulegen:

- In den klinischen Krebsregistern werden nur solche Daten verarbeitet, die im Rahmen der Behandlung der Patienten erhoben wurden.

- Durch interne Dienstanweisungen der registerführenden Krankenhäuser und durch vertragliche Regelungen der registerführenden Krankenhäuser mit den niedergelassenen Ärzten bzw. den anderen Krankenhäusern muß das konkrete Verfahren der Datenverarbeitung im Register genau festgelegt und die rechtliche Verantwortlichkeit und Kontrollmöglichkeit der jeweiligen speichernden Stellen und der behandelnden Ärzte sichergestellt werden.

- Der Zugriff auf personenbezogene Daten wird auf die jeweils behandelnden Ärzte beschränkt. Dies gilt auch für die Patientenstammdaten.

- Die Übermittlung von personenbezogenen Daten oder Auswertungen darf nur an die jeweiligen behandelnden Ärzte erfolgen. Die Übermittlung von Daten an Dritte hat in anonymisierter Form zu erfolgen. Das Verfahren der Herausgabe von personenbezogenen Daten und Auswertungen muß in den internen Dienstanweisungen der registerführenden Krankenhäuser und in den vertraglichen Regelungen zwischen den registerführenden Krankenhäusern und den niedergelassenen Ärzten bzw. den anderen Krankenhäusern vereinbart werden. Dabei muß auch verbindlich geklärt werden, welche Anforderungen an die Anonymisierung der Patientendaten gestellt werden, da sich gezeigt hat, daß in diesem Punkt zum Teil falsche Vorstellungen vorhanden sind. So genügt es z. B. nicht, einfach nur den Namen wegzulassen, wenn aus den übrigen Daten auf den Betroffenen geschlossen werden kann.

- Es versteht sich von selbst, daß die Einhaltung aller dieser rechtlichen und inhaltlichen Regelungen und Beschränkungen soweit wie möglich durch technische und organisatorische Maßnahmen zu unterstützen bzw. zu gewährleisten ist. Deshalb werden in dem Datenschutzkonzept Mindestanforderungen für die zu treffenden Maßnahmen und für die in einer Dienstanweisung zu regelnden Punkte formuliert, um die Zielvorgaben der Anlage zu § 6 BDSG zu erfüllen.

  Dabei gilt selbstverständlich: Sollten die eingesetzten Datenverarbeitungssysteme über die Mindestanforderungen hinausgehende zusätzliche Möglichkeiten zur Verbesserung des Datenschutzes (im klinischen Tumorregister) anbieten, sind diese auch zu nutzen. Die Mindestanforderungen können nicht abschließend sein, da sich z. B. der Stand der Technik ständig verändert.

Das Sozialministerium hat meine Vorschläge in einem neuen Entwurf aufgenommen, über den nun noch einmal unter Einbeziehung der betroffenen Stellen verhandelt werden soll.

5.4
Aids

5.4.1
Pauschale Forderungen

Auch 1988 sind wieder pauschale Forderungen nach einer Speicherung von Aids-Daten erhoben worden. Im April hat der Vorstand der Deutschen Gesellschaft für Innere Medizin auf dem Internistenkongreß in Wiesbaden empfohlen, sämtliche Aids-Infizierten bei Ärzten oder Ärztekammern zu registrieren. Dies sei notwendig, um Infektionsketten festzustellen und abzubrechen sowie „gewissenlose Verbreiter" der Infektion ausfindig zu machen.

Die Frage, was denn im Anschluß an eine solche Registrierung mit den Daten der Infizierten konkret geschehen soll, d. h. welche Stellen oder Personen diese Daten unter welchen Voraussetzungen und zu welchen Zwecken verwerten sollen, beantwortet der Vorstand allerdings nicht. Das überrascht um so mehr, als insbesondere auch die Datenschutzbeauftragten in den letzten Jahren immer wieder nachdrücklich darauf aufmerksam gemacht haben, daß diese Fragen genau beantwortet sein müssen, bevor über eine solche Datensammlung überhaupt angemessen diskutiert werden kann (s. hierzu auch 15. Tätigkeitsbericht, Ziff. 4.4.1, 16. Tätigkeitsbericht, Ziff. 6.1.4.1). Pauschale Forderungen dieser Art können die bestehenden Probleme nicht lösen. In einer Presseerklärung zu der Forderung des Vorstands der Deutschen Gesellschaft für Innere Medizin habe ich daher darauf hingewiesen, daß in der gesundheitspolitischen Diskussion zu Recht die Ansicht vorherrscht, Beratungs- und Hilfsangebote könnten wirksamere Instrumente zur Eindämmung der Immunschwäche sein als namentliche Melderegister. Auch die Enquete-Kommission des Bundestages hält in ihrem Zwischenbericht vom Juni 1988 eine personenbezogene Meldepflicht für entbehrlich. Hervorzuheben ist in diesem Zusammenhang auch die aktuelle Entwicklung in Schweden: Dort sollte ursprünglich eine „codierte" Meldepflicht, die ggfs. eine Identifikation der Betroffenen erlaubt hätte, eingeführt werden. Als Ergebnis einer äußerst kontroversen Diskussion wurde jedoch darauf verzichtet. Die Tests werden nunmehr völlig anonym durchgeführt (s. Zwischenbericht der Enquete-Kommission „Gefahren von Aids und wirksame Wege zu ihrer Eindämmung" vom 16. Juni 1988, Bundestags-Drucks. 11/2495, S. 73 und 96).

5.4.2
Aids-Tests

5.4.2.1
Richtlinien für Aids-Tests

Meine im letzten Tätigkeitsbericht (Ziff. 6.1.1) dargelegte Auffassung, daß Aids-Tests grundsätzlich nur mit Einwilligung der Betroffenen vorgenommen werden dürfen, wird offensichtlich sowohl von der Landesregierung als auch von allen Fraktionen im Landtag geteilt.

Das zeigt die Antwort der Landesregierung auf die Große Anfrage der SPD-Fraktion betreffend Aids (Drucks. 12/1773, S. 6), und das wurde deutlich in der Debatte des Landtags, die zu der Antwort sowie einem Antrag der CDU-Fraktion betreffend Aids (Drucks. 12/570) am 5. Mai 1988 stattfand (Plenarprotokoll 12/41 sowie Beschlußempfehlung und Bericht des Sozialpolitischen Ausschusses, Drucks. 12/1192). Am Schluß der Debatte wurde der Antrag der CDU-Fraktion einstimmig verabschiedet. In ihm wird die Landesregierung aufgefordert, Richtlinien zu erlassen, die das Verhalten der Gesundheitsbehörden im Hinblick auf Aids regeln. Dem Antrag zufolge sollen die Richtlinien sicherstellen, „daß die Gesundheitsbehörden Aids-Tests nur nach vorheriger Information und mit ausdrücklicher Einwilligung der Betroffenen vornehmen".

In ihrer Antwort auf die Kleine Anfrage einer Abgeordneten der F.D.P. betreffend Richtlinien für Aids (Drucks. 12/1767) hat das Sozialministerium im August mitgeteilt, daß entsprechende Richtlinien in Kürze vorgelegt werden (Drucks. 12/2786). Zuletzt hat die Landesregierung in ihrer Stellungnahme zu meinem 16. Tätigkeitsbericht noch einmal den Vorrang der Einwilligung betont, so insbesondere auch hinsichtlich der Aids-Tests in den Krankenhäusern (s. hierzu auch Ziff. 5.4.2.2.2), und zugesagt, daß Richtlinien noch in diesem Jahr erlassen werden (Drucks. 12/3068 zu Ziff. 6.1.1.2 des 16. Tätigkeitsberichts).

Die Einwilligung darf jedoch keine reine Formalität sein, sie muß tatsächlich die Entscheidungsfreiheit der Betroffenen gewährleisten. Deshalb habe ich im vergangenen Jahr stichprobenweise die Verfahren bei der Einholung der Einwilligungserklärung überprüft und mußte feststellen, daß den Anforderungen der Datenschutzgesetze an eine rechtswirksame Einwilligung nicht immer Rechnung getragen wird.

5.4.2.2
Fehlerhafte Einwilligungserklärungen

5.4.2.2.1
Nachträgliche Einwilligung

Eine schwarzafrikanische Asylbewerberin sucht im Oktober 1987 – nach ihren Angaben wegen Blutdruckbeschwerden – einen Arzt in Hünfeld auf. Der Arzt, der eine Infektionserkrankung vermutet, nimmt bei der Patientin Blut ab und läßt es u. a. auch auf Aids testen. Im November 1987 teilt er dem Kreisgesundheitsamt in Fulda schriftlich mit, daß bei einer Bewohnerin des Asylantenheimes in Burghaun „zweifelsfrei und institutskontrolliert" eine Aids-Infektion festgestellt worden sei. Außerdem äußert er den Verdacht, die „28 Jahre junge Frau" habe sowohl zu Männern innerhalb als auch außerhalb des Asylantenheimes intime Beziehungen. Den Namen der Frau teilt der Arzt nicht mit. Aufgrund dieser Angaben ermittelt das Gesundheitsamt mit Hilfe der Ausländerbehörde die Betroffene und fordert sie auf, sich bei der Gesundheitsbehörde vorzustellen. Als die Afrikanerin Ende November 1987 erscheint, wird ihr mit ihrer Einwilligung Blut abgenommen. Daß das Blut für einen Aids- Test bestimmt ist, darüber wird sie jedoch vor der Entnahme nicht aufgeklärt. Das Blut wird entnommen, ohne daß die Betroffene zuvor in einen solchen Test eingewilligt hat. Erst einen Tag später teilt ihr die Gesundheitsbehörde mit, das Blut werde auf Aids untersucht und läßt die Betroffene eine Einverständniserklärung unterschreiben.

Der Fall wurde von der Fraktion der GRÜNEN aufgegriffen (Drucks. 12/1730) und führte im März 1988 zu einer ausführlichen Debatte im Landtag (Protokoll der 33. Plenarsitzung vom 2. März 1988, S. 1747). Veranlaßt durch kontroverse Stellungnahmen des Innenministers und des Hessischen Datenschutzbeauftragten (Ausschußvorlagen INA/12/40 und 12/50 jeweils zur Drucks. 12/1730) kam es danach im Innenausschuß am 3. November 1988 zu einer weiteren eingehenden Diskussion.

Hauptstreitpunkt war und ist, ob das Gesundheitsamt Blut entnehmen durfte, ohne zuvor die Asylbewerberin darüber zu informieren, daß es einem Aids-Test diente, und ohne zuvor die ausdrückliche schriftliche Einwilligung der Betroffenen einzuholen. Das Hessische Datenschutzgesetz enthält eine eindeutige Vorgabe: Die Einwilligung muß vorliegen, bevor mit der Datenverarbeitung begonnen wird. Ist das nicht der Fall, so ist der Mangel nachträglich nicht mehr heilbar, die Datenverarbeitung ist und bleibt rechtswidrig.

Das Gesundheitsamt begründete später sein Vorgehen damit, die Blutentnahme habe sofort erfolgen müssen, da befürchtet worden sei, die Betroffene werde untertauchen. Zum Zeitpunkt der Entnahme habe jedoch kein Dolmetscher zur Verfügung gestanden, so daß Aufklärung und Einwilligung erst nachträglich möglich gewesen seien. Der Innenminister sieht in diesem Verfahren keinen Rechtsverstoß. Blutentnahme und Durchführung des Aids- Tests im Labor müssen seiner Ansicht nach getrennt beurteilt werden: Die Datenerhebung finde nicht schon mit der Blutentnahme, sondern erst mit der Blutuntersuchung statt. Die Blutuntersuchung sei aber erst nach vorheriger

Aufklärung und mit schriftlicher Zustimmung der Betroffenen erfolgt. Hätte die Asylbewerberin der Untersuchung nicht zugestimmt, so hätte nach Auffassung des Innenministers die Blutprobe ohne Durchführung des Aids-Tests vernichtet werden müssen.

Die Argumentation des Innenministers ist jedoch wenig überzeugend. Blutentnahme und spätere Laboruntersuchung des Blutes können nicht voneinander getrennt werden. Die Blutentnahme erfolgte in diesem Fall ausschließlich im Hinblick auf den Aids- Test und kann daher nur in diesem Zusammenhang rechtlich bewertet werden. Dies wird auch durch den Hinweis des Innenministers deutlich, daß das Blut hätte vernichtet werden müssen, wenn die Betroffene später ihr Einverständnis in die Laboruntersuchung nicht erklärt hätte. Es erscheint wenig sinnvoll, zunächst durch körperlichen Eingriff eine Blutprobe zu entnehmen und anschließend zu klären, ob die Blutprobe überhaupt verwendet werden darf. Im übrigen stehen diese Ausführungen des Innenministers auch im Widerspruch zu der Darstellung des Landrats, die Blutentnahme sei ohne Dolmetscher durchgeführt worden, weil ein „Untertauchen" der Betroffenen befürchtet worden sei. Die Datenerhebung begann daher schon mit der Blutentnahme. Nach der Blutentnahme lag bereits ein Datum über die Betroffene vor, das durch die später vorgenommene Laboruntersuchung noch konkretisiert wurde. Die Situation kann etwa damit verglichen werden, daß ein Photo von einem Bürger angefertigt wird, das später vergrößert wird, so daß er nunmehr erkennbar ist: Die Anfertigung des Photos stellt bereits die Erhebung eines – zumindest bestimmbaren – Datums dar, das durch technische Maßnahmen noch konkretisiert werden kann. Nur eine solche Sichtweise vermag auch der tatsächlichen Gefährdung für das informationelle Selbstbestimmungsrecht gerecht werden, denn nach der Blutentnahme hat die Betroffene im Regelfall keine faktischen Einflußmöglichkeiten mehr auf die weitere Verfahrensweise. Eine später verweigerte Zustimmung in die Verwendung des Blutes nützt zum Beispiel dann nichts mehr, wenn die Untersuchung bereits durchgeführt wurde und das Ergebnis bekannt ist. Von einem effektiven Datenschutz kann nur die Rede sein, wenn es ohne Einwilligung überhaupt nicht zu einer Datenerhebung, auch nicht zur Blutentnahme als dem ersten Teil der Datenerhebung, kommen darf.

Die im Innenausschuß vom Innenminister geäußerte Kritik, daß ich vor einem abschließenden Urteil über die Rechtswidrigkeit der Maßnahmen auch hätte prüfen müssen, ob ein rechtmäßiger Zwangstest auf der Grundlage des Bundesseuchengesetzes vorlag, geht an dem Problem vorbei. Einmal abgesehen von der Frage, ob im konkreten Fall überhaupt die gesetzlichen Voraussetzungen für einen Zwangstest gegeben waren, lag schon deshalb kein rechtmäßiger Zwangstest vor, weil der Betroffenen nicht vor der Blutentnahme eindeutig und vollständig bekanntgegeben wurde, daß ein Zwangstest bei ihr durchgeführt werden soll. Das Problem der Transparenz der Maßnahme für die Betroffene stellt sich daher insoweit genauso wie bei der Einwilligung. Im übrigen zeigt dieser Einwand des Innenministers sehr deutlich, wie notwendig eine von vornherein klare Verfahrensweise bei der Durchführung von Aids-Tests ist. Es geht nicht an, daß im nachhinein darüber diskutiert wird, ob die Verwaltungsmaßnahme aufgrund einer Einwilligung oder aufgrund der Vorschriften des Bundesseuchengesetzes erfolgte. Diese Rechtsgrundlagen dürfen nicht beliebig als Begründung für die Rechtmäßigkeit ausgetauscht werden.

Trotz dieser unterschiedlichen Einschätzung hat der Innenminister dem Sozialminister vorgeschlagen, daß die Einwilligung künftig in jedem Fall bereits vor der Blutentnahme eingeholt wird und ihn gebeten, eine einheitliche Handhabung durch die Gesundheitsämter sicherzustellen.

5.4.2.2.2
Pauschale Einwilligung

Seit November 1987 händigt die Universitätsklinik Frankfurt allen Patienten ein Informationsblatt über die Durchführung von Laboruntersuchungen aus, das über Aids-Tests folgende Passage enthält:

„Dabei müssen im Rahmen der Diagnose und Behandlung alle serologischen Laboruntersuchungen durchgeführt werden, die zur Abklärung Ihres Krankheitsbildes bzw. zur Feststellung Ihrer Krankheitsursache notwendig sind. Dies kann erforderlichenfalls u. a. auch die Durchführung von HIV-Tests zur Untersuchung auf Aids einschließen."

Die Universitätsklinik läßt die Patienten außerdem eine Einwilligungserklärung unterschreiben, in der es heißt:

„Mir ist bekannt, daß möglicherweise zu diagnostischen Zwecken Blut entnommen und untersucht werden muß und daß sich eine solche Untersuchung jetzt auch auf Aids erstreckt. Mit dem Umfang der Blutuntersuchung erkläre ich mich einverstanden. Das Ergebnis der Untersuchung unterliegt der ärztlichen Schweigepflicht."

Aids-Tests in Krankenhäusern sind keine Routinemaßnahmen. Dieser Auffassung stimmt die Landesregierung in ihrer Stellungnahme zu meinem 16. Tätigkeitsbericht (Drucks. 12/3068, zu Ziff. 6.11.1) ausdrücklich zu. Der Patient muß daher grundsätzlich vorher über den Test informiert und seine Einwilligung eingeholt werden. Ausnahmen können allenfalls für bestimmte eng begrenzte Situationen anerkannt werden (vgl. auch 16. Tätigkeitsbericht, Ziff. 6.11.1).

Die beiden Formblätter wurden vom Hessischen Ministerium für Wissenschaft und Kunst gemeinsam mit dem Sozialministerium und dem Justizministerium entwickelt. Nach Auskunft des Sozialministeriums wird erwogen, ihre Verwendung auch anderen Krankenhäusern zu empfehlen. Sowohl das Hessische Ministerium für Wissenschaft und Kunst als auch das Sozialministerium habe ich darauf hingewiesen, daß mit den entwickelten Formularen keine rechtswirksame Einwilligung eingeholt werden kann.

Aus den Formularen können die Patienten die Tragweite ihrer Einwilligungserklärung nicht erkennen. Sie wissen nicht, ob ein Test überhaupt durchgeführt wird und aus welchem Anlaß ggfs. ein Test erfolgt. Derart pauschale Erklärungen

verfehlen das mit dem Einwilligungserfordernis verbundene Ziel, die Betroffenen frei entscheiden zu lassen. Da vielfach die Auffassung vertreten wird, ein Krankenhaus sei grundsätzlich zur Behandlung eines Patienten nicht verpflichtet, wenn dieser seine Einwilligung in den Aids- Test verweigert, obwohl der Test aus medizinischer Sicht geboten ist und soweit die Durchführung des Tests notwendige Voraussetzung der Behandlung ist (so etwa die gemeinsamen Hinweise und Empfehlungen der Bundesärztekammer und der Deutschen Krankenhausgesellschaft zur HIV-Infektion), stellt sich auch die Frage, was eigentlich geschehen soll, wenn ein Patient bei Übergabe dieser Formblätter – also zu einem Zeitpunkt, zu dem überhaupt nicht feststeht, ob der Aids-Test medizinisch notwendig ist – seine Einwilligung verweigert. Die Behandlung darf in dieser Situation auf keinen Fall abgelehnt werden.

Ende November 1988 hat mir das Sozialministerium mitgeteilt, daß es meiner Kritik zustimmt und einen entsprechenden Erlaß an alle hessischen Krankenhäuser herausgegeben hat. Auch das Ministerium für Wissenschaft und Kunst will das Verfahren ändern.

5.4.2.2.3
Unklarheiten in der Einwilligungserklärung (Aids-Test nach Vergewaltigung)

Eine junge Frau, die vergewaltigt worden war, wurde unmittelbar nach der Straftat im Auftrag der ermittelnden Polizei in einem Krankenhaus ärztlich untersucht. Zusätzlich zur allgemeinen ärztlichen Untersuchung veranlaßte der Arzt einen Aids-Test. Das Testergebnis wurde zusammen mit dem allgemeinen Untersuchungsbericht an die Polizeibehörde weitergegeben.

Zu dem Fall erhielt ich eine Reihe von Eingaben, in denen nach der Zulässigkeit der Verfahrensweise des Krankenhauses gefragt wurde. Bei der Überprüfung stellte sich heraus, daß zwar eine Einwilligungserklärung der Betroffenen hinsichtlich der Durchführung des Aids-Tests und der Weitergabe des Testergebnisses vorlag, diese jedoch so unklar formuliert war, daß nicht von einer rechtswirksamen Einwilligung ausgegangen werden konnte.

Der Text der Erklärung lautete:

„Ich ... bin mit der Untersuchung durch den Frauenarzt und der Durchführung eines Aids-Testes (nach ausführlicher Aufklärung) wegen der stattgehabten Vergewaltigung einverstanden und entbinde ihn von der Ärztlichen Schweigepflicht gegenüber den Ermittlungsbehörden."

Formell lag damit zwar eine Einwilligung sowohl in die Durchführung des Aids-Tests als auch in eine Übermittlung des Untersuchungsergebnisses an die Ermittlungsbehörden vor.

Eine rechtswirksame Einwilligung in einen Aids-Test setzt jedoch u. a. eine genaue Information über den Zweck des Tests voraus. Im Formular war über den Zweck des Aids-Tests nichts gesagt. Da mir im Verlauf der Überprüfung immer wieder verschiedene Zwecke genannt wurden, zu denen der Test angeblich durchgeführt worden war, war zumindest zweifelhaft, ob die Betroffene zu diesem Punkt eine konkrete Information erhalten hatte. Der in dem Erklärungsformular enthaltene Zusatz „nach ausführlicher Aufklärung" bezog sich vermutlich eher auf medizinische Fragen.

Es geht auch nicht an, daß – wie hier – drei verschiedene Erklärungen zu einer Erklärung zusammengefaßt werden: die Einwilligung in die allgemeine Untersuchung, die Einwilligung in die Durchführung des Aids-Tests und die Entbindung von der ärztlichen Schweigepflicht.

Der Aids-Test wurde sowohl nach Auskunft des Hessischen Innenministeriums als auch des Regierungspräsidiums Darmstadt nicht im Auftrag der Polizei durchgeführt. Es ist aber nicht Aufgabe der Ärzte, den polizeilichen Auftrag – und sei es auch mit Einwilligung der Betroffenen – zu erweitern.

Als Zweck des Aids-Tests kam somit allenfalls das Interesse der Betroffenen selbst oder der Schutz des Krankenhauspersonals in Betracht.

Wenn jedoch der Aids-Test im Interesse der Betroffenen selbst oder zum Schutz des Personals durchgeführt wurde, bestand auf keinen Fall Anlaß, das Testergebnis an die Ermittlungsbehörden weiterzugeben. Dadurch, daß die verschiedenen Erklärungen zu einer Erklärung zusammengefaßt wurden, hatte die Betroffene weder die Möglichkeit, in die ärztliche Untersuchung ohne den Aids-Test einzuwilligen, noch konnte sie zusätzlich in den Aids-Test einwilligen, ohne gleichzeitig ihr Einverständnis in die Weitergabe des Testergebnisses zu erklären. Ihre Entscheidungsfreiheit war daher wesentlich eingeschränkt.

Das Sozialministerium hat sich meiner Bewertung angeschlossen, daß eine Weitergabe des Testergebnisses an die Polizeibehörde nicht zulässig war. Mit Erlaß vom 21. April 1988 hat es den Krankenhausträger auf die Rechtslage hingewiesen und ihn aufgefordert, dafür zu sorgen, daß sich ein derartiger Vorfall nicht wiederholt.

Wichtig ist für mich vor allem die Frage, wie in künftigen vergleichbaren Situationen verfahren werden soll. Das Hessische Justizministerium und das Innenministerium haben auf meine Anfrage die Ansicht geäußert, daß der Aids-Test bei einem Opfer einer Vergewaltigung nur in wenigen Ausnahmefällen strafprozessual relevant sei. Es kommt nunmehr darauf an, auf dieser Grundlage die künftige Verfahrensweise festzulegen.

5.4.2.3
Aids-Tests in Haftanstalten

Was die Rechtsgrundlage für Aids-Tests in Haftanstalten anbelangt, hat sich das Hessische Justizministerium bis heute nicht zu einer klaren Position durchringen können (vgl. hierzu auch 15. Tätigkeitsbericht, Ziff. 4.4.5, 16. Tätigkeitsbericht, Ziff. 6.11.3). Zum einen vertritt das Ministerium die Ansicht, die Gefangenen seien gesetzlich verpflichtet, sich einem Aids- Test zu unterziehen. Zur Begründung wird auf das Bundesseuchengesetz und auf § 56 Strafvollzugsgesetz sowie § 92 Hessisches Beamtengesetz verwiesen. Nach der Vorschrift des Strafvollzugsgesetzes ist für die körperliche und geistige Gesundheit der Gefangenen zu sorgen und haben diese die notwendigen Maßnahmen zum Gesundheitsschutz und zur Hygiene zu unterstützen. Das Beamtengesetz verpflichtet den Dienstherrn, auch für das gesundheitliche Wohl seiner Bediensteten zu sorgen und die erforderlichen Maßnahmen zu treffen.

Zum anderen ist das Justizministerium der Auffassung, daß der Test für die Gefangenen freiwillig sei. Es begründet dies damit, daß bei den Gefangenen, die die Teilnahme verweigern, keine zwangsweise Blutentnahme durchgeführt wird und keine Sanktionen getroffen werden. Allerdings würden die Gefangenen im Fall einer Verweigerung so behandelt, als ob sie HIV-infiziert seien. Zu meiner Frage nach dem konkreten Verfahren teilte das Justizministerium mit, daß in zwei Haftanstalten die Gefangenen schriftlich erklären, daß sie eine Untersuchung möchten, in den übrigen Haftanstalten würden die Gefangenen bei der Zwangsuntersuchung jeweils mündlich befragt. Auf irgendwelche „Rechtslagen" und rechtliche Verpflichtungen zur Untersuchung werde nicht hingewiesen. Die Gefangenen würden vielmehr ausdrücklich darüber informiert, daß ohne ihr Einverständnis keine Blutentnahme erfolge und erst recht nicht zwangsweise durchgeführt werde.

Ich bin nach wie vor der Auffassung, daß die hier erfolgte Verwendung der Begriffe „Einwilligung" und „Freiwilligkeit" irreführend und unzutreffend ist. Die Datenschutzgesetze treffen die klare Unterscheidung, daß eine Datenerhebung entweder aufgrund einer Rechtsvorschrift erfolgt oder aufgrund einer Einwilligung der Betroffenen (vgl. § 7 HDSG, § 3 BDSG). Dies sind Alternativen, die sich gegenseitig ausschließen.

Wenn in den Haftanstalten davon ausgegangen wird, daß die Gefangenen zur Teilnahme an dem Test rechtlich verpflichtet sind, so muß dies den Gefangenen eindeutig unter Nennung der Rechtsgrundlage mitgeteilt werden. Verzichten die Haftanstalten darauf, bei einer Weigerung der Gefangenen Zwangsmaßnahmen zur Durchsetzung des Tests anzuwenden, so mögen sie gute Gründe hierfür haben und es mag auch im Interesse der Gefangenen liegen, es rechtfertigt jedoch keinesfalls, davon zu sprechen, daß die Durchführung der Tests aufgrund einer „Einwilligung" bzw. „auf freiwilliger Grundlage" vorgenommen werden. Von einer Einwilligung im datenschutzrechtlichen Sinn kann nur dann gesprochen werden, wenn rechtlich und tatsächlich auch eine echte Entscheidungsfreiheit der Betroffenen besteht. Hiervon kann aufgrund der konkreten Umstände keine Rede sein.

6. Sozialverwaltung

6.1
Gesundheits-Reformgesetz (GRG)

Am 25. November 1988 hat der Bundestag das Gesetz zur Strukturreform im Gesundheitswesen (Gesundheits-Reformgesetz GRG) verabschiedet. Grundlage waren die von den Fraktionen der CDU/CSU und F.D.P. (Bundestags-Drucks. 11/2237) und der Bundesregierung (Bundestags-Drucks. 11/2493) eingebrachten gleichlautenden Gesetzentwürfe. Das Gesetz wird zu einer enormen Zunahme der Verarbeitung personenbezogener Patientendaten durch Krankenkassen und kassenärztliche Vereinigungen führen.

Ein gewichtiger datenschutzrechtlicher Einwand, der von Anfang an gegen das Gesetzesvorhaben stand, ist auch im Verlauf der parlamentarischen Beratungen nicht ausgeräumt worden: Es bestehen nämlich erhebliche Zweifel, ob das Grundprinzip des Datenschutzes, daß Behörden nur die personenbezogenen Daten verarbeiten dürfen, die sie zur Erfüllung ihrer Aufgaben unbedingt benötigen, hier ausreichend beachtet worden ist. Wie immer die einzelnen Ziele der Gesundheitsreform auch benannt worden sind, ob Verbesserung der Transparenz des Leistungsgeschehens angestrebt wird, die Voraussetzungen für eine qualifizierte Prüfung der Wirtschaftlichkeit, Zweckmäßigkeit und Notwendigkeit der abgerechneten Leistungen geschaffen oder Mißbrauch und Abrechnungsmanipulationen bekämpft werden sollen, letztlich geht es um ein Ziel: Kostendämpfung.

Genau hier setzt aber die gesundheitspolitische Kritik an, die auch die datenschutzrechtliche Wertung entscheidend beeinflußt. Wenn dieses Ziel, wie durchaus plausibel dargelegt wird, sehr viel einfacher und effektiver durch staatliche Einflußnahme auf die Pharmaindustrie erreicht werden kann, ist es datenschutzrechtlich kaum akzeptabel, statt dessen zunächst bei den Patienten und deren personenbezogenen Daten anzusetzen.

Auch wenn dieser Haupteinwand also fortbesteht, konnten die Datenschutzbeauftragten doch eine ganze Reihe von Verbesserungen im Gesetzgebungsverfahren erreichen (vgl. hierzu auch die Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 6. Juni 1988, abgedruckt unter Ziff. 16.3 dieses Berichts):

- Die Datenflüsse für die Wirtschaftlichkeitsprüfungen wurden eingeschränkt und die auszutauschenden Daten im Gesetz konkret katalogisiert.

- Für alle Stellen, die Versicherten- oder Patientendaten verarbeiten, sind jeweils Datenkatalog, Verwendungszweck der Daten, Aufbewahrungsmodalitäten und Löschungsfristen festgelegt.

- Krankenkassen und kassenärztliche Vereinigungen sind verpflichtet, jährlich eine Übersicht der von ihnen verarbeiteten Daten ihrer Aufsichtsbehörde vorzulegen und zu veröffentlichen.

- Besonders hervorzuheben ist die Einschränkung für den Medizinischen Dienst der Krankenversicherungen. Dieser darf nur Angaben zur Person und Hinweise auf zu führende Akten in Dateien speichern – mithin keine Dateien mit personenbezogenen medizinischen Daten aufbauen.

Die Verarbeitungspraxis werde ich genauestens überprüfen.

6.2
Sozialversicherungsausweis

Im Kampf gegen die Schwarzarbeit setzt die Bundesregierung ihre Hoffnung auf ein neues Instrument: den Sozialversicherungsausweis. Sie hat deshalb im August 1988 den Entwurf eines Gesetzes zur Einführung eines Sozialversicherungsausweises und zur Änderung anderer Sozialgesetze im Bundestag eingebracht (Bundestags-Drucks. 11/2807). Mit dem Ausweis sollen – so das erklärte Ziel des Entwurfs – darüber hinaus auch der Mißbrauch von Sozialleistungen und die mißbräuchliche Ausnutzung der Geringfügigkeitsgrenze, d.h. der Grenze, innerhalb der Beschäftigtenverhältnisse nicht versicherungspflichtig sind, bekämpft werden.

Nach dem Willen der Bundesregierung soll künftig jeder Beschäftigte einen fälschungssicheren Sozialversicherungsausweis erhalten, der u.a. die Versicherungsnummer der Rentenversicherung sowie den Namen des Beschäftigten enthält. Bei Beschäftigungsbeginn müßte der Ausweis dem Arbeitgeber vorgelegt werden. In bestimmten Wirtschaftsbereichen oder Wirtschaftszweigen müßten die Beschäftigten außerdem den Sozialversicherungsausweis während der Arbeit stets mitführen.

Hier gilt zunächst einmal die gleiche Kritik wie im Fall des Gesundheits-Reformgesetzes (vgl. Ziff. 6.1). Während die Gesundheitsreform beim Patienten und nicht etwa der Pharmaindustrie ansetzt, konzentriert sich die Bundesregierung mit dem Gesetz zur Einführung des Sozialversicherungsausweises in erster Linie auf die Kontrolle der Beschäftigten und weniger der Arbeitgeber. Auch hier ist bislang nicht ausgelotet worden, ob ein Kontrollmodell, das bei den Arbeitgebern ansetzt, nicht zumindest genauso effektiv, wenn nicht wirksamer wäre, und gleichzeitig in geringerem Maße in das informationelle Selbstbestimmungsrecht eingreifen würde.

Verfassungsrechtlich bedenklich ist auf jeden Fall, daß die Rentenversicherungsnummer zur Bekämpfung der Schwarzarbeit verwendet werden soll. Der Bundesgesetzgeber hat erst kürzlich aus dem Volkszählungsurteil des Bundesverfassungsgerichts die Konsequenz gezogen und in Art. 2 des Ersten Gesetzes zur Änderung des Sozialgesetzbuches vom 20. Juli 1988 (BGBl. I S. 1046) die Verwendung der Rentenversicherungsnummer abschließend geregelt. Soweit andere als Rentenversicherungsträger die Rentenversicherungsnummer verwenden dürfen, ist dies immer auf konkrete Aufgaben im Zusammenhang mit Leistungen nach dem Sozialgesetzbuch beschränkt. Dazu gehört aber nicht die Bekämpfung illegaler Beschäftigung.

6.3
Jugendhilfeakten: Einsichtsrecht des Hessischen Datenschutzbeauftragten

Eine Pflegemutter beschwerte sich bei mir darüber, daß das Jugendamt der Stadt Frankfurt in der Familienpflegeakte anscheinend über Auszüge aus Strafakten über ihre leiblichen Kinder verfüge. Nachprüfen konnte ich dies freilich nicht, da mir das Frankfurter Jugendamt generell Einsicht in Jugendhilfeakten verweigert.

Das Verhalten des Jugendamtes ist ein eindeutiger Rechtsverstoß. Dem Hessischen Datenschutzbeauftragten kann nicht – worauf sich das Jugendamt zunächst berief – das Sozialgeheimnis (§ 35 SGB I) entgegengehalten werden, er darf auch ohne ausdrückliche Einwilligung der Betroffenen Jugendhilfeakten einsehen.

Das Jugendamt hat nämlich übersehen, daß § 79 Abs. 3 Satz 2 SGB X ausdrücklich klarstellt, daß das Sozialgesetzbuch Rechtsstellung und Prüfkompetenzen der Landesdatenschutzbeauftragten unberührt läßt. Diese ergeben sich ausschließlich aus den jeweiligen Landesdatenschutzgesetzen, soweit Sozialleistungsträger auf Landes- oder kommunaler Ebene betroffen sind. Die auch aufgrund der verfassungsrechtlichen Kompetenzverteilung zwischen Bund und Ländern gebotene Anerkennung der autonomen Regelungsbefugnis der Länder für die Ausgestaltung der Aufgaben und Befugnisse „ihrer" Datenschutzbeauftragten kommt insofern einer „dynamischen Verweisung" gleich, als auch Kompetenzerweiterungen, die sich durch die Novellierung einzelner Landesgesetze ergeben, den Sozialleistungsbereich einschließen.

Das Jugendamt ist infolgedessen verpflichtet, dem Hessischen Datenschutzbeauftragten nicht nur alle gewünschten Auskünfte zu geben, sondern auch Einsicht in solche Unterlagen zu gewähren, die mit der Verarbeitung personenbezogener Daten zusammenhängen (§ 29 Abs. 1 HDSG).

Das Jugendamt kann die Akteneinsicht auch nicht – wie später geschehen – mit dem Hinweis verweigern, die Maßnahme sei nicht erforderlich. Hier wie sonst ist es ausschließlich Sache des Hessischen Datenschutzbeauftragten, zu

entscheiden, ob Akten eingesehen werden müssen und welche dies zu sein haben. Ebenso ist es ihm vorbehalten, darüber zu bestimmen, wo die Akten eingesehen werden sollen. Selbstverständlich wäge ich in jedem Einzelfall – gerade auch im Interesse aller betroffenen Bürgerinnen und Bürger – sorgfältig ab, welche Maßnahmen zur Ermittlung des Sachverhalts jeweils geeignet und notwendig sind.

6.4
Sozialhilfeanträge: Auskünfte durch Ärzte und Banken

Wer Sozialhilfe bekommen will, muß dem Sozialamt zunächst einmal selbst etwas liefern, nämlich Antworten auf eine Fülle von Fragen zu seiner Situation. Mitunter reichen den Sozialbehörden die Auskünfte der Antragsteller nicht aus, sondern es sind z. B. Nachfragen bei Ärzten oder Kreditinstituten nötig. Deshalb lassen die Behörden die Antragsteller oft Erklärungen unterschreiben, in denen diese der Erteilung der erforderlichen Auskünfte durch Dritte zustimmen.

Die Behörden stützen ihre Praxis auf § 60 SGB I, der den Antragsteller verpflichtet, alle für die Durchführung des Verfahrens benötigten Tatsachen anzugeben. Dazu gehört auch, daß er auf Verlangen der Behörde Auskünften anderer Stellen zuzustimmen hat. Es geht daher hier nicht um die Frage, ob der Antragsteller zustimmen muß, sondern in welchen Fällen dies zu geschehen hat und wie die Zustimmungserklärung aussehen muß. Unzulässig sind auf jeden Fall die folgenden vielfach verwendeten Formulierungen, mit denen sich die Sozialbehörden ermächtigen lassen, Auskünfte bei Ärzten und Banken einzuholen.

Beispiel 1:

IV Allgemeines

Besitz eines Kraftfahrzeuges ☐ Ja ☐ Nein

Fahrzeug wird selbst geführt ☐ Ja ☐ Nein

Finanzierung des Fahrzeuges mit öffentlichen Mitteln ☐ Ja durch _____ ☐ Nein

Angehörige führen notwendige Fahrten durch ☐ Ja ☐ Nein

Name, Vorname der Angehörigen _____ Anschrift _____

Umfang der Fahrten durch Angehörige _____

Erklärung des Hilfesuchenden

Ich versichere, daß die Angaben in diesem Antrag der Wahrheit entsprechen und keine Angaben verschwiegen wurden. Mir ist bekannt, daß ich mich durch unwahre oder unvollständige Angaben der Strafverfolgung aussetze und zu Unrecht bezogene Leistungen zurückzahlen muß.

Ich verpflichte mich, jede Änderung der Tatsachen, insbesondere die Veränderung der Einkommens-, Familien- und Aufenthaltsverhältnisse sofort unaufgefordert mitzuteilen.

Den behandelnden Arzt, die Kliniken und die ärztlichen Gutachter entbinde ich hiermit gegenüber dem Sozialamt von der ärztlichen Schweigepflicht. Ich bin damit einverstanden, daß das Sozialamt der Stadt Fulda bei anderen Stellen Auskünfte, die für die Entscheidung über meinen Antrag erforderlich sind, einholt und befreie die Stellen von den Vorschriften der §§67ff SGBX.

Datum _____ Unterschrift des Antragstellers bzw. des gesetzlichen Vertreters _____ Unterschrift des Aufnehmenden _____

Erforderliche Unterlagen für die Antragsbearbeitung

Dem Antrag sind folgende Unterlagen beizufügen:

1. Nachweis über alle Einkünfte (z.B. Lohnabrechnung, Sozialhilfebescheid, Wohngeldbescheid usw.)
2. Nachweis über alle Vermögenswerte (z.B. Girokontoauszüge, Sparbücher, Grundbuchauszug usw.)
3. Nachweis über die zu zahlende Kaltmiete (Mietvertrag oder Mietbescheinigung)
4. Bei bestehenden Zahlungsverpflichtungen (z.B. Versicherungsbeiträge, Zinsen und Abträge für Darlehen usw.) ist ebenfalls ein entsprechender Nachweis (z.B. Versicherungspolice, letzte Beitragsquittung, Darlehensvertrag usw.) beizufügen.
5. Ausgefüllte und unterschriebene Erklärung über bestehende Spar- und Girokonten (Formular liegt an)
6. Schwerbehindertenausweis
7. Bestallungsurkunde des Amtsgerichtes über Bestellung eines Vormundes oder Pflegers (nur soweit Vormundschaft oder Pflegschaft besteht)

Beispiel 2:

VII. Krankenversicherung des Hilfesuchenden (und des Ehegatten):

1. Mitglied der ..... Krankenkasse ..... seit ..... Beitrag mtl. ..... DM
2. Als Familienangehöriger des/der .....
   in der ..... Krankenkasse in .....
3. Bis zum ..... versichert bei der ..... Krankenkasse .....
   ausgeschieden weil .....
   (Anlage beachten)

VIII. Rentenversicherung des Hilfesuchenden (und des Ehegatten):

Beiträge wurden entrichtet von ..... bis ..... zur Arbeiterrentenversicherung
von ..... bis ..... zur Angestelltenversicherung
von ..... bis ..... zur Knappschaftsversicherung
von ..... bis ..... zur Handwerkerversicherung
von ..... bis ..... zur Seekassenrentenversicherung

Versicherungs-Nr. ..... Bez. d. Versicherungsanstalt .....
..... Rente/ Ruhegeld beantragt am ..... bei .....
.....

IX. Sonstige Ansprüche des Hilfesuchenden (und des Ehegatten):

1. Es wurden Ansprüche wegen .....
   gegen ..... geltend gemacht.
   Bei Unfällen:
   a) Art .....
   b) aufgenommen durch .....
   c) verschuldet durch .....
2. Sterbe-/ Lebensversicherung abgeschlossen am ..... bei .....
   Nr. der Police .....
   mitversichert sind folgende Angehörige: .....
   im Todesfall werden ..... DM gezahlt an .....
   im Erlebensfall sind DM ..... fällig am ..... und an ..... zu zahlen.

X. Arbeitsfähigkeit des Hilfesuchenden (und des Ehegatten)

1. Arbeitsfähig / nicht arbeitsfähig.
2. Ist die Arbeitsfähigkeit gemindert? .....
3. Nachweis der Arbeitsunfähigkeit oder Minderung der Arbeitsfähigkeit durch .....
4. Arbeitseinsatz aus folgenden sonstigen Gründen nicht möglich: .....
   .....
5. Beim Arbeitsamt in ..... am ..... zum Arbeitseinsatz gemeldet.
6. Nicht in Arbeit vermittelt, weil .....
7. Anerkennung als Schwerbehinderter/ MdE beantragt am ..... bei .....

XI. Sozialhilfe oder entsprechende Mittel wurden bereits früher / noch nicht — bezogen von .....
.....
Die zu gewährenden Barleistungen bitte ich auf folgendes Giro-/ Postscheckkonto (aus Sparkonto nicht möglich) zu überweisen:
Kto.Nr. ..... bei ..... BLZ: .....
Name u. Anschrift des Kontoinhabers: .....

XII. Ich versichere, daß meine vorstehenden Angaben wahr sind. Mir ist bekannt, daß ich wegen wissentlich falscher oder unvollständiger Angaben strafrechtlich verfolgt werden kann und für zu Unrecht erlangte Hilfe erstattungspflichtig bin. Mir ist ferner bekannt, daß meine Ansprüche gegen Drittverpflichtete im Rahmen der gesetzlich zulässigen Grenze auf den Träger der Sozialhilfe übergeleitet werden können. Ich bestätige ausdrücklich, davon unterrichtet worden zu sein, daß ich jede Änderung der Familien-, Einkommens- und Vermögensverhältnisse, vorübergehende Abwesenheit, Krankenhausaufenthalte usw., auch von Haushaltsangehörigen, unverzüglich und unaufgefordert dem Träger der Sozialhilfe mitzuteilen habe. Die Aufnahme jeder Arbeit, auch Gelegenheitsarbeit, werde ich vor Aufnahme der Arbeit gleicherweise anzeigen.
Die Behörden, Sparkassen und Banken sowie das Postsparkassenamt Hamburg/München ermächtige ich gegenüber dem Träger der Sozialhilfe zur uneingeschränkten Auskunftserteilung über meine Vermögensverhältnisse bzw. Konten und entbinde diese Stellen von der Schweigepflicht bzw. dem Bankgeheimnis.
Gleicherweise entbinde ich alle Ärzte, die mich behandelt haben oder denen ich vorgestellt worden bin oder werde, von der ärztlichen Schweigepflicht gegenüber dem Träger der Sozialhilfe.

.....
(Unterschrift des Antragstellers)

Antrag entgegengenommen und auf Vollständigkeit geprüft:
am ..... durch .....
(Name u. Dienstbezeichnung)

Derart pauschale Einwilligungserklärungen sind rechtlich unzulässig. Hier wie sonst gilt es, die vom Bundesverfassungsgericht in seiner Entscheidung zum Volkszählungsgesetz von 1983 formulierten Anforderungen zu beachten. Vor jeder Entscheidung über die Verarbeitung seiner Daten muß der Betroffene in der Lage sein, den Verarbeitungszweck und die Verarbeitungskonsequenzen genau zu übersehen. Nur solange dieser Forderung Rechnung getragen wird, hat der Betroffene die Chance, sein verfassungsrechtlich garantiertes informationelles Selbstbestimmungsrecht wahrzunehmen. Kurzum: Die Einwilligungserklärung muß daher den Verwendungszweck ebenso erläutern, wie den konkreten Anlaß, aus dem die Information verlangt wird, und überdies konkrete Angaben über den Empfänger sowie über den Umfang der zu offenbarenden Daten und den dafür erforderlichen Zeitpunkt enthalten.

Dem Bürger muß außerdem zunächst Gelegenheit gegeben werden, selbst mit entsprechenden Belegen entscheidungserhebliche Tatsachen glaubhaft zu machen. In aller Regel ist es deshalb nicht erforderlich und daher auch unzulässig, daß sich Sozialbehörden schon bei der Antragsstellung grundsätzlich ermächtigen lassen, Auskünfte bei Dritten einzuholen.

Eine empfehlenswerte Zustimmungserklärung für Auskünfte durch Ärzte sieht beispielsweise das unter meiner Mitwirkung geschaffene Formular für das automatisierte Berechnungsverfahren HES-SIAS (Hessisches Sozialhilfe Informations- und Abrechnungssystem) vor.

2.15 Begründung des Antrages

Weitere Ausführungen auf einem Beiblatt vornehmen.

Gültige vorgelegte Ausweispapiere

Art und Nummer _____

Ausstellende Behörde _____

Erklärung des Hilfesuchenden (oder des gesetzlichen Vertreters für den Hilfesuchenden):

Ich versichere, daß die vorstehenden Angaben vollständig sind und der Wahrheit entsprechen. Ich verpflichte mich, alle Änderungen, die für die Bewilligung der Leistung maßgebend sind — insbesondere Familien-, Einkommen- und Vermögensverhältnisse sowie Wohnungswechsel — unverzüglich und unaufgefordert der bewilligenden Stelle mitzuteilen. Mir ist bekannt, daß ich mich durch unvollständige oder unwahre Angaben strafbar mache und daß ich zu Unrecht bezogene Leistungen erstatten muß.

Ich ermächtige ebenfalls das Geldinstitut, an das Leistungen überwiesen wurden, mit Wirkung auch meinen Erben und etwaigen Verfügungsberechtigten gegenüber, überzahlte Beträge auf Anforderung des Sozialhilfeträgers zurückzuüberweisen.

Im Rahmen meiner Mitwirkungspflicht nach dem Sozialgesetzbuch (§§ 60—67 SGB, 1. Buch) bin ich verpflichtet, diejenigen Ärzte, die mich behandelt haben oder denen ich vorgestellt worden bin oder werde, auf Anforderung von der ärztlichen Schweigepflicht gegenüber dem Träger der Hilfe zu entbinden, soweit dies für die Gewährung der Hilfe erforderlich ist.

Mir ist bekannt, daß meine personenbezogenen Daten zur Durchführung der Berechnung von Leistungen in einer Anlage zur automatisierten Datenverarbeitung gespeichert werden.

Vorgelesen, genehmigt und unterschrieben:

_____ _____

(Unterschrift des Hilfesuchenden bzw. seines gesetzlichen Vertreters, falls er Antragsteller ist) **(Unterschrift des Ehegatten)**

Wenn Antragsteller und Hilfesuchender nicht identisch sind, Name und Anschrift des Antragstellers angeben:

_____

(Name und Vorname) **(Wohnort, Straße, Haus-Nr.)** **(Unterschrift)**

Zur Auskunfterteilung durch Ärzte, Sparkassen, Banken usw. ist eine besondere Erklärung abzugeben.

☐ **Die vorstehenden Angaben wurden überprüft und sind glaubhaft. Der Antrag wird befürwortet.**

☐ **Die folgenden Angaben erscheinen nicht glaubhaft, weil**

_____

_____

Antrag entgegengenommen und auf Vollständigkeit geprüft: _____

(Unterschrift und Dienstbezeichnung) **(Datum)**

Weiterleitungsvermerk (soweit erforderlich)

_____

(Ort) **(Datum)**

Abzusenden an: **Absendende Behörde:**

_____ _____

_____ _____

_____ _____

(Unterschrift und Dienstbezeichnung)

Eine Ermächtigung zur Einholung von Auskünften bei Banken könnte etwa folgendermaßen lauten:

K III/1 _____, den _____

_____
Name, Vorname

_____
Straße, Hausnummer

_____
PLZ, Wohnort

V o l l m a c h t s u r k u n d e gemäß § 172 BGB

Ich ermächtige und beauftrage hiermit die nachstehend genannte Bank / Sparkasse dem Landkreis Fulda, 6400 Fulda, Wörthstr. 15, Auskunft über den Stand und die Bewegungen auf meinem Konto / meinen Konten innerhalb des letzten halben Jahres zu erteilen.

_____ _____
Bezeichnung des Geldinstituts und Ort der Niederlassung

_____ _____

_____ _____

_____ _____

_____
Unterschrift, wie beim Geldinstitut hinterlegt

Der Hessische Landkreistag hat eine Arbeitsgruppe gebildet, die unter meiner Beratung Formularmuster entwerfen soll, die diese Grundsätze berücksichtigen.

7. Statistik

7.1
Volkszählung

7.1.1
Abschluß der manuellen Bearbeitung und Vernichtung der Erhebungsunterlagen

Lag der Schwerpunkt meiner Prüftätigkeit während der Erhebungsphase der Volkszählung im Jahre 1987 bei den Erhebungsstellen der Gemeinden (vgl. 16. Tätigkeitsbericht, Ziff. 3.4.2), ging es 1988 – wie im letzten Tätigkeitsbericht (Ziff. 3.7) angekündigt – in erster Linie um die datenschutzrechtlichen Anforderungen an die Aufbereitung, Auswertung und Vernichtung der Erhebungsunterlagen durch das Statistische Landesamt.

Vor allem im ersten Halbjahr 1988 wurden mehrfach Kontrollbesuche in den Außenstellen des Statistischen Landesamtes in Korbach und Wiesbaden (Luisenstraße) durchgeführt. Dabei wurden sowohl die räumlichen, organisatorischen, personellen und technischen Maßnahmen der Datensicherheit als auch die Einhaltung der datenschutzrechtlichen Vorgaben für die manuelle Bearbeitung der Erhebungsunterlagen geprüft. Mängel bei der Gebäudesicherung konnten – auch mit Hilfe von Fachleuten des Landeskriminalamtes – nach und nach beseitigt werden, so daß im Ergebnis ein datenschutzrechtlich akzeptabler Standard erreicht wurde. Trotz der insgesamt guten Kooperation mit dem Statistischen Landesamt im Bereich der Datensicherheit mußte ich im Februar 1988 eine Beanstandung wegen der monatelangen Verzögerung von Datensicherheitsvorkehrungen androhen und die Hessische Staatskanzlei einschalten.

Bei der manuellen Bearbeitung der Erhebungsunterlagen stand die Prüfung der Einhaltung des Trennungsgebotes nach § 15 Abs. 1 Volkszählungsgesetz 1987 im Vordergrund. Nach dieser Vorschrift waren die Hilfsmerkmale mit wenigen Ausnahmen unverzüglich nach Durchführung der Eingangskontrollen bei den Statistischen Ämtern von den Erhebungsmerkmalen zu trennen und gesondert aufzubewahren. Dazu zählten z. B. die Vor- und Familiennamen der Haushaltsmitglieder und des Wohnungsinhabers. Die Prüfergebnisse habe ich in einer ausführlichen Stellungnahme, zu der mich das Verwaltungsgericht Gießen aufgefordert hatte, im August 1988 dargelegt; dieses Papier ist auch in mehreren Verwaltungsstreitverfahren vor anderen Gerichten zitiert bzw. vorgelegt worden. Keine Beanstandung gab es im Hinblick auf die Trennung der Haushaltsmantelbögen von den übrigen Erhebungsunterlagen. Dagegen mußte ich kritisieren, daß die Trennung des Namensteils der Regionalliste von deren Organisationsteil erst nach dem Transport der Unterlagen von Korbach nach Wiesbaden erfolgte und beide Teile dort zwar getrennt, aber zusammen in einem Raum aufbewahrt wurden.

Wichtiger noch als die Trennung der Hilfs- und Erhebungsmerkmale ist allerdings für den Datenschutz die fristgerechte und ordnungsgemäße Vernichtung der Erhebungsunterlagen. Dafür schreibt § 15 Abs. 2 VZG vor, daß die Erhebungsvordrucke – dazu gehören nach der Rechtsprechung des Bundesverfassungsgerichts auch die Organisationspapiere – zum frühestmöglichen Zeitpunkt, spätestens zwei Wochen nach Feststellung der amtlichen Bevölkerungszahl des Landes, zu vernichten sind. Diese Bestimmung hat das Bundesverfassungsgericht dahingehend interpretiert, daß die Statistischen Landesämter gehalten seien, für jede der Erhebungsunterlagen den jeweils frühestmöglichen Zeitpunkt zu ermitteln und die Vernichtung zu diesem Zeitpunkt vorzunehmen. Art, Geschwindigkeit und Organisation der Datenaufbereitung hätten sich an diesem Gebot frühestmöglicher Löschung und Vernichtung zu orientieren (Beschluß vom 24.09.1987, Az.: 1 BvR 970/87; zu diesem Beschleunigungsgebot vgl. auch 16. Tätigkeitsbericht, Ziff. 3.7.1). Deshalb habe ich im Juli 1988 das Statistische Landesamt gebeten, mir ein detailliertes, nach der Art der Erhebungsunterlagen gegliedertes Konzept für die Vernichtung vorzulegen. Dabei habe ich klargestellt, daß das vom Bundesverfassungsgericht formulierte Beschleunigungsgebot es unter keinen Umständen zuläßt, alle Unterlagen bis zu dem gesetzlich möglichen spätesten Zeitpunkt, d. h. also zwei Wochen nach Feststellung der amtlichen Bevölkerungszahl des Landes, aufzubewahren; dies wurde und wird allerdings in anderen Bundesländern so praktiziert und teilweise von den Verwaltungsgerichten auch akzeptiert (vgl. z. B. VGH Baden-Württemberg, Beschluß vom 7. Dezember 1987, Az.: Z 10 S 482/87).

Über das Konzept zur Vernichtung der Erhebungsunterlagen gab es einen intensiven Schriftwechsel mit dem Statistischen Landesamt – der teilweise auch der Staatskanzlei zur Kenntnis gegeben wurde – und eine Reihe von Gesprächen zur Ermittlung bzw. Festlegung der Einzelheiten. Im Ergebnis konnte erreicht werden, daß das Land Hessen nicht nur als erstes Bundesland am 11. Oktober 1988 eine Gesamtbevölkerungszahl bekanntgegeben hat, sondern nach meiner Kenntnis auch mit der Vernichtung der Erhebungsunterlagen frühzeitiger begonnen hat als die anderen Bundesländer. Mit Schreiben vom 15. November 1988 hat mir das Statistische Landesamt mitgeteilt, daß zu diesem Zeitpunkt sämtliche Wohnungs- und Personenbögen beseitigt worden waren, und zwar auch aus solchen Gemeinden, die das Zählergebnis angefochten hatten. Auch mit dem Namensteil der Regionallisten und den Haushaltsmantelbögen aus den Kommunen, die keinen Widerspruch eingelegt hatten, wurde in gleicher Weise verfahren. Die Erhebungsbögen aus der Arbeitsstättenzählung sollten bis Januar 1989 vernichtet sein. Bei den Gemeinden, die gegen die für sie festgestellte Bevölkerungszahl Widerspruch eingelegt haben, wurden die Erhebungsunterlagen – mit Ausnahme der bereits vernichteten Wohnungs- und Personenbögen – bis zur Erstellung eines zusätzlichen „Protokolls", das die Korrektheit des Zählergebnisses durch nochmalige Nachzählung für ein mögliches Verwaltungsstreitverfahren belegen sollte, aufgehoben und danach vernichtet. Insgesamt ist damit die Masse der Erhebungsunterlagen aus der Volkszählung 1987 im Jahr 1988 vernichtet worden.

Im Hinblick auf die technische Abwicklung der Vernichtung der Erhebungsunterlagen hatte ich schon frühzeitig das Statistische Landesamt darauf hingewiesen, daß nur Unternehmen mit einem akzeptablen Sicherungsstandard mit der Vernichtung beauftragt werden könnten. Das beauftragte Unternehmen haben meine Mitarbeiter mehrfach unangemeldet aufgesucht und dabei sowohl die Einhaltung der Sicherungsmaßnahmen als auch phasenweise die Vernichtung der Belege selbst kontrolliert. Dabei konnten keine Mängel festgestellt werden.

7.1.2
Automatisierte Verarbeitung

Der zweite Schwerpunkt lag 1988 auf der Überprüfung der für die automatisierte Verarbeitung verwendeten Programme und der Kontrolle von Datensicherheit und Revisionsfähigkeit bei der automatisierten Verarbeitung der Volkszählungsdaten im Hessischen Statistischen Landesamt (HSL) und in dessen Auftrag in der Hessischen Zentrale für Datenverarbeitung (HZD).

7.1.2.1
Verschlüsselung

Zentrale Vorschrift für die maschinelle Verarbeitung der Volkszählungsdaten ist § 15 Abs. 3 VZG. Diese Bestimmung sieht vor, die laufenden Nummern und Ordnungsnummern durch verfremdete Ziffern, die nur die statistischen Zusammenhänge festhalten, zu ersetzen. Wie das Bundesverfassungsgericht zu Recht und entgegen einem verbreiteten Mißverständnis klargestellt hat, bleibt der Datenbestand aus der Volkszählung auch nach dieser Umcodierung personenbeziehbar; die Vergabe der Zufallsnummern verringert lediglich das Deanonymisierungsrisiko, weil eine Reindividualisierung nur mit technischem Zusatzwissen möglich ist. Mit der Ausgestaltung des einschlägigen Verfremdungsprogramms VZ 100 mit der Zielrichtung, eine größtmögliche faktische Anonymisierung zu erzielen, hat sich eine kleine Arbeitsgruppe der Datenschutzbeauftragten befaßt, an deren Arbeit ich mich beteiligt habe. Voraussetzung dafür, daß das Programm VZ 100 die Anforderungen des § 15 Abs. 3 und 4 VZG erfüllt, sind folgende Maßnahmen:

1. Die Startzahl für die Verschlüsselungsläufe wird nicht vorgegeben, vielmehr wird maschinell eine Zufallsstartzahl erzeugt.

2. Bei jedem Lauf muß die Zufallsstartzahl neu erzeugt werden, wobei der Umfang der in einen Lauf einbezogenen Datensätze möglichst klein sein muß.

3. Die Zufallsstartzahl darf weder angezeigt noch ausgedruckt und nicht länger als bis zum Programmende gespeichert werden.

4. Nur das notwendige Minimum an Mitarbeitern darf im Statistischen Landesamt bzw. im Rechenzentrum den Verfremdungsalgorithmus kennen.

Mit dem Hessischen Statistischen Landesamt ist geklärt, daß nach diesen Vorgaben verfahren wird.

7.1.2.2
Dezentrale Benutzerverwaltung

Die automatisierte Verarbeitung der Volkszählungsdaten erfolgt weitgehend in der Hessischen Zentrale für Datenverarbeitung, da das Statistische Landesamt kaum über eigene Rechnerkapazitäten verfügt.

Die HZD setzt in einem Pilotprojekt ACF2 (Access Control Facility) als neue Software für die Benutzer- und Zugriffskontrolle auf ihren Großrechnern ein. Bereits im letzten Tätigkeitsbericht (Ziff. 4.2.1) habe ich ausführlich Grenzen und Möglichkeiten dieser Datenschutzsoftware beschrieben und mich auch zu den Voraussetzungen und Rahmenbedingungen für eine Dezentralisierung der Benutzerverwaltung geäußert.

Deshalb lag es nahe, 1988 die Benutzerprofile und Berechtigungen für die Mitarbeiter des Hessischen Statistischen Landesamtes zu überprüfen, wie sie auf dem HZD-Rechner unter ACF2 für die Verarbeitung der Volkszählungsdaten definiert sind. Dabei habe ich festgestellt, daß das HSL bereits eine dezentrale Benutzerverwaltung vornimmt – auch für den Bereich der Volkszählung.

Die Einbeziehung der Volkszählung in ein solches Pilotprojekt ist jedoch besonders problematisch und ein unnötiges Risiko. Deshalb habe ich dem HSL und der HZD geraten, den Volkszählungsbereich aus dem Pilotprojekt zu nehmen. Das HSL ist dieser Anregung nicht gefolgt. Auch die von mir informierte Staatskanzlei sieht hier anscheinend keine Probleme.

Gegenüber der HZD habe ich aus diesem Anlaß grundsätzlich zur dezentralen Benutzerverwaltung und zu den „Datensicherungsstandards der HZD (DS-S)" Stellung genommen und eine Reihe von Fragen zu dem Pilotprojekt gestellt. Die HZD hat mir geantwortet, daß es sich hierbei um ein Pilotprojekt handelt, das auf das HSL beschränkt ist und mit dem „die dezentrale Benutzerverwaltung mit allen organisatorischen Randbedingungen erprobt werden" soll. „Dazu gehören u. a.

- Ablauf bei der Einstellung der USER-ID durch einen Benutzer;
- Ablauf bei einer Regeländerung durch einen Benutzer;
- organisatorische Abläufe beim Benutzer selbst;
- Kontrollmöglichkeiten und Hilfsleistungen seitens der HZD;
- Ausstattung der Stelle beim Benutzer (z. B. DV-Wissen);
- Schulungsmaßnahmen."

Die HZD will bis Anfang 1989 den Pilotversuch ausgewertet haben und das Ergebnis anschließend mit mir erörtern.

7.1.2.3
Revisionsfähigkeit der Datenverarbeitung

Die HZD bietet zwei grundsätzlich verschiedene Möglichkeiten für die Nutzung ihrer Rechner durch ihre Kunden an: Den „Betrieb von DV-Verfahren" und die „Bereitstellung von DV-Kapazitäten". Beim „Betrieb von DV-Verfahren" führt die HZD Aufträge nach Vorgaben der Benutzer (Art, Umfang, Terminierung) selbst durch. Sie ist dem Auftraggeber für die Richtigkeit, Vollständigkeit und Termintreue der Produktion verantwortlich. Dagegen stellt sie bei der „Bereitstellung von DV-Kapazitäten" dem Benutzer ihre maschinellen Ressourcen zur selbständigen Nutzung zur Verfügung.

Der wesentliche Unterschied beider Leistungsarten liegt nach Aussage der HZD in der Verantwortlichkeit für die Steuerung/Verwaltung der vorgehaltenen Ressourcen und für die Richtigkeit der erzielten Ergebnisse. Die unterschiedliche Verantwortlichkeit spiegelt sich auch in den von der HZD getroffenen technischen und organisatorischen Maßnahmen zur Datensicherheit wider. Diese Unterschiede werden aber meines Erachtens in den „Datensicherungsstandards der HZD (DS-S)" nicht hinreichend deutlich. Die HZD hat mir eine Überprüfung der Darstellung bei der nächsten Überarbeitung zugesagt.

Das HSL hat nur die Beleglesung als „Betrieb von DV-Verfahren" in der HZD durchführen lassen. Für dieses Verfahren wurden von der HZD besondere Maßnahmen zum Datenschutz getroffen.

Die ganze übrige maschinelle Verarbeitung wie z. B. die Plausibilitätsprüfung und die eigentlichen Auswertungen der Volkszählungsdaten wird in der Leistungsart „Bereitstellung von DV-Kapazitäten" abgewickelt. Auch in diesem Fall sind natürlich die Grundsätze der Funktionstrennung und der Revisionsfähigkeit des Verfahrensablaufs zu erfüllen (§ 10 Abs. 3 Nr. 10 HDSG). Einige der Maßnahmen können dann aber nicht von der HZD, sondern müssen vom HSL getroffen werden. Deshalb habe ich das HSL um eine ausführliche Beschreibung der für die Verarbeitung der Volkszählungsdaten getroffenen Maßnahmen gebeten. Was die Revisionsfähigkeit der Verarbeitung der Volkszählungsdaten anbelangt, konnte geklärt und stichprobenartig überprüft werden, daß sich der Verfahrensablauf nachvollziehen läßt.

7.1.3
Bußgeldverfahren

Wie bereits im letzten Tätigkeitsbericht dargestellt (vgl. Ziff. 3.7.4), werden die Bußgeldverfahren nach § 23 Bundesstatistikgesetz wegen verweigerter oder unvollständiger Ausfüllung der VZ-Erhebungsunterlagen vom Regierungspräsidium Kassel abgewickelt. Bis Ende 1988 waren von den Gemeinden mehr als 35.000 Anzeigen in Kassel eingegangen und etwa 5.000 Bußgeldbescheide bereits erlassen worden. Ich habe mich im Rahmen eines Prüfbesuchs beim Regierungspräsidium Kassel über die Einzelheiten der Verarbeitung und die getroffenen Vorkehrungen informiert. Dabei konnte ich mich davon überzeugen, daß das landeseinheitliche automatisierte Bußgeldverfahren HESOWI ohne Abweichungen auch für die Volkszählungsfälle eingesetzt wird. Es gab auch keinerlei Anhaltspunkte dafür, daß die vom Bundesverfassungsgericht noch einmal unterstrichene Zweckbindung der Bußgelddaten nicht beachtet wird.

7.1.4
Künftige Prüfungsschwerpunkte

Mit der Vernichtung der Erhebungsvordrucke und der Herstellung des endgültigen, in den Hilfsmerkmalen verfremdeten und auf die Blockseite bezogenen Datensatzes (Satzart 30) ist die Volkszählung 1987 für mich jedoch keineswegs abgeschlossen. Z.Zt. überprüfe ich die in § 1 Abs. 4 Volkszählungsgesetz vorgesehene Wiederholungsbefragung. Sie dient der Prüfung der Zuverlässigkeit der Ergebnisse aus der Haupterhebung; dabei werden für eine kleine Stichprobe der Bevölkerung die Daten aus einem auf sechs Fragen reduzierten Personenbogen abgeglichen mit den von den gleichen Personen im ersten Durchgang gemachten Angaben. Meine Prüfung erstreckt sich wie bei der Haupterhebung sowohl auf die manuelle Bearbeitung der Erhebungsunterlagen einschließlich der rechtzeitigen Vernichtung als auch auf die automatisierte Durchführung des Datenabgleichs. Der zweite unmittelbar anstehende Problembereich ergibt sich aus § 15 Abs. 4 Satz 4 VZG. Danach muß bei der Weitergabe oder Veröffentlichung

statistischer Ergebnisse aus der Volkszählung in kleinräumiger Gliederung ggf. höher als auf Blockseitenbasis aggregiert werden, um zu verhindern, daß ein Datensatz auf einen einzelnen Auskunftspflichtigen oder Betroffenen bezogen werden kann. Das entsprechende Programm liegt mir noch nicht vor.

7.2
Kommunalstatistik

7.2.1
Abschottung kommunaler Statistikstellen

7.2.1.1
Musterregelungen

Nach dem Hessischen Landesstatistikgesetz (HLStatG) vom 19. Mai 1987 (dazu zuletzt 16. Tätigkeitsbericht, Ziff. 5.1.3 und 13.2) sind die Aufgaben der Kommunalstatistik einer Stelle innerhalb der Gemeindeverwaltung zu übertragen, die organisatorisch von anderen Verwaltungsstellen getrennt und räumlich sowie personell „abgeschottet" ist (§ 12 Abs. 3). Diese „kommunale Statistikstelle" darf über Aufgaben der amtlichen sowie der Kommunalstatistik hinaus keine auf den einzelnen Betroffenen gerichtete Verwaltungsaufgabe wahrnehmen.

Das Bundesstatistikgesetz vom 22. Januar 1987 macht die Existenz einer solchen vom Verwaltungsvollzug abgeschotteten Statistikstelle zur Voraussetzung für die Übermittlung von Einzelangaben aus Bundesstatistiken an die Gemeinden (§ 16 Abs. 5 BStatG). Für die Volkszählung im besonderen gilt gleiches aufgrund § 14 Abs. 1 Satz 3 VZG 1987: Jede Kommune, die vom Statistischen Landesamt Volkszählungsdaten auf Blockseitenbasis – d.h. nicht nur aggregierte Angaben auf Gemeindeteil- oder Gemeindeebene – bekommen will, muß eine von den anderen Ämtern und Abteilungen abgetrennte Statistikstelle vorweisen. Da ohne diese organisatorische Maßnahme auch keine kommunalen Umfragen zulässig sind (vgl. dazu 16. Tätigkeitsbericht, Ziff. 5.1.3.2, und in diesem Bericht Ziff. 7.2.2), ist eine funktionierende Kommunalstatistik ohne eine solche spezialisierte Verwaltungseinheit kaum noch möglich.

Für viele Kommunen ergeben sich aus dieser Rechtslage erhebliche Konsequenzen für die gewachsene Verwaltungsstruktur, etwa weil die Statistik derzeit noch bei Ämtern mit Verwaltungsvollzugsaufgaben wie dem Hauptamt oder dem Bauamt angesiedelt ist. Andere Gemeinden, insbesondere die Großstädte, haben weniger Probleme, das Abschottungsgebot umzusetzen, da schon bisher eigenständige Statistikämter oder -abteilungen existierten.

Um den betroffenen Gebietskörperschaften Vorgaben für die Realisierung der statistikgesetzlichen Anforderungen an die Hand zu geben, habe ich in einer Arbeitsgruppe mitgewirkt, die der Hessische Städtetag organisiert hat und an der außerdem Fachstatistiker aus mehreren hessischen Städten sowie ein Vertreter der Staatskanzlei als oberster Aufsichtsbehörde für die Landesstatistik teilgenommen haben. Diese Arbeitsgruppe hat im vergangenen Jahr

- das Muster einer Organisationsverfügung des Oberbürgermeisters/Bürgermeisters über die Zuweisung von Aufgaben und Befugnissen an die kommunale Statistikstelle,
- das Muster einer Dienstanweisung für diese Stelle, die die organisatorischen und technischen Maßnahmen zur Wahrung des Statistikgeheimnisses und der strikten Zweckbindung enthält,
- das Muster einer Satzung über die regelmäßigen Datenübermittlungen durch andere Ämter an die kommunale Statistikstelle nach § 12 Abs. 4 HLStatG

erarbeitet. In der Dienstanweisung sind im einzelnen geregelt u.a. die aus dem Statistikgeheimnis resultierenden Verschwiegenheitspflichten der Mitarbeiter der Statistikstelle, die Aufbewahrung der Erhebungsunterlagen, die Maßnahmen der räumlichen Datensicherung und der Einsatz automatisierter Datenverarbeitung.

Der Hessische Städtetag hat diese drei Mustertexte allen kreisfreien und Sonderstatusstädten bereits zugesandt und in seinem Nachrichtendienst Nr. 19/1988 einen Hinweis darauf aufgenommen, daß diese Unterlagen auf Anforderung auch anderen Kommunen übersandt werden können. Die Städte Frankfurt und Wiesbaden haben ihre Kommunalstatistik bereits auf der Grundlage der von der Arbeitsgruppe vorgelegten Texte neu geordnet.

Zu beachten ist allerdings, daß diese Mustertexte keineswegs in allen oder auch nur den größeren Kommunen unverändert benutzt bzw. in Kraft gesetzt werden können. In jedem Fall ist genau zu prüfen, inwieweit die vorgeschlagenen Regelungen an die konkrete Situation in der jeweils betroffenen Gemeinde angepaßt werden müssen. Ich bin gerne bereit – wie bereits in vielen Fällen seit dem Inkrafttreten des Landesstatistikgesetzes geschehen –, auch künftig hierzu beratende Hinweise zu geben.

7.2.1.2
Abschottung der Statistikstellen von Stellen mit Planungsaufgaben

Der Umlandverband Frankfurt (UVF) wollte von mir begutachtet haben, ob er gleichfalls besondere Abschottungsmaßnahmen treffen müsse, um statistische Erhebungen durchführen zu dürfen und Einzelangaben aus Bundes- und Landesstatistiken erhalten zu können.

Das Abschottungsgebot des Hessischen Landesstatistikgesetzes gilt zwar auch für Gemeindeverbände und Zweckverbände (§ 12 Abs. 3 und 8), es verlangt jedoch nur die Trennung der Statistikstellen von solchen Stellen, die „auf den einzelnen Betroffenen gerichtete Verwaltungsaufgaben wahrnehmen". Die Frage war also, ob der Umlandverband Frankfurt, der fast ausschließlich Planungsaufgaben hat, als eine Stelle mit derartigen Verwaltungsaufgaben anzusehen ist.

Das Bundesverfassungsgericht hat im Volkszählungsurteil die Erstellung von Flächennutzungs- und Bebauungsplänen deshalb dem Verwaltungsvollzug zugeordnet, weil diese Pläne für die im jeweiligen Planungsgebiet gelegenen Grundstücke spezifizierte Festsetzungen über Art und Ausmaß der baulichen Nutzung und mithin Verwaltungsentscheidungen gegenüber dem Bürger träfen (BVerfGE 65, 1, 67). Diese Arten von Planung sind mithin nicht vereinbar mit dem gleichzeitigen Umgang mit statistischen Einzelangaben. Für andere Planungsformen ohne konkreten Bürgerbezug gilt dieses Prinzip dagegen nicht.

Beim UVF müssen daher die Überlegungen in Richtung einer Organisationsstruktur gehen, die nach unmittelbar bürgerbezogenen Planungsaufgaben einerseits sowie regional- und flächenbezogenen Planungen andererseits unterscheidet.

7.2.1.3
Statistikstellen und Wahlamt

Spezifische Organisationsprobleme entstehen auch da, wo die Kommunalstatistik mit dem Wahlamt verkoppelt ist, d. h. alle Mitarbeiter in beiden Bereichen tätig sind. Zwar sieht der oben (Ziff. 7.2.1.1) erwähnte Entwurf für eine Dienstanweisung für die Statistikstelle in Ziff. 4 ausdrücklich vor, daß eine befristete Zuordnung der in der Statistik tätigen Bediensteten zu der für die Durchführung von Wahlen zuständigen Organisationseinheit in der Wahlvorbereitungszeit möglich ist. Doch setzt diese Möglichkeit die prinzipielle Trennung der mit Wahlen und der mit Statistik befaßten Organisationseinheiten voraus. Dies ist auch deshalb konsequent, weil das Wahlamt etwa bei der Erteilung von Wahlscheinen, der Eintragung in das Wählerverzeichnis oder der Ablehnung dieser Eintragung Verwaltungsakte gegenüber dem Bürger erläßt und insoweit eindeutig dem Bereich Verwaltungsvollzug zuzuordnen ist.

Die für Januar 1989 terminierten Gespräche mit der Staatskanzlei, dem Städtetag und betroffenen Kommunen sollen dazu führen, ein Organisationsmodell zu finden, das den Vorgaben des § 12 HLStatG Rechnung trägt.

7.2.2
Kommunalstatistische Erhebungen durch private Institute

7.2.2.1
Rechtliche Anforderungen

Kommunen führen Umfragen häufig mit Hilfe privater Firmen durch. Dabei gilt: Werden die Arbeitsgänge von der Erhebung der Daten beim Bürger über die Erfassung bis zur Verarbeitung bzw. Auswertung nicht ausschließlich von der „abgeschotteten" kommunalen Statistikstelle (vgl. oben Ziff. 7.2.1) durchgeführt, sondern teilweise externen Privatfirmen, etwa Umfrageinstituten, übertragen, ist § 6 Hessisches Landesstatistikgesetz zu befolgen. Nach dieser Vorschrift ist die Beauftragung von Dritten mit einzelnen statistischen Arbeiten nur zulässig, sofern sichergestellt ist, daß die Datenschutzbestimmungen eingehalten werden und das Statistikgeheimnis gewahrt wird. Bei Kommunen ist der behördliche Datenschutzbeauftragte, bei Landesbehörden ist meine Dienststelle von dieser Vergabe zu unterrichten. Kommunen sind selbstverständlich nicht gehindert – wie bereits zahlreich geschehen –, zusätzlich zur Beratung des örtlichen Beauftragten auch meine Stellungnahme einzuholen.

Keine Anwendung findet das Landesstatistikgesetz, wenn die Gemeinde die gesamte Umfrage einer privaten Stelle überträgt. Gemeint sind damit Fälle, in denen die Kommunen nicht einzelne Arbeitsvorgänge nach außen vergeben, sondern nur das Untersuchungsthema festlegen und nach Abschluß der Umfrage den Auswertungsbericht des Instituts entgegennehmen.

Für die Einhaltung von Datenschutz und Statistikgeheimnis bei den beauftragten Privatfirmen ist es unerläßlich, daß dort zunächst einmal die für den nicht-öffentlichen Bereich geltenden Normen des Bundesdatenschutzgesetzes beachtet sind. Bei Markt- und Meinungsforschungsinstituten gilt der 4. Abschnitt des BDSG über die geschäftsmäßige Datenverarbeitung für fremde Zwecke. Solche Institute haben nach § 39 BDSG Meldepflichten gegenüber dem örtlich zuständigen Regierungspräsidium. Sie haben u. a. die verantwortlichen Funktionsträger, die Art der eingesetzten DV-Anlagen und die Art der verarbeiteten personenbezogenen Daten mitzuteilen. Sie müssen außerdem einen Datenschutzbeauftragten bestellen und diesen ebenfalls der Aufsichtsbehörde melden. Sie haben durch technische Maßnahmen sicherzustellen, daß Hilfsmerkmale, also vor allem Namen und Anschriften der Befragten, getrennt von den eigentlichen Befragungsdaten gespeichert werden (§ 36 BDSG). Darüber hinaus gelten die üblichen obligatorischen Standards der räumlichen, organisatorischen und technischen Datensicherung nach § 6 BDSG und der zugehörigen Anlage. Die genannten Pflichten treffen Umfrageinstitute völlig unabhängig davon, ob das Landesstatistikgesetz anzuwenden ist oder nicht.

Ich mußte bei der Überprüfung in den Geschäftsräumen wiederholt feststellen, daß diese Vorgaben von den mit den Umfragen betrauten Firmen nicht eingehalten wurden. Noch einmal: Ein privates Institut darf nicht mit der Erfassung

oder Auswertung von Bürgerdaten im Rahmen einer kommunalen Statistik beauftragt werden, wenn es die nach dem BDSG obligatorischen Maßnahmen nicht getroffen hat oder sie nicht jedenfalls noch vor Beginn der Umfrage realisieren kann und will. Sich davon zu überzeugen, ist zunächst Sache der den Vertrag abschließenden Kommune. Wiederholt mußte ich Gemeinden darauf aufmerksam machen, daß ich zwar gerne bereit bin, Räumlichkeiten und DV-Anlagen von Instituten – ggf. in Zusammenarbeit mit den Prüfbeamten des Regierungspräsidiums – zu kontrollieren, aber erwarte, daß zumindest die Einhaltung der Meldepflicht nach § 39 BDSG von den zuständigen Mitarbeitern der Kommune bereits vorgeprüft ist. Die Informationen aus dem Register der Meldungen nach § 39 BDSG stehen jedermann zur Verfügung.

7.2.2.2
Notwendige Unterlagen

Statistische Erhebungen, bei denen die Kommunen externe Stellen einsetzen wollen, kann ich nur dann datenschutzrechtlich bewerten, wenn mir folgende Unterlagen vorliegen:

1. Der Vertrag zwischen Kommune und Institut, der Gegenstand und Umfang der Auftragserteilung regelt. Vergessen wird dabei vielfach, genau festzulegen, was nach Durchführung der Untersuchung mit den Erhebungsunterlagen (z. B. Fragebögen) und den angefertigten Datenträgern geschehen soll, also insbesondere die Löschung bzw. Vernichtung zu diesem Zeitpunkt vorzusehen.

2. Das Anschreiben, mit dem das Institut selbst oder der Bürgermeister bzw. ein sonstiger Verantwortlicher der Kommune sich an den Bürger wendet und um Mitarbeit bittet. Hier ist in erster Linie wichtig, daß die Befragten korrekt über die Freiwilligkeit der Beantwortung, über Zweck, Art und Umfang der Erhebung und über die geplante Verfahrensweise bei der Verarbeitung ihrer Daten einschließlich der Löschung unterrichtet werden (vgl. § 9 Abs. 2 BDSG, § 14 Abs. 1 HLStatG). Abweichungen zwischen dem Vertrag (s.o. 1.) und dem Bürgeranschreiben – etwa was den Löschungszeitpunkt angeht – führen zu einer Falschinformation der Betroffenen und können selbstverständlich nicht toleriert werden.

3. Der Fragebogen, der den Befragten vorgelegt oder vom Interviewer im mündlichen Gespräch ausgefüllt wird. Die Sensitivität der erhobenen Informationen und der Grad ihrer Personenbeziehbarkeit bestimmen auch Art und Umfang der notwendigen Vorkehrungen zur statistischen Geheimhaltung und zur Datensicherung.

4. Bei schriftlichen Befragungen der Antwortumschlag. Diesen überprüfe ich daraufhin, ob durch die Formulierung der Empfängeranschrift gewährleistet ist, daß die ausgefüllten Fragebögen nicht an andere Stellen als entweder das beauftragte Institut oder die kommunale Statistikstelle gelangen.

Ein von mir erarbeitetes Merkblatt, das die wichtigsten Punkte enthält, die Kommunen bei der Durchführung von Erhebungen mit Fremdfirmen beachten müssen, wird Anfang 1989 zur Verfügung stehen.

8. Hochschulen

8.1
Verordnung über das Verfahren der Immatrikulation an den Hochschulen des Landes Hessen

Seit dem 1. August 1988 wird den Hessischen Universitäten, Kunsthochschulen und Fachhochschulen erstmalig detailliert vorgeschrieben, welche Studentendaten sie für welche Verwaltungszwecke verarbeiten dürfen und welche sonstigen Bedingungen dabei eingehalten werden müssen. An diesem Tag ist die Verordnung über das Verfahren der Immatrikulation an den Hochschulen des Landes Hessen vom 26. Mai 1988 in Kraft getreten (GVBl. I S. 228). Die Landesregierung hat damit endlich auf eine langjährige Forderung des Hessischen Datenschutzbeauftragten nach einer Regelung der Verarbeitung von Studentendaten für Verwaltungszwecke der Hochschulen reagiert (vgl. 13. Tätigkeitsbericht, Ziff. 2.4.2, 14. Tätigkeitsbericht, Ziff. 13.2.1, 15. Tätigkeitsbericht, Ziff. 11.1.5, 16. Tätigkeitsbericht, Ziff. 13.3). Die Verordnung ist aber auch eine Reaktion auf die vom Landtag anläßlich der Beratung meines 14. Tätigkeitsberichts einstimmig geäußerte Ansicht, „daß im Hochschulbereich Rechtsvorschriften über die konkrete Regelung über die Erhebung und Verarbeitung von personenbezogenen Daten zu Verwaltungszwecken geschaffen werden sollen" (Beschluß Nr. 7 zu meinem 14. Tätigkeitsbericht, Drucks. 11/6231 i.V.m. Protokoll der 84. Plenarsitzung vom 19. Juni 1986, S. 4979). Der Inhalt der Verordnung wurde mit mir abgestimmt und berücksichtigt weitgehend meine Forderungen.

8.1.1
Datensatz und Verwendungszweck

Anders als der Titel vermuten läßt, beschränkt sich die Verordnung keineswegs auf die Regelung der Datenverarbeitung im Zusammenhang mit der Immatrikulation. Sie enthält darüber hinaus auch Vorgaben für die Datenverarbeitung bei der Rückmeldung, der Beurlaubung, dem Studiengang und der Aufnahme eines Promotionsstudiums oder Doppelstudiums, der Mehrfachimmatrikulation und bei der Einschreibung als Zweit- oder Gasthörer. Für den Studenten wird dadurch eindeutig erkennbar, zu welchem konkreten Verwaltungszweck die Hochschule seine Daten erhebt und weiterverarbeitet.

Die Verordnung definiert abschließend, welche Studentendaten die Hochschulen für die genannten Verwaltungszwecke verarbeiten dürfen. Das sind nach der Rechtsprechung des Bundesverfassungsgerichts nur die für die jeweiligen Zwecke erforderlichen (BVerfGE 65, 46). Da die Vorstellungen der einzelnen Hochschulen über den Umfang der für Verwaltungszwecke erforderlichen Studentendaten zunächst höchst unterschiedlich waren, bereitete gerade die Festlegung dieses Datensatzes die größten Schwierigkeiten und zeitlichen Verzögerungen beim Zustandekommen der Verordnung.

Mit der genauen Definition des Datensatzes und der engen Bestimmung des Verwendungszweckes ist die wichtigste Voraussetzung für eine verfassungskonforme Verarbeitung der Studentendaten geschaffen, denn das Bundesverfassungsgericht hat die Zulässigkeit des Zwangs zur Angabe personenbezogener Daten davon abhängig gemacht, daß der Verwendungszweck bereichsspezifisch und präzise bestimmt ist und die Angaben für diesen Zweck geeignet und erforderlich sind (BVerfG a.a.O).

8.1.2
Studentenausweis

In einem Punkt, der in der Vergangenheit immer wieder Anfragen und Beschwerden von Studenten provozierte, hat die Immatrikulationsverordnung jetzt für Klarheit gesorgt: Die inhaltliche Ausgestaltung des Studentenausweises bleibt nicht mehr der einzelnen Hochschule überlassen, sondern § 4 Abs. 3 der Verordnung schreibt vor, welche Angaben der Studentenausweis zu enthalten hat. Dies war deshalb geboten, weil der Studentenausweis häufig auch hochschulexternen Personen oder Stellen vorgelegt wird. Der Student kann dabei oft – zumindest faktisch – nicht frei über die Offenbarung seiner Daten entscheiden, etwa wenn er bestimmte Preisermäßigungen erhalten will. Durch die Vorschrift wird nunmehr sichergestellt, daß der Studentenausweis künftig nur Daten enthält, die für den Verwendungszweck, d.h. den Nachweis, daß der Betroffene an einer Hochschule als Student immatrikuliert ist, unerläßlich sind.

8.1.3
Matrikelnummer

Eine Reaktion auf eine übliche Datenverarbeitungspraxis in den Hochschulen ist die Vorschrift in § 1 Abs. 5 Satz 2 der Immatrikulationsverordnung. In den Hochschulen werden beispielsweise häufig in allgemein zugängigen Räumen Listen von Teilnehmern an Veranstaltungen oder Listen mit Prüfungsergebnissen ausgehängt. Angesichts des Massenbetriebs ist dies oft die verwaltungstechnisch einfachste Form, die Betroffenen zu informieren. Datenschutzrechtlich akzeptabel ist das Verfahren jedoch nur, wenn für Dritte nicht erkennbar ist, auf welche Person sich die Daten beziehen. Das ist dann weitgehend gewährleistet, wenn die Angaben unter einer Kennziffer erfolgen, die grundsätzlich nur den Beteiligten bekannt ist. Dazu bietet sich zunächst die Matrikelnummer an. Voraussetzung für deren Verwendung ist allerdings, daß nicht aus ihr auf die betroffene Person geschlossen werden kann. Daher verbietet die Immatrikulationsverordnung Angaben nach § 2 Abs. 1 der Verordnung, d.h. Angaben zur Person, wie z.B Familienname, Geburtsdatum etc., in die Matrikelnummer aufzunehmen.

8.1.4
Löschungspflicht und Löschungsfristen

Die Verordnung läßt auch den gegenwärtig bei der automatisierten Verarbeitung der Studentendaten erreichten Entwicklungsstand nicht unberücksichtigt. Fast sämtliche Hochschulen wickeln ihre Studentenverwaltung im Wege der automatisierten Datenverarbeitung ab. Für die Dauer der Speicherung bzw. Löschung dieser Daten gab es jedoch bislang keine konkreten Vorschriften, entsprechend unterschiedlich sind die Hochschulen verfahren. Die Immatrikulationsverordnung (§ 1 Abs. 4) gibt den Hochschulen jetzt auf, innerhalb eines Jahres nach der Exmatrikulation bis auf Name, Studiengang, Matrikelnummer und Datum der Immatrikulation und Exmatrikulation sämtliche automatisiert gespeicherten personenbezogenen Daten zu löschen. Die verbleibenden Daten, die bis zu 60 Jahre gespeichert werden dürfen, haben lediglich die Funktion eines Aktennachweissystems. Die Daten der Studienbewerber, die nicht immatrikuliert wurden, müssen spätestens nach 2 Jahren vollständig gelöscht werden.

Mit der Löschungspflicht und den knappen Löschungsfristen geht die Immatrikulationsverordnung weit über die Anforderungen des Hessischen Datenschutzgesetzes hinaus und setzt damit zweifellos Maßstäbe für andere bereichsspezifische Datenverarbeitungsregelungen.

8.2
Hochschulstatistik

8.2.1
Hochschulstatistikgesetz

Die dringend erforderliche Novellierung des Hochschulstatistikgesetzes vom 21. April 1980 steht immer noch aus. Dies ist um so unverständlicher, als seit etlichen Jahren Konsens darüber besteht, daß das geltende Gesetz den Anforderungen, die das Bundesverfassungsgericht im Volkszählungsurteil von 1983 für Statistiken formuliert hat, nicht entspricht und deshalb geändert werden muß. Die Bundesregierung hatte auch bereits im Januar 1986, also noch in der vergangenen Legislaturperiode, dem Bundesrat einen Gesetzentwurf zugeleitet (Bundesrats-Drucks. 64/86). Dieser Entwurf verzichtete aus rechtlichen und methodischen Erwägungen allerdings auf die umstrittene Studienverlaufssta-

tistik. Gemeint ist damit eine statistische Aufbereitungsmethode, bei der mit Hilfe konstanter Identifikationsmerkmale Individualangaben der Studenten semesterweise zusammengeführt werden, um so Aussagen über Verweildauer, Studien- oder Hochschulwechsel sowie Studienerfolg und Studienabbruch zu erhalten. Der Streit, der um diese Teilstatistik der Hochschulstatistik entstanden ist, scheint die Hauptursache zu sein, daß das Warten auf die Novellierung wie das Warten auf Godot anmutet.

Auch wenn der zu Beginn des Jahres 1988 an Bundestag und Bundesrat gegangene 8. Bericht des beim Statistischen Bundesamt gebildeten Ausschusses für Hochschulstatistik (Bundestags- Drucks. 11/1993, Bundesrats-Drucks. 111/88) zum wiederholten Mal ein Plädoyer für die Unverzichtbarkeit der Studienverlaufsstatistik enthält, sehe ich keinen Grund, meine bereits im 14. Tätigkeitsbericht (Ziff. 5.2.1) begründete Ablehnung aufzugeben. In diesem Punkt bin ich im übrigen einer Meinung mit dem Hessischen Statistischen Landesamt und der Hessischen Landesregierung, die erst kürzlich wieder in einem Schreiben an das Statistische Bundesamt ihre ablehnende Haltung zur Studienverlaufsstatistik bekräftigt hat.

8.2.2
Exmatrikuliertenstatistik

Probleme gibt es freilich nicht nur bei der Novellierung des Hochschulstatistikgesetzes sondern auch mitunter beim Vollzug des gegenwärtigen Gesetzes. Der AStA einer Fachhochschule hatte Zweifel an der Zulässigkeit der Datenerhebung, die die Hochschulverwaltung bei der Exmatrikulation durchführte und bat mich um Stellungnahme.

Studierende dieser Fachhochschule, die sich exmatrikulieren wollten, hatten ein Durchschreibformular auszufüllen, das als Erhebungsbogen für die Exmatrikuliertenstatistik nach § 8 Nr. 1 Hochschulstatistikgesetz sowie als Exmatrikulationsantrag und Entlastungsbescheinigung diente. Das Originalblatt, das bei der Fachhochschule verblieb und zu der Studentenakte genommen wurde, enthielt folgende Angaben:

1. Teil:
Martrikelnummer, Name, Vorname, Geburtsname, Geburtsdatum, Geburtsort, Kreis des Geburtsortes, Land des Geburtsortes, Geschlecht, Semester, mit dessen Ablauf die Exmatrikulation erfolgen sollte und Grund der Exmatrikulation mit einem Schlüssel für 36 mögliche Antworten. Gefragt wurde u. a., ob das Studium wegen finanzieller oder familiärer Gründe, wegen Krankheit oder Einberufung zum Wehrdienst aufgegeben bzw. unterbrochen werde.

2. Teil:
Antrag auf Exmatrikulation.

3. Teil:
Entlastungsbescheinigungen des Fachbereichs, AStA, Studentenwerks, der Bibliotheken, Institute usw.

Die erste Durchschrift enthielt komplett die Angaben des Originalblattes und war für den Antragsteller bestimmt. In der zweiten waren lediglich die Angaben des ersten Teils enthalten. Diese Durchschriften schickte die Fachhochschule semesterweise an das Hessische Statistische Landesamt. Die Daten des ersten Teils erhob die Fachhochschule bei den Studenten, die die Exmatrikulation beantragten. Lediglich für Studierende, die sich nicht rückmeldeten und nicht exmatrikulierten, füllte die Verwaltung die Fragen selbst aus.

Die Datenerhebung, die die Fachhochschule für Zwecke der Hochschulstatistik bei den Studierenden, die sich exmatrikulierten, durchführte, war rechtswidrig, denn nach § 8 Satz 1 Hochschulstatistikgesetz sind die Daten für die Exmatrikuliertenstatistik (§ 8 Nr. 1 HStatG) vom Statistischen Landesamt bei der Hochschule zu erheben. Auskunftspflichtig ist gem. § 13 Abs. 1 Nr. 5 Hochschulstatistikgesetz nicht der Studierende, sondern der Leiter der Hochschule.

Bei den Studenten durften die Daten im ersten Teil des Erhebungsbogens für die Exmatrikuliertenstatistik selbst mit deren Einwilligung nicht personenbezogen erhoben werden. Das Hessische Statistische Landesamt liefert nämlich seit 1984 bzw. dem Wintersemester 1985/86 aus verfassungsrechtlichen Gründen keine fallbeziehbaren hochschulstatistischen Angaben mehr an das Statistische Bundesamt. Nach Auskunft des Statistischen Landesamts werden deshalb von den Hochschulen für die Hochschulstatistik auch keine personenbezogenen Daten mehr verlangt. Da die personenbezogene Erhebung der im ersten Teil des Exmatrikulationsformulars enthaltenen Angaben für die Hochschulstatistik, d. h. für einen mit der rechtmäßigen Aufgabenerfüllung der Fachhochschule verbundenen Zweck nicht mehr erforderlich ist, wäre sie daher nach dem Hessischen Datenschutzgesetz selbst bei Einwilligung der Betroffenen unzulässig (§ 11 Abs. 1 HDSG).

Es war auch kein anderer Zweck ersichtlich, zu dem die Fachhochschule sämtliche Angaben, die im ersten Teil des Formulars enthalten waren, zulässigerweise erheben durfte. Mit Ausnahme der Matrikelnummer benötigte sie die Daten insbesondere nicht zu Verwaltungszwecken. Wie mir die Verwaltung der Hochschule bestätigte, genügen für die Abwicklung der Exmatrikulation Matrikelnummer, Name und Exmatrikulationsantrag. Die Angaben zum Grund der Exmatrikulation, ob also z. B. das Studium aus finanziellen oder familiären Gründen oder wegen Krankheit aufgegeben wurde, durfte die Fachhochschule deshalb gem. § 11 Abs. 1 HDSG für Verwaltungszwecke weder erheben

noch speichern. Das Original des Exmatrikulationsformulars durfte daher mit diesen Angaben auch nicht zu den Studentenakten genommen werden.

Das bedeutet zusammengefaßt: Hochschulen können und dürfen dem Hessischen Statistischen Landesamt für die Hochschulstatistik nur die Exmatrikulationsgründe mitteilen, die ihnen aus dem Vollzug des § 40 Hessisches Hochschulgesetz, der die Exmatrikulation regelt, bekannt geworden sind. Die Daten dürfen allerdings nicht personenbezogen übermittelt werden.

Hochschulverwaltung und Hessisches Statistisches Landesamt haben sich meiner Ansicht angeschlossen. Mit letzterem wurde daraufhin eine Änderung der Datenerhebung vereinbart. Die Hochschulen erheben für die Exmatrikuliertenstatistik keine Daten mehr bei den Studenten. Sie liefern dem Statistischen Landesamt nur noch die Angaben Geschlecht, Geburtsjahr und Exmatrikulationsgrund. Es werden jedoch nur solche Gründe übermittelt, die der Hochschule aus dem Vollzug des Hessischen Hochschulgesetzes bei der Exmatrikulation bekannt geworden sind, d. h.:

a) Exmatrikulation durch den Studenten: Beendigung des Studiums nach bestandener Prüfung, sonstige Gründe (die nicht spezifiziert werden);

b) Exmatrikulation durch die Hochschule: Beendigung des Studiums nach bestandener Prüfung, nicht zur Rückmeldung erschienen (ohne Studienabschluß), vom Studium ausgeschlossen, sonstige Gründe (ebenfalls keine Spezifizierung).

9. Forschung

9.1
Gedenkstätte Breitenau/Guxhagen

Historiker empfinden zunehmend den Datenschutz als Bedrohung ihrer beruflichen Existenz. Es ist in der Tat nicht zu leugnen, daß sich die Fälle häufen, in denen Geschichtswissenschaftlern unter Berufung auf den Datenschutz der Zugang zu Akten mit personenbezogenen Unterlagen verwehrt wird. Ob dies Ausdruck eines gesteigerten Datenschutzbewußtseins der Behörden ist, oder der Datenschutz nur als willkommenes Mittel dient, um ein ohnehin als lästig empfundenes Verlangen abzuweisen, läßt sich nicht immer klar erkennen. Daß jedoch meistens Verfahren gefunden werden können, die den Forschern den Datenzugang ermöglichen und gleichzeitig den Persönlichkeitsschutz der Betroffenen gewährleisten, zeigt der Fall der Gedenkstätte Breitenau/Guxhagen.

9.1.1
Hintergrund

Auch hier lauteten die Schlagzeilen in der Presse zunächst: „Datenschutz bedroht Archiv der KZ-Gedenkstätte Breitenau". Der Hintergrund: Die ehemalige Landesarbeitsanstalt Breitenau, in der anfangs nur sogenannte Korrigenden (z. B. Alkoholiker und Prostituierte) sowie Fürsorgezöglinge untergebracht waren, wurde in der Zeit des Nationalsozialismus außerdem zur Unterbringung von Schutzhäftlingen genutzt. Um die ca. 3000 Akten dieser Personen ging der Streit.

Die Akten enthalten den Namen des Schutzhäftlings, Datumsangaben über Zugang und Abgang, detaillierte Personenbeschreibungen, Angaben über Religion, Eltern, Soldatentätigkeit, Stand oder Gewerbe, Ehepartner sowie Verlobungs- und Verwandtschaftsverhältnisse, Schutzhaftbefehle, sogenannte Hinterlegungsblätter, in denen die den Gefangenen abgenommenen Gegenstände verzeichnet sind, Korrespondenz zwischen der Lagerverwaltung und der Gestapo (u. a. Verfügungen zum Transport in die Vernichtungslager Auschwitz, Sachsenhausen, Buchenwald etc.) und zurückgehaltene Briefe von Gefangenen.

Der 1953 gebildete Landeswohlfahrtsverband (LWV) Hessen hatte die Akten von dem damals gleichzeitig aufgelösten Bezirkskommunalverband Kassel, dem Träger der Landesarbeitsanstalt Breitenau, übernommen und 1980 der Gesamthochschule Kassel (GhK) für ein wissenschaftliches Forschungsprojekt zur Verfügung gestellt. Der Leiter des Forschungsprojekts verwaltete sie zunächst in seinem Arbeitszimmer der GhK. 1984 richtete die GhK in der Außenstelle Guxhagen des psychiatrischen Krankenhauses Merxhausen, dessen Träger der LWV ist, die „Gedenkstätte Breitenau" ein, die sowohl Forschungszwecken als auch der politischen Bildung dient. Seit dieser Zeit wurden die Akten dort aufbewahrt und genutzt. Ende 1987 verlangte der LWV von der GhK unter Hinweis auf datenschutzrechtliche Erfordernisse die Herausgabe der Akten. Die GhK, die daraufhin ihr Projekt gefährdet sah, weigerte sich jedoch zunächst, die Akten zurückzugeben.

9.1.2
Rückgabepflicht

In diesem Streit, mit dem sich auch der Landtag ausführlich beschäftigt hat, bat mich der LWV um eine gutachtliche Stellungnahme. Die datenschutzrechtliche Prüfung ergab, daß die GhK die Akten an den LWV herausgeben mußte, da ihr für die Datenverarbeitung die notwendige gesetzliche Befugnis (§ 7 Abs. 1 Hessisches Datenschutzgesetz) fehlte,

denn rechtlich zuständige Stelle für die Speicherung und sonstige Verarbeitung der Daten in den Akten der Schutzhäftlinge der ehemaligen Landesarbeitsanstalt Breitenau ist der LWV.

Bei den Akten handelt es sich eindeutig um Unterlagen der ehemaligen Landesarbeitsanstalt Breitenau. Die Anstalt hatte die Akten mit der Aufschrift „Landesarbeitsanstalt und Landesfürsorgeheim Breitenau" angelegt und geführt. Auch wenn sie Verfügungen der Gestapo enthalten, werden sie dadurch nicht zu Gestapo-Akten, denn die Verfügungen sind regelmäßig an die Lagerverwaltung gerichtet. Nach Auflösung der Landesarbeitsanstalt übernahm deren Träger, der Bezirkskommunalverband Kassel die Akten. Dessen Rechtsnachfolger ist der LWV. Die Zuständigkeit für die Verwaltung der Akten, d.h. für die Verarbeitung der in den Akten enthaltenen Daten, ist damit auf den LWV übergegangen.

Der LWV darf als zuständige speichernde Stelle die Akten, deren Daten zur rechtmäßigen Erfüllung der in seiner Zuständigkeit liegenden Aufgaben nicht mehr erforderlich sind, und deshalb gesperrt sein müssen (§ 19 Abs. 2 Ziff. 2 Hessisches Datenschutzgesetz), nicht dauerhaft einer anderen Stelle, die kein staatliches oder kommunales Archiv ist, überlassen (§ 19 Abs. 7 HDSG).

Die Archivregelung ist neu in das Hessische Datenschutzgesetz aufgenommen worden und gilt erst seit dem 1. Januar 1987. Es konnte dennoch dahingestellt bleiben, ob der LWV vor Inkrafttreten des neuen HDSG – das alte galt nicht für Akten – der GhK die Akten als Archivgut zu dem Zweck, sie auf Dauer zu sichern, nutzbar zu machen und wissenschaftlich zu verwerten, übergeben durfte, denn dies war nicht erfolgt. Der LWV hatte zwar der GhK die Akten zur Bearbeitung in deren Räumen überlassen, allerdings mit dem schriftlichen Vermerk, daß die Akten „als wissenschaftliche Leihgabe für die Zeit ihrer Bearbeitung zur Verfügung gestellt würden".

9.1.3
Verwaltungsmodelle

Die Akten mußten zwar an den LWV zurückgegeben, aber deswegen keineswegs zwangsläufig aus der Gedenkstätte entfernt werden. Bei ausreichender Datensicherheit bestanden keine datenschutzrechtlichen Bedenken gegen einen Verbleib der Unterlagen in den Räumen der Gedenkstätte.

Ich habe seinerzeit den Beteiligten hierzu verschiedene Verwaltungsmodelle vorgeschlagen. Ausgangspunkt war immer, daß der LWV die Verfügungsmacht über die Akten behalten mußte. Das eine Modell sah vor, daß der LWV die Akten der Schutzhäftlinge als Archiv der Gedenkstätte führt oder – das Einverständnis der GhK vorausgesetzt – die Trägerschaft für die gesamte Gedenkstätte übernimmt und die von der Gedenkstätte zusätzlich beschafften Archivalien mit den Schutzhaftakten im Archiv zusammengefaßt würden. Der LWV konnte außerdem den Leiter des Forschungsprojekts der GhK mit der Leitung des Archivs betrauen oder gemäß § 4 Abs. 1 Hessisches Datenschutzgesetz mit einzelnen Datenverarbeitungsmaßnahmen beauftragen. Im zweiten Modell übergab der LWV die Akten gemäß § 19 Abs. 7 HDSG einem staatlichen oder kommunalen Archiv und dies hätte in der Gedenkstätte eine Art „Außenstelle" unterhalten. Die Beteiligten haben letztlich auf der Grundlage des ersten Vorschlags eine Vereinbarung getroffen, die dem LWV die Verfügungsmacht über die Akten und der GhK die ungehinderte Weiterführung der Forschungs- und Bildungsarbeit der Gedenkstätte garantiert.

9.2
Jugendgerichtshilfeberichte

Den Forschern wird der Zugang zu personenbezogenen Daten zugegebenermaßen auch manchmal durch gesetzliche Sperren blockiert, die aus der Sicht des Datenschutzes nicht immer unbedingt erforderlich erscheinen. Die Nutzungseinschränkung für Jugendgerichtshilfeberichte dürfte in diese Kategorie fallen. Diese Einschätzung habe ich im vergangenen Frühjahr auch gegenüber dem Hessischen Justizministerium geäußert, das mich um Stellungnahme zu der Frage gebeten hatte, inwieweit Jugendgerichtshilfeberichte für Forschungszwecke verwendet werden dürfen.

Die Jugendgerichtshilfe spielt eine bedeutende Rolle im Jugendstrafverfahren. Sie hat die Aufgabe, im Gerichtsverfahren die erzieherischen, sozialen und fürsorgerischen Gesichtspunkte zur Geltung zu bringen und zu diesem Zweck die beteiligten Behörden durch Erforschung der Persönlichkeit, der Entwicklung und der Umwelt des beschuldigten Jugendlichen oder Heranwachsenden zu unterstützen (§ 4 Nr. 4 Jugendwohlfahrtsgesetz i.V.m. § 38 Abs. 2 Jugendgerichtsgesetz). Daraus wird unmittelbar deutlich, daß die Berichte der Jugendgerichtshilfe oft äußerst sensible Daten enthalten, es ist jedoch ebenso einsichtig, daß gerade diese Daten insbesondere für die Justizforschung von besonderem Interesse sind. Genau diese Forschungsdisziplin hat jedoch keinen Zugang zu den Daten der Jugendgerichtshilfeberichte. Die Daten unterliegen nämlich dem Sozialdatenschutz und dürfen daher allenfalls für wissenschaftliche Forschungsprojekte im Sozialleistungsbereich weiterverwendet werden (§ 75 Sozialgesetzbuch – SGB X).

Der Grund: Das Jugendamt erbringt die Jugendgerichtshilfe als Sozialleistung im Sinne des Sozialgesetzbuches und hat daher als Träger dieser Leistung das Sozialgeheimnis (§ 35 SGB I) zu beachten. Das ergibt sich eindeutig aus dem Jugendwohlfahrtsgesetz (JWG), das gemäß Art. II § 1 Nr. 16 SGB I als besonderer Teil des Sozialgesetzbuches gilt. Nach § 4 Nr. 4 Jugendwohlfahrtsgesetz zählt zu den Aufgaben des Jugendamtes die Jugendgerichtshilfe nach den Vorschriften des Jugendgerichtsgesetzes. Daß das Jugendamt in diesem Fall als Sozialleistungsträger tätig wird, bestätigt auch § 27 SGB I, der den Bürger über die Leistungstatbestände und die Leistungsträger im Sozialleistungsbereich Jugendhilfe

informieren soll. Dort ist die Jugendgerichtshilfe ausdrücklich als Sozialleistung aufgeführt und das Jugendamt als zuständiger Leistungsträger erwähnt. Zwar regelt auch § 38 Jugendgerichtsgesetz die Jugendgerichtshilfe, diese Vorschrift konkretisiert jedoch lediglich die dem Jugendamt sozialgesetzlich zugewiesene Aufgabe.

Würde man das Jugendamt, soweit es Jugendgerichtshilfe ausübt, nicht als Sozialleistungsträger ansehen, hätte dies erhebliche Nachteile für deren Funktionsfähigkeit. Da das Jugendamt keine gesetzliche Befugnis hätte, personenbezogene Angaben aus der übrigen Jugendhilfe an die Jugendgerichtshilfe zu übermitteln, dürfte der Vertreter der Jugendgerichtshilfe Daten, die das Jugendamt über die Beschuldigten im Rahmen der übrigen Jugendhilfe gespeichert hat, nicht verwenden. Er müßte die für den Bericht erforderlichen Daten vielmehr selbständig erheben, was praktisch wohl kaum möglich wäre.

Da also die Jugendgerichtshilfeberichte dem Sozialgeheimnis unterliegen, darf das Jugendgericht die personenbezogenen Angaben nur zu dem Zweck verwenden, zu dem sie offenbart worden sind (§ 78 SGB X). Daraus folgt, daß die personenbezogenen Daten der Jugendgerichtshilfeberichte Dritten grundsätzlich nicht für wissenschaftliche Zwecke zugänglich gemacht werden dürfen, denn die Daten wurden dem Gericht nur für die Durchführung eines konkreten Strafverfahrens offenbart und dürfen daher nur zu diesem Zweck verwendet werden. Das Sozialgesetzbuch (§ 75 SGB X) läßt wie gesagt nur eine Ausnahme zu: Die Daten dürften – wenn die sonstigen dort genannten Bedingungen erfüllt sind – für die wissenschaftliche Forschung im Sozialleistungsbereich genutzt werden.

Nach der gegenwärtigen Rechtslage können somit Forscher aus anderen Bereichen nur solche Jugendgerichtsakten einsehen, aus denen zuvor die Jugendgerichtshilfeberichte entfernt worden sind. Dieses insbesondere für die Justizforschung, die sicherlich das stärkste Interesse an den Daten hat, höchst unbefriedigende Ergebnis läßt sich freilich nur durch eine bundesgesetzliche Regelung korrigieren.

10. Kommunen

10.1
Einsichtsrecht in Abrechnungsunterlagen

In vielen Gemeinden ist es gängige Praxis, bei Heranziehung von Anliegern zu Straßenbeiträgen die gesamten Abrechnungsunterlagen einige Wochen zur Einsichtnahme öffentlich auszulegen. Die Unterlagen geben u. a. Auskunft über die betroffenen Grundstückseigentümer, die Grundstücksgrößen und die Beträge, die die einzelnen Anlieger zu zahlen haben. Eine solch umfassende Datenübermittlung ist jedoch unzulässig.

Das Akteneinsichtsrecht des § 18 Abs. 4 Hessisches Datenschutzgesetz ist beschränkt auf Daten des Betroffenen; der Zugang zu personenbezogenen Daten Dritter ist in dieser Vorschrift ausdrücklich verwehrt.

Das bedeutet freilich nicht, daß die Anlieger nicht auch Daten ihrer Nachbarn erfahren dürfen. § 29 Abs. 1 des Hessischen Verwaltungsverfahrensgesetzes gibt nämlich grundsätzlich allen an einem Verwaltungsverfahren Beteiligten ein Akteneinsichtsrecht; eine Einschränkung auf personenbezogene Daten des Betroffenen besteht nicht. Auch wenn es sich wie hier um ein Kommunalabgabeverfahren handelt, bei dem weitgehend die Vorschriften der Abgabenordnung anzuwenden sind (vgl. § 2 Abs. 2 Nr. 1 Hessisches Verwaltungsverfahrensgesetz, § 4 Abs. 1 Kommunalabgabengesetz), gilt dies. Der Hessische Verwaltungsgerichtshof ist allerdings anderer Ansicht und meint, daß in Angelegenheiten, in denen Rechtsvorschriften der Abgabenordnung anzuwenden sind, nach § 2 Abs. 2 Nr. 1 HVwVfG das Hessische Verwaltungsverfahrensgesetz generell nicht gilt. Dagegen bin ich der Auffassung, daß der Anwendungsbereich des Verwaltungsverfahrensgesetzes nur insoweit eingeschränkt wird, als das Kommunalabgabengesetz tatsächlich enumerativ auf Bestimmungen der Abgabenordnung verweist, und das ist für das Einsichtsrecht nicht der Fall. Deshalb kann der Bürger auch bei Kommunalabgaben Akteneinsicht nach dem Verwaltungsverfahrensgesetz verlangen.

Das Einsichtsrecht ist jedoch nicht grenzenlos, es besteht nur insoweit, als ein Beteiligter den Akteninhalt kennen muß, um seine rechtlichen Interessen geltend machen oder verteidigen zu können. Deshalb ist es unzulässig, den Einblick in eine Aufstellung zu gewähren, aus der die auf sämtliche Anlieger entfallenden Beiträge und die bereits geleisteten Vorschüsse zu entnehmen sind.

10.2
Anzeigepflicht der Stadtverordneten

Die nach der Hessischen Gemeindeordnung bestehende Pflicht der Stadtverordneten, ihre Mitgliedschaft in Vereinen, Gesellschaften, Verbänden usw. mitzuteilen, hat auch im abgelaufenen Jahr wieder zu Auseinandersetzungen geführt (vgl. bereits 16. Tätigkeitsbericht, Ziff. 5.3). Zur Debatte stand diesmal das Mitteilungsverfahren, insbesondere wer die Mitteilung erhält.

§ 26 a der Hessischen Gemeindeordnung legt fest, daß die Mitgliedschaft dem Vorsitzenden des Organs anzuzeigen ist, dem der Betroffene angehört und der Vorsitzende eine Zusammenstellung der Anzeigen dem Finanzausschuß zur Unterrichtung zuzuleiten hat.

Der Gesetzgeber hat bewußt von einer Pflicht zur Veröffentlichung der Zusammenstellung der Anzeigen abgesehen. Vielmehr hat er die Unterrichtung des Finanzausschusses als angemessen und ausreichend erachtet. Daraus ist zu folgern, daß die Unterrichtung des Finanzausschusses in einer nicht-öffentlichen Ausschußsitzung erfolgen muß. Bei diesem Verfahren haben alle Fraktionen der Gemeindevertretung die Möglichkeit, sich über die Vereinsmitgliedschaften der Gemeindevertreter zu informieren, denn die Hessische Gemeindeordnung eröffnet allen Fraktionen die Teilnahme an den Sitzungen des Finanzausschusses (§ 62 Abs. 4 Satz 2).

Einzelne Stadtverordnete haben darüber hinaus nur ausnahmsweise das Recht, die Mitgliedschaftsanzeigen anderer Stadtverordneter einzusehen. So muß z. B. ein Mitglied des Bauausschusses die Möglichkeit haben, sich über die Vereinsmitgliedschaften anderer Ausschußmitglieder zu informieren, wenn es der Meinung ist, daß die Zugehörigkeit zu einem bestimmten Verein bei einer anstehenden Beschlußfassung keine freie Entscheidung zuläßt. Durch diese Akteneinsicht würden keine schutzwürdigen Belange der Betroffenen beeinträchtigt.

Um Mißbräuchen entgegenzuwirken, dürfte es sich allerdings empfehlen, den Stadtverordneten, der die Akten einsieht, besonders auf seine Verschwiegenheitspflicht hinzuweisen und den Finanzausschuß bzw. den Vorsitzenden des Ausschusses über die Einsichtnahme zuvor zu unterrichten.

10.3
Ausstellung von Wählbarkeitsbescheinigungen

Aus Anlaß der Kommunalwahlen 1989 wollten mehrere Gemeinden wissen, wie sie bei der Ausstellung von Wählbarkeitsbescheinigungen verfahren sollen. Die Parteien und Wählergruppen haben ihre Wahlvorschläge vor der Kommunalwahl beim Wahlleiter einzureichen. Den Wahlvorschlägen beizulegen ist die Bescheinigung des Gemeindevorstandes, daß die Bewerber die Voraussetzungen der Wählbarkeit erfüllen (§ 13 Abs. 2 Nr. 2 Kommunalwahlgesetz).

Gegenwärtig geschieht dies oftmals folgendermaßen: Die politischen Parteien und Wählergruppen reichen bei den Kommunen Kandidatenlisten ein und erhalten daraufhin für die benannten Personen Wählbarkeitsbescheinigungen. Eine Einwilligungserklärung der Betroffenen wird nicht eingeholt.

Diese Vorgehensweise ist jedoch datenschutzrechtlich unzulässig. Bei der Übergabe der Bescheinigungen an die Parteien handelt es sich um eine Datenübermittlung einer öffentlichen Stelle an Private, die weder durch § 16 Hessisches Datenschutzgesetz noch durch Spezialgesetz gerechtfertigt ist. Zwar legt das Kommunalwahlgesetz fest, daß mit den Wahlvorschlägen auch die Wählbarkeitsbescheinigungen der Bewerber bei dem Wahlleiter einzureichen sind. Diese Vorschrift sieht aber weder ausdrücklich vor noch setzt sie zwingend voraus (§ 7 Abs. 1 Nr. 1 HDSG), daß die Wählbarkeitsbescheinigungen ohne Einwilligung der Betroffenen den Parteien ausgehändigt werden.

Einige Gemeinden sind daher dazu übergegangen, die Parteien bzw. Wählergruppen darauf hinzuweisen, daß sie Einwilligungserklärungen der Kandidaten vorlegen müssen, um Wählbarkeitsbescheinigungen direkt von der Kommune erhalten zu können.

In anderen Gemeinden holen sich die Bewerber die Wählbarkeitsbescheinigungen persönlich bei der Stadt ab und reichen sie zum Zwecke ihrer Kandidatur dann bei ihrer Partei ein. Auch dieses Verfahren erfüllt die datenschutzrechtlichen Anforderungen.

Möglich wäre auch, daß die Parteien bzw. Wählergruppen der Kommune die Kandidatenliste vorlegen und die Kommune dann die Wählbarkeitsbescheinigungen den einzelnen Bewerbern zusendet und diese die Wählbarkeitsbescheinigungen selbst an die Parteien übermitteln.

10.4
Straßenverkehrsbehörde informiert Bürgermeister über Fahrerlaubnisentziehungen von Einwohnern der Gemeinde

Der Bürgermeister einer hessischen Gemeinde wunderte sich, daß er regelmäßig von der Straßenverkehrsbehörde des Landratsamtes Mitteilungen erhielt, in denen er darüber informiert wurde, welchen Einwohnern seiner Gemeinde die Fahrerlaubnis entzogen worden war und in welchen Fällen die Behörde Fahrverbote ausgesprochen hatte. Da er dies nicht für erforderlich hielt, bat er das Landratsamt, ihm keine weiteren Benachrichtigungen mehr zu schicken. Die Straßenverkehrsbehörde war jedoch nicht gewillt, von ihrer Praxis abzuweichen und übersandte dem Bürgermeister weiterhin ihre Mitteilungen.

Die Datenübermittlungen waren eindeutig rechtswidrig. Es zählt nicht – wie der Landrat in seiner von mir angeforderten Stellungnahme meinte – zu den Aufgaben des Bürgermeisters als Ortspolizeibehörde, die Einhaltung von Fahrverboten zu überwachen.

Nur unter Einschaltung des Hessischen Ministeriums für Wirtschaft und Technik konnte ich den überflüssigen Informationsaustausch unterbinden. Das Ministerium ist gleichfalls der Auffassung, daß nur die Dienststellen der Vollzugspolizei informiert werden müssen. Es wies den Landrat an, den Gemeinden keine Fahrerlaubnisentziehungen und Fahrverbote mehr mitzuteilen.

11. Finanzverwaltung

11.1
Reform der Abgabenordnung

Für Steuerverfahren gelten nur ausnahmsweise Bestimmungen des Hessischen Datenschutzgesetzes, grundsätzlich ist die bundesgesetzliche Abgabenordnung maßgeblich. Dort fehlen allerdings bislang speziell auf die Finanzverwaltung zugeschnittene Datenschutzvorschriften. Dies möchte die Bundesregierung nun ändern und hat daher im November 1988 einen Referentenentwurf für ein Gesetz über bereichsspezifische Datenschutzvorschriften im Anwendungsbereich der Abgabenordnung vorgelegt.

Der Entwurf hat eine Reihe von Mängeln, von denen hier jedoch nur einer erwähnt werden soll, weil er besonders gravierend ist: Es geht um die Einschränkung der Kontrollkompetenz des Datenschutzbeauftragten.

Was Steuerbehörden gegenwärtig immer wieder versuchen, die Kontrolle durch den Datenschutzbeauftragten unter Berufung auf das Steuergeheimnis abzuwehren oder zu erschweren, soll nach den Vorstellungen der Bundesregierung Gesetz werden. Der Referentenentwurf zur Änderung der Abgabenordnung sieht vor, daß dem Datenschutzbeauftragten dem Steuergeheimnis unterliegende Daten nur offenbart werden dürfen, wenn der Betroffene eingewilligt hat oder dem schriftlichen Hinweis des Datenschutzbeauftragten, daß er beabsichtige, die Verarbeitung von Daten des Betroffenen zu kontrollieren, nicht wiersprochen hat. Eine ähnliche Regelung enthält der Entwurf für ein neues Bundesdatenschutzgesetz vom 5. November 1987.

Eine solche Beschränkung hätte zur Folge, daß über den Einzelfall hinausgehende Prüfungen von Datenverarbeitungsverfahren durch den Datenschutzbeauftragten erheblich behindert, wenn nicht sogar unmöglich gemacht würden.

Das Bundesverfassungsgericht hat im Volkszählungsurteil von 1983 die besondere Bedeutung unabhängiger Datenschutzbeauftragter betont (BVerfGE 65, 46, 60). Es sieht in der Kontrolle durch die Datenschutzbeauftragten eine wesentliche Sicherung zum Schutz des informationellen Selbstbestimmungsrecht des einzelnen. Nur eine umfassende Kontrollkompetenz des Datenschutzbeauftragten kann die mangelnde Möglichkeit des einzelnen ausgleichen, überaus komplexe administrative Zusammenhänge sowie hochtechnisierte Verarbeitungsprozesse zu durchschauen. Gerade im Bereich der Finanzverwaltung, die in großem Umfang besonders sensible personenbezogene Daten verarbeitet, ist eine Einschränkung der Kontrollmöglichkeit völlig inakzeptabel.

11.2
Informationssystem über steuerliche Auslandsbeziehungen

Beim Bundesfinanzministerium, genauer beim Bundesamt für Finanzen, existiert bereits seit einiger Zeit ein automatisiertes Informationssystem über steuerliche Auslandsbeziehungen. Gespeichert sind dort Daten über sogenannte „Steuerausländer", d. h. Ausländer, die keinen Wohnsitz in der Bundesrepublik haben, hier aber der beschränkten Einkommens-, Lohnsteuer- oder Vermögenssteuerpflicht unterliegen. Außerdem enthält das Informationssystem Daten über Steuerbeziehungen von Inländern mit dem Ausland. Registriert sind also z. B. Daten von Ausländern, die Grundbesitz in der Bundesrepublik haben und daraus Einkünfte erzielen oder Daten von Steuerinländern mit Beteiligungen an ausländischen Gesellschaften.

Seit Februar 1988 verfügt die Hessische Steuerverwaltung im Finanzamt Frankfurt am Main – Börse über eine Online-Verbindung zu dem Informationssystem und kann somit direkt aus der Datei Daten über Steuerpflichtige abrufen.

Für dieses Steuerdatenabrufverfahren fehlt aber derzeit noch eine ausreichende Rechtsgrundlage. Erst die geplante Steuerdatenabrufverordnung kann hier Abhilfe schaffen. Der Referentenentwurf des Bundesfinanzministeriums vom 9. Juni 1988 sieht vor, daß ein Datenabrufverfahren nur eingerichtet werden darf, wenn es unter Berücksichtigung der Menge oder der häufigen Nutzung der Daten oder der Notwendigkeit, die Daten für bestimmte Verfahren beschleunigt zu nutzen, angemessen ist. Ob diese Voraussetzungen für den Online-Anschluß im Frankfurter Finanzamt erfüllt sind, wäre dann erst noch zu prüfen.

Ich habe deshalb das Hessische Finanzministerium aufgefordert, bis zum Inkrafttreten der Steuerdatenabrufverordnung auf das Verfahren zu verzichten. Das Ministerium ist darauf jedoch nicht eingegangen, sondern sieht in dem Verfahren ein Pilotprojekt, für das § 30 Abs. 6 der Abgabenordnung als Rechtsgrundlage ausreiche. Die Vorschrift läßt in der Tat den automatisierten Abruf von Steuerdaten zu, ist allerdings zu unbestimmt, um als alleinige Rechtsgrundlage dienen zu können, sondern bedarf der gesetzlichen Konkretisierung durch die Steuerdatenabrufverordnung.

11.3
Mitteilungspflichten privater Stellen bei Honorarzahlungen

Der pädagogischen Arbeitsstelle des Volkshochschulverbandes e.V. waren Zweifel an der Rechtmäßigkeit der Mitteilungen gekommen, die sie regelmäßig über Empfänger von Honorarzahlungen an das Finanzamt schickte. Die Überprüfung, um die mich das Hessische Ministerium für Wissenschaft und Kunst gebeten hatte, ergab, daß diese Zweifel berechtigt waren.

KKD 12/4060/62

Für Behörden ist mit § 93 a Abgabenordnung die rechtliche Voraussetzung für solche sogenannten Kontrollmitteilungen an Finanzämter geschaffen worden (vgl. 15. Tätigkeitsbericht, Ziff. 11.3.4). Für private Stellen gibt es dagegen keine entsprechende gesetzliche Regelung. Die Mitteilungen der pädagogischen Arbeitsstelle erfolgten vielmehr aufgrund der Verwaltungsvorschrift zu § 44 Landeshaushaltsordnung (StAnz. S. 1474, 1481, 1482). Das ist jedoch keine ausreichende Rechtsgrundlage, derartige Mitteilungspflichten müssen gesetzlich angeordnet werden.

Das Finanzministerium ist ebenfalls dieser Auffassung und hat mit Rundschreiben vom 22. November 1988 die in der Verwaltungsvorschrift enthaltene Mitteilungspflicht für private Stellen aufgehoben.

11.4
Mitteilung von Steuermeßbescheiden an Gemeinden

Nicht alle Steuern werden bekanntermaßen allein von den Finanzämtern erhoben. Bei den Gewerbe- und Grundsteuern (Realsteuern) beispielsweise sind staatliche Finanzverwaltung und Gemeinden gemeinsam tätig. Die Finanzverwaltung ermittelt für die Grundsteuer und Gewerbesteuer die Besteuerungsgrundlagen und setzt den Steuermeßbescheid fest. Die Gemeinden erlassen dann, entsprechend dem von ihnen festgesetzten Hebesatz, den Grundsteuer- bzw. Gewerbesteuerbescheid.

Gemäß § 184 Abs. 3 Abgabenordnung in der Fassung des Steuerbereinigungsgesetzes 1986 darf das Finanzamt den Gemeinden den Inhalt des Steuermeßbescheides insgesamt offenbaren. Diese Regelung dient Rationalisierungszwekken, da nunmehr die Gemeinden den Steuermeßbescheid zusammen mit dem Steuerbescheid bekanntgeben können. Folge ist jedoch, daß der Gemeinde nicht nur die zur Gewerbesteuerberechnung notwendigen Meßzahlen, welche wenig Aufschluß über betriebsinterne Fakten geben, mitgeteilt werden, sondern darüber hinaus eine Vielzahl weiterer Daten, wie z. B. Gewinne, Einheitswerte, Dauerschulden. Besonders Gewerbetreibende in kleineren Gemeinden fühlen sich dadurch erheblich beeinträchtigt.

Mit dieser Beeinträchtigung müssen sich die Betroffenen aber keineswegs abfinden, denn eine derart weitgehende Datenübermittlung ist datenschutzrechtlich unzulässig, da sie weder für die Aufgabenerfüllung der Finanzämter noch der Gemeinden erforderlich ist. Bei Anträgen auf Stundung und auf Erlaß oder Aussetzung der Vollziehung des Steuerbescheids beispielsweise können die Gemeinden problemlos bei den Finanzämtern rückfragen.

11.5
Kontopfändung bei Kreditinstituten

Ein Bürger war mit seinen Steuerzahlungen in Verzug geraten. Daraufhin ließ das Finanzamt allen örtlichen Banken und Sparkassen Pfändungsverfügungen zustellen. In seiner Beschwerde teilte mir der Betroffene mit, er habe bei keiner dieser Banken ein Konto unterhalten. Dem hielt das Finanzamt entgegen, der Steuerschuldner habe zuvor telefonisch erklärt, daß er mit den örtlichen Kreditinstituten über einen Kredit zur Tilgung seiner Abgabenrückstände verhandele. Da sich eine Pfändung auch auf künftig enstehende Forderungen erstrecken könne, habe es deshalb die Pfändungsverfügungen erlassen.

Das Vorgehen des Finanzamtes verstieß gegen das Steuergeheimnis. Den Kreditinstituten dürfen die Finanzämter Steuerdaten Dritter nur offenbaren, wenn die Voraussetzungen für eine Pfändung vorliegen. Das war hier nicht der Fall.

Zwar ist es richtig, daß grundsätzlich auch künftige Forderungen pfändbar sind. Voraussetzung ist jedoch, daß die Forderungen bestimmt oder wenigstens bestimmbar und ihr Rechtsgrund verhanden ist. Pfändbar sind also z. B. künftige Gehaltsforderungen. Es genügt dagegen nicht, wenn nur die Möglichkeit besteht, daß eine Forderung entsteht.

Hier war der Verdacht naheliegend, daß es sich um unzulässige „Ausforschungspfändungen" handelte, d. h., daß mit Hilfe der Pfändungsverfügungen und der daraus folgenden Erklärungspflichten der Drittschuldner (der Banken) erst herausgefunden werden sollte, ob der Steuerschuldner möglicherweise Guthaben bei einer der Banken hatte. Es ist jedoch nicht zulässig, Pfändungen mit dem Ziel der Sachverhaltsermittlung durchzuführen.

12. Datensicherheit

12.1
Einsatz von Arbeitsplatzcomputern

Die Probleme, die sich beim Einsatz von Arbeitsplatzcomputern (APC) für den Datenschutz ergeben, habe ich bereits im 15. Tätigkeitsbericht beschrieben (vgl. dort, Ziff. 9).

Inzwischen ist selbstverständlich die technologische Entwicklung weiter fortgeschritten: Die Leistungsfähigkeit der Prozessoren ist mit den 32-Bit-Systemen (z. B. 80386-Prozessor) deutlich angestiegen und die Speicherkapazität peripherer Direktzugriffsspeicher (Festplatten) hat sich von bis zu 40 MB auf etwa 300 MB erhöht. Insbesondere dann, wenn Betriebs- und Anwendungssysteme eingesetzt werden, die diese neuen Möglichkeiten voll ausnutzen, kann man

häufig nicht mehr von „persönlichen" Computern (PC) zur individuellen Datenverarbeitung sprechen. In Fachkreisen werden leistungsfähigere Geräte als „Workstation" (Arbeitsstation) bezeichnet. Häufig erfolgt die Nutzung auch nicht mehr durch einen einzigen Benutzer, sondern durch mehrere, je nach Betriebssystem nacheinander oder gleichzeitig. Zumindest im Bereich der öffentlichen Verwaltung setzt sich zunehmend die Bezeichnung „Arbeitsplatzcomputer" für Geräte unterschiedlicher Leistungsklassen vom einfachen PC bis zur Workstation durch.

Anlaß, dieses Thema erneut aufzugreifen, sind nun nicht neue Probleme, sondern die zwischenzeitlich geschaffenen bzw. weiterentwickelten Lösungsmöglichkeiten für einige der seinerzeit dargestellten Probleme. Dies betrifft insbesondere den weit verbreiteten Einsatz von APC unter dem Betriebssystem MS-DOS bzw. PC-DOS, auf den ich mich im folgenden beschränken will.

12.1.1
Leistungsumfang von Datenschutzsoftware

Für MS-DOS bzw. PC-DOS sind eine Reihe Zusatzprodukte verschiedener Hersteller erhältlich, mit denen datenschutztechnische Maßnahmen realisiert werden können. Diese Zusatzprodukte bestehen teilweise aus Software, teilweise aus einer Kombination von Hard- und Software. Ihre Leistungsfähigkeit hat sich in den letzten zwei bis drei Jahren beachtlich erhöht. Die Maßnahmen, die jetzt mit diesen Produkten realisierbar sind, haben sich deutlich an diejenigen für Großrechner angenähert.

Die folgende Tabelle ist – dies sei ausdrücklich betont – keine Wunschliste von Datenschutzbeauftragten. Sie ist vielmehr eine Aufzählung der Funktionen und Mechanismen von ganz wenigen dieser Produkte. Hiermit ist klar, daß nicht jedes Produkt alle Punkte realisiert. Aber dem Stand der Technik entsprechende Zusatzprodukte erfüllen den größten Teil der angegebenen Funktionen, zumindest dann, wenn ihr Leistungsumfang voll genutzt wird.

1. Konzept
- Verwaltung mehrerer Benutzer
- Verteilung der Verwaltungsfunktionen auf verschiedene Personen (Kontrolle der Privilegierten, siehe auch 4. Protokollierung)

2. Festplatte, Diskette
- Online-Verschlüsselung der gesamten Festplatte oder einzelner Partitions (1)
- Platten-Paßwort
- Besonderer Schlüssel für jede Partition
- Kein Systemstart von Diskette
- Online- bzw. Offline-Verschlüsselung von Disketten
- Offline-Verschlüsselung von Dateien

3. Benutzer-Paßwörter
- Paßwortwechsel durch den Benutzer
- Begrenzte Gültigkeitsdauer
- Paßwortwechsel und -eingabe ohne Anzeige (Paßwortwechsel erfordert dann die zweimalige identische Eingabe)
- Mindestlänge einstellbar
- Wechsel zu den letzten Paßwörtern nicht möglich
- Nur einwegverschlüsselte Speicherung

4. Protokollierung
- LOGIN, LOGOUT
- Erfolglose LOGIN-Versuche
- Überschreitung der Berechtigungen
- Programmaufrufe
- Dateien (Eröffnen, Anlegen, Lesen, Schreiben, Ausführen)
- Betriebssystemkommandos (auch residente Kommandos, wie z. B. DIR)
- Auswertung der Protokolldatei durch eine andere Person als den Systemverwalter (evtl. mit Vier-Augen-Prinzip). Grund: Kontrolle des Systemverwalters, Verhinderung einer Auswertung der Protokolldaten zu Zwecken der Leistungskontrolle.

5. Einschränkungen auf Benutzerebene
- Sperrung der Diskettenlaufwerke und Drucker
- Beschränkung auf Lesen bzw. Schreiben von Disketten
- Daten werden beim Zugriff auf Diskettenlaufwerke (automatisch) ver-/entschlüsselt.
- Der Benutzer kann zwar Sicherungskopien erstellen, aber nicht auf einem anderen System oder durch einen anderen Benutzer zurücksichern (lassen).

- Benutzerkennung mit Benutzerprofil für
  - Benutzungszeiten
  - Zugriffsberechtigung für Dateien
  - Zugriffsberechtigung für Programme und Kommandos

- Beschränkung des Festplattenzugriffs auf der Partition- und/oder Verzeichnisebene
- Verbot, bestimmte Befehls- oder Datei-Namen zu benutzen (z. B. *.DBF, FORMAT)

6. Tastatur, Bildschirm
- erneute Eingabe des Paßworts sowie Dunkelstellung des Bildschirms nach Ablauf einer bestimmten Zeitspanne ohne Benutzeraktivitäten
- Dunkelstellung des Bildschirms durch Benutzer (sogenannte Pausenschaltung)
- Abschließen mit Software

Diese Tabelle stellt keinen vollständigen und abschließenden Kriterienkatalog zur Auswahl eines geeigneten Zusatzproduktes dar. Sie kann aber als Anregung verstanden werden, die anhand einer Schwachstellenanalyse, in die außer den technischen auch die organisatorischen und baulichen Rahmenbedingungen einbezogen werden müssen, für jedes konkrete Projekt modifiziert werden kann.

Produkte, die in die engere Wahl kommen, sollten dann vorgeführt und getestet werden. Dabei ist es sinnvoll, außer der Wirksamkeit der Datenschutzfunktionen auch die Verträglichkeit mit der eingesetzten Standard-, Anwendungs- und ggf. auch Netzwerksoftware zu überprüfen. In dieser Auswahlphase können dann auch weitere Kriterien herangezogen werden, wie z. B.:

- Implementierungsaufwand,
- Hauptspeicherbedarf,
- Umfang und Verständlichkeit der Bedienungsanleitung,
- Existenz einer Benutzerführung mit Menuesteuerung,
- Unterstützung bei der Durchführung von Sicherungsläufen,
- Verfügbarkeit freier Steckplätze bei Hardwarezusätzen,
- Verträglichkeit mit anderen Betriebssystemen.

12.1.2
Untersuchung von Datenschutzsoftware

Auch in diesem Jahr habe ich wieder zwei Produkte in ihrer jeweils neuesten Version auf einem PC – im stand-alone Betrieb – installiert, mich mit ihrem Konzept beschäftigt und ihre Wirksamkeit untersucht.

Die Datenschutzsoftware-Produkte OCULIS plus Version 3.0 (Copyright IBD Informations- und Beratungsdienste GmbH) und SAFE- Guard Plus Version 3.0 B (Copyright uti-maco Software GmbH) sind beide mehrbenutzerfähig und erlauben die Kontrolle der Festplatte(n) des APC und der Aktivitäten des Benutzers, insbesondere wenn er mit der Festplatte arbeiten will oder muß. Die Abschottung mehrerer Benutzer untereinander sowie eine weitgehende Protokollierung sind ebenfalls möglich.

Für die Schutzmechanismen können dabei drei logische Ebenen unterschieden werden:

1. Der Zugang zum Gerät bzw. zur Festplatte (Benutzerkontrolle)

2. Die Abschottung der Benutzer eines Gerätes untereinander

3. Weitere Einschränkungen der möglichen Aktivitäten der Benutzer.

Die Zugriffskontrolle kann auf den Ebenen zwei und drei realisiert werden.

12.1.2.1
SAFE-Guard Plus

Ziel des Einsatzes von SAFE-Guard Plus ist nicht nur die Unterstützung des Datenschutzes. Es sind vielmehr auch verschiedene Funktionen vorhanden, die insgesamt zu einer größeren Datensicherheit führen sollen. Besonders zu erwähnen sind die Benutzerführung mit Menuesystem und Dateiverwaltung sowie die Backup-Option (d. h. die Möglichkeit, den Verlust von Daten bei Fehlern und Ausfällen durch Datensicherung zu vermeiden).

12.1.2.1.1
Systemverwaltung

Verwaltungsfunktionen können auf zwei verschiedene Personen verteilt werden:

- Der Systemverwalter stellt alle SAFE-Guard Plus Parameter einschließlich der Protokollierung ein und legt für jeden Benutzer dessen Berechtigungen und Einschränkungen fest. Die Vergabe eingeschränkter Verwaltungsbefugnisse an (lokale) Untersystemverwalter ist möglich.

- Durch die Vergabe eines Paßworts für die Protokolldatei durch eine andere Person als den Systemverwalter – z. B. durch den Datenschützer oder den Revisor – kann die Auswertung der Protokolldatei dem Systemverwalter entweder ganz entzogen oder ihm nur gemeinsam mit dem Datenschützer ermöglicht werden (Vier-Augen-Prinzip).

12.1.2.1.2
Technisches Konzept

SAFE-Guard ist in verschieden kombinierbaren Ausführungen erhältlich. Als wirkungsvolles Datenschutzprodukt kommt aus meiner Sicht aber nur SAFE-Guard Plus, die Kombination der Software SAFE-Guard mit Hardware in Form der Zusatzsteckkarte (Board), in Betracht.

Aus technischen Gründen – die Zusatzsteckkarte für das in meinem Hause vorhandene PS/2-Modell war noch nicht lieferbar – mußte ich meine Tests leider auf SAFE-Guard beschränken. Testergebnisse zum Gesamtsystem SAFE-Guard Plus können deswegen nicht dargestellt werden.

Bei Verwendung der Zusatzkarte wird nicht nur die Festplatte verschlüsselt, sondern auch der Systemstart vom Diskettenlaufwerk unterbunden, so daß das Laden von SAFE-Guard nicht mehr verhindert werden kann.

Der Softwareteil SAFE-Guard ist ein residentes Programm (2), welches die Benutzerführung vornimmt, die Einhaltung des Benutzerprofils (Berechtigungen und Einschränkungen) überwacht und die Protokollierung durchführt.

Auf die Datenschutzlücken (Umgehungsmöglichkeiten) bei Einsatz von SAFE-Guard ohne Hardwarezusatz wird im Handbuch hingewiesen.

12.1.2.1.3
Benutzerkontrolle

Um Zugang zu der Festplatte zu erhalten, muß der Benutzer seine Benutzerkennung und sein persönliches Paßwort eingeben. Das Paßwort wird nie im Klartext angezeigt; Länge, Aufbau und Gültigkeitszeitraum können vom Systemverwalter vorgegeben werden. Nach der erfolgreichen Eingabe kann der Benutzer auf allen Partitions und Verzeichnissen arbeiten, für die er zugelassen wurde. Sanktionen bei Falscheingaben (Rechnersperre, Kaltstart etc.) sind möglich. Ferner kann der Benutzungszeitraum des Gerätes z. B. auf bestimmte Wochentage und Arbeitszeiten beschränkt werden. Ein neues Paßwort darf nicht mit den letzten vier Paßwörtern identisch sein.

12.1.2.1.4
Abschottung der Benutzer und Verschlüsselung

SAFE-Guard Plus bietet verschiedene Verschlüsselungsverfahren an. Die oben bereits erwähnte sogenannte „Online"-Verschlüsselung der gesamten Festplatte wird mit Hilfe der Hardware-Zusatzkarte (Board) durchgeführt. Die Dateien sind immer verschlüsselt. Beim Lesen von Daten wird lediglich der angeforderte Datenbereich – nicht die ganze Datei – entschlüsselt. Beim Schreiben werden entsprechend die Daten verschlüsselt in die Datei gespeichert. Diese Ver- bzw. Entschlüsselung wird automatisch durchgeführt, also ohne daß der Benutzer bzw. sein Programm dies anfordern muß.

SAFE-Guard führt diese Online-Verschlüsselung nicht mit einem benutzerabhängigen Paßwort durch, laut Handbuch ist damit eine Abschottung von Benutzern untereinander nicht möglich.

Bei der sogenannten „Offline"-Verschlüsselung von Dateien muß die Datei vor der eigentlichen Verarbeitung komplett entschlüsselt und danach wieder komplett verschlüsselt werden. Aus Sicherheitsgründen wird hierbei eine neue Datei erzeugt und nach Abschluß der Ver-/Entschlüsselung die Ursprungsdatei physikalisch gelöscht. Die Verschlüsselung erfolgt hier mit einem Benutzer- oder anwendungsbezogenen Paßwort, wobei der Anwender zwischen zwei Verschlüsselungsverfahren wählen kann: Einem dem DES- Verfahren (Data Encryption Standard) entsprechendes und einem einfacheren Rotationsalgorithmus des Herstellers. Diese Offline- Verschlüsselung ist z. B. für Sicherungskopien und zum Datenträgertransport sinnvoll einsetzbar.

Die Online-Verschlüsselung kann mit der Offline-Verschlüsselung kombiniert werden; dies sollte in Betracht gezogen werden, wenn eine wirksame Abschottung der Benutzer erforderlich ist oder sensible Daten verarbeitet werden.

12.1.2.1.5
Weitere Einschränkungen

Erlaubnisse und Verbote auf Programmebene werden überwiegend über die Benutzerführung realisiert. Für jeden Menuepunkt kann geregelt werden:

- Protokollierung (Programmaufrufe aus der Benutzerführung und Dateizugriffe über die Dateiverwaltung; nicht aber Dateizugriffe, die aus einem Anwendungsprogramm ausgeführt werden (auch nicht, wenn der Aufruf unter der Kontrolle von SAFE-Guard erfolgt))
- Sperren des Zugangs zum Betriebssystem aus dem aufgerufenen Anwendungsprogramm heraus
- Sperre der Standard-Hardcopy

Zusätzlich können an jedem Menuepunkt Programme aufgerufen werden, mit denen z. B. Dateiattribute gesetzt, Verzeichnisse geschützt oder Dateien ent- bzw. verschlüsselt werden (solche Programme sind im Lieferumfang enthalten).

Da die Wirksamkeit einiger Schutzmechanismen voraussetzt, daß der Benutzer keinen direkten Zugang zum DOS erhält, wird ein Zusatzprogramm zur Dateiverwaltung mitgeliefert, mit dem der Benutzer menuegesteuert und kontrolliert die wichtigsten Betriebssystemfunktionen, wie z. B. Kopieren, Umbenennen oder Löschen von Dateien, ausführen kann. Der Funktionsumfang, der von diesem Dateiverwaltungsprogramm bereitgestellt wird, kann für jeden Benutzer individuell eingeschränkt werden. Funktionen, die vom Systemverwalter für den Benutzer gesperrt wurden, werden diesem auch nicht angezeigt.

Zusätzlich können bestimmte Dateinamensanhänge (Extensions) und Laufwerke von einer Bearbeitung über das Dateiverwaltungsprogramm ausgeschlossen werden.

Alle Schutzmechanismen auf dieser Ebene greifen nur, wenn und soweit dem Benutzer wirklich der Zugang zur Betriebssystemebene (COMMAND.COM) verwehrt wird. Auf diesen Umstand – der in der Konzeption von SAFE-Guard begründet ist – wird im Handbuch mehrfach hingewiesen.

Dies heißt z. B., wenn man den Betriebssystem-Zugang für das Textverarbeitungsprogramm MS-WORD (MS-WORD ist eingetragenes Warenzeichen von Microsoft) sperrt, kann auch die Rechtschreib- Prüfung nicht mehr direkt aus MS-WORD aufgerufen werden; sie müßte in diesem Fall als Menuepunkt unter der SAFE-Guard- Benutzerführung definiert werden.

Für höchste Sicherheitsanforderungen empfiehlt der Hersteller: „Programme, bei denen der Zugang zum System mit SAFE-Guard nicht unterbunden werden kann, bzw. die eine Manipulation fremder Dateien und/oder die Ausführung von DOS-Befehlen zulassen, sollten nicht installiert werden." Dies sollte unbedingt beachtet werden, da z. B. Programm- und Kommandoaufrufe von der Betriebssystemebene aus von SAFE-Guard nicht protokolliert werden können.

Der Systemverwalter hat bei SAFE-Guard grundsätzlich Zugang zur DOS-Ebene.

12.1.2.1.6
Softwareimport und -export

Die Einschleusung von sogenannten „Viren" und „trojanischen Pferden" in Programme hat in letzter Zeit für erhebliche Unruhe in Unternehmen gesorgt. Betroffen sind nicht nur Rechner, die an Netze angeschlossen sind, sondern auch isolierte Geräte. Letzteres hat die Aufmerksamkeit auf das Problem gelenkt, ob und wie der unbefugte Software-Import und der Einsatz von Raubkopien ausgeschlossen werden kann.

Zur Verhinderung unerwünschten Imports und Exports von Software bietet SAFE-Guard an, das Diskettenlaufwerk benutzerabhängig zu sperren bzw. nur zum Lesen oder Schreiben freizugeben. Zur Durchführung der Datensicherung wird zusätzlich ein e i g e n e s Datensicherungsprogramm angeboten, mit dem unter der Benutzerführung die Festplatte sowohl schnell als auch verschlüsselt gesichert werden kann.

Zum Schutz vor Manipulation/Einschleusen von Programmen kann SAFE-Guard eine programmspezifische Kontrollzahl ermitteln, die beim Programmaufruf mitgegeben und geprüft wird.

12.1.2.2
OCULIS plus Version 3.0

12.1.2.2.1
Systemverwaltung und -zugang

Die Verwaltungsfunktionen können auf drei verschiedene Personen verteilt werden, nämlich Installateur, Systemverwalter und Datenschützer:

- Der Installateur vergibt das Installationspaßwort, ohne das OCULIS plus nicht deinstalliert werden kann (auch nicht vom Systemverwalter); er hat darüber hinaus keine weiteren Funktionen.

- Der Systemverwalter legt für jeden Benutzer dessen Berechtigungen und Einschränkungen sowie den Umfang der Protokollierung fest; er kann aber selbst weder OCULIS plus deinstallieren noch die Protokollierung ausschalten.

- Der Datenschützer/Revisor stellt die für alle Benutzer gültige Mindestprotokollierung ein und wertet die Protokolldatei aus.

12.1.2.2.2
Technisches Konzept

Der Schutzeffekt von OCULIS plus basiert auf der Online- Verschlüsselung der Festplatte entweder komplett oder einzelner Partitions. D.h., die zu schützenden Partitions werden während der Installation von OCULIS plus mit einem nicht näher beschriebenen Verfahren verschlüsselt. Dabei kann für jede Partition ein eigener Schlüssel angegeben werden. Dieser Schlüssel dient später als Partition-Paßwort. Die Daten des berechtigten Benutzers werden ihm mit Hilfe

dieses Paßworts beim Lesen jeweils entschlüsselt zur Verfügung gestellt und beim Schreiben jeweils verschlüsselt weggeschrieben.

Die Ver- und Entschlüsselung wird mittels eines Geräte-Treibers (Device-Driver) durchgeführt, der während des Boot-Vorgangs geladen wird. Ein Umgehen bzw. Ersetzen des Geräte-Treibers ist technisch möglich, aber sinnlos, soweit die Festplatte bzw. Partition verschlüsselt ist: DOS selbst erkennt verschlüsselte Partitions nicht als Laufwerk; aber auch der Systemspezialist, der sich auf anderen Wegen Zugang verschafft, fängt mit den verschlüsselten Daten nichts an.

Wird die gesamte Festplatte verschlüsselt, so kann das System nur noch von einem Diskettenlaufwerk aus gestartet werden. Der Geräte-Treiber für die Festplatte muß sich dann auf der Diskette befinden, mit der das System gestartet wird. Andernfalls, wenn also mit einer „normalen" DOS-Diskette gebootet wird, wird die Festplatte nicht als solche erkannt; ein Zugriff ist dann nicht möglich.

12.1.2.2.3
Benutzerkontrolle

Um Zugang zu einer geschützten Partition zu erhalten, muß der Benutzer außer seiner Benutzerkennung das Partition-Paßwort und sein persönliches Paßwort kennen. Beide Paßwörter sind acht Zeichen lang und werden niemals angezeigt.

Das persönliche Paßwort kann vom Systemverwalter neu eingerichtet und vom Benutzer geändert werden. Ein erzwungener Paßwortwechsel durch den Benutzer nach Ablauf eines vom Systemverwalter vorzugebenden Gültigkeitszeitraums sowie eine benutzerbezogene Beschränkung des Benutzungszeitraums z. B. auf bestimmte Wochentage und Arbeitszeiten ist bislang nicht vorgesehen. Der Hersteller hat für die nächste Version von OCULIS plus entsprechende Änderungen zugesagt. Auch meine sonstigen Anregungen sollen dabei soweit wie möglich berücksichtigt werden.

12.1.2.2.4
Abschottung der Benutzer untereinander

Die Abschottung mehrerer Benutzer untereinander kann sowohl auf Partition- als auch auf Verzeichnisebene im Root-Directory (oberstes Inhaltsverzeichnis eines Direktzugriffsspeichers (Platte, Diskette)) erfolgen.

Der Schutz auf Partitionebene wird über das Partition-Paßwort, mit dem diese Partition verschlüsselt wurde, realisiert. Auch wenn auf dieser Partition kein weiterer Benutzer arbeiten darf, muß der Benutzer vom Systemverwalter explizit für alle auf dieser Partition existierenden Verzeichnisse (nur Einträge im Root- Directory) zugelassen werden (Verbot mit Erlaubnisvorbehalt). Es ist nicht möglich, das Partition-Paßwort an einen Benutzer zu binden; es kann auch – im Gegensatz zum Benutzerpaßwort – nur von dem Systemverwalter gewechselt werden.

Der Schutz auf Verzeichnisebene sorgt dafür, daß mehrere Benutzer auf einer Partition arbeiten und dennoch voneinander abgeschottet werden können. Es sind sowohl allgemeine als auch private Verzeichnisse möglich. Verzeichnisse, für die der Benutzer nicht berechtigt ist, werden für diesen als ungültig gekennzeichnet, so daß ein Zugriff über das DOS nicht möglich ist.

Tests ergaben aber, daß es auf anderem Wege möglich ist, die Abschottung mehrerer Benutzer durch private Verzeichnisse in derselben Partition zu unterlaufen. Deshalb empfehle ich die Vergabe einer eigenen Partition für jeden Benutzer. Sie bietet die größtmögliche Sicherheit, da jede Partition anders verschlüsselt werden kann. Wenn es einem Benutzer überhaupt gelingt, die Daten einer anderen Partition zu lesen, so werden ihm diese verschlüsselt angezeigt.

12.1.2.2.5
Weitere Einschränkungen

OCULIS plus kann die möglichen Aktivitäten des Benutzers individuell sehr weitgehend einschränken. Realisiert wird dies über sogenannte DOS-Zeichenketten, mit denen Befehle, Dateinamen oder Fragmente hiervon, die der Benutzer nicht verwenden soll, definiert werden. Bei jeder Ausführung eines Programms oder dem Eröffnen einer Datei vergleicht OCULIS plus den von der Tastatur eingegebenen oder vom Programm übergebenen Datei-/Programmnamen mit den für den Benutzer definierten DOS-Zeichenketten und weist bei Übereinstimmung die Ausführung der angeforderten Funktion zurück.

Beispiel:
Restriktion: 123
Auswirkung: 1. 123.EXE kann nicht ausgeführt werden.
2. DEMO.123 kann nicht angelegt werden.

Soll z. B. die Ausführung von 123.EXE unterbunden, das Anlegen der Datei DEMO.123 aber erlaubt sein, so kann die Wirkung der DOS- Zeichenketten durch sogenannte Schlüsselwörter eingeschränkt werden.

Schlüsselwörter existieren für
- Programmaufrufe
- COMMAND.COM-Befehle (z. B. DIR)
- Öffnen von Dateien
- Anlegen von Dateien
- Warmstart
- Programmabbruch
- Hardcopy
- Zugriff auf Diskettenlaufwerk (Lesen, Schreiben, Verschlüsseln)

In diesem Teil des Benutzerprofils kann auch geregelt werden:
- Blockieren der Tastatur
- Dunkelstellung des Bildschirms und Abfrage des Benutzerpaßworts
- Abfragen des Benutzerpaßworts nach Ablauf einer bestimmten Zeitspanne ohne Benutzeraktivitäten
- Vergabe einer besonderen LOGON-Prozedur
- Verschärfung der vom Datenschützer eingestellten Minimal- Protokollierung

Die Protokollierung der Benutzeraktivitäten (Kommando- und Programmaufrufe, Dateizugriffe) ist an keine Voraussetzungen (Benutzerführung, Menuesystem etc.) gebunden. D.h., es werden auch alle Dateizugriffe, die von Anwendungsprogrammen ausgeführt werden, protokolliert.

12.1.2.2.6
Softwareimport und -export

Das Installieren und Sichern von Software bzw. Dateien kann von OCULIS plus benutzerspezifisch geregelt werden. Diese Schutzfunktion wird durch eine durchgängige benutzerspezifische automatische Online-Verschlüsselung der Disketten realisiert. Diese Verschlüsselung ist nicht von dem Einsatz bestimmter Sicherungssoftware abhängig, sondern gilt für alle Programme.

Damit läßt sich auch erreichen, daß Software weder importiert noch exportiert werden kann, weil weder ein unverschlüsseltes Programm von der Diskette eingelesen und ausgeführt, noch ein verschlüsseltes Programm auf Diskette unverschlüsselt ausgegeben werden kann.

Zur Transportsicherung bietet derselbe Hersteller ein anderes Produkt an (ABATON), das eine Offline-Verschlüsselung mit einem gesonderten (Transport-)Paßwort vornimmt.

12.1.2.3
Fazit

Beide Programme entsprechen dem Stand der Technik und sind bei sorgfältiger Generierung sicherlich geeignet, den Zugriff auf die Festplatte und bei SAFE-Guard Plus zusätzlich das Booten des Systems zu kontrollieren.

Art und Qualität der verwendeten kryptographischen Verfahren wurden nicht untersucht. Negative Auswirkungen der Online- Verschlüsselung auf das Antwortzeitverhalten konnten nicht festgestellt werden.

Hinsichtlich der Abschottung der Benutzer untereinander und der weiteren Einschränkungen bestehen vom Konzept und der Implementierung her große Unterschiede. Diese Unterschiede können bei der Entscheidungsfindung über den Einsatz von Datenschutzsoftware anhand des Anforderungskatalogs relevant werden.

12.1.3
Anforderungen an zukünftige Entwicklungen

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat am 10. Oktober 1988 einen Beschluß für Datensicherheit beim Einsatz kleinerer DV-Anlagen gefaßt (s. Ziffer 16.7 dieses Berichts). Darin werden u. a. die Hersteller von Hard- und Software aufgefordert, Hilfsmittel verfügbar zu machen, „die es einer datenverarbeitenden Stelle ermöglichen,

- ohne organisatorisch strukturiertes Rechenzentrum und damit auch ohne Funktionstrennungen bei der Arbeitsabwicklung,

- ohne organisatorische Trennung zwischen Anwendung und Durchführung der automatisierten Datenverarbeitung und

- trotz Verzichts auf Detailkenntnisse der automatisierten Datenverarbeitung bei Vorgesetzten und der für die Revision zuständigen Organisationseinheit

sicherzustellen, daß bei der Verarbeitung auf der eingesetzten Datenverarbeitungsanlage eine verbindlich vorgeschriebene Verarbeitungslogik eingehalten wird. Dazu ist es unter anderem erforderlich, Verfahren bereitzustellen, die

gewährleisten, daß Programme ausschließlich in der freigegebenen Fassung zum Ablauf kommen. Systemprogramme und Anwendungsprogramme könnten dazu mit einem geeigneten kryptografischen Verfahren versiegelt werden, wodurch Manipulationen erkennbar würden."

Die Hersteller von Datenschutz-Zusatzprodukten sind dabei, Netzwerkversionen für MS-DOS bzw. PC-DOS zu erstellen. An der Übertragung auf andere Betriebssysteme wird gearbeitet. Auch die Entwicklung und Implementierung geeigneter kryptographischer Verfahren u. a. für die Sicherstellung einer verbindlichen Verarbeitungslogik und für die Abschottung von Benutzern untereinander ist mit Sicherheit noch nicht abgeschlossen; hier könnte die Speicherchipkarte neue Impulse geben.

Aber nicht nur die Hersteller, sondern auch die Anwender sind gefordert. Sie müssen die erforderlichen und angemessenen technischen und organisatorischen Maßnahmen treffen; hierzu habe ich bereits in meinem 15. Tätigkeitsbericht (Ziff. 9.) ausführlich Stellung genommen, so daß ich mich auf Neuerungen beschränken kann.

Einen besonders wichtigen Punkt sehe ich darin, den Anwendern auf dem APC wirklich nur die Software zur Verfügung zu stellen, die zum Arbeiten benötigt wird. Insbesondere haben sogenannte Dienstprogramme und andere systemnahe Programme sowie Programme, mit denen die Schutzfunktionen der Zusatzsoftware unterlaufen werden können, auf einem APC nichts zu suchen.

Der Einsatz von Dienstprogrammen sollte dem Systembetreuer vorbehalten bleiben, der im Bedarfsfalle solche Programme von der Diskette laden kann. Da sehr leistungsfähige Dienstprogramme bei privaten Nutzern sehr weit verbreitet sind, sind darüber hinaus Maßnahmen zur Verhinderung eines Softwareimports besonders wichtig (s.o. 12.1.2.1.6 und 12.1.2.2.6).

Softwarehersteller bieten, insbesondere für den Bereich der Datenbanksoftware, zunehmend zwei Versionen an: Das vollständige Softwaresystem als Entwicklungsversion und daneben eine sogenannte RUN-TIME-Version, mit der fertige Anwendungsprogramme ablaufen, aber nicht mehr oder nur unter erschwerten Bedingungen verändert oder weiterentwickelt werden können. Damit besteht die Möglichkeit, auf einem APC, dem Entwicklungsrechner, die (evtl. zentrale) (Anwendungs-)Programmentwicklung vorzunehmen und den eigentlichen Anwendern (z. B. in den Fachabteilungen) auf einem oder mehreren Produktionsrechnern nur das ablauffähige Anwendungssystem zur Verfügung zu stellen. Dies erlaubt eine Verbesserung der Funktionstrennung zwischen Entwicklung und Produktion. Die Überlegung, wo eine Entwicklungsversion erforderlich und wo eine RUN-TIME-Version ausreichend ist, kann auch unter finanziellen und technischen Aspekten interessant sein: Lizenzen für RUN-TIME-Versionen sind billiger und benötigen weniger Speicherplatz.

Daß auch hier unbefugter Software-Import verhindert werden muß und eine Vernetzung der APC's die Funktionstrennung wieder gefährden oder aufheben kann, versteht sich von selbst.

(1) Partition
Festplattenbereich, der vom Betriebssystem wie eine selbständige Festplatte behandelt wird (logisches Laufwerk). Jede Partition verfügt über eine eigene Dateizuordnungstabelle (FAT – File Allocation Table) und ein eigenes Hauptverzeichnis (Root Directory)

(2) Residente Programme sind Anwendungsprogramme, die nach ihrem ersten Aufruf im Hauptspeicher verbleiben und durch festgelegte Ereignisse, wie z. B. das Auslösen eines bestimmten Interrupts oder das Drücken einer bestimmten Tastenkombination, aktiviert werden.

12.2
Aktenaufbewahrung

Bei Prüfungen stellt sich immer wieder heraus, daß die von § 10 Hessisches Datenschutzgesetz für die Verarbeitung personenbezogener Daten geforderten technischen und organisatorischen Sicherheitsmaßnahmen nicht oder nicht in ausreichendem Maße getroffen worden sind. Besonders nachlässig wird in dieser Hinsicht oft mit Akten verfahren. Dabei stellt § 10 Abs. 2 HDSG unmißverständlich klar, daß auch hier – und nicht nur bei der automatisierten Datenverarbeitung – die Datensicherheit gewährleistet sein muß. Das Gesetz verlangt ausdrücklich Maßnahmen, die verhindern, daß Unbefugte bei der Bearbeitung, der Aufbewahrung, dem Transport und der Vernichtung der Akten die darin enthaltenen personenbezogenen Daten zur Kenntnis nehmen können.

12.2.1
Landwirtschaftsämter

Bei meinen stichprobenweisen Kontrollbesuchen einiger Landwirtschaftsämter zur Überprüfung des Datenschutzes im Zusammenhang mit der Milch-Garantiemengen-Verordnung hatte ich festgestellt, daß die Sicherung der Akten gegen Zugriffe Unbefugter „völlig unzureichend" war (16. Tätigkeitsbericht, Ziff. 12.3.2,). Um mir einen Überblick darüber zu verschaffen, ob es sich bei den festgestellten Datensicherungsmängeln um Einzelfälle handelte oder um eine für die Verwaltung in diesem Bereich typische Erscheinung, habe ich in einer 25 Kontrollbesuche umfassenden Prüfserie alle siebzehn Landwirtschaftsämter, das Weinbauamt und die drei Dienststellen des Landesamtes für Ernährung, Landwirtschaft und Landentwicklung in Kassel, Frankfurt und Wiesbaden überprüft. Erhebliche Mängel in der

Datensicherung waren bei fast allen Dienststellen der Landwirtschaftsverwaltung festzustellen. Vorwiegend handelte es sich um Mängel bei der Aktenaufbewahrung sowie bei der Aktenvernichtung.

Aus dem Datengeheimnis (§ 9 HDSG) und dem Zweckbindungsgrundsatz (§ 13 HDSG) ergibt sich, daß Zugang zu den Akten nur die jeweils für deren Bearbeitung zuständigen Bediensteten haben dürfen. Daraus folgt: Akten müssen grundsätzlich unter Verschluß aufbewahrt werden. Mit Ausnahme von drei Ämtern für Landwirtschaft und Landentwicklung, nämlich Heppenheim, Korbach und Reichelsheim – die bereits mit neuerem Mobiliar ausgestattet sind – war die Aktenaufbewahrung bei allen anderen Dienststellen zu beanstanden. Am schlimmsten erwies sich die Situation der Aktenunterbringung in den Ämtern für Landwirtschaft und Landentwicklung, die in einem Gebäude zusammen mit mehreren Dienststellen anderer Verwaltungen untergebracht sind; dort ist ein nicht geringer Teil der Akten in offenen Regalen auf Fluren untergebracht, die der Öffentlichkeit zugänglich sind. Bei den anderen Dienststellen zeigte sich die Situation nicht ganz so kraß, aber immer noch aus der Sicht des Datenschutzes als inakzeptabel: Diese Dienststellen sind fast alle mit altersschwachen, nicht oder nicht mehr verschließbaren Schränken ausgestattet, die teilweise selbst in geschlossenem Zustand keine sichere Aufbewahrung gewährleisten. Auch die Arbeitsräume sind zum großen Teil (wegen fehlender Schlüssel) nicht mehr verschließbar oder werden jedenfalls üblicherweise nicht verschlossen. Das bedeutet, nicht zuletzt im Hinblick auf die bestehende gleitende Arbeitszeit, daß bei Abwesenheit des Sachbearbeiters andere Bedienstete oder auch private Besucher der Dienststelle wie auch die Mitarbeiter des Reinigungsdienstes ohne Schwierigkeiten Akten einsehen, vernichten oder entfernen könnten.

In den meisten der geprüften Fälle haben sich Amtsleitung und Mitarbeiter redlich bemüht, die Situation zu verbessern, wegen mangelnder Haushaltsmittel bisher jedoch ohne durchgreifenden Erfolg.

Auch das Problem der Aktenvernichtung muß in absehbarer Zeit eine Lösung in der Weise finden, daß jedes Amt über wenigstens einen eigenen Reißwolf verfügt. Bisher ist dies nur bei zwei Dienststellen der Fall. Nur so kann gewährleistet werden, daß Entwürfe, Notizen, Duplikate und dergleichen Unterlagen mit sensitiven Daten – über den Papierkorb und die allgemeine Müllabfuhr – Unbefugten in die Hände fallen. Die bisher von den meisten Amtsleitungen gezwungenermaßen gefundenen Hilfslösungen setzen alle den Aktentransport zu Vernichtungsfirmen oder Zwischenlagern voraus, was nach langjähriger Erfahrung eine häufige Quelle von Datenschutzpannen ist.

Ich habe die geschilderten Mängel bei Aktenaufbewahrung und Aktenvernichtung gemäß § 27 HDSG beanstandet. Eine durchgreifende Verbesserung der Datenschutzsituation in der Landwirtschaftsverwaltung setzt jedoch voraus, daß mehr Haushaltsmittel als bisher vorgesehen zur Anschaffung verschließbarer Schränke bzw. zur Modernisierung vorhandenen Mobiliars bereitgestellt werden.

Es muß davon ausgegangen werden, daß sich ähnliche Prüfergebnisse, was die Datensicherheit angeht, auch in anderen Bereichen der Landesverwaltung zeigen würden. In allen Dienststellen sollten deshalb unter Beteiligung des behördlichen Datenschutzbeauftragten sogenannte „Schwachstellenanalysen" aufgestellt werden, aus denen Art und Umfang der vorhandenen Datensicherungsmängel erkennbar sind. Nur so sehe ich auf lange Sicht eine Möglichkeit, bei der Verbesserung insbesondere der Datensicherung Prioritäten zu setzen und die vorhandenen Mittel möglichst effektiv zu verwenden.

12.2.2
Sozialamt Friedberg

Durch Fernseh- und Presseberichte erfuhr ich, daß beim Sozialamt des Wetteraukreises in Friedberg Akten entwendet worden waren. Ein Teil dieser Akten wurde in einem Müllcontainer eines Supermarktes in der Nähe des Kreishauses gefunden.

Bei einer sofortigen Überprüfung im Sozialamt des Wetteraukreises stellte ich fest, daß ca. 40 Akten, die aussortierte Vorgänge aus den Jahren 1985 und älter über einmalige Beihilfen an Nichtseßhafte enthielten und die in das Achiv des Kreisausschusses im Keller des Kreisgebäudes gebracht werden sollten, zunächst auf einem Aktenschrank im Flur des Sozialamtes gelagert und von dort entwendet worden waren. Der hier ursächliche organisatorische Mangel konnte mit Hilfe meiner Beratung umgehend beseitigt werden.

Bei dieser Prüfung ergab sich außerdem, daß ein Teil der Sozialamtsakten in einfachen Holzschränken – die zwar zum Zeitpunkt meines Besuchs verschlossen waren – aus Raummangel auf dem Flur aufbewahrt werden. Eine solche Form der Aufbewahrung bietet keine ausreichende Datensicherheit, deshalb habe ich verlangt, die Akten nicht mehr in diesen Schränken zu lagern.

12.2.3
Amt für Verteidigungslasten; Nebenstelle Wiesbaden

Eine Bürgerin beschwerte sich, daß in der Nebenstelle Wiesbaden des Amtes für Verteidigungslasten Belege über Gehaltsabrechnungen offen und für jedermann zugänglich auf dem Flur gelagert würden. Das Amt für Verteidigungslasten, Nebenstelle Wiesbaden, bearbeitet die Lohn- und Gehaltsabrechnungen von ca. 3.500 Zivilbeschäftigten bei den ausländischen Streitkräften. Die aufgrund der Beschwerde vorgenommene Überprüfung ergab neben anderen Mängeln auch hier wiederum gravierende Datensicherheitsmängel bei der Aktenaufbewahrung:

Die Eingangshalle des Gebäudes war zwar mit einem Pförtner besetzt, der aber keine Zugangskontrolle durchführte, sondern nur Auskünfte erteilte. Trotz des starken Besucherverkehrs konnten die Diensträume nicht verschlossen werden, da nur einige Bedienstete Schlüssel für die Büroräume besaßen, so daß die Türen auch in Abwesenheit (bei Besprechungen oder Mittagspausen) offen blieben. Nach Dienstschluß blieben die Büros unverschlossen. Unterlagen (Lohnkonten, Pfändungsbeschlüsse, Lohnlisten usw.) wurden in den Büros in nicht verschlossenen Schreibtischen und Holzschränken verwahrt. Im Flur der Behörde befand sich ein großer Karton, in dem sich Belege über Gehaltsabrechnungen aus dem Jahre 1985 befanden, die vernichtet werden sollten. Diese Unterlagen konnten von jedem Besucher eingesehen werden. Eine Dienstanweisung, die technische und organisatorische Datenschutzmaßnahmen regelte, war nicht vorhanden.

Die festgestellten Mängel sind teilweise umgehend beseitigt worden. Eine weitere Prüfung erübrigt sich jedoch, da mir das Amt für Verteidigungslasten in Frankfurt mit Schreiben vom 1. Dezember 1988 mitgeteilt hat, daß die Außenstelle zum 1. April 1989 geschlossen wird.

12.3
Gesundheitsdaten im Müll

12.3.1
Der Fall

Die Redaktion der Frankfurter Rundschau hatte Tonbandkassetten zugespielt bekommen, auf denen besprochene Diktierplatten der Frankfurter Stadtverwaltung kopiert waren. Zum Teil handelte es sich um äußerst sensible personenbezogene Daten. So enthielt beispielsweise ein diktiertes Schreiben Einzelangaben über Dienstunfälle und Krankheitsverläufe mehrerer mit Namen und Wohnanschrift genannter städtischer Mitarbeiter.

Es stellte sich heraus, daß Mitarbeiter der mit der Beschaffung von Bürogeräten befaßten kommunalen Dienststelle große Mengen besprochener und nicht gelöschter Diktierplatten samt den dazugehörenden Abspielgeräten ausgesondert und kurzerhand auf den Müll geworfen hatten. An den gebotenen Datenschutz war kein Gedanke verschwendet worden. Als Folge dieser Verfahrensweise gerieten Datenträger in falsche Hände und wurden zumindest in einem Fall, in dem auch ein Ermittlungsverfahren der Staatsanwaltschaft anhängig ist, zur Androhung einer strafbaren Handlung benutzt.

12.3.2
Die Reaktion der Stadt

Auf meine Anfrage, wie künftig sichergestellt werden soll, daß sich ein solcher Fall nicht wiederholt, hat mir die Stadt Frankfurt mitgeteilt, durch eine amtliche Verfügung „Amts-/Dienstgeheimnis, Vertraulichkeit von Unterlagen, Datenschutz" (Nachrichten für die Stadtverwaltung, Nr. 31, S. 330) sei der Umgang mit Unterlagen und Datenträgern, die schutzwürdige Daten enthalten, neu geregelt worden. Diese Verfügung, die auch die Vernichtung der Unterlagen regelt, gelte sowohl für Akten und sonstige Schriftstücke als auch für Datenträger wie Diktierplatten, -kassetten, Micro-Disketten und Carbonfarbbänder (Einmalfarbbänder). Um den Mitarbeitern der Stadt das Problem ganz besonders vor Augen zu führen, werde diesen die Verfügung gegen Unterschrift zur Kenntnis gegeben.

12.3.3
Die Besonderheit des Falles

Pannen bei der Entsorgung von Schriftstücken, Akten und Datenträgern hat es in der Vergangenheit immer wieder gegeben. Auch sind die Einzelheiten der in meinen Tätigkeitsberichten kommentierten Fälle oft gleich: mangelndes Datenschutzbewußtsein, unvollständige bzw. fehlende Vorschriften und eben einfach Schlamperei. Trotzdem weist dieser Fall eine Besonderheit auf.

Die Stadt hat zwar schnell und richtig reagiert, vertrat aber in ihrer Entgegnung auf meine Anfrage die Ansicht, Diktierplatten fielen „... nicht in den Schutzbereich des Hessischen Datenschutzgesetzes ...". Dies ist schlicht falsch. Mit der Neufassung des Hessischen Datenschutzgesetzes vom 11. November 1986 ist die für das alte Gesetz geltende Beschränkung auf Datenverarbeitung in Dateien aufgehoben worden. § 2 Abs. 2 HDSG bestimmt jetzt, daß Datenverarbeitung jede Verwendung gespeicherter oder zur Speicherung vorgesehener personenbezogener Daten ist. Der Begriff des Speicherns, der einschließlich seiner Definition in § 2 Abs. 2 Ziff. 2 HDSG unverändert aus dem Zweiten Hessischen Datenschutzgesetz von 1978 übernommen wurde, schließt eben auch das Aufnehmen von Daten auf einem Datenträger, d. h. beispielsweise das Aufzeichnen von Sprache auf einem Tonband ein.

Ich habe den Magistrat der Stadt Frankfurt auf diese Rechtslage hingewiesen.

13. Behördeninterner Datenschutzbeauftragter

13.1
Aufgaben

Das neue Hessische Datenschutzgesetz verpflichtet in § 5 Abs. 2 jede datenverarbeitende Stelle, einen behördeninternen Beauftragten für den Datenschutz zu bestellen. Die Frage, welche Beschäftigten für diese Funktion in Frage kommen, habe ich bereits im 16. Tätigkeitsbericht (Ziff. 2.2.1) erörtert. Im letzten Jahr wandten sich nun eine Vielzahl von Behörden, insbesondere Kommunen, an mich mit der Frage nach der Ausgestaltung der Aufgaben des behördeninternen Datenschutzbeauftragten.

Zwar sind in § 5 Abs. 2 HDSG bereits einige Aufgabengebiete des behördeninternen Beauftragten für den Datenschutz genannt, jedoch ist diese Aufzählung keinesfalls abschließend.

Zunächst ist festzustellen, daß der behördeninterne Beauftragte für den Datenschutz nicht nur den Leiter der Behörde, sondern auch die Bediensteten in Belangen des Datenschutzes berät. Er sollte organisatorisch direkt der Behördenleitung unterstellt sein.

Ausdrücklich erwähnt das HDSG die Mitwirkung bei der Meldung der Dateien zum Register des Hessischen Datenschutzbeauftragten und bei der Erstellung des Geräteverzeichnisses. Außerdem hat der behördeninterne Datenschutzbeauftragte bei der Überwachung der nach § 10 HDSG erforderlichen technischen und organisatorischen Datensicherheitsmaßnahmen mitzuwirken. Die datenverarbeitende Stelle hat ihn in die Entscheidungen einzubeziehen, indem sie ihn informiert und bei Beratungen hinzuzieht. Darüber hinaus sollte der behördeninterne Datenschutzbeauftragte von sich aus die Fachreferate auf technische und organisatorische Datensicherheitsmängel hinweisen und an der Beseitigung der Mängel beratend mitwirken.

Das Hessische Datenschutzgesetz überträgt dem behördeninternen Beauftragten für den Datenschutz die Aufgabe, bei der Beantwortung von Auskunftsbegehren des Hessischen Datenschutzbeauftragten mitzuwirken. Der behördliche Datenschutzbeauftragte ist sicher in besonderem Maße dazu geeignet, zunächst Ansprechpartner des Hessischen Datenschutzbeauftragten zu sein und erste Informationen zu geben bzw. einzuholen. Dies darf jedoch nicht dahingehend mißverstanden werden, daß der behördeninterne Beauftragte für den Datenschutz ausschließlicher Ansprechpartner des Hessischen Datenschutzbeauftragten ist. Jeder behördliche Mitarbeiter ist verpflichtet, unmittelbar und umfassend die vom Hessischen Datenschutzbeauftragten verlangten Auskünfte zu geben (§ 29 HDSG).

Aus der generellen Zuständigkeit des Datenschutzbeauftragten für Datenschutzfragen innerhalb seiner Behörde ergibt sich als weitere Aufgabe die Beratung der Ämter im Hinblick auf die Erforderlichkeit der erhobenen Daten. Insofern ist es auch sinnvoll, wenn die Ämter ihn bereits bei der Gestaltung von Formblättern einschalten.

Unsicherheit besteht bei den Behörden oftmals über die rechtlichen Voraussetzungen für die Löschung oder auch die Sperrung von personenbezogenen Daten. Wenn sich diese nicht bereits aus Verwaltungsvorschriften ergeben (z. B. gemeinsamer Erlaß des Hessischen Innenministers und des Hessischen Finanzministers vom 20.10.1986, StAnz. 1986, S. 2107 betreffend die Aufbewahrungsbestimmung für Akten und sonstiges Schriftgut der Dienststellen des Landes Hessen), sollte der Datenschutzbeauftragte auf behördeninterne Dienstanweisungen hinwirken.

Besonderes Augenmerk sollte der Datenschutzbeauftragte darauf richten, welche Übermittlungen die Ämter regelmäßig oder auch in Einzelfällen vornehmen, und ob die datenschutzrechtlichen Anforderungen dabei eingehalten werden.

Daraus darf freilich nicht geschlossen werden, datenschutzrechtliche Fragen seien allein Sache des Beauftragten für den Datenschutz. Im Gegenteil: Verantwortlich für die Einhaltung der Datenschutzvorschriften ist und bleibt der Behördenleiter.

Auch wenn der interne Datenschutzbeauftragte hauptsächlich eine beratende Funktion innerhalb der Verwaltung hat, kann es darüber hinaus sinnvoll sein, ihm die Aufgabe eines „Ansprechpartners für den Bürger" zuzuweisen, etwa wenn es um die Geltendmachung des Auskunftsrechts bzw. des Akteneinsichtsrechts geht.

13.2
Behördlicher Datenschutzbeauftragter und Personalvertretung

Wiederholt wurde auch die Frage zum Verhältnis des behördeninternen Datenschutzbeauftragten zur Personalvertretung gestellt.

Der Personalrat hat ein Mitbestimmungsrecht bei der Bestellung und der Abberufung des Datenschutzbeauftragten (§ 74 Abs. 1 Ziff. 3 Hessisches Personalvertretungsgesetz – HPVG –). Damit soll u. a. sichergestellt werden, daß der behördliche Datenschutzbeauftragte auch das Vertrauen der Bediensteten besitzt. Weitere Festlegungen gibt es weder im HDSG noch im HPVG.

Der Personalrat hat jedoch über das Mitbestimmungsrecht hinausgehende Aufgaben und Kompetenzen in datenschutzrechtlichen Fragen: So hat er über die Einhaltung der Gesetze zu wachen, die zugunsten der Beschäftigten gelten (§ 62

Abs. 1 Ziff. 2 HPVG – dazu gehören auch die Datenschutzregeln. Bei der Einführung automatisierter Verarbeitung von Beschäftigtendaten hat er mitzuwirken (§ 81 Abs. 1 HPVG). Diese Aufgabenfelder überschneiden sich mit denen des behördlichen Datenschutzbeauftragten. Hinzu kommt, daß in aller Regel der Personalrat bei diesen Fragen auf sachverständige Unterstützung angewiesen ist. So wie jeder Bedienstete kann auch der Personalrat sich vom Datenschutzbeauftragten beraten lassen. Eine Unterrichtungspflicht, wie ich sie in meinem 13. Tätigkeitsbericht (Ziff. 3.3.2) gefordert habe, gibt es jedoch nicht. Der Personalrat kann dem Datenschutzbeauftragten auch keine Aufträge erteilen, bestimmte Vorgänge zu überprüfen. Ansprechpartner für ihn bleibt der Dienststellenleiter. Dieser entscheidet bei konkreten Beschwerden darüber, in welcher Form diesen nachgegangen wird.

14. Hessisches Privatrundfunkgesetz

Im Dezember 1988 ist das Gesetz über den privaten Rundfunk in Hessen (HPRG) in Kraft getreten (GVBl. I S. 385). Dieses Gesetz regelt die Veranstaltung von privatem Hörfunk, Fernsehen und Fernsehtext sowie die Weiterverbreitung von Rundfunkprogrammen in Hessen.

Schon im Referentenentwurf vom Mai 1988 war ein ausführlicher Abschnitt über Datenschutz und Datensicherung enthalten. Die Regelungen basierten weitgehend auf den bereits in den Medien- und Rundfunkgesetzen anderer Bundesländer aufgenommenen Datenschutznormen. Zu nennen sind hier u. a. das Hamburgische Mediengesetz, das Landesmediengesetz Baden-Württemberg und das Kabelpilotprojektgesetz des Landes Berlin.

Aufgrund meiner ausführlichen Stellungnahme vom 31. Mai 1988 wurde die Fassung des Referentenentwurfs nach Abstimmung mit den Ressorts und der Staatskanzlei im Regierungsentwurf (Drucks. 12/2478) in einigen Punkten geändert.

Grundsätzlich ist mit der Veranstaltung und Verbreitung von ausschließlich aus Werbung finanzierten privaten Rundfunkprogrammen eine Erhebung und Verarbeitung von Daten der Teilnehmer nicht verbunden. Die Regelungen des Neunten Abschnitts des HPRG über den Datenschutz beziehen sich daher vor allem auf die Situation, daß Programme über Abonnements oder Einzelentgelte finanziert werden und die Abrechnung nicht dezentral über beim Teilnehmer installierte Einrichtungen erfolgt. Für die dann anfallenden Abrechnungs- und Verbindungsdaten stellen sich die gleichen datenschutzrechtlichen Probleme wie bei den Telekommunikationsdienstleistungen in Form der Individualkommunikation, z. B. beim Bildschirmtext: Es gilt, die Erstellung persönlicher Nutzungsprofile zu verhindern und die Anonymität der individuellen (Programm-)Auswahl zu sichern.

§ 53 HPRG verlangt daher vor allem, daß aus den Abrechnungsdaten nicht feststellbar sein darf, welche einzelnen Sendungen oder Programme der Teilnehmer empfangen hat (Abs. 2). Hinzu kommen das sofortige Löschungsgebot für Verbindungsdaten und das Verbot der Übermittlung von Abrechnungs- und Verbindungsdaten an Dritte – mit Ausnahme des Rundfunkveranstalters, der selbst das Inkasso der Entgelte abwickelt (Abs. 3).

Bemerkenswert ist weiterhin die speziell auf den Rundfunk bezogene Konkretisierung des allgemeinen datenschutzrechtlichen Gebots der Datensicherung (vgl. § 10 HDSG, § 6 BDSG) in § 51 Satz 2 HPRG: Danach sind Kabelnetze und andere Kommunikationseinrichtungen technisch so auszugestalten, daß personenbezogene Daten nicht verfälscht, gestört oder zu anderen als Gegendarstellungs- und Abrechnungszwecken verarbeitet werden dürfen.

Die Kontrollzuständigkeit für die Einhaltung des Datenschutzes hat der Gesetzgeber im gesamten Anwendungsbereich des HPRG dem Hessischen Datenschutzbeauftragten übertragen (§ 54 HPRG). Betroffen sind – neben der Hessischen Landesanstalt für privaten Rundfunk in der Rechtsform einer Anstalt des öffentlichen Rechts – auch die privatrechtlich verfaßten Kabelgesellschaften, Rundfunkveranstalter usw. Für letztere ist also die Überwachungszuständigkeit des Regierungspräsidenten als Aufsichtsbehörde nach § 30 BDSG nicht gegeben. Materiell, d. h. für die Zulässigkeit der Verarbeitung von Teilnehmerdaten, bleibt es dagegen bei der Anwendbarkeit des Bundesdatenschutzgesetzes ergänzend zu den bereichsspezifischen Normen der §§ 51 bis 53 HPRG. Beanstandungen wegen unzulässiger Datenverarbeitung kann der Hessische Datenschutzbeauftragte allerdings gegenüber privaten Rundfunkgesellschaften nicht direkt aussprechen; vielmehr muß er die Landesanstalt einschalten. Mit dieser Regelung hat der Gesetzgeber die Parallele gezogen zu § 3 Abs. 6 des HDSG, der dem Hessischen Datenschutzbeauftragten die Kontrollzuständigkeit für die Teilnehmer- und Abrechnungsdaten beim Hessischen Rundfunk eingeräumt hat (vgl. dazu Ziff. 15.3 dieses Berichts). Damit wird vor allem der Anforderung der Staatsferne, die die Judikatur des Bundesverfassungsgerichts aus der grundgesetzlichen Garantie der Rundfunkfreiheit ableitet, Rechnung getragen. Diese Staatsferne ist gewährleistet durch die Anbindung des Datenschutzbeauftragten an den Landtag und damit die Legislative statt – wie in anderen Bundesländern – an die Landesregierung.

15. Bilanz

15.1
Archivgesetz
(10. Tätigkeitsbericht, Ziff. 3.2, 11. Tätigkeitsbericht, Ziff. 2.3, 12. Tätigkeitsbericht, Ziff. 4.1, 13. Tätigkeitsbericht, Ziff. 4.1.7, 14. Tätigkeitsbericht, Ziff. 11.2, 15. Tätigkeitsbericht, Ziff. 1.1.2.1 i.V.m. 1.1.2.3, 16. Tätigkeitsbericht, Ziff. 1.2.1)

Nach einjähriger Stagnation ist 1988 die Diskussion um ein Hessisches Archivgesetz wieder in Bewegung geraten. In diesem Jahr sind dem Hessischen Landtag gleich zwei Entwürfe für ein Landesarchivgesetz zugegangen. Am 12.

Februar 1988 hat die Fraktion der GRÜNEN ihren Gesetzentwurf für ein Hessisches Archivgesetz eingebracht (Drucks. 12/1641), und seit dem 20. September 1988 liegt dem Parlament außerdem ein Entwurf der SPD-Fraktion zur Beratung vor (Drucks. 12/3040).

Notwendigkeit und Dringlichkeit des Landesarchivgesetzes sind mittlerweile allgemein anerkannt. In der Sitzung des Landtagsinnenausschusses vom 1. Juni 1988 haben jetzt auch alle Fraktionen zum Ausdruck gebracht, daß sie eine gesetzliche Regelung des Archivbereichs für dringend erforderlich halten (Kurzbericht, 11. Sitzung des Innenausschusses, S. 4). Wie es scheint, stehen also die Chancen gut, daß es im kommenden Jahr zur Verabschiedung eines Landesarchivgesetzes kommen wird und damit meine in den letzten sieben Tätigkeitsberichten immer wieder erhobene Forderung endlich erfüllt wird.

Beide Gesetzentwürfe erfüllen die grundsätzlichen datenschutzrechtlichen Anforderungen, die an ein Archivgesetz zu stellen sind. Dazu zählen beispielsweise die Festlegung der Aufgaben der öffentlichen Archive und die Definition der archivwürdigen Materialien. Was bislang nur als Erlaßregelung existiert, nämlich die Pflicht der Behörden, Unterlagen, die sie nicht mehr benötigen, auszusondern und dem zuständigen Archiv anzubieten, wird gesetzlich verankert.

Die Anbietungspflicht soll auch für solche Unterlagen gelten, die besonderen Geheimhaltungsbestimmungen unterliegen. Das betrifft unter anderem Gesundheits-, Sozial- und Finanzämter, die bei der Verarbeitung personenbezogener Daten die ärztliche Schweigepflicht, das Sozialgeheimnis bzw. das Steuergeheimnis zu beachten haben und durch diese speziellen gesetzlichen Geheimhaltungsvorschriften derzeit gehindert sind, ihre nicht mehr benötigten Dokumente aus dem Verwaltungsvollzug externen Archiven zu übergeben. Wenngleich die Weitergabe dieser personenbezogenen Daten für Archivzwecke in der Datenschutzdiskussion nicht unumstritten ist und mitunter gefordert wird, derartige Angaben dürften nur in anonymisierter Form an öffentliche Archive übermittelt werden, habe ich hier keine Bedenken gegen eine unbeschränkte Anbietungspflicht. Es genügt, wenn die gesetzlichen Nutzungsregelungen für Archive der besonderen Schutzwürdigkeit dieser Daten ausreichend Rechnung tragen, was etwa durch verlängerte Sperrfristen erreicht werden kann.

Die Regelungen zur Nutzung des Archivgutes, das zeichnet sich deutlich ab, werden wohl den Hauptstreitpunkt bilden. Sowohl der Gesetzentwurf der Fraktion der GRÜNEN als auch der Entwurf der SPD-Fraktion privilegieren den Zugang zu Dokumenten zur Geschichte des Nationalsozialismus. Der Entwurf der Fraktion der GRÜNEN nimmt diese Unterlagen ausdrücklich von den Sperrfristen aus und scheint auch darüber hinaus den Zugang zu diesen Materialien an keinerlei Voraussetzungen binden zu wollen. Der SPD-Entwurf schlägt vor, das Hessische Ministerium für Wissenschaft und Kunst, als oberste Archivbehörde des Landes, solle für wissenschaftliche Forschungsvorhaben abweichend von den sonst im Entwurf vorgesehenen Schutzfristen die Benutzung von staatlichem Archivgut zur Geschichte des Nationalsozialismus genehmigen, sofern durch geeignete Maßnahmen sichergestellt werde, daß die Benutzung nicht zu einer Beeinträchtigung schutzwürdiger Interessen der in dem Archivgut namentlich genannten Personen führe. In der ersten Lesung des Gesetzentwurfs der SPD-Fraktion am 12. Oktober 1988 haben sich die Koalitionsfraktionen insbesondere gegen diese Ausnahmeregelung gewandt und ein Sonderrecht für Archivalien zur Geschichte des Nationalsozialismus abgelehnt (Protokoll der 56. Plenarsitzung vom 12. Oktober 1988, S. 2938 u. 2941).

Bei den beiden Entwürfen wird es jedoch nicht bleiben. Die Landesregierung hat angekündigt, daß sie – dem Wunsch des Innenausschusses folgend – dem Landtag voraussichtlich Anfang des Jahres 1989 einen eigenen Entwurf für ein Landesarchivgesetz vorlegen werde (Protokoll der 6. Sitzung des Unterausschusses Informationsverarbeitung und Datenschutz vom 7. September 1988, S. 7). Der Innenausschuß hat daraufhin am 8. September 1988 in einem Beschluß dem federführenden Ausschuß für Wissenschaft und Kunst empfohlen, gemeinsam mit den beteiligten Ausschüssen eine Anhörung zum Gesetzentwurf der Fraktion der GRÜNEN und dem von der Landesregierng angekündigten Entwurf durchzuführen. (Der Entwurf der SPD-Fraktion lag für diesen Zeitpunkt noch nicht vor.) Weiter heißt es in dem Beschluß: „Der Innenausschuß geht davon aus, daß dieser Gesetzentwurf der Landesregierung dem Landtag zu Beginndes nächsten Jahres zugeleitet wird." (Protokoll der 14. Sitzung des Innenausschusses vom 8. September 1988, S. 5).

15.2
Benachrichtigung (§ 18 Abs. 2 HDSG) (16. Tätigkeitsbericht, Ziff. 2.3)

Mit Wirkung vom 31. Dezember 1988 ist die Benachrichtigungspflicht nach dem Hessischen Datenschutzgesetz (HDSG) neu geregelt worden (Gesetz vom 21. Dezember 1988 zur Änderung des HDSG, GVBl. I S. 424; s. auch den Gesetzentwurf der Fraktionen von CDU und F.D.P., Landtags-Drucks. 12/3324).

Zunächst zu dem, was sich nicht ändert:

Die Gesetzesänderung läßt die Grundnorm für die Benachrichtigung, § 18 Abs. 2 HDSG, unberührt. Nach dieser Vorschrift ist jeder Bürger dann, wenn seine Daten erstmals automatisiert gespeichert werden, schriftlich über Zweck, Art, Umfang und Rechtsgrundlage dieser Speicherung sowie die Sperrungs- und Löschungsfristen zu unterrichten. Unangetastet bleibt auch die Verpflichtung, spätere Änderungen dieser Angaben ebenfalls dem Betroffenen mitzuteilen. Nicht modifiziert wurde auch die aus Gründen der Verwaltungsvereinfachung vorgesehene Möglichkeit, die Benachrichtigung mit der Erhebung zu verbinden. Gemeint ist damit in erster Linie, daß bereits auf einem dem Bürger zur Ausfüllung vorgelegten Formular, dessen Daten für die automatisierte Verarbeitung vorgesehen sind, die Informationen über die beabsichtigte Speicherung aufgedruckt sind.

Geändert worden ist dagegen die Übergangsvorschrift des § 42 Abs. 1 HDSG. Sie lautet in der Neufassung wie folgt: „Waren personenbezogene Daten am 1. Januar 1987 in automatisierten Dateien gespeichert, erfolgt die Benachrichtigung nach § 18 Abs. 2 nur dann, wenn die speichernde Stelle bei der Erfüllung ihrer laufenden Aufgaben dem Betroffenen Bescheide oder sonstige Schriftstücke zusendet. Dies gilt auch für Dateien, die am 1. Januar 1987 nicht automatisiert waren, sofern sie bis zum 31. Dezember 1990 automatisiert werden."

Nach der bisherigen Fassung des § 42 Abs. 1 HDSG war den datenverarbeitenden Stellen für „Alt-Daten", die bei Inkrafttreten des HDSG am 1. Januar 1987 bereits automatisiert gespeichert waren, eine zweijährige Übergangsfrist für die Durchführung der Benachrichtigung eingeräumt worden. Diese Frist wäre am 31. Dezember 1988 abgelaufen. Da viele hessischen Behörden trotz dieser nach meiner Auffassung ausreichenden Übergangsfrist entweder aus Nachlässigkeit oder mit Hinweis auf die – angeblich oder wirklich – hohen Kosten für ihre Alt- Datenbestände keine Benachrichtigungen versandt hatten, sah sich der Gesetzgeber zum Eingreifen veranlaßt. Ich habe mich an der Formulierung der jetzigen Gesetzesfassung beteiligt, um die Substanz des Benachrichtigungsgebots, nämlich die Schaffung von Transparenz für den Bürger über Ort und Hintergrund der Verarbeitung seiner Daten, zu erhalten und weitergehende Vorschläge in Richtung auf eine völlige Abschaffung der Benachrichtigung gegenstandslos zu machen.

Der neue § 42 Abs. 1 HDSG wandelt für eine weitere zweijährige Übergangsfrist bis zum 31. Dezember 1990 für bestimmte Datenkategorien die regelmäßige Benachrichtigung in eine „Anlaßbenachrichtigung" um. Dabei erfolgt eine Benachrichtigung nicht in jedem Falle der erstmaligen automatisierten Speicherung, sondern nur dann, wenn die speichernde Stelle bei der Erfüllung ihrer laufenden Aufgaben dem Betroffenen ohnehin Bescheide oder sonstige Schriftstücke zusendet. Zu unterscheiden sind nach dem neuen Recht folgende vier Fallgruppen (vgl. dazu auch den Einführungserlaß des Hessischen Ministeriums des Innern vom 21. Dezember 1988, StAnz. 1/1989 S. 3):

1. Daten waren bereits am 1. Januar 1987 automatisiert gespeichert: Anlaßbenachrichtigung.

2. Daten waren am 1. Januar 1987 manuell in einer Datei gespeichert, die insgesamt bis zum 31. Dezember 1990 auf automatisierte Verarbeitung umgestellt wird: Anlaßbenachrichtigung. Beispiel hierfür ist die Automatisierung von bisher als Karteien geführten Personalausweisdateien. Bei dieser Fallgruppe ist zu beachten, daß die Anlaßbenachrichtigung nur für die zum Stichtag der Umstellung auf Automatisierung betroffenen Datensätze gilt. Anders ausgedrückt: Für spätere Einspeicherungen vor oder nach dem 31. Dezember 1990 gilt auch bei diesen Dateien die volle Benachrichtigungspflicht.

3. Daten waren am 1. Januar 1987 manuell registriert und werden als Einzeldatensatz nach dem 1. Januar 1987 in eine bereits bestehende automatisierte Datei eingespeichert: Regelbenachrichtigung. Sofern noch nicht erfolgt, muß die Benachrichtigung nachgeholt werden.

4. Daten waren am 1. Januar 1987 weder manuell noch automatisiert gespeichert, sondern werden erstmals nach diesem Zeitpunkt maschinell verarbeitet: Regelbenachrichtigung.

Nach diesen erheblichen Einschränkungen der Benachrichtigungspflicht werde ich in Zukunft intensiv darauf achten, daß für die in dem neuen § 42 Abs. 1 HDSG genannten Fallkategorien die Information des Bürgers in Fällen, in denen dem Betroffenen von der Behörde Schriftstücke zugesendet werden, auch tatsächlich realisiert wird. Dazu sind organisatorische Maßnahmen notwendig; beispielsweise müssen bei Sachbearbeitern, die mit personenbezogenen Daten aus solchen „Alt-Dateien" umgehen, ausreichend Benachrichtigungsformulare vorrätig sein, um sie im Schriftverkehr mit dem Bürger beifügen zu können. Auch werde ich verstärkt überprüfen, ob bei der Gestaltung von Erhebungsformularen der Benachrichtigungstext aufgenommen wird. Schließlich ist auf den Ablauf der Übergangsfrist in zwei Jahren insofern bereits jetzt hinzuweisen, als der Problemdruck, der der jetzigen Gesetzesänderung zugrunde liegt, vielfach dadurch entstanden ist, daß der vom Gesetzgeber gewährte Zeitraum nicht für die entsprechenden technischen und organisatorischen Vorkehrungen zur Vorbereitung einer Regelbenachrichtigung genutzt wurde.

15.3
Kontrollbefugnis beim Hessischen Rundfunk (§§ 3 Abs. 6, 24, 37 Abs. 2 HDSG)
(16. Tätigkeitsbericht, Ziff. 2.6)

Die Kontroverse mit dem Intendanten des Hessischen Rundfunks über die Vereinbarkeit meiner uneingeschränkten Kontrollbefugnis bei den nicht-redaktionellen Daten mit der grundgesetzlich gebotenen Staatsferne des Rundfunks konnte auch 1988 noch nicht beigelegt werden.

Ich habe mit Schreiben vom 1. September 1988 alle Mitglieder des Rundfunk- und des Verwaltungsrats über den Vorgang und meinen Standpunkt eingehend unterrichtet. In diesen Aufsichtsgremien ist auch über die unbefriedigende Situation diskutiert worden. Mit Schreiben vom 6. September 1988 hat der Intendant des Hessischen Rundfunks seine Auffassung bekräftigt, Überwachungskompetenz und Berichtspflicht seien beim Hessischen Rundfunk nicht gegenüber dem Landtag, sondern ausschließlich gegenüber den autonomen Kontrollgremien des Hessischen Rundfunks zu vollziehen. Eine solche Verfahrensweise kann jedoch nur bei einer entsprechenden Änderung des HDSG in Betracht kommen.

Ohne eine solche Novellierung wäre zwar eine gerichtliche Klärung des Umfangs meiner Zuständigkeiten denkbar. Diesen Weg hat ein Abgeordneter des Hessischen Landtags in einer Presseerklärung im Oktober vorgeschlagen. Eine

entsprechende Klage zu erheben wäre allerdings nicht meine Angelegenheit, sondern die des Hessischen Rundfunks. Ich selbst sehe keine Veranlassung, eine solche gerichtliche Klärung herbeizuführen, wobei dahinstehen kann, ob mir überhaupt eine Klagebefugnis zusteht.

Als Kompromiß bleibt allenfalls die Möglichkeit, neben dem Intendanten – was ohnehin immer vorgesehen war – auch den Anstaltsgremien vor einer evtl. Aufnahme von Passagen, die den Hessischen Rundfunk betreffen, in den Tätigkeitsbericht Gelegenheit zur Stellungnahme zu geben. Diesen Vorschlag habe ich anläßlich einer gemeinsamen Sitzung von Rundfunkrat und Verwaltungsrat am 16. Dezember 1988 unterbreitet und erläutert; eine Reaktion steht noch aus.

Die Landesregierung hat in ihrer Antwort auf die Kleine Anfrage der Abgeordneten Dr. Müller u. a. ihre Auffassung zu dieser Frage dargelegt (Drucks. 12/3705 vom 6. Dezember 1988). Sie teilt meine Ansicht, daß der Grundsatz der Staatsfreiheit des Rundfunks die im HDSG vorgesehene Datenschutzkontrolle nicht ausschließt.

15.4
Aids-Hinweise in polizeilichen Informationssystemen
(16. Tätigkeitsbericht, Ziff. 6.1.2)

Im 16. Tätigkeitsbericht habe ich die Speicherung personenbezogener Aids-Daten in den polizeilichen Informationssystemen INPOL und HEPOLIS kritisiert. Bei einer Prüfung hatte ich festgestellt, daß die Datensätze von ca. 700 Personen das Merkmal „Ansteckungsgefahr" enthielten. Die Erforderlichkeit dieser Speicherung war und ist bis heute nicht ausreichend begründet. Der allgemeine Hinweis der Polizei, sie benötige dieses Merkmal, um ihre Beamten bei Einsätzen besonders schützen zu können, genügt jedenfalls nicht.

Eine von der Innenministerkonferenz (IMK) am 3. Oktober 1986 beauftragte Arbeitsgruppe, die unter Beteiligung der Datenschutzbeauftragten Kriterien für die Speicherung erarbeiten sollte, hat nun – auch unter Berücksichtigung des Beschlusses der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 7. Dezember 1987 – zur Speicherung personenbezogener Aids- Daten in polizeilichen Informationssystemen (16. Tätigkeitsbericht, Ziff. 14.4) ein Ergebnis vorgelegt, das die Innenministerkonferenz in ihrer Sitzung Anfang Oktober 1988 zustimmend zur Kenntnis genommen hat.

Der Aids-Hinweis soll danach künftig nur noch in einige wenige Dateien der beiden Informationssysteme aufgenommen werden und zwar in den Kriminalaktennachweis (KAN) und die Dateien Personenfahndung, Erkennungsdienst und Rauschgift. Die Speicherung liegt im Ermessen der Bundes- und Landesbehörden. Durch DV-technische Vorkehrungen soll sichergestellt werden, daß die Stelle, die für die Eingabe des Hinweises verantwortlich ist, aus dem Datensatz direkt ersichtlich ist. Dies war bisher nicht der Fall. Für das Merkmal „Ansteckungsgefahr" ist eine Aufbewahrungsdauer von zwei Jahren vorgesehen. Es darf nur eingespeichert werden, wenn ärztliche oder amtliche Hinweise oder Angaben des Betroffenen selbst vorliegen,

„– daß der Betroffene unter einer nach § 3 Abs. 1 und 2 Bundesseuchengesetz meldepflichtigen Krankheit leidet oder

– daß der Betroffene gem. § 2 dieses Gesetzes krank, krankheitsverdächtig, ansteckungsverdächtig, Ausscheider oder ausscheidungsverdächtig ist und eine Ansteckung eine schwerwiegende Gesundheitsgefährdung bedeuten würde. Auf die Art der Krankheit ist hinzuweisen. Bei HIV-Infektionen erfolgt dies durch den Zusatz „Vorsicht Blutkontakte"".

Meine Kritik, daß wegen des Ungleichgewichts zwischen der Zahl der gespeicherten Datensätze mit dem Merkmal „Ansteckungsgefahr" und der Menge der tatsächlich infizierten Personen eine sinnvolle Auswertung gar nicht erfolgen kann, wird trotz dieser Verbesserungen jedoch nicht entkräftet. Im Gegenteil: Die jüngst von den Innenministern der Länder Niedersachsen, Nordrhein- Westfalen und Rheinland-Pfalz getroffenen Entscheidungen bestätigen meine Einschätzung: Den dortigen Polizeibehörden wurde die Erfassung des Aids-Hinweises für die Zukunft untersagt, bestehende Speicherungen wurden gelöscht. Bislang konnte sich das Hessische Innenministerium noch nicht dazu entschließen, diesem Beispiel zu folgen.

15.5
Unterrichtung der Gemeinde über Sozialhilfebescheide
(16. Tätigkeitsbericht, Ziff. 7.1)

Verschiedene Landkreise haben auch im vergangenen Jahr Sozialhilfebescheide an die Wohnsitzgemeinden weitergeleitet. Unter Hinweis auf die von mir im 16. Tätigkeitsbericht (Ziff. 7.1) dargelegte datenschutzrechtliche Unzulässigkeit dieser Praxis hat eine Gemeinde beim Kreisausschuß eine Einstellung dieses Verfahrens angeregt. Der Kreis lehnte jedoch ab. Auf meine Intervention hin hat das Hessische Sozialministerium nunmehr in einer Stellungnahme, die sich auch auf Äußerungen des Hessischen Städtetages und des Hessischen Landkreistages beruft, meine Ansicht bekräftigt. Das Sozialministerium stellt ebenfalls ausdrücklich klar, daß es keine funktionelle Einheit zwischen der Gemeinde, die den Antrag entgegennimmt, und dem Landkreis, der den Antrag bearbeitet, gibt.

Die in der Vergangenheit unzulässigerweise an die Gemeinden übermittelten Bescheide, die ohne Rechtsgrundlage offenbart worden sind, müssen nunmehr vernichtet werden.

15.6
Aufbewahrungsfristen für Kriminalakten der hessischen Polizei (16. Tätigkeitsbericht, Ziff. 9.1)

Die Praxis bei der Vergabe von Speicherungsfristen im Hessischen Polizeiinformationssystem (HEPOLIS) und bei der Festlegung der Aufbewahrungsfristen für Kriminalakten hatte ich 1987 in fünf hessischen Polizeidienststellen überprüft. Dabei hatte sich gezeigt, daß die einzelnen Dienststellen die in den „Richtlinien für die Führung kriminalpolizeilicher personenbezogener Sammlungen" (KpS-Richtlinien) enthaltenen Hinweise für die Speicherungsdauer höchst verschieden umsetzen.

Das Hessische Ministerium des Innern nahm im Mai 1988 zu meinem Prüfbericht Stellung. Wesentliche Teile seiner Antwort sind in der Stellungnahme der Landesregierung zu meinem 16. Tätigkeitsbericht (Landtags-Drucks. 12/3068) enthalten.

Das Ministerium hatte zwar für die einzelnen Dienststellen unterschiedliche Quoten bei der Vergabe von zehnjährigen Aussonderungsprüffristen erwartet, war aber überrascht von der Größe der Unterschiede und sah sich „zu unverzüglichen Maßnahmen" veranlaßt. Das Prüfergebnis wurde intensiv auf einer polizeiinternen Fachtagung erörtert. Dort wurde u. a. festgehalten:

„Für die Bemessung der Anzahl der Personen, für die auf drei Jahre verkürzte Aktenlaufzeiten zu bestimmen sind, ist zu berücksichtigen, daß einerseits unter besonderen Umständen auch „Bagatelltäter" eine zehnjährige Aktenlaufzeit erfahren können, daß aber umgekehrt noch eine Vielzahl weiterer Tatverdächtiger wegen Fällen geringer Bedeutung eine verkürzte Aktenlaufzeit von drei Jahren erfährt."

„Die Entscheidung, wann ein „Fall von geringer Bedeutung" vorliegt, hängt von verschiedenen Faktoren ab und kann nicht anhand eines abschließend regelnden Straftatenkataloges getroffen werden. Es sind u. a. folgende Faktoren zu berücksichtigen:

- Art der Straftat (z. B. Beleidigung, üble Nachrede, Verleumdung, Hausfriedensbruch, fahrlässige Körperverletzung, vorsätzliche Körperverletzung mit geringen Folgen, Sachbeschädigung, Erschleichung von Leistungen)
- Umstände und Folgen der Tat (z. B. geringer Unrechtsgehalt, nachhaltige Rufschädigung bei Verleumdung, Höhe des Schadens bei Sachbeschädigung und Betrug)
- Prognose des Täters (z. B. kriminelle Energie, politisches Motiv beim Hausfriedensbruch)
- Opfer (z. B. ältere Personen, Arglosigkeit ausgenutzt u. a.)"

Bei einer konsequenten Anwendung dieser Grundsätze müßte – so das Ministerium – die Struktur aller Datenspeicherungen in HEPOLIS wie folgt aussehen:

45%	aller ermittelten Tatverdächtigen sind wegen der ihnen vorgeworfenen Delikte (leichte Körperverletzung, Ladendiebstahl, Leistungserschleichung, Beleidigung, Sachbeschädigung, Verstoß gegen Ausländer- bzw. Asylverfahrensgesetz) in aller Regel als „Fälle von geringer Bedeutung" einzustufen.
15 bis 30%	sind weitere „Fälle von geringer Bedeutung" aufgrund anderer Kriterien (siehe oben), insbesondere in den Bereichen einfacher Diebstahl, Unterschlagung und Betrug.
15%	sind Fälle, bei denen aufgrund ihrer Schwere (z. B. Mord, Sexualdelikte, Erpressung) in aller Regel eine Aufbewahrungsdauer von zehn Jahren festzusetzen ist.
Ca. 10%	sind weitere Fälle, die wegen der Art und Weise ihrer Begehung ebenfalls zehn Jahre lang aufzubewahren sind.

Damit wäre einerseits für mindestens 60% aller Datensätze von einer verkürzten Speicherungsdauer von drei Jahren auszugehen, andererseits fielen etwa 25% der Datensätze von vornherein unter die Zehnjahresprüffrist. Der Rest von etwa 15% müßte individuell zugeordnet werden. Der von mir geforderten Einführung einer zusätzlichen Frist von fünf Jahren für den „mittleren Bereich" hat das Innenministerium zwar widersprochen. Werden allerdings 60 bis 75% der Fälle mit einer Dreijahresfrist gespeichert, wie es das Ministerium anstrebt, würde im wesentlichen das gleiche Ziel erreicht. Mit anderen Worten: Werden die KpS-Richtlinien so interpretiert und führt dies zu der damit verbundenen geänderten Struktur von HEPOLIS-Datenspeicherungen, kann ich meine Forderung nach einer Änderung der Richtlinien zurückstellen.

Dazu müssen allerdings erst noch die Voraussetzungen geschaffen werden. Das Ministerium stellt nämlich selbst zutreffend fest: „Noch nicht bei allen Dienststellen ist die für eine sachgerechte Beurteilung der Vorgänge als Fälle geringer Bedeutung notwendige Flexibilität vorhanden ... Es wird daher notwendig sein, die Sachbearbeiter noch intensiver mit allen Kriterien vertraut zu machen, die für eine Beurteilung als Fall geringer Bedeutung ausschlaggebend sein können."

Das Hessische Landeskriminalamt wird künftig jährlich die Kriminalaktenbestände der Dienststellen nach Aussonderungsprüfjahren gegliedert auswerten und bei erheblichen Abweichungen mit den jeweiligen Dienststellen nach den Ursachen forschen.

15.7
Prüfung des polizeilichen Informationssystems APIS
(16. Tätigkeitsbericht, Ziff. 9.2)

Aufgrund der Prüfung der Speicherungspraxis in der dem „polizeilichen Staatsschutz" dienenden „Arbeitsdatei PIOS-Innere Sicherheit" im Jahr 1987 mußte ich eine Reihe von Rechtsverstößen beanstanden. Obwohl das Informationssystem für Staatsschutzdelikte von größerer Bedeutung konzipiert worden ist, waren in der Datei vornehmlich Bagatellstraftaten registriert, bei denen lediglich die „politische Motivation" der Täter Ursache der Speicherung war.

Das galt auch für die unter dem Stichwort „Volkszählung" gespeicherten Datensätze. Wer an einem Informationsstand Flugblätter verteilt hatte, in denen zum Beschädigen der Volkszählungserhebungsbögen aufgefordert wurde, geriet in den Verdacht, „politisch motiviert" eine Straftat (Aufruf zur Sachbeschädigung) begangen zu haben. Nach Ziff. 2.1.10 der Errichtungsanordnung zu APIS werden derartige Taten als „Staatsschutzdelikte" angesehen.

Meine Beanstandung veranlaßte das Hessische Innenministerium zu einer Überprüfung aller im Zusammenhang mit der Volkszählung gespeicherten Fälle. Die Fraktion der GRÜNEN beantragte, Daten hessischer Gegner und Verweigerer der Volkszählung 1987, denen keine Staatsschutzstrafsachen im Sinne des Grundgesetzes Art. 74 a, § 120 des Gerichtsverfassungsgesetzes oder lediglich Vergehen im Zusammenhang mit der Durchführung der Volkszählung 1987 zur Last gelegt worden waren, aus der Datei APIS zu löschen (Drucks. 12/1486).

Im Laufe des Jahres 1988 haben sich der Landtagsunterausschuß Informationsverarbeitung und Datenschutz und der Innenausschuß des Landtages mehrmals mit der Speicherung von Daten über Volkszählungsgegner im Informationssystem APIS befaßt.

Zu Beginn des Jahres 1988 waren in der Datei APIS im Zusammenhang mit der Volkszählung 1987 33 Fälle mit insgesamt 49 Personendatensätzen gespeichert. Wegen der Bedeutung oder der Art und Weise der Ausführung verschiedener Taten hatte ich in 10 Fällen keine datenschutzrechtlichen Bedenken. Von den verbleibenden 23 Fällen, die ich für bedenklich halte, wurden 16 im Laufe des Jahres 1988 gelöscht; in 7 Fällen ist die Berechtigung zur Speicherung nach wie vor zwischen dem Innenministerium und mir umstritten.

Zwei Grundprobleme der Datei APIS bestehen weiterhin. Zwar qualifizierte auch das Hessische Ministerium des Innern einen großen Teil der gespeicherten Straftaten als „Bagatelldelikte", doch zieht es daraus nicht den Schluß, auf die Erfassung dieser Sachverhalte künftig zu verzichten. Nahezu sämtliche Löschungen wurden mit dem Hinweis vorgenommen, die Speicherung dieser Daten sei seinerzeit gerechtfertigt gewesen, zum Löschungszeitpunkt aber nicht mehr erforderlich. Dem Verhältnismäßigkeitsgrundsatz sei dadurch Rechnung getragen, daß die vorgesehene Dauer der Speicherung auf nur zwei Jahre festgelegt wurde. Zum anderen sollten Delikte, die im Strafgesetzbuch als Staatsschutzdelikte bezeichnet werden, nicht in jedem Fall in APIS gespeichert werden. In zwei der sieben umstrittenen Fälle räumt das Innenministerium selbst ein, daß die Straftaten nicht geeignet sind, die freiheitliche demokratische Grundordnung, den Bestand oder die Sicherheit des Bundes oder eines Landes ernsthaft zu beeinträchtigen. In diesen Fällen sieht das Ministerium die Voraussetzungen der Errichtungsanordnung dennoch als erfüllt an, da die Straftaten gegen die erwähnten Gemeinschaftsgüter gerichtet gewesen seien. Dem ist entgegenzuhalten, daß angesichts der Folgen, die für den Betroffenen aus einer Speicherung seiner Daten in APIS entstehen können, eine tatsächliche Gefährdung der Rechtsgüter gegeben sein muß.

Dem Antrag der Fraktion der GRÜNEN wollte sich der Innenausschuß des Landtages nicht anschließen. Er hat vielmehr am 8. September 1988 dem Plenum empfohlen, den Antrag aufgrund der Stellungnahme und der Maßnahmen der Landesregierung für erledigt zu erklären (Protokoll der 14. Sitzung des Innenausschusses vom 8. September 1988).

15.8
Änderung des Straßenverkehrsgesetzes
Einführung des „Zentralen Verkehrsinformationssystems" (ZEVIS)
(16. Tätigkeitsbericht, Ziff. 13.1)

Im letzten Tätigkeitsbericht habe ich das Sicherungssystem, mit dem verhindert werden soll, daß die Polizeibehörden aus dem Zentralen Verkehrsinformationssystem (ZEVIS) des Kraftfahrtbundesamtes rechtswidrig Daten abrufen, als Farce bezeichnet. Das System sieht vor, daß bei jeder fünfzigsten Anfrage Informationen über den Grund der Anfrage eingegeben werden müssen, bevor das System Auskunft erteilt. Nach meiner damaligen Einschätzung war diese Sicherung leicht zu umgehen, indem nämlich die Anfrage abgebrochen wird und kurz darauf erneut eine Abfrage erfolgt, die dann zu den 98 v.H. der nicht überprüfbaren Abfragen gehören würde.

Die Präsidentin des Kraftfahrtbundesamtes hat dem widersprochen und erklärt, durch technische Vorkehrungen sei sichergestellt, daß eine Datenabfrage, bei der zur Protokollierung aufgefordert wurde, nicht abgebrochen werden

könne. Die Datenstation bleibe solange für jede weitere Transaktion gesperrt, bis der Bediener die Protokolldaten angegeben habe.

Die Prüfung, die ich daraufhin beim Landeskriminalamt vorgenommen habe, hat dies für Hessen bestätigt. Allerdings haben Kontrollen des Bayerischen Datenschutzbeauftragten ergeben, daß meine Kritik zumindest für dieses Bundesland berechtigt ist. Die bayerische Polizei vermag nach ihrem Zugriffssystem durch kurzes Abschalten der Verbindung die Aufforderung zur Eingabe von Zusatzdaten zu umgehen.

15.9
Basisdokumentation Psychiatrie (BADO) des Landeswohlfahrtsverbandes Hessen
(14. Tätigkeitsbericht, Ziff. 3.3, 15. Tätigkeitsbericht, Ziff. 11.1.2)

Nach mehrjähriger Diskussion konnte 1988 mit dem LWV endlich eine Einigung über Art und Weise der Durchführung der psychiatrischen Basisdokumentation erzielt werden.

Mit Hilfe der psychiatrischen Basisdokumentation sollen Informationen über die Nutzung psychiatrischer Krankenhäuser gewonnen werden. Die Daten sollen u. a. darüber Auskunft geben, welche Patienten in stationäre psychiatrische Behandlung gelangen, wie dies erfolgt und wohin sie entlassen werden. Vorgesehen ist, daß die BADO-Daten in den psychiatrischen Kliniken erhoben und mit Hilfe von Personal Computern gespeichert und verarbeitet werden. Die Kliniken erstellen dann jeweils statistische Auswertungen für die Hauptverwaltung des Landeswohlfahrtsverbandes. Die Hauptverwaltung führt die Auswertungen der Kliniken zusammen und wertet sie kliniküübergreifend aus.

Der LWV hat die zunächst vorgesehene Verfahrensweise in zahlreichen Punkten entsprechend meinen Empfehlungen abgeändert. Im Zusammenhang mit der Beschaffung eines neuen Rechners soll auch die Datensicherheit im Rechenzentrum der Hauptverwaltung weiter verbessert werden. Sofern dies so geschieht, daß alle meine hierzu aus Anlaß des Prüfbesuchs, den ich dort 1985 durchgeführt habe, formulierten Kritikpunkte beseitigt werden, sind meine Bedenken gegen die Durchführung der Basisdokumentation ausgeräumt. Dies habe ich dem LWV, dem Hessischen Landtag und dem Hessischen Sozialministerium mitgeteilt.

1.
Verarbeitung in den Kliniken

Was die Verarbeitung der BADO-Daten in den Kliniken anbelangt, so kam es mir insbesondere darauf an, daß die Daten im ärztlichen Bereich der Kliniken verbleiben und die erforderlichen technischen und organisatorischen Maßnahmen zur Sicherung dieser sensiblen Daten getroffen werden, ferner auch darauf, daß die Kliniken als datenverarbeitende Stellen im Sinne des Hessischen Datenschutzgesetzes über eine ausreichende Kontrollmöglichkeit bei der Verarbeitung und Übermittlung ihrer Daten an den Landeswohlfahrtsverband verfügen. Sofern in den Kliniken Programme eingesetzt werden sollen, die nicht von ihnen selbst, sondern z. B. in der Hauptverwaltung erstellt wurden, muß den Kliniken eine vollständige Kontrolle der eingesetzten Programme und der erzeugten Ausgabedaten möglich sein und sie müssen diese Kontrolle auch tatsächlich ausüben. Dies ist nunmehr gewährleistet.

2.
Übermittlung an die Hauptverwaltung des LWV

Ein Schwerpunkt der Diskussion war die Übermittlung der BADO- Daten an die Hauptverwaltung des Landeswohlfahrtsverbandes. Dabei bestand von Anfang an Konsens darüber, daß die BADO-Daten der ärztlichen Schweigepflicht im Sinne von § 203 Strafgesetzbuch unterfallen. Das Verfahren mußte daher so ausgestaltet werden, daß „eine Identifizierung des einzelnen Patienten im Zusammenhang mit der Speicherung und Auswertung auszuschließen" ist (vgl. die Antwort des Hessischen Ministers für Arbeit, Umwelt und Soziales vom 27. 08. 1984 auf die kleine Anfrage betr. die Einführung der medizinischen Basisdokumentation – (Drucks. 11/1789). Wenngleich über die rechtliche Ausgangslage Übereinstimmung bestand, bereitete doch die konkrete Ausgestaltung des Verfahrens erhebliche Schwierigkeiten. Das ursprünglich vorgesehene Verfahren der Anonymisierung habe ich bereits in meinem 14. Tätigkeitsbericht als unzulänglich bezeichnet. Auch eine Reihe weiterer vom Landeswohlfahrtsverband vorgeschlagener Anonymisierungsverfahren habe ich als nicht ausreichend angesehen zur Sicherstellung der ärztlichen Schweigepflicht. Da der Landeswohlfahrtsverband beabsichtigt, die BADO-Daten für vielfältige – über den ursprünglich mit der Basisdokumentation Psychiatrie hinausgehende –, und nicht von vornherein eingrenzbare Zwecke zu nutzen, z. B. auch für Wirtschaftlichkeitsprüfungen, müssen an die Anonymisierung der BADO-Daten sehr strenge Anforderungen gestellt werden. Andererseits hat der Landeswohlfahrtsverband immer wieder nachdrücklich sein Interesse dargelegt, aussagekräftige statistische Daten von den Kliniken zu erhalten.

Zentrales Problem war die Frage, ob die BADO-Auswertungen, die von den Kliniken an die Hauptverwaltung weitergegeben werden, kleine Feldbesetzungen enthalten dürfen, die grundsätzlich die Möglichkeit einer Identifizierung der Patienten eröffnen. Das nunmehr vorgesehene Verfahren berücksichtigt einerseits das Interesse des Landeswohlfahrtsverbandes an aussagekräftigen Daten und wahrt andererseits die ärztliche Schweigepflicht. Die Hauptverwaltung erhält in kryptografierter Form von jeder Klinik die Standardtabellensätze einschließlich der exakten niedrigen Feldbesetzungen, damit sie die Tabellensätze aller Kliniken präzise addieren kann. Die kompletten Tabellensätze mit den niedrigen Feldbesetzungen werden aber in der Hauptverwaltung nur für die Addition verwendet. Vor jeder Ausgabe der Daten in der Hauptverwaltung kommt eine Feldunterdrückungsprozedur zur Anwendung, so

daß zur weiteren Nutzung der BADO-Daten nur Tabellen ohne kleine Feldbesetzungen zur Verfügung stehen. In jedem Fall ist auch eine Weitergabe von BADO-Auswertungen an Dritte mit kleinen Feldbesetzungen ausgeschlossen.

3.
Festlegungen der Verfahrensweise

Die vorgesehene Verfahrensweise wird in den wesentlichen Punkten in der „Arbeitsanweisung für die Mitarbeiter in den Krankenhäusern des Landeswohlfahrtsverbandes Hessen, die mit der Bearbeitung der medizinischen (psychiatrischen) Basisdokumentation (BADO) beauftragt sind", der „Arbeitsanweisung für die Mitarbeiter/innen in der Hauptverwaltung des Landeswohlfahrtsverbandes Hessen, die mit der maschinellen Datenverarbeitung und der Bedienung von Personal Computern beauftragt sind", der „Dienstanweisung Datenschutzbeauftragter LWV" und der „Geschäftsanweisung zur Sicherstellung des Datenschutzes in den Krankenhäusern und Kliniken des Landeswohlfahrtsverbandes Hessen" entsprechend festgelegt.

4.
Rückgabe der bereits an die Hauptverwaltung weitergegebenen Daten

Nachdem ich den LWV mehrfach nachdrücklich darauf hingewiesen hatte, daß die in den vergangenen Jahren bereits von den Kliniken an die Hauptverwaltung übermittelten unzulänglich anonymisierten BADO-Daten dort nicht länger aufbewahrt werden dürfen, hat mir der LWV im Juni dieses Jahres mitgeteilt, daß alle Daten an die Kliniken zurückgegeben wurden.

Wiesbaden, den 3. Februar 1989

gez. Professor Dr. Simitis

16. Materialien

16.1
Beschluß der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 14. März 1988 zur polizeilichen Datenverarbeitung bis zum Erlaß bereichsspezifischer gesetzlicher Regelungen

Eines der dringendsten datenschutzrechtlichen Anliegen ist die Schaffung bereichsspezifischer Grundlagen für die Datenverarbeitung der Sicherheitsbehörden. Dies gilt ebenso für die Nachrichtendienste. Schon seit Jahren haben die Datenschutzbeauftragten entsprechende Forderungen erhoben. Spätestens seit dem „Volkszählungsurteil" des Bundesverfassungsgerichts vom 15. Dezember 1983 ist das gesetzliche Regelungsdefizit offenbar. So hat der Bayerische Verfassungsgerichtshof in einer Entscheidung vom 9. Juli 1985 bezogen auf die polizeiliche Datenverarbeitung hervorgehoben, es sei geboten, daß der Gesetzgeber die Materie regele, die bisher Gegenstand der „Richtlinien für die Führung kriminalpolizeilicher personenbezogener Sammlungen (KpS)" ist.

Mit der Erhebung, Speicherung und Weitergabe personenbezogener Daten greift die Polizei in die Grundrechte der Betroffenen ein, ohne daß dafür immer die verfassungsrechtlich gebotenen gesetzlichen Grundlagen vorhanden sind. So haben schon einige Gerichte die polizeiliche Datenverarbeitung zum Zwecke vorbeugender Straftatenbekämpfung bis zum Erlaß bereichsspezifischer gesetzlicher Grundlagen für unzulässig erklärt. Gleichwohl kommen die gesetzgeberischen Initiativen zur Behebung dieses Zustandes nur äußerst schleppend voran.

Allerdings hat das Bundesverfassungsgericht dem Gesetzgeber in der Vergangenheit Übergangsfristen zur Beseitigung von Regelungsdefiziten zugebilligt, wenn damit eine sonst eintretende Funktionsunfähigkeit staatlicher Einrichtungen vermieden werden kann, die der verfassungsmäßigen Ordnung noch ferner stünde als der bisherige Zustand.

Dabei ist auf folgendes hinzuweisen:

I.
Übergangsfristen können ihrer Natur nach nicht unbegrenzt in Anspruch genommen werden. Das Bundesverfassungsgericht hat ausdrücklich darauf hingewiesen, daß sie dann nicht mehr anerkannt werden können, wenn der Gesetzgeber eine Neuregelung ungebührlich verzögert.

II.
Während der Übergangsfrist reduziert sich die Befugnis zu Eingriffen auf das, was für die geordnete Weiterführung eines „funktionsfähigen Betriebes" unerläßlich ist. Es ist mithin unzulässig und mit den vom Bundesverfassungsgericht festgestellten reduzierten Befugnissen unvereinbar, bereits bestehende Datenverarbeitungsabläufe noch auszuweiten, etwa durch den Aufbau neuer Datenbanken oder die Ausschöpfung neuer technischer Möglichkeiten, soweit die Eingriffe in die Rechte der Betroffenen damit eine neue Qualität erreichen.

III.
Besondere Zurückhaltung hat sich die Polizei dort aufzuerlegen, wo Eingriffe in das informationelle Selbstbestimmungsrecht noch weitere Grundrechte betreffen:

- Die Feststellungen von Personalien, damit verbundene Datenabgleiche und Speicherungen sowie Film- und Videoaufnahmen sind anläßlich von öffentlichen Versammlungen während der Übergangszeit nur dann als zulässig anzusehen, wenn Anhaltspunkte dafür vorliegen, daß strafbare Handlungen begangen werden.

- Die Nutzung technischer Hilfsmittel zur verdeckten Datenerhebung durch Lauschangriffe in Wohnungen muß grundsätzlich ausgeschlossen sein.

IV.
Der Einsatz von verdeckten Ermittlern und V-Leuten sowie langfristige Observationen und polizeiliche Beobachtung dürfen nur zugelassen werden, wenn konkrete Anhaltspunkte für bestimmte schwere Straftaten bestehen. Es muß festgelegt werden, wer diese Maßnahmen anordnen darf, wie die anfallenden Erkenntnisse verwertet werden dürfen und wann die Betroffenen zu unterrichten sind.

V.
Im Hinblick auf die von den Verfassungsgerichten für die Übergangszeit geforderte Beschränkung auf das, was für die geordnete Weiterführung eines „funktionsfähigen Betriebs" unerläßlich ist, erinnern die Datenschutzbeauftragten an ihre früheren Beschlüsse zur polizeilichen Datenverarbeitung. Danach sind künftig insbesondere folgende Datenverarbeitungsvorgänge zu unterlassen:

- Speicherung diskriminierender personenbezogener Hinweise in polizeilichen Informationssystemen;

- Speicherung (ehemals) verdächtiger Personen zu Zwecken vorbeugender Straftatenbekämpfung ohne verantwortbare kriminologische Prognose;

- Speicherung von Daten über Personen, bei denen eine Anklageerhebung mangels öffentlichen Interesses abgelehnt wurde;

- Speicherung von Daten über Kinder, die der Begehung einer Straftat verdächtigt werden;

- Weitergabe von Informationen, die mit speziellen polizeilichen Befugnissen erhoben wurden, an andere als Polizeidienststellen.

16.2
Beschluß der Konferenz der Datenschutzbeauftragten des Bundes und der Länder zur Änderung und Ergänzung des Personenstandsgesetzes vom 15. März 1988

I.
Die Datenschutzbeauftragten des Bundes und der Länder begrüßen vor dem Hintergrund der bereits in ihrem Konferenzbeschluß vom 6./7. Juni 1983 gegebenen Empfehlung zur Verbesserung des Datenschutzes im Bereich personenstandsrechtlicher Regelung die unter Federführung des Bundesministers des Innern zwischen Bund und Ländern angelaufenen Beratungen und Vorarbeiten für ein Fünftes Gesetz zur Änderung und Ergänzung des Personenstandsgesetzes. Positiv bewerten sie insbesondere die Absicht,

a) die Mitteilungspflichten des Standesbeamten gesetzlich zu verankern,

b) die Einsicht in die Personenstandsbücher und die Erteilung von Auskünften und Urkunden präziser zu regeln, insbesondere eigenständige Vorschriften über die Auskunft bzw. Einsicht für Zwecke wissenschaftlicher Forschung zu schaffen,

c) das öffentliche Aufgebot wegfallen zu lassen (Streichung des geltenden § 3 PStG, Änderung des Ehegesetzes)

II.
Mangels einer Rechtsgrundlage für die standesamtliche Herausgabe personenbezogener Daten zur Veröffentlichung von Personenstandsfällen darf der Standesbeamte eine Mitteilung zu diesem Zwecke grundsätzlich nur dann machen, wenn der Betroffene eingewilligt hat. Im Interesse der Normenklarheit und Verhältnismäßigkeit empfehlen die Datenschutzbeauftragten jedoch, gesetzlich festzulegen,

- in welchen Fällen,
- in welchem Umfang,
- unter welchen Voraussetzungen

der Standesbeamte auf der Grundlage der Einwilligung der Betroffenen eine Mitteilung zur Veröffentlichung von Personenstandsfällen machen darf.

III.
Insbesondere empfehlen die Datenschutzbeauftragten:

1.
Auf die Eintragung des Berufs in Personenstandsbüchern sollte verzichtet werden. Auch in den geltenden §§ 12, 15 b, 21, 30, 37 und 46 a sollte diese Angabe fallengelassen werden.

Die Angabe des Berufes ist für die Beurkundung nicht erforderlich. Für Identifizierungszwecke stehen genügend andere Merkmale zur Verfügung. Die Angabe ist wegen ihrer begrifflichen Ungenauigkeit für die Identifizierung auch nicht geeignet. Es bleibt weitgehend dem Betroffenen überlassen, ob er seinen erlernten oder ausgeübten Beruf angibt und welche Bezeichnung er dafür wählt (z. B. Beamter, Jurist, Verwaltungsjurist, Regierungsrat, Referent), während die übrigen Eintragungen in die Personenstandsbücher präzise geregelt sind. Die bessere Aussagefähigkeit der Bücher für die spätere historische Forschung reicht als Begründung für die Erhebung des Berufs nach Auffassung der Datenschutzbeauftragten nicht aus.

2.
Die Berechtigung von Behörden und bestimmten öffentlichen Stellen, Auskunft aus einem und Einsicht in einen Personenstandseintrag sowie Erteilung von Personenstandsurkunden zu verlangen, sollte in einer gesonderten Vorschrift bereichsspezifisch geregelt werden. Eine „Durchsicht dieser Bücher" wie bislang § 61 PStG vorsieht, sollte künftig weder Behörden und bestimmten öffentlichen Stellen noch anderen Personen erlaubt sein. Es sollte sichergestellt werden, daß die Gewährung von Auskunft und Einsicht nicht routinemäßig, sondern nur auf Ersuchen im Einzelfall erfolgen darf. Ein Direktzugriff auf Personenstandseintragungen ist dementsprechend auszuschließen.

3.
Die Gewährung von Informationen an Behörden und bestimmte sonstige Stellen sollte an die gleichzeitige Benachrichtigung des Betroffenen gebunden werden. Damit wird der Forderung des Bundesverfassungsgerichts in seinem Volkszählungsurteil Rechnung getragen, daß der Bürger wissen muß, wer was wann über ihn weiß.

4.
Die Gewährung von Informationen zum Zwecke wissenschaftlicher Forschung sollte durch gesetzliche Vorschriften bereichsspezifisch geregelt werden. Dabei sollte das Prinzip der Gewährung von Auskunft und Einsicht nur mit Einwilligung der Betroffenen als Regelfall an den Anfang gestellt werden. Daran anschließend sollte als Ausnahme vorgesehen werden, daß es der Einwilligung dann nicht bedarf, wenn das öffentliche Interesse an der Durchführung des Forschungsvorhabens das Geheimhaltungsinteresse des Betroffenen erheblich überwiegt, die Einholung der Einwilligung nicht möglich ist und der Zweck des Forschungsvorhabens auf andere Weise nicht erreicht werden kann.

Im Falle der Einwilligung wie auch im Ausnahmefall bedarf es einer gesetzlichen Bindung der gewährten Informationen an den Zweck eines im Auskunftsersuchen zu bestimmenden Forschungsvorhabens. Die Konkretisierung ist unerläßlich, weil nur bei möglichst konkreter Bestimmung des Forschungsprojekts eine rechtsverbindliche Einwilligung zustandekommen kann und weil die erforderliche Güterabwägung im Falle der subsidiär zulässigen Datenweitergabe auf gesetzlicher Grundlage ebenfalls eine genauere Kenntnis erfordert.

Das Verhältnis der Vorschriften zugunsten wissenschaftlicher Forschung zu Vorschriften, die der Ahnenforschung bzw. zeitgeschichtlichen Forschung entgegenkommen sollen, bedarf – besonders mit Blick auf die erheblichen Abgrenzungsprobleme in der Praxis – näherer Präzisierung.

5.
Für Orts- bzw. Zeitangaben in Urkunden, namentlich in Sterbeurkunden, sollte eine Regelung vorgesehen werden, durch die Peinlichkeiten für die Betroffenen vermieden werden. Insbesondere sollten Sterbeurkunden so gefaßt werden, daß sie Dritten keinen Anlaß zu Spekulationen über die näheren Umstände des Todes geben. Angaben des Sterbeortes sollten sich auf die Bezeichnung der Gemeinde beschränken. Ist der Sterbeort nicht bekannt, so sollte die Bezeichnung der Gemeinde angegeben werden, in der der Verstorbene tot aufgefunden wurde, ohne daß erkennbar gemacht wird, daß besondere Umstände vorliegen. Als Zeitpunkt des Todes sollte der Sterbetag eingetragen werden, ohne daß erkennbar wird, ob innerhalb dieses Tages der genaue Zeitpunkt, der ungefähre Zeitpunkt oder lediglich ein Zeitraum festzustellen war. Für den Fall, daß im Sterbebuch ein über mehrere Tage reichender Zeitraum anzugeben ist, sollte bestimmt werden, daß in der Sterbeurkunde ein Todestag (der ungefähre Zeitpunkt im Rahmen dieses Zeitraumes) eingesetzt wird.

Soweit es im Einzelfalle zur Klärung von Rechtsverhältnissen – z. B. im Erbrecht – ausnahmsweise auf eine möglichst genaue Zeitangabe ankommt, ist dieser Bedarf durch die zugunsten von Behörden bzw. Gerichten vorgesehene Auskunft aus bzw. Einsicht in den Personenstandseintrag, d. h. in das Sterbebuch, hinreichend gedeckt.

6.
Neben den Vorschriften über Informationsgewährung auf Ersuchen bedarf es präziser Rechtsgrundlagen für die Mitteilungspflichten des Standesbeamten, denen ein Ersuchen nicht vorausgeht. Die als Mitteilungsempfänger vorgesehenen Behörden und Stellen sollten im Gesetz abschließend genannt, der Umfang der Mitteilungsinhalte beschrieben und klargestellt werden, daß die Mitteilung der Angaben nur zu einem bestimmten Verwendungszweck erfolgt, der in der Zuständigkeit der Empfängerbehörde bzw. -stelle liegt und gesetzlich bestimmt ist.

Außerdem sollte festgelegt werden, daß es für den etwaigen Einsatz automatischer Datenverarbeitung zur Erfüllung der Mitteilungspflichten verordnungsmäßiger Regelungen bedarf.

7.
Es sollte sichergestellt werden, daß bei einer Inkognito-Adoption Minderjähriger eine Unterrichtung der Meldebehörde der leiblichen Eltern des adoptierten Kindes über das Erlöschen des Verwandtschaftsverhältnisses bzw. die Änderung des Namens des adoptierten Kindes nicht erfolgt. Es sollte jedenfalls vom Standesbeamten kein Informationsweg zur Meldebehörde des Annehmenden und zur Meldebehörde der bisherigen Verwandten führen. Die Datenschutzbeauftragten nehmen hierzu auf eine frühere Erklärung des Bundesministers des Innern Bezug, daß eine Mitteilungspflicht des Standesbeamten an die für den Wohnort der leiblichen Eltern zuständige Meldebehörde mit dem Offenbarungsverbot des § 1758 BGB nicht vereinbar wäre, und halten an dem gleichlautenden Beschluß der Datenschutzbeauftragten vom 6./7. Juni 1983 fest.

An welche Meldebehörde die Mitteilung über die Geburt zu richten ist, bedarf auch in den Fällen näherer Konkretisierung, in denen sich schon kurz nach der Geburt Anhaltspunkte dafür ergeben, daß das Kind für eine Adoptionsvermittlung in Betracht kommt, es also nicht in die Hauptwohnung der leiblichen Eltern bzw. Mutter aufgenommen, sondern in Adoptionspflege gegeben wird. Mit Rücksicht auf die Bestimmung des § 1747 Abs. 3 Satz 1 BGB, wonach die Einwilligung der Eltern bzw. der Mutter eines nichtehelichen Kindes in eine Adoption erst erteilt werden kann, wenn das Kind acht Wochen alt ist, sollte im Falle des Vorliegens derartiger Anhaltspunkte zunächst von einer Mitteilung an die für die Hauptwohnung der Eltern bzw. der Mutter eines nichtehelichen Kindes zuständige Meldebehörde abgesehen werden. Die Meldung an die zuständige Meldebehörde sollte dann erfolgen, wenn feststeht, ob und ggf. zu wem das Kind in Adoptionspflege gegeben wird.

16.3
Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder sowie der Datenschutzkommission Rheinland- Pfalz vom 6. Juni 1988 zur Neufassung des Bundesdatenschutzgesetzes

Die Datenschutzbeauftragten stellen mit Bedauern fest, daß der vorliegende Entwurf einer Neufassung des Bundesdatenschutzgesetzes im wesentlichen die gleichen Mängel aufweist wie der entsprechende Entwurf der 10. Legislaturperiode des Deutschen Bundestages. Diese Mängel haben die Datenschutzbeauftragten bereits in ihrer Entschließung vom 14. März 1986 aufgezeigt.

Die Datenschutzbeauftragten halten es insbesondere für verfehlt, das allgemeine Datenschutzrecht aufzusplittern in ein streng auf die Datenverarbeitung in Dateien bezogenes Bundesdatenschutzgesetz und ein den Datenschutz in Akten regelndes Verwaltungsverfahrensgesetz, das weite und wichtige Verwaltungsbereiche (z. B. Finanzverwaltung und Sozialverwaltung) ebensowenig erfaßt wie die Strafverfolgung, und dessen Einhaltung sich überdies weitgehend der Datenschutzkontrolle entzieht.

Die Datenschutzbeauftragten stellen ferner fest, daß bei der Vorbereitung des Entwurfs ihre Empfehlungen sowie die zwischenzeitlich von einigen Bundesländern erlassenen, in wesentlichen Punkten vorbildlichen Neuregelungen des Datenschutzes nahezu unberücksichtigt geblieben sind.

Die Datenschutzbeauftragten verkennen nicht, daß auch der jetzige Entwurf einige Verbesserungen gegenüber dem geltenden Recht aufweist. Insgesamt jedoch werden die in der Begründung des Entwurfs genannten Ziele der beabsichtigten Weiterentwicklung des Bundesdatenschutzgesetzes nicht erreicht:

- Die Anpassung an die Grundsätze des Urteils des Bundesverfassungsgerichts vom 15. Dezember 1983 zum Volkszählungsgesetz ist in mehrfacher Hinsicht nicht gelungen: So enthält der Entwurf keine ausdrückliche Regelung der Datenerhebung, obwohl gerade diese den Bürger unmittelbar belastet; die geplante Regelung im Verwaltungsverfahrensgesetz reicht nicht aus. Auch erfährt der Grundsatz der Zweckbindung zu weitgehende Ausnahmen und die Transparenz der Datenverarbeitung, insbesondere das Recht des Betroffenen auf Auskunft, bleibt hinter verfassungsrechtlichen Anforderungen zurück.

- Dem technologischen Fortschritt auf dem Gebiet der Informations- und Kommunikationstechnik (z. B. Arbeitsplatzcomputer, neue optische Speichermedien, Videoaufzeichnungen, Telekommunikation und Vernetzung) wird der Entwurf nicht gerecht. Der im Entwurf verwandte Dateibegriff und die Beibehaltung des bisherigen Katalogs technischer und organisatorischer Datensicherungsmaßnahmen vernachlässigen die technische Entwicklung.

- Die Kontrollbefugnis des Bundesbeauftragten für den Datenschutz wird insgesamt eingeschränkt, insbesondere durch den Ausschluß systematischer Kontrollen bei der Erhebung und Verwendung personenbezogener Informationen außerhalb von Dateien. Keinesfalls kann eine Einschränkung der Kompetenz der Landesbeauftragten durch den Bundesgesetzgeber hingenommen werden.

- Die Datenschutzvorschriften für den nichtöffentlichen Bereich orientieren sich nicht an dem Grundsatz der Zweckbindung und räumen unvertretbare Verarbeitungsprivilegien ein.

Der Entwurf entspricht daher nicht den Erwartungen an ein zeitgemäßes Datenschutzrecht als Ausprägung des verfassungsrechtlich garantierten Rechts des Bürgers auf informationelle Selbstbestimmung. Dieses Recht ist erst jüngst

durch das Bundesverfassungsgericht in seiner Entscheidung vom 9. März 1988 bestätigt worden. Dort heißt es: „In dieses Recht wird nicht nur dann eingegriffen, wenn der Staat vom einzelnen die Bekanntgabe persönlicher Daten verlangt oder diese der automatisierten Datenverarbeitung zuführt .... Das Recht auf informationelle Selbstbestimmung schützt vielmehr wegen seiner persönlichkeitsrechtlichen Grundlage generell vor staatlicher Erhebung und Verarbeitung personenbezogener Daten und ist nicht auf den jeweiligen Anwendungsbereich der Datenschutzgesetze des Bundes und der Länder oder datenschutzrelevanter Sonderregelungen beschränkt."

Die Konsequenz daraus muß eine möglichst lückenlose und präzise Regelung des Datenschutzes sein, um Rechtssicherheit für Bürger und Verwaltung herzustellen.

16.4
Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder sowie der Datenschutzkommission Rheinland- Pfalz vom 6. Juni 1988 zum Entwurf eines Gesetzes zur Strukturreform im Gesundheitswesen (Gesundheits-Reformgesetz – GRG)

Die Konferenz der Datenschutzbeauftragten stellt fest, daß es in Verhandlungen zwischen dem Bundesbeauftragten für den Datenschutz und dem Bundesminister für Arbeit und Sozialordnung gelungen ist, eine Reihe von Forderungen des Datenschutzes im Regierungsentwurf gegenüber den Vorentwürfen zu verwirklichen.

Gleichwohl halten die Datenschutzbeauftragten eine Verbesserung des Persönlichkeitsschutzes der Krankenversicherten im weiteren Gesetzgebungsverfahren vor allem in den folgenden Punkten für notwendig:

I.
Erfassung medizinischer Daten und Grundsatz des geringstmöglichen Eingriffs

Die im Zusammenhang mit Leistungen der gesetzlichen Krankenversicherung vorgesehene automatisierte Verarbeitung von Daten der Versicherten, Ärzte und Zahnärzte darf der Gesetzgeber wegen des damit verbundenen gravierenden Eingriffs in das Selbstbestimmungsrecht der Versicherten nur zulassen, wenn damit tatsächlich auch die erklärten Ziele des Gesetzgebungsvorhabens gefördert, namentlich ein wesentlicher Beitrag zur Kostendämpfung geleistet werden kann, und sich dies nicht auch durch weniger einschneidende Maßnahmen erreichen läßt. So würde es für die Erstellung von Statistiken, die für die Bewertung und Beeinflussung des Leistungsgeschehens wichtig sind, genügen, einen anonymisierten Transparenzbestand zu bilden. Darüber hinaus wäre zu fragen, ob es nicht ausreicht, statt der vorgesehenen versichertenbezogenen umfassenden Datenspeicherung nur die rechtlichen und organisatorischen Voraussetzungen zur Überprüfung von Einzelfällen festzulegen.

II.
Festlegung des Verwendungszwecks personenbezogener Daten

Gegen die Nutzung personenbezogener Daten, soweit sie für die Überprüfung der Abrechnung medizinischer Leistungen und zur Kontrolle der Wirtschaftlichkeit erforderlich ist, bestehen keine grundsätzlichen Bedenken. Nach der Rechtsprechung des Bundesverfassungsgerichts muß der Verwendungszweck erhobener Daten vom Gesetzgeber normenklar festgelegt werden. Für Kassenärztliche Vereinigungen und für den Medizinischen Dienst fehlt es im Gesetzentwurf an einer Festlegung des Verwendungszwecks. Der Gesetzentwurf stellt außerdem nicht sicher, daß Daten der Krankenkassen nur für deren Zwecke verwendet werden. Eine Verwendung medizinischer Daten über den eigentlichen Aufgabenbereich der Krankenkassen, der Kassenärztlichen Vereinigungen und des Medizinischen Dienstes hinaus darf wegen der besonderen Sensibilität der Daten nur für eng umschriebene Ausnahmefälle zugelassen werden. Die allgemeinen Offenbarungsvorschriften des SGB X lassen eine zu weitgehende Nutzung durch Dritte zu.

Dies gilt um so mehr, als die im Entwurf bereits einbezogene technische Entwicklung (maschinenlesbare Datenträger, Krankenversicherungskarte) immer mehr dazu führen wird, daß die versicherungsbezogenen Krankheitsdaten in maschinenlesbarer Form und damit vielfältig verwertbar vorliegen werden.

Die Konferenz begrüßt die Verbesserungsvorschläge der Ausschüsse des Bundesrates.

III.
Vereinbarungen der Verbände

Der Gesetzentwurf überläßt die Regelung der Abrechnung der kassenärztlichen Versorgung einschließlich der dafür erforderlichen Datenübermittlung den Vereinbarungen der Verbände der Krankenkassen und Kassenärztlichen Vereinigungen. Verschiedene Vereinbarungen greifen nachhaltig in das informationelle Selbstbestimmungsrecht der Versicherten ein, ohne daß diese – insbesondere als Pflichtversicherte – eine Wahlmöglichkeit hätten. Das betrifft z. B. Festlegungen über den Inhalt von Rezepten und Krankenscheinen, die Einbeziehung Dritter zu Prüfzwecken, Meldung von Behinderungen an die Krankenkassen.

Da der Gesetzgeber nach der Rechtsprechung des Bundesverfassungsgerichts alles Wesentliche selbst regeln muß, reicht es nicht aus, die Regelungsbefugnis an die Verbände zu delegieren. Vielmehr müßte der Umfang der Eingriffe in das informationelle Selbstbestimmungsrecht und der Mindestinhalt der datenschutzrechtlichen Regelungen konkreter als bisher gesetzlich festgelegt werden. Das gilt auch für die Voraussetzungen zur Einführung maschinenlesbarer

Krankenversicherungskarten. Darüber hinaus wäre klarzustellen, daß die Verarbeitung und Nutzung personenbezogener Daten für andere als die im Gesetz genannten Fälle nicht durch Vereinbarung vorgesehen werden kann. Der Gesetzgeber sollte überdies ein Verfahren vorsehen, in dem die Wahrung der Rechte der Patienten bei Erlaß solcher Vereinbarungen überprüft wird (z. B. Genehmigungsvorbehalt; eine Genehmigung dürfte nur erteilt werden, wenn in den Vereinbarungen die Forderungen des Datenschutzes der Versicherten angemessen berücksichtigt sind).

Der Inhalt der Vereinbarungen ist dem Betroffenen auf Verlangen zugänglich zu machen.

IV.
Medizinischer Dienst

Im Hinblick auf die Schutzwürdigkeit der beim Medizinischen Dienst anfallenden Krankheitsdaten sind gesetzliche Regelungen erforderlich über

- Art und Umfang der zu verarbeitenden Daten
- Zweckbestimmung und Verwendungsmöglichkeit (etwa im Bereich des Sozialmedizinischen Dienstes der Rentenversicherungsträger)
- Vermeidung einer med. Zentraldatei
- Informationsrechte der Betroffenen
- Einschränkung der Offenbarungsbefugnisse gegenüber Dritten
- Löschungszeitpunkte

Die Konferenz begrüßt auch hier die in diese Richtung zielenden Vorschläge der Ausschüsse des Bundesrates.

V.
Auskunftsanspruch

Wegen der zentralen Bedeutung des Auskunftsanspruchs ist im Gesetzestext deutlich klarzustellen, daß auf Verlangen des Versicherten Auskunft über Leistungen und Kosten sowie nach Maßgabe des § 83 SGB X auch über die Diagnose zu erteilen ist. Der Auskunftsanspruch darf nicht durch Satzung beschränkt werden. Der Anspruch muß auch gegenüber dem Medizinischen Dienst bestehen.

VI.
Aufbewahrungsfristen

Der verfassungsrechtliche Verhältnismäßigkeitsgrundsatz gebietet, die Speicherungsdauer personenbezogener Daten auf das erforderliche Maß zu begrenzen. Hierzu sind konkret bestimmte Aufbewahrungsfristen unerläßlich.

Im Gesetzentwurf ist bisher nur bei den Krankenkassen eine nach Jahren festgelegte Frist für die Aufbewahrung von Daten über Leistungsvoraussetzungen (z. B. Art der Erkrankung, Arbeitsunfähigkeitszeiten) vorgesehen. Die Speicherungsdauer für andere Daten bei Krankenkassen und Kassenärztlichen Vereinigungen (z. B. verordnete Medikamente, ärztliche Leistungen, Überweisungen, Abrechnungsunterlagen) ist im Gesetzentwurf nicht konkret befristet. Nach dem Grundsatz der Normenklarheit und dem Wesentlichkeitsgebot des Bundesverfassungsgerichts hat der Gesetzgeber hier selbst eine bestimmte Aufbewahrungsfrist festzulegen.

Die Konferenz begrüßt auch hier die in diese Richtung zielenden Vorschläge der Ausschüsse des Bundesrates. Sie weist jedoch darauf hin, daß die Aufbewahrungsfrist jeweils am Tage der jeweiligen Leistungsgewährung beginnen muß.

VII.
Zentrale Krankheitsdatei der Unfallversicherungsträger

Der Gesetzentwurf räumt den Unfallversicherungsträgern die Möglichkeit ein, eine zentrale Krankheitsdatei einzurichten.

Angesichts der schon früher diskutierten vielfältigen datenschutzrechtlichen Probleme zentraler Krankheits- und Gefährdungsregister muß der Gesetzgeber jedoch gleichzeitig mit der Erlaubnis zur Einrichtung dafür sorgen, daß für solche Register ausreichende rechtliche und organisatorische Schutzvorkehrungen wirksam werden. Vorzusehen ist insbesondere eine Einwilligung der Betroffenen in die Speicherung seiner Daten.

Sicherzustellen ist ferner:

- die Verantwortlichkeit für die gespeicherten Daten (speichernde Stelle)
- Art und Umfang der zu speichernden Daten

– die konkrete Zweckbestimmung der Daten in dem betreffenden Register

– Zugriffsrechte

Sicherzustellen ist schließlich, daß die Patientendaten nicht aus dem durch § 35 SGB I geschützten Bereich (Sozialgeheimnis) herausgelöst werden.

16.5
Beschluß der Konferenz der Datenschutzbeauftragten des Bundes und der Länder sowie der Datenschutzkommission Rheinland-Pfalz vom 10. Oktober 1988

Aktuelle Probleme des Datenschutzes in der Telekommunikation

Mit Inkrafttreten der Telekommunikationsordnung am 1. Januar 1988 hat die Deutsche Bundespost den Übergang von bisher getrennten Fernmeldenetzen zu einem einzigen, diensteintegrierten digitalen Telekommunikationsnetz für die Übermittlung aller Nachrichtenarten eingeleitet; künftig fallen an zentralen Stellen erheblich mehr und leichter auswertbare personenbezogene Daten an als bisher, die je nach Dienstart mehr oder weniger präzise Rückschlüsse auf das Verhalten der Teilnehmer erlauben. In der Telekommunikationsordnung wurden die Empfehlungen der Konferenz der Datenschutzbeauftragten des Bundes und der Länder zur Verbesserung des Datenschutzes und zur Beherrschung der möglichen Risiken bisher leider nur zum Teil befolgt.

Auch das Bundesdatenschutzgesetz kann mit seinen allgemeinen Vorschriften die Risiken nicht auffangen; dies gilt auch für die bisher bekanntgewordenen Novellierungsentwürfe. Hier bedarf es weiterer spezieller Regelungen. Bei der Novellierung des Bundesdatenschutzgesetzes muß vor allem sichergestellt werden, daß sämtliche beim Einsatz neuer Telekommunikationstechniken und -dienste anfallenden Daten in den Geltungsbereich des Gesetzes fallen. Deshalb muß z. B. selbstverständlich sein, daß alle personenbezogenen Daten aus der Bild-, Sprach-, Text- und Datenübertragung geschützt werden. Die Regelung der Zulässigkeit der Verarbeitung personenbezogener Daten, deren Kontrolle und der erforderlichen technisch-organisatorischen Maßnahmen müssen an die neuen technischen Gegebenheiten angepaßt werden.

Das Grünbuch der Europäischen Gemeinschaften über die Entwicklung des gemeinsamen Marktes für Telekommunikationsdienstleistungen und Telekommunikationsgeräte zeigt, daß der Datenschutz bei der geplanten Liberalisierung des Angebots von Dienstleistungen und Geräten nur unzureichend berücksichtigt wird. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder weist nachdrücklich darauf hin, daß das nationale Datenschutzrecht nicht durch ein Gemeinschaftsrecht überlagert werden darf, das im Ergebnis zu weniger Datenschutz führt als das nationale Recht. Die frühzeitige Einbindung des Datenschutzes in die jetzt folgenden Beratungen – auch auf EG-Ebene – ist daher dringend erforderlich.

Die Länder sind im Rahmen ihrer Zuständigkeit zum Erlaß von Regelungen zur Nutzung der Telekommunikation verpflichtet, auch die notwendigen Datenschutzvorschriften zu erlassen. Der Bildschirmtext-Staatsvertrag kann hierzu als Vorbild dienen. In einem derartigen Staatsvertrag müssen auch die materiellen Voraussetzungen zum Betrieb privater Telekommunikationsdienste und deren Zulassung geregelt werden.

16.6
Beschluß der Konferenz der Datenschutzbeauftragten des Bundes und der Länder sowie der Datenschutzkommission Rheinland-Pfalz vom 10. Oktober 1988

Sicherstellung des Datenschutzes bei der Poststrukturreform

Die Bundesregierung hat dem Parlament den Entwurf eines Poststrukturgesetzes vorgelegt, in dem eine teilweise Privatisierung des Fernmeldewesens vorgesehen ist. Eine Verwirklichung hätte zur Folge, daß für die künftigen privaten Telekommunikationsanbieter weniger strenge Datenschutzregelungen gelten als im Betrieb der Bundespost.

Das Poststrukturgesetz muß deshalb über die bisherigen Regelungen hinaus sicherstellen, daß auch in den Bereichen, in denen Endeinrichtungen durch Private betrieben oder sonstige Netzfunktionen durch Private wahrgenommen werden, ebenso strenge Datenschutzregelungen gelten, wie sie im Bereich der Bundespost notwendig sind.

Hierzu reicht die Verordnungsermächtigung, die die Bundesregierung nur unzureichend zum Tätigwerden verpflichtet, nicht aus. Außerdem könnte der Datenschutz durch private Geschäftsbedingungen unterlaufen werden. Notwendig ist eine abschließende gesetzliche Regelung, die den Umfang der Daten auf das unerläßliche Ausmaß beschränkt, eine strenge Zweckbindung vorsieht und für den Bürger die Datenflüsse offenlegt. Dies gilt auch für personenbezogene Daten, die beim Betrieb privater Telekommunikationsdienstleistungen (§ 1 Abs. 4 Entwurf Fernmeldeanlagengesetz) anfallen. Solche Dienstleistungen dürfen nur zugelassen werden, wenn sie den gesetzlichen Anforderungen entsprechen.

Die gesetzliche Regelung sollte von den Unternehmen der Deutschen Bundespost und von den privaten Unternehmen auch verlangen, daß diese technische und organisatorische Maßnahmen durchführen, um eine datenschutzgerechte und sichere Telekommunikation zu gewährleisten. Schließlich muß auch für die privaten TK-Anbieter eine angemessene Kontrolle vorgesehen werden.

16.7
Beschluß der Konferenz der Datenschutzbeauftragten des Bundes und der Länder sowie der Datenschutzkommission Rheinland-Pfalz vom 10. Oktober 1988 zum Entwurf einer Steuerdaten-Abruf-Verordnung – StDAV – (Stand 9. Juni 1988)

Die Konferenz begrüßt es, daß der Bundesminister der Finanzen bei der Vorbereitung einer Steuerdaten-Abruf-Verordnung einigen vom Bundesbeauftragten für den Datenschutz einvernehmlich mit den Landesbeauftragten für den Datenschutz und der Datenschutzkommission Rheinland-Pfalz ausgesprochenen Empfehlungen für eine datenschutzrechtliche Verbesserung gefolgt ist.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder sowie die Datenschutzkommission Rheinland-Pfalz erhebt jedoch ernste Bedenken gegen die nach dem derzeitigen Entwurf weiterhin vorgesehene Einrichtung von automatisierten Datenabrufverfahren für die obersten Finanzbehörden und für die Oberfinanzdirektion. Die Einführung solcher Datenabrufverfahren bedeutet, daß bei den Oberfinanzdirektionen, den obersten Finanzbehörden der Länder und beim Bundesminister der Finanzen zentrale Abrufmöglichkeiten geschaffen werden können, die diesen Behörden einen unmittelbaren automatisierten Zugriff auf Steuerdaten der Finanzämter ihres Zuständigkeitsbereiches ermöglichen.

Solche zentralen Datenabrufmöglichkeiten sind für die Erfüllung der Aufgaben der Aufsichtsbehörden nicht erforderlich. Bei etwaigen Verfahren im Rahmen der Aufsicht sind ohnehin die Akten heranzuziehen. Von diesen Aufsichtsbehörden sind bei der Bearbeitung von steuerlichen Einzelfällen in aller Regel auch keine Entscheidungen unter Zeitdruck zu treffen.

Von der Einrichtung solcher Datenabrufverfahren ist kein ins Gewicht fallender Rationalisierungseffekt zu erwarten. Solche Verfahren können aber dazu führen, daß dem besonderen Steuergeheimnis unterliegende Daten auf sehr einfache Weise Personen bekannt werden, die sie für die Erfüllung ihrer Aufgaben nicht benötigen. Dem gilt es vorzubeugen. Die Datenschutzkonferenz schlägt daher vor, in dem Entwurf der Steuerdaten-Abruf-Verordnung automatisierte Datenabrufverfahren für Oberfinanzdirektionen und oberste Finanzbehörden nicht vorzusehen.

16.8
Beschluß der Konferenz der Datenschutzbeauftragten des Bundes und der Länder sowie der Datenschutzkommission Rheinland-Pfalz vom 10. Oktober 1988 zur Datensicherheit beim Einsatz kleinerer Datenverarbeitungsanlagen

Beim Einsatz kleinerer Datenverarbeitungsanlagen, vor allem von persönlichen Computern (PC), bereiten die Datensicherheit und die Ordnungsmäßigkeit der Verarbeitung personenbezogener Daten besondere Probleme. Im Hinblick auf diese Probleme geben die Datenschutzbeauftragten des Bundes und der Länder folgende Empfehlungen:

I.
Vor jeder Entscheidung, ob für die Arbeiten eines Aufgabengebiets ein PC oder eine sonstige kleinere Datenverarbeitungsanlage eingesetzt werden kann, muß geprüft werden, ob die dabei erzielbare Datensicherheit ausreichend ist. Bei dieser Prüfung müssen insbesondere die Empfindlichkeit der Daten und der Grad der Verbindlichkeit der Verarbeitungslogik berücksichtigt werden. Die Verarbeitung personenbezogener Daten mit einem automatisierten Verfahren, das keine angemessene Datensicherheit bietet, verstößt gegen die Datenschutzgesetze.

II.
Eine speichernde Stelle hat auch bei der Verarbeitung personenbezogener Daten auf einem PC oder einer sonstigen kleineren Datenverarbeitungsanlage die technischen und organisatorischen Maßnahmen zu treffen, die je nach Art der zu schützenden Daten geeignet sind, die Datensicherheit zu gewährleisten. Sofern die Datensicherheit mit den verfügbaren Maßnahmen nicht in dem erforderlichen Umfang gewährleistet werden kann, muß auf den Einsatz des PC oder der kleineren Datenverarbeitungsanlage verzichtet werden.

Um die Datensicherheit zu gewährleisten, sind insbesondere die dem neuesten Stand entsprechenden technischen Maßnahmen zu treffen.

Weisungen sollten schriftlich erfolgen und in einer Dienstanweisung zusammengefaßt werden. Durch Kontrollen der Arbeitsdurchführung ist sicherzustellen, daß alle Vorschriften und Weisungen befolgt werden.

III.
Die Hersteller von Hard- und Software werden aufgefordert, für kleinere Datenverarbeitungsanlagen einschließlich der persönlichen Computer Verfahren zu entwickeln und bereitzustellen, die einen Betrieb dieser Geräte mit einem Maß an Datensicherheit ermöglichen, das demjenigen großer Rechenzentren entspricht. Vor allem müssen Hilfsmittel verfügbar gemacht werden, die es einer datenverarbeitenden Stelle ermöglichen,

- ohne organisatorisch strukturiertes Rechenzentrum und damit auch ohne Funktionstrennungen bei der Arbeitsabwicklung,
- ohne organisatorische Trennung zwischen Anwendung und Durchführung der automatisierten Datenverarbeitung und

– trotz Verzichts auf Detailkenntnisse der automatisierten Datenverarbeitung bei Vorgesetzten und der für die Revision zuständigen Organisationseinheit

sicherzustellen, daß bei der Verarbeitung auf der eingesetzten Datenverarbeitungsanlage eine verbindlich vorgeschriebene Verarbeitungslogik eingehalten wird. Dazu ist es unter anderem erforderlich, Verfahren bereitzustellen, die gewährleisten, daß Programme ausschließlich in der freigegebenen Fassung zum Ablauf kommen. Systemprogramme und Anwendungsprogramme könnten dazu mit einem geeigneten kryptografischen Verfahren versiegelt werden, wodurch Manipulationen erkennbar würden.

Für persönliche Computer und sonstige kleinere Datenverarbeitungsanlagen sollten zur Datensicherheit Systemprogramme und systemnahe Programme mit einem an der Ausstattung großer Anlagen orientierten Leistungsumfang zur Verfügung gestellt werden. Wesentliche der Datensicherheit dienende Komponenten sollten in das Betriebssystem integriert werden, um Manipulationen und Umgehungsmöglichkeiten zu erschweren.

Sachwortverzeichnis zum 17. Tätigkeitsbericht