



12. Wahlperiode

Drucksache **12/21**

HESSISCHER LANDTAG

19. 02. 87

Fünfzehnter Tätigkeitsbericht des Hessischen Datenschutzbeauftragten

Mit Schreiben vom 19. Februar 1987 legt der Datenschutzbeauftragte gemäß § 29 des Hessischen Datenschutzgesetzes vom 31. Januar 1978 dem Landtag folgenden Tätigkeitsbericht vor:

Eingegangen am 19. Februar 1987 · Ausgegeben am 16. April 1987

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

INHALTSVERZEICHNIS

	Seite
1. Zur Situation	9
1.1 Gesetzgebung	9
1.1.1 HDSG-Novellierung	9
1.1.2 Übergangsbonus	11
1.2 Verarbeitung von Gesundheitsdaten	14
1.2.1 Aids	14
1.2.2 Zunahme der automatisierten Datenverarbeitung im Gesundheitsbereich	17
1.3 Volkszählung	19
1.4 Verdrängte und neue Probleme	21
1.4.1 Informationsverlangen der Europäischen Gemeinschaft	21
1.4.2 Genomanalyse und Datenschutz	22
2. Novellierung der Datenschutzgesetze	23
2.1 Die Vorgaben des Bundesverfassungsgerichts	23
2.2 Das neue Hessische Datenschutzgesetz	24
2.2.1 Gesetzgebungsverfahren	24
2.2.2 Leitprinzipien	25
2.2.3 Anwendungsbereich	25
2.2.4 Verbesserung der Bürgerrechte	26
2.2.5 Konsequenzen für die hessischen Behörden	27
2.2.6 Besonderer Datenschutz	29
2.2.7 Informationsbroschüre	30
2.3 Novellierung des Bundesdatenschutzgesetzes (BDSG)	31
2.3.1 Kritik	31
2.3.2 Konsequenzen	31
3. Kommunen	32
3.1 Beratung von Kommunen	32
3.1.1 Gewerberegister	32
3.1.2 Paßdaten	33
3.2 Datenübermittlung an private Personen oder Stellen	33
3.2.1 Einwohnermeldeämter	34
3.2.2 Gewerbemeldestellen	35
3.3 Meldedaten von psychisch Kranken im Adreßbuch	35
3.3.1 Vorfall	35
3.3.2 Konsequenzen	36

4.	Gesundheit	36
4.1	Datenverarbeitung im Krankenhaus	36
4.1.1	Allgemeine Entwicklung	36
4.1.2	Konkrete Regelungen sind notwendig	37
4.1.3	Interne Abschottungen	38
4.1.4	Aufnahmeformulare	39
4.2	Krebsregister	40
4.2.1	Registerarten	40
4.2.2	Prüfung des klinischen Tumorregisters in den Städtischen Kliniken Darmstadt	42
4.2.3	Prüfung des klinischen Tumorregisters im Klinikum der Frankfurter Universität	45
4.2.4	Konsequenzen	47
4.3	Prüfung des Laborsystems LABOSYS des DV-Verbundes	48
4.3.1	Ziel und Verfahren der Prüfung	48
4.3.2	Das System LABOSYS	49
4.3.3	Realisierung in den Städtischen Kliniken Wiesbaden	50
4.4	Aids	52
4.4.1	Personenbezogene Meldepflicht	52
4.4.2	Meldungen an das Aids-Register des Bundesgesundheitsamtes	54
4.4.3	Durchführung und Verwendung von Aids-Tests	54
4.4.4	Aids-Tests des Gesundheitsamtes Frankfurt	55
4.4.5	Aids in Justizvollzugsanstalten	55
5.	Justiz	58
5.1	Justizmitteilungsgesetz	58
5.1.1	Kritische Punkte	58
5.1.2	Positive Ansätze	58
5.2	Reform der Strafprozeßordnung	59
5.2.1	Neue Regelungsvorschläge	59
5.2.2	Kritik einzelner Vorschläge	60
5.2.3	Resümee	62
5.3	Auskünfte aus dem Grundbuch	62
5.3.1	Auskünfte	62
5.3.2	Prüfungspflicht des Grundbuchamtes	62
6.	Sicherheitsbehörden	63
6.1	Polizeilicher Zugriff auf Meldedaten	63
6.1.1	Trennung von Polizei und Melderegister	63
6.1.2	Übergangsregelung	63
6.1.3	Meldedatenübermittlungsverordnung	63
6.1.4	„Datenfernverarbeitung im Einwohnerwesen - Polizeiauskunftssystem - EWOTP“	64

6.2	Sicherheitsüberprüfung in kerntechnischen Anlagen	65
6.2.1	Gegenwärtige Situation	65
6.2.2	Die geplante Richtlinie	65
6.3	Sicherheitsgesetze	66
6.3.1	Verabschiedete und geplante Gesetze	66
6.3.2	Änderung des Straßenverkehrsgesetzes Einführung des "Zentralen Verkehrsinformationssystems" (ZEVIS)	66
6.3.3	Personalausweisgesetz, Paßgesetz und § 163d Strafprozeßordnung	67
6.3.4	Entwurf eines Gesetzes zur Änderung des Bundesverfassungsschutzgesetzes	68
6.3.5	Vor-Entwurf eines "Gesetzes über die informationelle Zusammenarbeit der Sicherheits- und Strafverfolgungsbehörden des Bundes und der Länder in Angelegenheiten des Staats- und Verfassungsschutzes und nachrichtendienstlicher Tätigkeit" (Zusammenarbeitsgesetz - ZAG)	70
6.3.6	Vorgaben für Hessen	70
7.	Ausländerzentralregister	70
7.1	Überlegungen zur Neukonzeption	70
7.2	Datenschutzrechtliche Bewertung	71
7.2.1	Index-Register	71
7.2.2	Regelung der Datenverwendung	71
8.	Statistik	72
8.1	Landesstatistikgesetz	72
8.1.1	Bedeutung	72
8.1.2	Regelungsinhalt	73
8.1.3	Auskunftspflicht	73
8.1.4	Kommunalstatistik	74
8.1.5	Übermittlung statistischer Einzelangaben	74
8.2	Volkszählung 1987	76
8.2.1	Ausführungsverordnung zu § 9 Abs. 3 Volkszählungsgesetz 1987	76
8.2.2	Verwaltungsvorschrift	77
8.2.3	ADV in den örtlichen Erhebungsstellen	77
8.2.4	Zentrale Volkszählungsstelle für Hessen	78
9.	Individuelle Datenverarbeitung mit Personal-Computer (PC)	79
9.1.	Technologischer Fortschritt	79
9.2	Technische Ausstattung und Einsatzarten der Personal-Computer	79
9.3	Stärken und Schwächen des Personal-Computers	79
9.3.1	Vorzüge	79
9.3.2	Die Stärken des Personal-Computers sind auch seine Schwächen	80
9.4	Datenschutz und Datensicherung bei Datenverarbeitung mit Personal-Computern	82
9.4.1	Problemdarstellung	82
9.4.2	Abgrenzung der Begriffe	82
9.4.3	Organisatorische Ansätze	82
9.4.4	Die Anwendung des § 10 HDSG	89

9.5	Nutzung privater Personal-Computer für dienstliche Zwecke	97
9.5.1	Verarbeitung dienstlicher Daten auf privaten PC in Privaträumen	97
9.5.2	Verarbeitung dienstlicher Daten auf privaten PC in Diensträumen	97
9.5.3	Regularien der Genehmigung	97
10.	Recht auf Information / "Freedom of Information"	98
10.1	Europarat	98
10.2	Griechenland	98
10.3	Norwegen	98
10.4	Kanada	99
10.5	Frankreich	99
11.	Bilanz	100
11.1	Beschlüsse des Landtags zum 14. Tätigkeitsbericht	100
11.1.1	Zu Ziff. 3.2 "Prüfung des Rechenzentrums des AOK-Landesverbandes"	100
11.1.2	Zu Ziff. 3.3 "Basisdokumentation Psychiatrie (BADO) des Landeswohlfahrtsverbandes Hessen"	100
11.1.3	Zu Ziff. 4.1.1 "Demonstrationsanmeldung - Datenübermittlung"	101
11.1.4	Zu Ziff. 4.2 "Zweckwidrige Auswertung von Protokoll Daten"	102
11.1.5	Zu Ziff. 13.2.1 "Studentendaten"	102
11.1.6	Zu Ziff. 8.3 "Datensicherheit in Datennetzen"	103
11.1.7	Zu Ziff. 7.1 "Telekommunikationsordnung"	103
11.2	Sonstige Punkte des 14. Tätigkeitsberichts	104
11.2.1	Zu Ziff. 6 "Melderecht: Meldedatenübermittlungsverordnung"	104
11.2.2	Zu Ziff. 13.1.6 "Hinweis- und Spurendokumentationssysteme"	105
11.3	Frühere Tätigkeitsberichte	106
11.3.1	Bildschirmtext (13. Tätigkeitsbericht, Ziff. 3.1.1)	106
11.3.2	Fernmeß- und Fernwirkdienste (13. Tätigkeitsbericht, Ziff. 3.1.2)	106
11.3.3	Übermittlung amtsärztlicher Zeugnisse an den Dienstherrn (11. Tätigkeitsbericht, Ziff. 5.2.3, 5.2.4, 12. Tätigkeitsbericht, Ziff. 2.1.6.1, 13. Tätigkeitsbericht, Ziff. 4.2.2.1)	107
11.3.4	Kontrollmitteilungen an die Finanzämter - Zur Reform der Abgabenordnung (11. Tätigkeitsbericht, Ziff. 2.1.6)	107
11.3.5	Automatisierte Telefondatenerfassung (9. Tätigkeitsbericht, Ziff. 3.1.4, 11. Tätigkeitsbericht, Ziff. 2.2.2)	108
12.	Materialien	109
12.1	Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 27. Januar 1986 zu den "Sicherheits- und Datenschutzgesetzen"	109
12.2	Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 14. März 1986 zur Änderung des Bundesdatenschutzgesetzes	110
12.3	Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 18. April 1986 zur Änderung des Bundesverfassungsschutzgesetzes	113
12.4	Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 14. März 1986 zum Datenschutz im Krankenhaus	115

KERNPUNKTE DES 15. TÄTIGKEITSBERICHTS

1. Der Hessische Gesetzgeber hat mit dem neuen, am 1. Januar 1987 in Kraft getretenen Datenschutzgesetz als erster auf die zuletzt durch das Bundesverfassungsgericht in seiner Entscheidung zum Volkszählungsgesetz formulierten Anforderungen an eine verfassungskonforme Datenschutzregelung reagiert und zugleich versucht, die in den vergangenen Jahren durch die Kontrolle der Verarbeitung gewonnenen Erfahrungen in Vorschriften umzusetzen, die einen besseren Datenschutz gewährleisten (Ziff. 2.2).
2. Das neue Hessische Datenschutzgesetz reicht, trotz der Verbesserung des Datenschutzes, für einen wirklich wirksamen Datenschutz nicht aus. Bereichsspezifische gesetzliche Vorschriften sind nach wie vor unentbehrlich. Dazu zählen in erster Linie gesetzliche Regelungen für die Verarbeitung personenbezogener Daten durch die Polizei und den Verfassungsschutz, bei der Erhebung und Verwertung von Angaben für statistische Zwecke oder im Zusammenhang mit der Krankenhausbehandlung (Ziff. 1.1.2.1 und 1.1.2.3).
3. Die Verabschiedung bereichsspezifischer gesetzlicher Regelungen läßt sich nicht beliebig verschieben. Die Verfassung toleriert keinen als "Dauerbonus" verstandenen "Übergangsbonus". Der Gesetzgeber ist vielmehr verpflichtet, eine an den möglichen Konsequenzen der Verarbeitung für den Bürger ausgerichtete Prioritätenliste aufzustellen und zugleich bis zur Verabschiedung der notwendigen gesetzlichen Regelungen den Zugriff auf personenbezogene Angaben soweit wie möglich einzuschränken sowie von der Einführung neuer Verarbeitungstechniken abzusehen. Zudem: Für eine ganze Reihe erforderlicher gesetzlicher Regelungen liegen bereits Vorschläge vor. Wo sie vorhanden sind, kann der Übergangsbonus nicht über 1988 hinausreichen (Ziff. 1.1.2).
4. Ein konsequenter Datenschutz zwingt darüber hinaus, sich einer Reihe neuer Probleme zu stellen, aber auch bislang vernachlässigte Bereiche aufzugreifen:
 - So ist es dringend erforderlich, auf die Entwicklung der Gentechnologie mit gezielten Datenschutzregelungen zu reagieren, die eine transparente, kontrollierbare und die Manipulation des einzelnen - über genetische Register, die systematische Verwertung "genetischer Fingerabdrücke" für Verwaltungszwecke oder "Genomanalysen" als Zugangsvoraussetzung für Arbeitsplätze - ausschließende Datenverarbeitung gewährleisten (Ziff. 1.4.2).
 - So kommt es in Anbetracht der zunehmenden Verwendung von Personal-Computern ganz besonders darauf an, neue Vorkehrungen zu entwickeln, die es auch und gerade mit Hilfe technischer Mittel ermöglichen, den Datenschutz aufrechtzuerhalten (Ziff. 9).
 - So muß endlich dafür gesorgt werden, daß die Grundsätze des Datenschutzes auch im Rahmen der für die Europäische Gemeinschaft durchgeführten Erhebungen beachtet werden. Die Gemeinschaft hat in der Vergangenheit selbst auf die Bedeutung der Datenschutzkonvention des Europarates hingewiesen und ihre Mitglieder aufgefordert, die Konvention zu ratifizieren. Sie muß deshalb auch in ihrem Zuständigkeitsbereich die Maßstäbe beachten, die sie bei anderen für unerläßlich ansieht. Erhebungen, wie sie bislang vor allem im Bereich der Landwirtschaft durchgeführt werden, können und dürfen nicht weiter hingenommen werden (Ziff. 1.4.1).
5. Der Gesetzgeber muß sich weit mehr als bisher der Verarbeitung von Gesundheitsdaten annehmen. In erster Linie geht es dabei um gesetzliche Vorschriften zur Verwendung automatisierter Verarbeitungsverfahren in Krankenhäusern. Das Krankenhaus darf nicht als Informationseinheit gesehen und behandelt werden, innerhalb derer Patientendaten uneingeschränkt ausgetauscht werden dürfen. Vielmehr gilt es auch hier, streng an den verschiedenen Verarbeitungszwecken ausgerichtete Zugangsbarrieren zu errichten (Ziff. 4.1 und 12.4).
6. Datenschutzforderungen im Zusammenhang mit Krebsregistern sind bisher weitgehend an den epidemiologischen Registern ausgerichtet gewesen. Mehr und mehr übernehmen mittlerweile die klinischen Krebsregister die Funktion der epidemiologischen Register, ja sie entwickeln sich zu allgemeinen Patientenregistern. Die Ausarbeitung klarer Datenschutzkonzepte ist insofern unerläßlich. Zugleich gilt es zu prüfen, ob und unter welchen Voraussetzungen eine gesetzliche Regelung getroffen werden muß (Ziff. 4.2).
7. Laborsysteme sind ein weiteres typisches Zeichen für die fortschreitende Automatisierung innerhalb der Krankenhäuser. Der Tätigkeitsbericht weist am Beispiel der Städtischen Kliniken Wiesbaden auf vorhandene Sicherungsmängel und notwendige Schutzvorkehrungen hin (Ziff. 4.3).

8. Aids war und ist zuvörderst ein medizinisches Problem. Spätestens jedoch seit der immer offener und nachdrücklicher formulierten Forderung nach einer Meldepflicht haben gesellschaftliche und rechtliche Aspekte die Diskussion zu überlagern begonnen. Um so dringlicher erscheint es, sich nicht mit den allgemein gehaltenen Hinweisen auf die Notwendigkeit einer Meldepflicht zufriedenzugeben, sondern eine genaue Antwort auf die Frage nach den Modalitäten und den Konsequenzen der Meldung zu verlangen. Die Meldepflicht kann sich sehr schnell zur Vorstufe einer Isolierung und Diskriminierung der Aids-Infizierten verwandeln. Alle Anstrengungen müssen sich daher zunächst und vor allem auf eine nachhaltige Aufklärung, eine intensive Erforschung der Verbreitungswege und gezielte, die Diskriminierung ausschließende Maßnahmen konzentrieren. Solange deshalb nicht überzeugend dargelegt wird, daß es keinen anderen Weg für eine wirksame Bekämpfung von Aids gibt, bleibt es bei der bereits im vergangenen Tätigkeitsbericht getroffenen Feststellung: Eine personenbezogene Meldepflicht ist verfassungswidrig. Nicht minder kritisch gilt es die zahlreichen Versuche zu betrachten, die Meldepflicht auf Umwegen zu erreichen, etwa durch die Untersuchungspflicht einzelner, immer größerer Teile der Bevölkerung (Ziff. 1.2.1.2 und 4.4).
9. Der Bundesgesetzgeber hat mit der Verabschiedung des neuen Volkszählungsgesetzes eine den Anforderungen des Grundgesetzes und des Bundesverfassungsgerichts entsprechende Grundlage für die für Mai 1987 geplante Erhebung geschaffen. Die rechtliche Beurteilung der Volkszählung kann und darf sich allerdings nicht in einer Würdigung des Volkszählungsgesetzes erschöpfen. Genauso wichtig sind die von der Verwaltung zu treffenden und zu verantwortenden organisatorischen Maßnahmen zur Durchführung der Volkszählung. Auf diese Maßnahmen muß sich deshalb jetzt alle Aufmerksamkeit konzentrieren (Ziff. 1.3 und 8.2).
10. Eine bereits in früheren Berichten wiederholt betonte Erfahrung bestätigt sich erneut: Der Datenschutz ist, allen gegenteiligen Behauptungen zum Trotz, kein Beitrag zur Erhöhung der Verwaltungskosten. Konsequenz praktizierte Datenschutzvorschriften können im Gegenteil sehr wohl dazu beitragen, die Verwaltungstätigkeit zu rationalisieren und die Verwaltungskosten zu vermindern, wie das im Tätigkeitsbericht erwähnte Beispiel der Neuorganisation der Ausweiskartei einer Gemeinde beweist (Ziff. 3.1.2).
11. Die Veröffentlichung von Adreßbüchern ist nach wie vor einer der ständig wiederkehrenden Anlässe für Konflikte mit den Datenschutzbestimmungen. Die Meldebehörden sollten Namen und Anschriften von Personen, die sich in Krankenanstalten, Justizvollzugsanstalten, Heimen oder ähnlichen Einrichtungen befinden, nur mit Einwilligung der Betroffenen an Adreßbuchverlage übermitteln (Ziff. 3.3).
12. Das Melderecht ist einer der ersten Bereiche gewesen, in denen sich der Gesetzgeber für eine bereichsspezifische Datenschutzregelung entschlossen hat. Trotzdem gibt es immer noch eine korrekte Anwendung des Datenschutzes gefährdende Konflikte. So bietet das vom Kommunalen Gebietsrechenzentrum Wiesbaden im Auftrag des Hessischen Ministers des Innern für den Direktzugriff der Polizei auf Einwohnermeldedaten entwickelte Verfahren der Polizei die Möglichkeit einer rechtlich unzulässigen Verwertung von Daten (Ziff. 6.1).
13. Die früher schon geäußerte Kritik an der Sicherheitsüberprüfung von Personal in kerntechnischen Anlagen und bei der Beförderung und Verwendung von Kernbrennstoffen hat zu Regelungsvorschlägen geführt, die in einer ganzen Reihe von Punkten eine erhebliche Verbesserung gegenüber der bisherigen Praxis aufweisen. Dennoch darf eine sich in Verwaltungsvorschriften erschöpfende Richtlinie kein Ersatz für die auch hier dringend erforderliche gesetzliche Regelung sein. Die Richtlinie kann deshalb allenfalls als Übergangslösung hingenommen werden (Ziff. 6.2).
14. Der Bundesjustizminister hat auf die Forderung nach einer verfassungskonformen, die Anforderungen des Datenschutzes beachtenden Regelung der Justizmitteilungen mit einem im Dezember 1986 vorgelegten Entwurf einer gesetzlichen Regelung reagiert. Die vorgeschlagenen Bestimmungen halten allerdings einer verfassungsrechtlichen Prüfung nicht stand (Ziff. 5.1).
15. Auch die ebenfalls vom Bundesjustizminister angestrebte Novellierung der Strafprozeßordnung bleibt hinter den vom Bundesverfassungsgericht festgelegten Anforderungen an eine verfassungskonforme Verarbeitung personenbezogener Daten zurück (Ziff. 5.2).
16. Besondere Aufmerksamkeit verdient schließlich der Versuch, das Ausländerzentralregister neu zu regeln. Erste Vorschläge sind von einer beim Bundesminister des Innern eingerichteten Arbeitsgruppe vorgelegt worden. Sie lassen eine Reihe für den Datenschutz wichtiger Punkte außer acht (Ziff. 7).

1. Zur Situation

1.1

Gesetzgebung

1.1.1

HDSG-Novellierung

1986 stand für den Datenschutzbeauftragten verständlicherweise ganz im Zeichen des am 6. November 1986 vom Landtag verabschiedeten und am 1. Januar 1987 in Kraft getretenen neuen Hessischen Datenschutzgesetzes (Ziff. 2.2). Fast zwei Jahre hat es von der Vorlage der ersten Novellierungsvorschläge bis zur Verabschiedung des endgültigen Gesetzestextes gedauert. Nahezu jede Bestimmung wurde im Laufe der langen und intensiven parlamentarischen Beratung umformuliert. Das Gesetz spiegelt deshalb, ungeachtet der Meinungsverschiedenheiten über einige wenige Vorschriften, die gemeinsamen Anstrengungen aller Fraktionen für einen besseren Datenschutz wider.

1.1.1.1

Ziele

Zwei Ziele galt es zu erreichen: Der Gesetzgeber mußte zum einen die in den vergangenen acht Jahren gesammelten Erfahrungen verarbeiten. Zweimal hatte er schon Bedingungen für die Verarbeitung personenbezogener Daten festgelegt. Beide Male war zugleich sichtbar geworden, wie sehr es darauf ankommt, die Verarbeitungsregelung als das Ergebnis eines ständigen Lernprozesses zu verstehen und deshalb in den gesetzlichen Vorkehrungen eine zwar notwendige, aber immer nur vorläufige Antwort auf die durch die Verarbeitung aufgeworfenen Probleme zu sehen. 1970 reagierte der hessische Gesetzgeber als erster auf die sich abzeichnenden Auswirkungen der automatisierten Datenverarbeitung. Seither hat sich nicht nur die Verarbeitungstechnik geändert. Ebenso wenig ist zu übersehen, daß eine Datenschutzgesetzgebung wohl ohne die Automatisierung nicht denkbar wäre, sich aber unter keinen Umständen in Vorschriften über die automatisierte Verarbeitung erschöpfen darf. Konsequenterweise hatte das zweite, 1978 verabschiedete Datenschutzgesetz eine sehr viel differenziertere Regelung gebracht. Mehr als eine vorsichtige Öffnung war es allerdings nicht. Kaum verwunderlich, wenn deshalb die Tätigkeitsberichte Jahr für Jahr daran erinnerten, daß die Wirkung des Datenschutzes verpufft und seine Glaubwürdigkeit verlorengeht, solange der Wechsel von automatisierten Informationssystemen zu manuell geführten Akten genügt, um die einzelnen Verarbeitungsanforderungen einschließlich der Rechte des Betroffenen und der Kontrolle durch den Datenschutzbeauftragten auszuschalten. Das neue, dritte Datenschutzgesetz bringt hier, wie in einer Vielzahl anderer für die Funktionsfähigkeit und Überzeugungskraft des Datenschutzes wichtiger Punkte, längst fällige Korrekturen und Ergänzungen.

Noch mehr freilich als die offenkundig notwendige Anpassung an die Erfahrungen der letzten Jahre bestimmte das zweite Ziel den Verlauf der parlamentarischen Beratungen: eine gesetzliche Regelung zu verabschieden, die den vom Bundesverfassungsgericht in seiner Entscheidung zum Volkszählungsgesetz festgelegten Kriterien einer den Ansprüchen des Grundgesetzes genügenden Datenschutzgesetzgebung voll entspricht. Die mittlerweile weit verbreitete Taktik, die Entscheidung des Bundesverfassungsgerichts als gleichsam äußerste Konzession an den Datenschutz auszugeben, die zwar hingenommen werden muß, in keinem Fall aber überboten werden darf, hat jedoch beim hessischen Gesetzgeber zu keinem Zeitpunkt verfangen. Gewiß, wer das Gesetz aufmerksam liest, stellt sehr bald fest, wie konsequent es sich an den Forderungen des Gerichts orientiert. Die unmißverständlich vorgeschriebene Zweckbindung jeder Verarbeitung ist ebenso bezeichnend dafür wie die strikte Verpflichtung, personenbezogene Daten grundsätzlich nur beim Betroffenen zu erheben. Der Gesetzgeber ist dennoch nicht bei der Entscheidung stehengeblieben. Er hat vielmehr vor dem Hintergrund der Überlegungen des Bundesverfassungsgerichts mit Hilfe zahlreicher zusätzlicher Verarbeitungsanforderungen zu demonstrieren versucht, wie eine den Datenschutz als unmittelbare Folge verfassungsrechtlicher Grundsätze verstehende Regelung aussehen muß. Es genügt, auf die Benachrichtigungspflicht, so sehr man im übrigen über die Details debattieren mag, die erweiterten Kontrollbefugnisse des Datenschutzbeauftragten oder die Sondervorschrift zur Verarbeitung von Arbeitnehmerdaten zu verweisen.

Eines ändert sich dadurch nicht: Das neue Hessische Datenschutzgesetz ist die erste und bislang einzige umfassende Verarbeitungsregelung, die der Aufforderung des Bundesverfassungsgerichts nachkommt, einen verfassungskonformen Datenschutz sicherzustellen. Auf den ersten Blick kein besonderes Verdienst, im Gegenteil nicht mehr als eine schlicht selbstverständliche Aufgabe. Wie schwer sie freilich zu erfüllen ist, zeigt sich an der gescheiterten Novellierung des Bundesdatenschutzgesetzes. Am Konsens über die Notwendigkeit einer Neufassung fehlte es nicht, nur waren die Vorschläge weit von jedem, in der Entscheidung des Bundesverfassungsgerichts näher umschriebenen Mindestmaß an verfassungsrechtlich verbindlichen Vorgaben entfernt. Mehr noch: Stellenweise drängte sich der Eindruck auf, die vorgeschlagene Regelung habe den Datenschutz nicht ausbauen oder zumindest absichern, sondern einschränken wollen. So wurden die verschiedensten "Geheimnisse" zum Anlaß genommen, um die Kontrollbefugnisse des Datenschutzbeauftragten zu reduzieren, erhielt die Verarbeitung für private Zwecke einen Sonderstatus, geriet Fachaufsicht zur Kontrollschranke oder war von der Verarbeitung in Akten nur in einigen, höchst unzulänglichen Bestimmungen im Verwaltungsverfahrensgesetz die Rede.

1.1.1.2

Datenschutz als permanente Regelungsaufgabe

So augenfällig freilich der Kontrast zur gescheiterten Novellierung des Bundesdatenschutzgesetzes ist, so wenig läßt sich ernsthaft behaupten, das Hessische Datenschutzgesetz sei die denkbar beste, ja die einzig mögliche Regelung. Schon deshalb, weil für das neue, dritte Datenschutzgesetz nichts anderes gilt als für seine beiden Vorgänger. Die gesetzliche Regelung steht wiederum vor allem unter dem Vorbehalt einer sich unablässig ändernden Verarbeitungstechnik. Wer daran zweifelt, braucht nur den Abschnitt über die Personal-Computer (Ziff. 9) zu lesen. Auf die möglichen Folgen einer mit ihrer Hilfe konsequent dezentralisierten Verarbeitung war schon früher hingewiesen worden. Was jedoch noch vor kurzem manchem als reine Spekulation erschien, verdichtet sich jetzt mehr und mehr zu einer der zentralen Anwendungs-, wenn nicht sogar Existenzfragen des Datenschutzes. Auf den ersten Blick mag es nicht der Rede wert erscheinen, wenn ein Beamter den Personal-Computer mit nach Hause nimmt, um dort weiter zu arbeiten oder seinen eigenen Personal-Computer auch für dienstliche Aufgaben nutzt. Die Folgen kann man sich freilich leicht ausmalen. Die üblichen, vom Gesetzgeber gerade erst wieder bestätigten Sicherheitsvorkehrungen drohen ebenso leerzulaufen wie die vom Bundesverfassungsgericht für unabdingbar erklärten Kontrollmaßnahmen des Datenschutzbeauftragten. Kurzum, die Notwendigkeit gezielter rechtlicher Reaktionen zeichnet sich bereits deutlich ab. Zudem wäre es völlig unzutreffend zu meinen, die Personal-Computer seien die auf absehbare Zeit einzige Modifikation der Verarbeitungstechnik, bei der wirklich von ernsthaften Folgen für den Datenschutz gesprochen werden könne. Die in den siebziger Jahren immer wieder aufgestellte Behauptung, eine Alternative zu einer zentralen, sich in immer größeren Datenbanken abspielenden Verarbeitung könne es gar nicht geben, ist genauso nachdrücklich vorgetragen worden. Mittlerweile mag sich freilich kaum noch jemand an sie erinnern.

Zudem: Der hessische Gesetzgeber hat zwar den Anfang gemacht. Er ist aber mit seiner Entscheidung einer Verpflichtung nachgekommen, die auch die übrigen Landes- sowie den Bundesgesetzgeber trifft. Das Bundesverfassungsgericht hat an der Aufgabe des Staates, für einen konsequenten und wirksamen Datenschutz zu sorgen, keinen Zweifel gelassen. Keines der bestehenden Gesetze kann unter diesen Umständen in seiner gegenwärtigen Form aufrechterhalten werden. So gesehen, ist das neue Gesetz nicht mehr als ein Anreiz zur Weiterentwicklung des Datenschutzes. Für den hessischen Gesetzgeber bedeutet dies: Genauso wie sich jetzt Bundes- und andere Landesgesetzgeber mit der von ihnen geschaffenen Regelung auseinandersetzen müssen, wird er, und zwar sehr bald, nicht umhin können, sich zu fragen, ob das Hessische Datenschutzgesetz noch den Maßstäben genügt, die durch die zu erwartenden weiteren Regelungen formuliert werden.

1.1.1.3

Anwendung

Das Hessische Datenschutzgesetz kann ebensowenig wie irgendeine andere gesetzliche Regelung für sich in Anspruch nehmen, alle Konflikte aufgegriffen zu haben und deshalb auch auf sämtliche Anwendungsfragen überzeugende Antworten zu bieten. Die langen und mühevollen Beratungen sind nicht ohne Folgen für die Gesetzesformulierung geblieben. Sie spiegelt die oft komplizierten Kompromisse wider und erschwert damit die Interpretation. Mit das beste Beispiel dafür ist die Verpflichtung, personenbezogene Daten grundsätzlich nur beim Betroffenen zu erheben (§ 12). Eigentlich eine Selbstverständlichkeit. Wie schwer es freilich fällt, sie in eine klare und praktikable Regelung umzusetzen, zeigt schon ein Blick in den § 12 mit seinen umständlichen, aber unvermeidlichen Unterscheidungen zwischen der Erhebung bei öffentlichen Stellen und außerhalb des öffentlichen Bereichs oder, für Außenstehende nur schwer nachvollziehbar, zwischen Erhebungen, die zwar "beim Betroffenen" stattfinden, allerdings das eine Mal mit, das andere Mal ohne seine Kenntnis. Sicher, im Nachhinein mag es zuweilen einfach erscheinen, kürzer und verständlicher zu formulieren. Gesetze tragen aber nun einmal unweigerlich den Stempel ihres Entstehungsprozesses. Je zahlreicher die Einwände und je größer deshalb die Widerstände waren, desto komplizierter der Weg, den der Gesetzgeber letztlich gewählt hat.

Und noch etwas: Der Gesetzgeber hat seine Entscheidung nicht vor dem Hintergrund einer Vielzahl, die verschiedensten Verarbeitungsbereiche detailliert behandelnder Datenschutzvorschriften getroffen. Nach wie vor fällt dem Datenschutzgesetz die Aufgabe zu, die meisten Verarbeitungsvorgänge zu regeln. Wie bisher war deshalb der Gesetzgeber gezwungen, immer wieder Formulierungen den Vorzug zu geben, die möglichst allgemein gehalten sind. Die Kehrseite sind allerdings erneut Aussagen, die zwangsläufig nicht die Präzision aufweisen, die sich unschwer erreichen läßt, wenn nicht mehr verlangt wird als eine klare Antwort auf die Fragen, die mit wenigen, klar umrissenen Fällen zusammenhängen.

Um so vorsichtiger gilt es bei der Interpretation des Gesetzes zu sein. Zweierlei gilt es besonders zu beachten: Zum einen kommt es bei jeder Zweifelsfrage vor allem darauf an, sich der Aufgabe des Gesetzes bewußt zu sein. Noch einmal deshalb: Der Gesetzgebungsprozeß war durch das Bestreben bestimmt, den Datenschutz zu verbessern. Für die Interpretation der Gesetzesvorschriften kann dies nur bedeuten: Die Auslegung der gesetzlichen Regelung darf nicht dazu benutzt werden, eben dieses Ziel zu unterlaufen. Im Zweifel verdient daher die Interpretation den Vorrang, die den Datenschutz sichert.

Zudem: Sowohl die Vor- als auch die Entstehungsgeschichte des Gesetzes sind jedenfalls in einem Punkt für dessen Anwendung besonders wichtig. Sie zwingen dazu, Schwerpunkte zu setzen, sich also sehr genau zu überlegen, wann der Datenschutz wirklich auf dem Spiel steht. Man kann, anders ausgedrückt, den Datenschutz auch dadurch, und zwar höchst erfolgreich unterlaufen, daß man ihn lächerlich macht. Wer etwa die Entscheidung des Gesetzes, jede Verarbeitung einzubeziehen, zum Anlaß nimmt, um nunmehr auch nur dem geringsten Hinweis auf eine personenbezogene Angabe eine genaue "Datenschutzprüfung" vorzuschalten, der endet in der Tat bei langen, mit allen juristischen Feinissen ausgestatteten Überlegungen darüber, ob überhaupt und wenn ja, unter welchen Voraussetzungen Namensschilder an den Türen von Amtszimmern angebracht werden dürfen. Jeder Schritt in diese Richtung ist das genaue Gegenteil einer auf die konsequente Verwirklichung des Datenschutzes bedachten Gesetzesanwendung. Die scheinbar überaus exakte Interpretation ist nur der willkommene Vorwand, um den längst als lästig empfundenen Datenschutz lächerlich erscheinen zu lassen und sich seiner damit hoffentlich ein und für allemal zu entledigen.

Genauso gefährlich ist die Tendenz, jede Nachfrage nach personenbezogenen Daten zunächst einmal mit einem pauschalen Hinweis auf den Datenschutz abzuwehren. So merkwürdig es klingen mag: Die Entscheidung für ein neues Datenschutzgesetz hält von solchen Reaktionen nicht ab, sondern begünstigt sie. Genaugenommen spricht alles dafür, daß sich die Erfahrung mit der Entscheidung des Bundesverfassungsgerichts wiederholen wird. Die klare, inzwischen auch noch vom Gesetzgeber bestätigte Stellungnahme zugunsten des Datenschutzes erspart in den Augen mancher Behörde lange Überlegungen darüber, wie es im konkreten Fall um den Zugang zu den Daten steht. Wer will schon über eine von der Verfassung verlangte Schutzvorkehrung richten. Zudem weiß mittlerweile fast jeder, daß bei einer Verwendung personenbezogener Angaben Datenschutzgesichtspunkte eine wichtige Rolle spielen. Unter diesen Umständen ist in der Tat nichts einfacher, als unvermittelt auf den Datenschutz zu verweisen. Die Folgen waren und sind bedenklich. Die Konturen des Datenschutzes verschwimmen, Konflikte, die sich außerhalb seiner Anwendungsgrenzen, wie etwa bei der Interpretation der Personenstandsvorschriften, abspielen, werden ihm plötzlich zugerechnet und selbst dort, wo personenbezogene Daten gar nicht erst zur Debatte stehen, gerät die "informationelle Selbstbestimmung" zum Informationshindernis, wie etwa bei der Weitergabe von Angaben zur Investitionstätigkeit von Unternehmen, die sich als juristische Personen betätigen, durch die statistischen Ämter. Kein Wunder, wenn deshalb der Datenschutz diskreditiert wird, ja zum Sündenbock für jede Informationsschwierigkeit gerät. Vermeiden läßt sich eine solche Entwicklung nur, wenn immer wieder in Erinnerung gerufen wird, daß die gesetzliche Regelung einen klar abgegrenzten Anwendungsbereich hat. Wer sich deshalb auf den Datenschutz beruft, muß zunächst und vor allem in der Lage sein, zu erklären, welche gesetzlichen Vorschriften genau gemeint und wieso sie auf den konkret zur Debatte stehenden Fall anzuwenden. Der Respekt vor der Entscheidung des Gesetzgebers verpflichtet zu einer strikten Einhaltung der Anwendungsgrenzen des HDSG und verbietet den inflationären Umgang mit dem Datenschutz.

1.1.2

Übergangsbonus

1.1.2.1

Bereichsspezifische Regelungen sind nicht beliebig aufschiebbar

Spätestens seit der Entscheidung des Bundesverfassungsgerichts zum Volkszählungsgesetz steht freilich fest: Ein verfassungskonformer Datenschutz muß zweigleisig angelegt sein. Allgemeine gesetzliche Regelungen reichen nicht aus, bereichsspezifische sind genauso erforderlich. Der hessische Gesetzgeber hat infolgedessen nur einen Teil seiner Aufgabe erfüllt. Die Verpflichtung zu bereichsspezifischen Datenschutzregelungen ist durch die Verabschiedung des Datenschutzgesetzes weder erledigt noch aufgeschoben. Sie ist im Gegenteil dringlicher denn je. Gewiß,

das neue Gesetz liefert einen verbesserten allgemeinen Verarbeitungsrahmen. Die Verfassung verlangt aber mehr. Ihren Anforderungen entspricht jedenfalls dann, wenn es für den Betroffenen keine Alternative zur Preisgabe seiner Daten gibt, nur eine Regelung, die den Anlaß, den Umfang sowie die Bedingungen der Verarbeitung genau festlegt und sich just durch diese Zuspitzung auf einen bestimmten Verarbeitungsbereich von den allgemeinen Datenschutzvorschriften abhebt. Erst unter dieser Voraussetzung kann der Betroffene einen wirklich wirksamen Schutz erwarten und die verarbeitende Stelle mit Verarbeitungsbedingungen rechnen, die sich konkret auf ihre Aufgabenstellung einlassen.

Ohne Zweifel hat nun der hessische Gesetzgeber, wie das Beispiel des Meldegesetzes zeigt, die Notwendigkeit bereichsspezifischer Regelungen akzeptiert. Ebenso wenig ist zu bestreiten, daß für mindestens vier andere Bereiche, angefangen bei der Novellierung des HSOG (vgl. 14. Tätigkeitsbericht, Ziff. 4.3) über das Archiv- und Statistik- bis hin zum Krankenhausgesetz (vgl. Ziff. 8.1 bzw. 4.1.2), Vorschläge vorliegen. Weitere, mindestens ebenso notwendige Regelungen, wie etwa das Verfassungsschutzgesetz, ließen sich unschwer hinzufügen.

Der Gesetzgeber ist allerdings in jedem dieser Fälle nicht nur dazu verpflichtet, sich für Sondervorschriften zu entscheiden, er darf auch den Zeitpunkt der Verabschiedung nicht beliebig hinausschieben. Gerade diese Feststellung pflegt freilich auf Widerspruch zu stoßen. Gar nicht erst zu übersehen ist er dort, wo schlichtweg behauptet wird, das Bundesverfassungsgericht habe sich schließlich nur zum Volkszählungsgesetz geäußert. Wenn deshalb der Gesetzgeber überhaupt eine Verpflichtung habe, dann eben lediglich die, die kritisierte Regelung durch eine neue zu ersetzen und das sei ja geschehen. Wer allerdings so argumentiert, läßt bei der Lektüre der Entscheidung den aus seiner Perspektive zugegeben unangenehmen einleitenden Teil der Begründung einfach weg. Das Gericht beläßt es nicht bei Äußerungen zum Volkszählungsgesetz, sondern stellt zunächst den Bezug zwischen dem Datenschutz und der Verfassung her und leitet daraus verbindliche Verhaltensanforderungen an den Gesetzgeber ab. Zu diesen Anforderungen gehört auch und gerade die Verpflichtung zu bereichsspezifischen gesetzlichen Regelungen.

1.1.2.2

Kein "Bonus-Automatismus"

Sehr viel vorsichtiger fällt der Widerspruch gegen bereichsspezifische Regelungen dort aus, wo lediglich ein "Übergangsbonus" zugunsten des Gesetzgebers in Anspruch genommen wird. Gemeint ist damit, daß es verfassungsrechtlich zulässig sei, jedenfalls für eine Übergangszeit ohne die an sich gebotene bereichsspezifische Regelung auszukommen. Zur Begründung wird die Rechtsprechung des Bundesverfassungsgerichts herangezogen. Das Gericht hat in der Tat in einer Reihe von Fällen dem Gesetzgeber einen an bestimmte Voraussetzungen gebundenen "Übergangsbonus" zugestanden. Soviel sollte freilich zunächst bedacht werden: Einen "Bonus-Automatismus" gibt es nicht, so verständlich im übrigen der Wunsch nach einer Übergangszeit sein mag. Der Toleranzspielraum hängt vielmehr vom jeweiligen Konfliktgegenstand ab. Die Bereitschaft des Bundesverfassungsgerichts, einen "Übergangsbonus" zu gewähren, läßt sich daher nicht ohne weiteres auf die Verpflichtung übertragen, eine verfassungskonforme Verarbeitung personenbezogener Daten sicherzustellen. Ehe ein solcher Schluß gezogen wird, gilt es, sich etwa mit der Bedeutung der informationellen Selbstbestimmung und damit mit den möglichen Konsequenzen der Verzögerung einer gesetzlichen Regelung auseinanderzusetzen.

Genausowenig hilft ein abstrakter Hinweis auf die Notwendigkeit weiter, die Funktionsfähigkeit staatlicher Einrichtungen zu erhalten. Sicher, das Bundesverfassungsgericht hat diesen Gesichtspunkt besonders hervorgehoben, ihm allerdings keineswegs den unbedingten Vorrang eingeräumt. Wer sich darauf beruft, muß vielmehr nachweisen, daß die zu befürchtende Funktionsunfähigkeit schwerer wiegt als der bisherige verfassungswidrige Zustand. Eines darf dabei nicht außer acht gelassen werden: Keineswegs geht es durchweg darum, wie etwa bei den Datenschutzgesetzen, eine schon vorhandene gesetzliche Regelung zu überprüfen und soweit erforderlich zu novellieren. In einer ganzen Reihe von Fällen fehlt nach wie vor jegliche gesetzliche Grundlage. Es genügt an die Diskussion über die Sicherheitsgesetze zu erinnern. Für eine korrekte verfassungsrechtliche Bewertung kann es aber nicht gleichgültig sein, ob die Verarbeitung auf korrekturbedürftigen Vorschriften beruht oder jeder gesetzlichen Rechtfertigung entbehrt.

Selbst wenn man sich aber bereitfindet, eine Übergangszeit zu akzeptieren, kann und darf die bisherige Verarbeitungspraxis nicht uneingeschränkt fortgeführt werden. Der "Übergangsbonus" soll dem Gesetzgeber helfen, eine neue verfassungskonforme Regelung vorzubereiten, nicht jedoch die Betroffenen zwingen, eine rechtlich nicht mehr haltbare Verwendung ihrer Daten unverändert hinzunehmen. Verarbeitungsbedingte Eingriffe in die informationelle Selbstbestimmung sind vielmehr auf das für die Funktionsfähigkeit der staatlichen Einrichtungen unerläßliche Mindestmaß zu reduzieren. Darüberhinaus müssen schwerwiegende Eingriffe, soweit es nur geht, vermieden und pauschale Regelungen möglichst eng ausgelegt werden. Schließlich eignet sich die Übergangszeit nicht dazu, den Anwendungsbereich der automatischen Datenverarbeitung auszubauen oder gar neue Verarbei-

tungstechniken einzuführen. Sinn der gesetzlichen Regelung ist es gerade, die Automatisierungsrisiken einzudämmen. Bis zur Entscheidung des Gesetzgebers kann daher bestenfalls der jeweilige Verarbeitungsstand, jedenfalls teilweise, toleriert werden, nicht jedoch eine, zumal mit Hilfe verbesserter Techniken betriebene Intensivierung der Verarbeitung. Ohne die ausdrückliche Billigung des Gesetzgebers darf es, anders ausgedrückt, keine Statusveränderung geben.

1.1.2.3

Vorrangige Regelungen - Fristen

Der "Übergangsbonus" ist auch kein Freibrief für den Gesetzgeber, die Verarbeitungsregelung solange hinauszuschieben wie er nur möchte. Konzidiert wird lediglich ein zeitlich beschränkter Reflexionsprozeß. Daraus folgt zunächst die Verpflichtung, Prioritäten festzulegen. Der Gesetzgeber hat, genaugenommen, keine Alternative. Die Palette der bereichsspezifischen Regelungen ist viel zu breit. Zwar darf keine von ihnen vernachlässigt werden. Doch geht es nicht an, gerade wenn man sich an der Tragweite des Eingriffs in die informationelle Selbstbestimmung orientiert, sie alle auf eine Stufe zu stellen. Niemand wird beispielsweise die Notwendigkeit eines Archivgesetzes anzweifeln. Gemessen aber an der Bedeutung, die etwa der polizeilichen Datenverarbeitung für den Betroffenen zukommt, ist die Archivregelung weniger dringlich. Konsequenterweise kann der Gesetzgeber den Regelungsgegenstand nicht beliebig wählen. Er muß vor allem anderen danach fragen, wo die Verarbeitung für den einzelnen besonders folgenreich ist und sich überdies zunächst auf die Verarbeitungsbereiche konzentrieren, in denen es gegenwärtig noch an Regelungen fehlt oder für die nur wenige, eine verfassungskonforme Interpretation nicht erlaubende Vorschriften existieren. So gesehen, stehen die gesetzlichen Regelungen der Verarbeitung personenbezogener Daten durch die einzelnen Sicherheitsbehörden ebenso wie die Vorschriften zur Verwendung der Krankenhausdaten oder zu den Mitteilungen in Strafsachen (Ziff. 6.1) und die Novellierung der Strafprozeßordnung (Ziff. 6.2) an der Spitze der Prioritätenskala. Sicher, der Landesgesetzgeber kann nur einige dieser Anforderungen erfüllen. Seine Entscheidungen setzen aber, wie sich auch und gerade am neuen Datenschutzgesetz erweist, Akzente, die weit über die Landesgrenzen hinauswirken. Eines sollte klar sein: Solange es an der notwendigen bereichsspezifischen Regelung fehlt, gibt das neue Hessische Datenschutzgesetz den Bewertungsmaßstab ab. § 3 Abs. 1 bezieht die gesamte Landes- und Kommunalverwaltung in den Anwendungsbereich des Gesetzes ein. Alle Behörden und öffentlichen Stellen sind demnach verpflichtet, sich bei der Verarbeitung personenbezogener Daten nach den Anforderungen des Datenschutzgesetzes zu richten. Gewiß, gerade das Beispiel der polizeilichen Datenverarbeitung zeigt, welche Schwierigkeiten dabei entstehen können. Sie rechtfertigen es aber nicht, sich über die im Datenschutzgesetz festgehaltenen Erwartungen hinwegzusetzen. Der bereits vorliegende Vorschlag des Hessischen Ministers des Innern zur Novellierung des HSOG ist sicherlich ein wichtiger Anhaltspunkt dafür, wie sich in Kenntnis und unter Berücksichtigung des Datenschutzgesetzes eine verfassungskonforme Interpretation der bestehenden HSOG-Bestimmungen vollziehen muß. Geholfen ist aber damit allenfalls kurzfristig. Ganz gleich, ob man aus der Perspektive des Datenschutzes oder der spezifischen polizeilichen Aufgaben argumentiert, eine Verarbeitungsregelung, die vor dem Hintergrund allgemeiner Datenschutzbestimmungen und mit Hilfe bloßer Gesetzesvorschläge erfolgt, operiert nicht nur auf einer rechtlich bedenklichen, sondern auch für alle Beteiligten kaum verlässlich abschätzbaren Rechtsgrundlage. Der Gesetzgeber darf deshalb nicht hinnehmen, daß die schon bestehende Unsicherheit durch weitere langwierige Erörterungen möglicher Regelungsinhalte noch erhöht wird. Er muß vielmehr in unmittelbarer Zukunft für eine endgültige Regelung sorgen.

An der polizeilichen Datenverarbeitung zeigt sich noch etwas: Der "Übergangsbonus" verliert seinen Sinn, wenn die Bereitschaft, ihn zu akzeptieren, nicht an überschaubare Fristen gekoppelt wird. Die schlichte Aussage, der Gesetzgeber müsse möglichst bald handeln und dürfe unter keinen Umständen seine Entscheidung schuldhaft verzögern, genügt nicht. Darüber, was "möglichst bald" wirklich bedeutet, läßt sich ebenso lange und erfolglos spekulieren wie über die Bedingungen, unter denen dem Gesetzgeber ein "schuldhaftes" Verhalten vorgeworfen werden kann. So verständlich deshalb vage Formulierungen kurz nach der Entscheidung des Bundesverfassungsgerichts waren, so wenig kann man sich auf Dauer mit ihnen zufriedengeben. Ein "Übergangsbonus" der ausschließlich mit Hilfe so allgemeiner Maßstäbe beurteilt wird, ist kein "Übergangs-", sondern ein "Dauerbonus". Drei Jahre nach der Entscheidung des Bundesverfassungsgerichts läßt sich daher die Frage nach dem Ablauf der Übergangsfrist kaum noch umgehen. Leicht fällt die Antwort nach wie vor nicht. Immerhin gibt es mittlerweile Orientierungspunkte.

Zunächst: Eine globale Frist scheidet von vorneherein aus. Gerade weil der Gesetzgeber an eine durch die Verfassung selbst indizierte Prioritätenskala gebunden ist, kann es keine generelle, ohne Rücksicht auf die einzelnen bereichsspezifischen Regelungen festgelegte Frist geben. Anders ausgedrückt: Je schärfer der verarbeitungsbedingte Eingriff, desto kürzer die "Übergangsfrist".

Zudem: Für die meisten unter Datenschutzgesichtspunkten besonders sensiblen Verarbeitungsbereiche liegen inzwischen Regelungsvorschläge vor. Die Diskussion über die Verarbeitung personenbezogener Daten durch die Sicherheitsbehörden, den Zugriff auf die Gesundheitsdaten oder die statistischen Erhebungen vollzieht sich längst vor dem Hintergrund detaillierter Regelungsvorstellungen. Meinungsverschiedenheiten bestehen sicherlich nach wie vor. Der Dissens ändert allerdings nichts daran, daß die Anforderungen an eine verfassungskonforme Regelung inzwischen genau beschrieben sind. Die Anhörung im Bundestag zu den "Sicherheitsgesetzen" geben darüber genauso Aufschluß wie die intensiven Vorarbeiten zur Novellierung des HSOG. Nichts anderes gilt für die Statistik. Der Bundesgesetzgeber hat sich bereits festgelegt, für den Landesgesetzgeber gibt es ausformulierte Vorschläge. Der Gesetzgeber braucht insofern nur Position zu beziehen. Das mag gerade bei politisch umstrittenen Regelungsbereichen schwerfallen. Rechtlich kann sich der Gesetzgeber der Entscheidung allerdings nicht weiter entziehen. Tolerierbar ist unter diesen Umständen nur noch der für den Abschluß des bereits begonnenen Entscheidungsprozesses erforderliche Zeitraum.

Daß es sich dabei keineswegs um eine unrealistische Erwartung handelt, beweist die Novellierung der Straßenverkehrsordnung (vgl. Ziff. 6.3.2). Sie war ursprünglich Teil der Vorlage, die auch das Bundesdatenschutzgesetz und die "Sicherheitsgesetze" umfaßte, und ist mit diesen anderen Vorschlägen beraten worden. Ebenso wenig wie in den übrigen Fällen kann von einer uneingeschränkten Zustimmung die Rede sein. Sicher, die schnelle Verabschiedung ist allein sicherheitspolitischen Überlegungen zu verdanken. Eine mindestens genauso schnelle Reaktion darf aber vom Gesetzgeber dort erwartet werden, wo es um nichts Geringeres geht als um die Erfüllung einer sich unmittelbar aus der Verfassung ergebenden Pflicht. Soweit daher Vorschläge schon existieren, läuft die Übergangsfrist sowohl für den Landes- als auch für den Bundesgesetzgeber spätestens Ende 1988 ab, und zwar unter Berücksichtigung der durch die Parlamentswahlen bedingten Verzögerungen.

Darüber hinaus müßte bis dahin nicht nur eine den weiteren Entscheidungsverlauf bestimmende Prioritätenliste aufgestellt, sondern eine Reihe zusätzlicher Regelungsvorschläge vorliegen. Gemessen an den bisherigen parlamentarischen Reaktionen, ist dies ebenfalls eine realistische Erwartung. Der Hessische Landtag hat auch und gerade im Zusammenhang mit den Beratungen des Datenschutzgesetzes die Notwendigkeit weiterer Gesetzesinitiativen betont. Zu erinnern ist an den im Hinblick auf die in § 12 HDSG vorgesehenen Ausnahmen vom Grundsatz der Erhebung beim Betroffenen gefaßten Beschluß, sich in allernächster Zeit mit den für die Verarbeitung personenbezogener Daten im Rahmen des Umweltschutzes erforderlichen gesetzlichen Vorschriften zu beschäftigen.

1.2

Verarbeitung von Gesundheitsdaten

Das neue Hessische Datenschutzgesetz mag unter Datenschutzgesichtspunkten unstreitig das wichtigste Ereignis des vergangenen Jahres sein, der Tätigkeitsbericht hat trotzdem einen anderen Schwerpunkt: die Verarbeitung von Gesundheitsdaten (Ziff. 4). Dafür gibt es zwei Gründe: zum einen eine langfristige, in den bisherigen Berichten wiederholt angesprochene Entwicklung, die konsequente Nutzung der automatischen Verarbeitung für immer mehr Informationssysteme und Register im Gesundheitsbereich (Ziff. 4.1, 4.2 und 4.3), zum anderen einen aktuellen Anlaß, die Aids-Diskussion (Ziff. 4.4).

1.2.1

Aids

Aids war und ist zuvörderst ein medizinisches Problem. Je deutlicher sich freilich die Grenzen ärztlicher Hilfe abzeichneten, desto mehr begannen gesellschaftliche und rechtliche Aspekte die Diskussion zu überlagern. War anfangs beispielsweise, wenn überhaupt, eher am Rande von einer Meldepflicht die Rede, so steht diese Maßnahme mittlerweile im Mittelpunkt nahezu aller Überlegungen. Und wo zunächst lediglich über Mittel und Wege gesprochen wurde, die möglicherweise Betroffenen rechtzeitig zu informieren, diskutiert man jetzt Zwangstests, ja die Forderung, die gesamte Bevölkerung regelmäßigen Untersuchungen zu unterziehen. Spätestens seit Verfahren verlangt werden, die mit einer immer umfangreicheren Erhebung und Verarbeitung personenbezogener Angaben verbunden sind, läßt sich die Aids-Diskussion jedoch nicht mehr unabhängig vom Datenschutz führen. In diesem Sinn hatte bereits der letzte Tätigkeitsbericht auf einzelne Datenschutzaspekte aufmerksam gemacht, und aus dem gleichen Grund widmet der diesjährige Bericht den Aids-Problemen einen eigenen Abschnitt.

1.2.1.1

Keine Verfassungskonforme Aids-Bekämpfung ohne Datenschutz

Es scheint sich von selbst zu verstehen, daß jede Maßnahme, bei welcher Angaben über Infizierte verwendet werden, auf ihre Vereinbarkeit mit den Datenschutzgrundsätzen zu prüfen ist. Schließlich zählt schon die Übermittlung von Angaben über infizierte Strafgefangene, ganz zu schweigen von einer Meldepflicht, zu den gleichsam klassischen Anwendungsfällen der Datenschutzbestimmungen. Und doch fehlt es nicht an kritischen,

zuweilen sogar überaus scharf formulierten Gegenstimmen. Das Argumentationsmuster ist nicht ganz unbekannt. Da wird zunächst nachdrücklich davor gewarnt, den Datenschutz zum Selbstzweck zu erheben, um dann ebenso nachdrücklich daran zu erinnern, daß dem Anspruch der Wenigen auf Schutz ihrer Angaben das Recht der Vielen auf Schutz ihrer Gesundheit entgegenstehe. So gesehen, scheint jede weitere Diskussion überflüssig, ja gefährlich. Wer will schon einen Datenschutz verteidigen, der nach Ansicht jener Kritiker nur noch den Sinn hat, denjenigen die Geheimhaltung ihrer Daten zu ermöglichen, die zum Gefahrenherd für die öffentliche Gesundheit geworden sind. Derart radikale Simplifizierungen mögen sich dazu eignen, unliebsame Diskussionen zu erschweren oder zu verhindern, zum Verständnis der Probleme oder gar zu deren Lösung tragen sie freilich wenig bei. Ohne Zweifel ist der Gesundheitsdatenschutz eine der wichtigsten staatlichen Aufgaben. Welche staatlichen Verpflichtungen man dem Grundgesetz auch immer entnehmen mag, verfassungskonform ist die staatliche Gesundheitspolitik nur dann, wenn sie nicht an den Kranken und gesundheitlich Gefährdeten vorbei formuliert wird; sie hat deren Probleme und deren Schutz zu berücksichtigen. Die Verfassung garantiert, anders ausgedrückt, kein "Recht auf Gesundheit" - gleichsam als Blankoermächtigung zu einseitig repressiven Maßnahmen. Für Aids wie für jede andere Krankheit gilt vielmehr: Legitim und legal sind einzig Maßnahmen, die ein Höchstmaß an Schutz gewährleisten, ohne dabei den Respekt vor der Integrität der Betroffenen aus den Augen zu verlieren. Konkret heißt dies: Sowohl der Gesetzgeber als auch die öffentliche Verwaltung müssen bei jeder zur Diskussion stehenden Vorkehrung - so überzeugend, ja selbstverständlich sie auf den ersten Blick erscheinen mag - stets die Auswirkungen auf die Betroffenen mitbedenken, um unter mehreren möglichen Reaktionen jeweils derjenigen den Vorzug zu geben, die mit der geringsten Belastung für die Betroffenen verbunden ist. Nur unter dieser Voraussetzung läßt sich die verfassungsrechtlich verbindliche Vorgabe einhalten, in der Gesundheitspolitik eine allen Bürgern gegenüber bestehende Verpflichtung zu sehen, sie also nicht als Instrument zu benutzen, den Wünschen und Ängsten der vielen "Gesunden" auf Kosten der wenigen "Kranken" Rechnung zu tragen.

1.2.1.2

Meldepflicht

Wer sich dafür einsetzt, Informationen über einzelne Infizierte, etwa mit Hilfe einer Meldepflicht, zu sammeln, muß deshalb zwei Punkte berücksichtigen: Zunächst geht es darum, sowohl das Informationsziel als auch den Kreis der Informationsempfänger klar zu umschreiben. Die übliche, regelmäßig wiederkehrende Aussage, man wolle mehr und vor allem Genaueres über die Verbreitung von Aids sowie über die Infizierten selbst wissen, reicht nicht aus. Gerade weil sich die Übertragungsgefahr nicht leugnen läßt, weil die ständig wachsende Zahl der Infizierten ebensowenig zu übersehen ist wie die Aussichtslosigkeit therapeutischer Anstrengungen, jedenfalls für die nächste Zukunft, können unversehens andere Zielsetzungen die Oberhand gewinnen. Eine personenbezogene Sammlung von Angaben über Aids- Infizierte kann der erste Schritt auf dem Weg zu Maßnahmen sein, die eindeutig auf die Isolierung der Infizierten hinauslaufen. Über die Meldepflicht lassen sich die Virusträger eingrenzen und identifizieren, über die Infizierten-Datei konkret an die Adresse der Registrierten formulierte Maßnahmen treffen und mit Sanktionen versehen. Genau dieser Punkt wird von den Befürwortern einer Meldepflicht im unklaren gelassen. Es wird beispielsweise nicht eindeutig festgestellt, ob die Registrierung im Hinblick auf bestimmte Berufe - etwa Friseur, Tischler, Angestellte in Lebensmittelgeschäften, Apotheker, Lehrer und Ärzte - eine Zugangssperre zur Folge haben soll. Nirgends finden sich unmißverständliche Aussagen darüber, ob die Registrierung dazu dienen soll, Aids-infizierte Kinder aus den Schulen herauszunehmen. Nirgends wird ferner deutlich erklärt, inwieweit die Registrierung die Grundlage für Eheverbote abgeben soll und wie es um Maßnahmen steht, die Aids-Infizierte daran hindern sollen, Kinder zu bekommen. Und nirgends wird schließlich ein Wort darüber verloren, ob die Registrierung sich als organisatorische Vorstufe für die strafrechtliche Ahndung von Verstößen der Aids-Infizierten gegen bestimmte Verhaltensvorschriften erweisen könnte.

Man mag jede solche Absicht bestreiten. Doch beginnt mit der Meldepflicht unweigerlich die systematische Verarbeitung von Daten über Aids-Infizierte. Sobald ein Register, zumal ein automatisch geführtes, zur Verfügung steht, ist es möglich, die gespeicherten Angaben für die verschiedensten Maßnahmen zu nutzen. Die Wahrscheinlichkeit, daß es zu einer solchen Entwicklung kommt, ist dann besonders groß, wenn sich, wie bei Aids, Ratlosigkeit und Angst mischen. Wenn selbst die Medizin machtlos ist, dann neigt eine verängstigte, sich unmittelbar bedroht führende Gesellschaft dazu, rechtliche und organisatorische Maßnahmen, die auf eine radikale Isolierung der Infizierten zielen, als den einzig gangbaren Ausweg anzusehen. Solche Maßnahmen suggerieren nicht nur entschlossene Aktivität, sondern vermitteln, was vielleicht noch wichtiger ist, den Eindruck, man grenze den Gefahrenherd ein, sondere die Gefahrträger aus, fördere einen "Selbstreinigungsprozeß" der Gesellschaft. Was mit den Infizierten dann geschieht, vollzieht sich gleichsam außerhalb der Gesellschaft und trifft eine nicht mehr zu ihr gehörende Gruppe.

Meldepflicht und Registrierung bahnen für die Infizierten den Weg, der sie aus der Gesellschaft hinaus- und in die ausgegrenzte Gruppe hineinführt. Meldepflicht und Registrierung sichern, so gesehen, das für eine flexible, sich immer weiter eskalierende Ausgrenzungsstrategie erforderliche Informationsminimum. Sollten Zweifel an der

Verlässlichkeit der Information aufkommen, ist der nächste Schritt bereits vorgezeichnet: Im Unterschied zur Meldepflicht kann man sich einer allgemeinen Untersuchungspflicht kaum entziehen. Deshalb eignet sich eine generelle Verpflichtung, sich untersuchen zu lassen, nach Meinung ihrer Befürworter, am ehesten dazu, die Mängel der Meldepflicht zu korrigieren. So weit braucht man freilich nicht unbedingt zu gehen. Es genügt schon, die immer wieder geforderten, teilweise bereits praktizierten Zwangstests an möglichst großen Bevölkerungsgruppen durchführen zu lassen, also etwa an allen Schulkindern, Studenten, Autofahrern und Bundeswehrangehörigen, um ein vergleichbar umfassendes Ergebnis zu erzielen, ohne allzuviel öffentliches Aufsehen zu erregen.

Aids ist also keineswegs nur ein medizinisches Problem: Die Krankheit könnte sich als Auslöser einer möglicherweise fundamentalen sozialen Destabilisierung erweisen. Wer die Tragweite einer Isolierung beurteilen will, darf sich nicht mit Überlegungen zu den einzelnen Maßnahmen begnügen. Die große Zahl der Betroffenen muß mitberücksichtigt werden. Längst ist nicht mehr von einigen hundert oder allenfalls einigen tausend Infizierten die Rede. Selbst konservative Schätzungen übersteigen mittlerweile die Zahl hunderttausend. Und auch die anfänglich noch recht optimistischen Annahmen hinsichtlich der Zahlenrelation von Infizierten und manifest Erkrankenden sind inzwischen sehr viel ungünstigeren Prognosen gewichen. Die nach wie vor verbreitete Auffassung, Aids sei gleichsam der Preis für die Zugehörigkeit zu bestimmten sozialen Gruppen, derjenigen der Homosexuellen und der Drogensüchtigen, ist längst fragwürdig geworden. Schon ein flüchtiger Blick auf die Krankengeschichten und die inzwischen nachgewiesenen Übertragungswege zeigt, daß solche Behauptungen zwar viel über die Einstellung zu diesen beiden Gruppen, aber wenig über die Aids-Realität aussagen. Kurzum, Isolierungsmaßnahmen sind quantitativ wie qualitativ mit weitreichenden, kaum absehbaren Folgen verbunden. Quantitativ - weil es sich nicht um einen kleinen, überschaubaren und nicht weiter wachsenden Kreis von Betroffenen handelt, sondern weil mit Steigerungsraten gerechnet werden muß, die schon in Kürze zu einer Verdoppelung der ohnehin beträchtlichen Zahl der Infizierten führen dürften. Qualitativ - weil Isolierungsmaßnahmen Grundrechte einer immer größeren Bevölkerungsgruppe aufheben und die Bundesrepublik mit Vorkehrungen konfrontieren, die politisch wie rechtlich in krassem Widerspruch zu den das Grundgesetz tragenden Vorstellungen stünden. Illustriert sei dies an zwei Beispielen: der mittlerweile offen diskutierten Forderung nach einer Zwangsinternierung wenigstens einer Gruppe von Aids-Kranken sowie den allerdings noch etwas zurückhaltender formulierten Vorstellungen über die Art und Weise, wie der Geschlechtsverkehr verhindert und die Geburt von Aids-infizierten Kindern vermieden werden könnten.

Die verfassungsrechtliche Auseinandersetzung über sämtliche zur Debatte stehenden Maßnahmen, von der Meldepflicht über die Zwangstests bis hin zu einer allgemeinen Untersuchungspflicht, kann und darf deshalb nicht erst bei der Frage beginnen, wer, unter welchen Umständen und in welchem Umfang Zugang zu den jeweils ermittelten Daten haben soll. Anders ausgedrückt: Die verfassungsrechtlichen Anforderungen beziehen sich nicht nur auf die Durchführung der Meldepflicht, sondern auf die Frage, ob sie überhaupt zulässig ist. Solange die Folgen der einzelnen Maßnahmen nicht konsequent offengelegt, sondern weitgehend verdrängt werden, solange ferner die Unmöglichkeit anderer, weniger einschneidender Vorkehrungen nicht überzeugend nachgewiesen wird und sofern die Wirksamkeit der zur Diskussion stehenden Maßnahmen zweifelhaft erscheint, müssen alle in diese Richtung zielenden Bestrebungen an der Verfassung scheitern.

Es kommt also gerade bei der Meldepflicht entscheidend darauf an, sowohl nach den möglichen Auswirkungen zu fragen als auch nach ihrem spezifischen ärztlichen Nutzen. Wo man differenzierte, die Situation der Infizierten und die Erkenntnisse der Ärzte berücksichtigende Überlegungen erwarten können sollte, findet sich nach wie vor meistens nur ein generalisierter Hinweis auf die unbestrittene Gefährlichkeit von Aids. Und anstatt die oft wiederholte Warnung der Ärzte ernstzunehmen, allein die öffentliche Diskussion der Meldepflicht habe viele Infizierte davon abgehalten, sich an spezialisierte Ärzte zu wenden, damit also letztlich die Ansteckungsgefahr eher erhöht, gibt man sich mit Bemerkungen zu den administrativen Aspekten zufrieden. Solange jedoch den Reaktionen der Betroffenen keine Beachtung geschenkt wird und die Folgen eingeschränkter Kooperationsbereitschaft unberücksichtigt bleiben, verbietet sich auch unter rechtlichen Gesichtspunkten eine Einführung der Meldepflicht.

1.2.1.3

Information und Schutz vor Benachteiligungen

Mit Warnungen vor politischem und administrativem Aktionismus ist es freilich nicht getan. Die verfassungsrechtlichen Bedenken gegen eine Meldepflicht befreien den Staat nicht von seiner Handlungspflicht; sie rücken vielmehr andere Handlungsbereiche in den Vordergrund. Die derzeit wichtigste staatliche Aufgabe ist eine konsequente und umfassende Information der Öffentlichkeit. Manches wurde und wird schon dafür getan. Die Informationsmöglichkeiten sind jedoch nicht ausgeschöpft. Wer wirklich alles unternehmen möchte, um ein Höchstmaß an Information zu verbreiten und zugleich das langsame Abgleiten der Infizierten in die Isolierung mit all den damit verbundenen Folgen zu vermeiden, darf auf Bequemlichkeit und Vorurteile keine Rücksicht nehmen. Kaum jemand dürfte sich beispielsweise darüber freuen, zur besten Fernsehzeit und mitten in den populärsten Unterhal-

tungssendungen an Aids erinnert zu werden. Trotzdem ist neben Anzeigen, Plakaten oder besonderen Veranstaltungen in Schulen gerade das Fernsehen ein unverzichtbares Medium, welches dabei helfen kann, die medizinischen und sozialen Konsequenzen einzudämmen. Die Gesellschaft muß Aids als ihr ureigenes Problem begreifen und die Auseinandersetzung mit den Aids-Folgen als eine Aufgabe verstehen, welche ohne die Bereitschaft der gesamten Bevölkerung, sich fortlaufend zu informieren und das individuelle Verhalten entsprechend einzurichten, nicht erfüllt werden kann.

So gesehen, ist es Sache des einzelnen, freiwillig und von sich aus alle notwendigen Schutzvorkehrungen zu treffen, und Sache des Staates, ihn dabei so effektiv wie möglich zu unterstützen. Dafür sind allerdings nicht nur verbesserte Untersuchungseinrichtungen, gezielte Hilfen wie etwa Substitutionstherapien für Drogensüchtige und eine intensivierte Forschung und Information hinsichtlich der Ansteckungswege erforderlich. Mindestens ebenso wichtig sind rechtliche Regelungen, die die Infizierten vor Benachteiligungen schützen, welche sehr wohl auch jene treffen können, die sich an der Bekämpfung von Aids freiwillig beteiligen. In diesem Sinne weist der Tätigkeitsbericht auf die Notwendigkeit einer ausreichenden Anonymisierung freiwillig weitergegebener und zentral verarbeiteter Fallberichte hin (vgl. Ziff 4.4.2).

Von besonderem Gewicht sind die Folgen, die eine freiwillige Untersuchung für die Beschäftigungschancen haben kann. Die Erfahrungen mit dem Bundeszentralregister mahnen zur Vorsicht. Eine gesetzlich gesicherte Abschottung der Information nutzt den Betroffenen nichts, wenn sie vom Arbeitgeber aufgefordert werden, von sich aus einen Registerauszug vorzulegen. Noch so ausgeklügelte, die Unzugänglichkeit der Ergebnisse einer freiwilligen Aids-Untersuchung garantierende Datenschutzvorschriften können die Betroffenen nicht vor Situationen bewahren, in denen ihnen letztlich nichts anderes übrig bleibt, als das Ergebnis der Untersuchung mitzuteilen, womit sie vor allem die Möglichkeit aufs Spiel setzen, einen Arbeitsplatz zu bekommen. Je mehr sich die Betroffenen jedoch dieser Gefahr bewußt werden, desto mehr schwindet die Hoffnung auf freiwillige Kooperation und eine von der gesamten Gesellschaft getragene Reaktion auf die Aids-Gefahren.

Um Mißverständnissen vorzubeugen: Es geht nicht darum, dem öffentlichen oder privaten Arbeitgeber jede Möglichkeit zu nehmen, sich über den Gesundheitszustand potentieller Arbeitnehmer, also auch über eine Aids-Infektion, zu informieren. Zur Debatte steht etwas anderes: Mit dem "freiwillig" eingereichten Aids-Attest wird möglicherweise nicht nur der Zugang zu einem bestimmten Arbeitsplatz versperrt, sondern tendenziell jegliche Beschäftigungsmöglichkeit ausgeschlossen. Wer deshalb die "freiwillige" Vorlage, ohne weitere Überlegungen anzustellen, als selbstverständlich akzeptiert, ist bereit, einer immer größeren Bevölkerungsgruppe die Chance einer beruflichen Betätigung, und zwar auf Dauer, zu verwehren. Die Isolierung mag intendiert sein oder nicht, sie ist unübersehbar. Unter diesen Umständen nützt es nichts, sich hinter den traditionellen Vorstellungen über das Frage- und Entscheidungsrecht des Arbeitgebers oder über die Einstellungsvoraussetzungen bei Beamten und Angestellten des öffentlichen Dienstes zu verschanzen. Der Gesetzgeber muß sich vielmehr zum einen um eine gesetzliche Regelung bemühen, die die mögliche Diskriminierung der Aids-Infizierten zumindest einzuschränken versucht, zum anderen muß er gezielt und konkret alle sich bietenden Chancen der Beschäftigung ausschöpfen.

Noch ist es für eine sorgfältige langfristige gesetzliche Reaktion nicht zu spät. Doch fördert weitere Verzögerung unweigerlich jene Maßnahmen, die offen oder verdeckt auf Isolierung hinauslaufen. So sehr eine rationale Diskussion erwünscht und erforderlich ist, um zu wohlüberlegten, die Infektionsgefahren wie die Situation der Infizierten berücksichtigenden gesetzlichen und administrativen Regelungen zu gelangen - die ihr gesetzten zeitlichen Grenzen dürfen nicht ignoriert werden. Die Zeichen einer wachsenden Emotionalisierung und Politisierung und damit die Gefahren eines irrationalen Aktionismus sind bereits unverkennbar. Soll diese Entwicklung aufgehalten werden, gibt es keine Alternative zu einer kompromißlosen Aufklärung und zu spezifischen Vorkehrungen, welche die notwendige Hilfe sowie die Abwehr von Benachteiligungen gewährleisten. Der Datenschutz spielt dabei gewiß eine wichtige Rolle; er kann aber die eigentlichen Maßnahmen zur Bewältigung der Infektionsgefahr und der Infektionskonsequenzen nicht ersetzen. Anders ausgedrückt: Der Gesetzgeber und die öffentliche Verwaltung müssen den Datenschutz in allen diesbezüglichen Überlegungen berücksichtigen, ihn aber immer nur als Teil einer Gesamtregelung sehen. Der Datenschutz zwingt dazu, sich der Gefahren einer unkontrollierten Verbreitung von Gesundheitsdaten, und zwar nicht nur für die Infizierten, sondern für die Gesellschaft insgesamt, bewußt zu sein.

1.2.2

Zunahme der automatisierten Datenverarbeitung im Gesundheitsbereich

Jahr für Jahr haben die Tätigkeitsberichte auf die mit der Verarbeitung von Patientendaten verbundenen Gefahren und die Notwendigkeit besonderer gesetzlicher Regelungen hingewiesen. Die entscheidenden Fragen sind freilich immer noch offen, gesetzliche und administrative Schutzvorkehrungen dringender denn je. Der Tätigkeitsbericht stellt zwei ebenso wichtige wie bezeichnende Problemkomplexe in den Vordergrund: die Verarbeitung von Patientendaten in den Krankenhäusern (Ziff. 4.1) und die klinischen Krebsregister (Ziff. 4.2).

1.2.2.1

DV im Krankenhaus

Mit einer der entscheidenden Gründe, wenn nicht sogar die ausschlaggebende Ursache für die intensiverte Verarbeitung von Patientendaten war und ist die Forderung, die Gesundheitskosten zu begrenzen. Die Patientendaten gewinnen unter diesen Umständen eine ganz neue Bedeutung: Sie werden zur unentbehrlichen Informationsquelle, und zwar sowohl für die Kontrolle der jeweils erbrachten Leistungen als auch für die Entwicklung von langfristig angelegten Sparmaßnahmen. Die automatisierte Verarbeitung schafft die besten denkbaren Voraussetzungen dafür. Sie ermöglicht es, auf die vorhandenen, zu ganz anderen Zwecken erhobenen Angaben zurückzugreifen und sie für die Vielzahl der sich im Rahmen der Kontrolle und der weiteren Planung stellenden Fragen systematisch zu verwerten. Die in den früheren Tätigkeitsberichten ausführlich behandelten Modellversuche (vgl. z.B. 12. Tätigkeitsbericht, Ziff. 3.2.3) sind dafür genauso beispielhaft wie die im diesjährigen Bericht besprochenen Folgen des novellierten Krankenhausfinanzierungsgesetzes und der Bundespflegesatzverordnung.

Einmal mehr zeigt sich: Rationalisierungsbestrebungen sind mit einer wachsenden Inanspruchnahme von Patientendaten verknüpft. Der Tätigkeitsbericht verweist nicht nur auf die zunehmende Zahl automationsgestützter Verfahren, sondern gibt auch zu erkennen, wie die Organisation der Krankenhäuser mit einem ständig weiter verfeinerten Informationsnetz überzogen wird, das ohne Patientendaten nicht auskommt, eine im übrigen längst nicht abgeschlossene Entwicklung. Die Entstehung neuer ebenso umfassender wie zentralisierter Informationssysteme zeichnet sich bereits deutlich ab. Stichworte wie "Krankenhauskommunikationssysteme" geben klar zu erkennen, daß die intensive interne Informationsverarbeitung mehr und mehr durch einen nicht minder intensiven externen Informationsaustausch ergänzt wird.

Wohlgermerkt, genauso wie bisher geht es nicht darum, die Notwendigkeit einer kostenbewußten Gesundheitspolitik in Frage zu stellen. So wenig aber das Ziel zur Diskussion steht, so sehr gilt es darüber nicht zu vergessen: Sowohl der Gesetzgeber als auch die Gesundheitsverwaltung sind bei der Wahl ihrer Mittel an verfassungsrechtliche Vorgaben gebunden. Patientendaten sind keine Informationsquelle, die jederzeit für jedes organisatorisch-administrative Ziel angezapft werden kann. Wie bei allen anderen Verarbeitungsbereichen ist vielmehr auch hier zunächst der Grundsatz zu beachten: Die Patientendaten müssen solange unzugänglich bleiben, wie die Rationalisierungsziele ohne Rückgriff auf personenbezogene Angaben erreicht werden können. Die Verarbeitung von Patientendaten für organisatorisch-administrative Zwecke darf nicht zur Regel werden. Gerade weil sie sich jedoch nicht immer vermeiden läßt, kommt es in ganz besonderem Maße darauf an, das Recht der Betroffenen sicherzustellen, zu wissen, was mit ihren Daten geschieht, und auch auf den Verarbeitungsprozeß Einfluß nehmen zu können. Nur: Gerade die Verarbeitung von Patientendaten mahnt zur Vorsicht gegenüber der zwar grundsätzlich notwendigen, in ihrer Bedeutung aber immer wieder überschätzten "Einwilligung" des Betroffenen in die Verarbeitung. Für den Patienten gibt es nichts Wichtigeres als die Behandlung. Auf sie konzentrieren sich seine Überlegungen und Wünsche und nicht etwa auf die Auseinandersetzung mit der Verwendung von Informationen zu seiner Person. Der Gesetzgeber kann sich deshalb nicht mit der üblichen Verweisung auf die "Einwilligung" aus der Affäre ziehen. Er muß für Korrektive sorgen, die der besonderen Situation in der sich der Patient befindet, Rechnung tragen.

Die immer breitere Streuung der Patientendaten verpflichtet zudem den Gesetzgeber ebenso wie die Krankenhausverwaltung zu strengen Abschottungsmaßnahmen. Sowohl innerhalb der Krankenhäuser als auch und erst recht bei übergreifenden Informationssystemen muß es verbindliche, abschließend geregelte Zugangsbeschränkungen geben. Das Krankenhaus ist keine Informationseinheit, innerhalb derer die Patientendaten frei zirkulieren dürfen. Auch innerhalb des Krankenhauses gilt es strikt nach den jeweils wahrgenommenen Aufgaben zu unterscheiden, den Zugriff auf die Patientendaten und deren Verwendung also ausschließlich aufgabenorientiert zu bestimmen.

Schließlich: Überlegungen zur Verarbeitung von Patientendaten können und dürfen die Bedeutung nicht außer acht lassen, die der Kenntnis dieser Angaben für die medizinische Forschung zukommt. Zugleich bestätigt sich: Allgemeine Wissenschaftsklauseln, wie sie auch im neuen Hessischen Datenschutzgesetz enthalten sind, reichen nicht aus. Sie sind nur eine erste Annäherung. Der Gesetzgeber muß deshalb für differenzierte, am besonderen Forschungszusammenhang orientierte Regelungen sorgen. Die Krankenhausgesetzgebung ist, so gesehen, ein zwingender Anlaß, um die allgemeine Vorschrift über die Verarbeitung personenbezogener Daten zu wissenschaftlichen Zwecken zu überprüfen und durch eine besondere, die Situation des Patienten ebenso wie die Aufgaben und die verfassungsrechtliche Sonderstellung der wissenschaftlichen Forschung berücksichtigende, Regelung zu ersetzen. Der Tätigkeitsbericht unterstreicht einmal mehr die Notwendigkeit einer solchen Regelung (Ziff. 4.1.2).

1.2.2.2

Klinische Krebsregister

Wann immer in der Vergangenheit von Krebsregistern die Rede war, konzentrierte sich die Aufmerksamkeit auf die im Hinblick auf eine verlässliche epidemiologische Forschung geplante oder bereits realisierte Verarbeitung von Patientendaten. Schon der 12. Tätigkeitsbericht (Ziff. 2.1.4.2) hatte freilich darauf aufmerksam gemacht, daß im Schatten dieser allgemein diskutierten Register weitere, unter Datenschutzgesichtspunkten nicht minder bedeutende Zusammenstellungen von Angaben über krebskranke Patienten entstehen. Gemeint sind die klinischen Krebsregister. Der diesjährige Bericht erinnert nicht nur daran, sondern bestätigt die seinerzeit schon ausgemachte Tendenz, klinische Register mehr und mehr in eine generelle, verselbständigte Form der Patientendokumentation zu verwandeln. Zudem: Je mehr Zweifel an den für die epidemiologischen Register vorgesehenen Regelungen geäußert wurden, je offensichtlicher sich ihre Verabschiedung verzögerte, desto deutlicher entwickelten sich die klinischen Register zu einer Ersatzdokumentation. Beides unterstreicht: Allgemeine Unterscheidungen, wie sie die Landesregierung getroffen hat, mögen zur besseren Beschreibung der ursprünglichen Zwecke beitragen, sind aber inzwischen fragwürdig. Ganz abgesehen davon, zeigt gerade die im Tätigkeitsbericht referierte Prüfung des klinischen Tumormregisters in den Städtischen Kliniken Darmstadt, daß es mit noch so exakten Beschreibungen allein nicht getan ist.

Notwendig ist in jedem Fall ein auf die klinischen Krebsregister zugeschnittenes Datenschutzkonzept. Überlegungen zu den Registern dürfen sich mit anderen Worten, nicht in Äußerungen zu den epidemiologischen Registern erschöpfen. Mit im Vordergrund eines solchen Konzepts muß die klare Unterscheidung zwischen klinischer Dokumentation und der Nachsorgedokumentation unter Beteiligung externer Stellen stehen. Ebenso erforderlich sind genaue Aussagen zur Funktion der Register, zu den Voraussetzungen und Grenzen der Datenverwendung, zu den Kontrollmöglichkeiten sowie den Rechten der Patienten.

Vor allem die konkreten Prüfungserfahrungen verstärken jedoch die Zweifel, ob man es bei den letztlich unverbindlichen Vorstellungen eines Datenschutzkonzepts belassen kann. Schon die hohe Sensitivität der Daten spricht nicht anders als beim epidemiologischen Register für verbindliche Vorschriften. Hinzu kommt die mittlerweile offensichtliche Parallellität, ja weitgehende Ergänzung und Austauschbarkeit der epidemiologischen und klinischen Register. Schließlich gilt es die intensive Nutzung, vor allem also die mit der Nachsorge zwangsläufig verbundene Verbreitung der Daten zu bedenken.

Für den Patienten steht sehr viel auf dem Spiel. Der Gesetzgeber darf die hohe mit der Erkrankung einhergehende Belastung ebensowenig übersehen wie die komplizierten Organisationsabläufe, wie sie nun einmal für Krankenhäuser typisch sind. Der Rückzug in pauschale Einwilligungskonstruktionen verbietet sich, so wenig es im übrigen angeht, dem Patienten Informationen generell vorzuenthalten oder gar ihn völlig aus dem Entscheidungsprozeß über die Verarbeitung seiner Daten auszuschalten. Um wieder auf die Prüfungserfahrungen zurückzugreifen: Das Einwilligungsförmular ist ein Musterbeispiel dafür, wie unter dem Vorzeichen einer für die Entscheidung des Patienten notwendigen Information Mißverständnisse geradezu provoziert, falsche Eindrücke erweckt und entscheidungserhebliche Aussagen verdrängt werden. Zugegeben: Nichts ist wahrscheinlich schwieriger und zuweilen lästiger als der Dialog mit dem Patienten und seine verständliche Unterrichtung. Trotzdem: Die Krankheit hebt nicht sein Recht auf, zu erfahren wohin seine Daten kommen und wer sie zu welchem Zweck benutzt, aber auch grundsätzlich selbst über die Voraussetzungen und die Grenzen der Verarbeitung zu entscheiden. Die Erfahrungen mit den Formularen und die Einsicht in die Schwierigkeiten einer "Einwilligung" zählen mit zu den Gründen, die dafür sprechen, die klinischen Krebsregister an feste gesetzliche Regelungen zu binden.

1.3

Volkszählung

1983 war die Volkszählung am fehlenden Datenschutz gescheitert. Kaum verwunderlich, wenn deshalb die Vorbereitungen für die für Ende Mai 1987 geplante Erhebung gerade an ihrer Übereinstimmung mit den vom Bundesverfassungsgericht präzisierten Anforderungen des Datenschutzes gemessen werden. Ebensowenig überrascht es, daß sich die Aufmerksamkeit zunächst nahezu ausschließlich auf das neue Volkszählungsgesetz konzentriert hat. Schließlich hatte sich der Konflikt an den Mängeln der früheren gesetzlichen Regelung entzündet und auch die vom Bundesverfassungsgericht formulierten Erwartungen richteten sich in erster Linie an den Gesetzgeber. Nur: Mit der Verabschiedung des Volkszählungsgesetzes sind noch keineswegs alle Bedingungen für eine den Datenschutz gewährleistende, verfassungskonforme Erhebung erfüllt. So viel ist sicherlich nicht zu bestreiten: Die lange und intensive parlamentarische Beratung hat zu einer gesetzlichen Regelung geführt, die jedenfalls für die unmittelbar anstehende Zählung ein verfassungsrechtlich korrektes Verfahren vorsieht.

Mit dieser Feststellung allein ist es aber nicht getan. Das Gesetz ist nur der erste, allerdings unverzichtbare Schritt auf dem Weg zu einer verfassungskonformen Erhebung, der zweite, nicht minder wichtige ist die administrative Durchführung. Sich mit ihren Details zu beschäftigen, mag lästig, ja kleinlich erscheinen. Dem Bürger ist aber letztlich wenig mit den allgemeinen Aussagen des Volkszählungsgesetzes genützt. Ob die Verarbeitung seiner Daten wirklich den verfassungsrechtlichen Anforderungen entspricht, läßt sich erst in Kenntnis der verschiedenen, für die Durchführung der Erhebung notwendigen administrativen Maßnahmen sagen, angefangen bei der Auswahl der Zähler über die Einrichtung und die Organisation der Erhebungsstellen bis hin zu der Ausgestaltung und Auswertung der Fragebögen.

Der Tätigkeitsbericht weist auf eine Reihe wichtiger damit verbundener Probleme hin. Wohlgermerkt, angesprochen ist nur ein Ausschnitt der gegenwärtig diskutierten Fragen. Ganz gleich aber, ob man die im Bericht erwähnten oder die weiteren noch offenen Punkte nimmt, die Erfahrungen des letzten Jahres legen zwei Schlüsse nahe: Bis zur Erhebung sind es nur noch einige Monate. Der Vorbereitungsprozeß ist jedoch keineswegs abgeschlossen. Nach wie vor gibt es ungelöste Fragen, die vor der Erhebung rechtlich einwandfrei beantwortet werden müssen. Um Mißverständnisse zu vermeiden: Die Hindernisse lassen sich durchaus rechtzeitig überwinden, sofern wirklich alle notwendigen Anstrengungen unternommen und zugleich Reaktionen vermieden werden, die den Anschein erwecken, als ob man die administrativen Details vernachlässigen könne.

Genau diese Tendenz hat freilich die Vorbereitung der Volkszählung von Anfang an begleitet. Nicht von ungefähr hatte das Bundesverfassungsgericht an die Notwendigkeit erinnert, das Vertrauen der Bürger zu gewinnen. Der Erfolg statistischer Erhebungen hängt eben entscheidend von der Bereitschaft der Bürger zur Kooperation ab. Deshalb bedarf es in Wirklichkeit keiner weiteren Überlegungen darüber, daß gerade derjenige, der auf die Erhebung Wert legt, ja sie für unverzichtbar erklärt, alles tun muß, um nicht zuletzt durch eine rechtzeitige, einwandfreie Organisation Zweifel zu zerstreuen. Noch so oft wiederholte Äußerungen zur Bedeutung der Volkszählung nützen solange nichts, wie die organisatorischen Vorbereitungen nicht in einer Weise getroffen werden, die den Bürger davon überzeugt, daß Kritik und Mißtrauen fehl am Platz sind.

Daß aber genau dieser Punkt viel zu wenig bedacht wurde, zeigt sich schon an dem vom Statistischen Bundesamt ursprünglich vorgelegten Haushaltsmantelbogen. Völlig korrekt enthielt der Bogen ein Verzeichnis der dem jeweiligen Haushalt angehörigen Personen mit Name und Anschrift, überaus befremdlich dagegen war der aufgedruckte Hinweis, der sich auch in dem als Anlage zum Haushaltsmantelbogen vorgesehenen Informationsblatt fand: "Ihr Name wird nicht auf elektronischen Datenträgern gespeichert". Dem Statistischen Bundesamt konnte es nicht unbekannt sein, daß ein großer Teil der Gemeinden die Zählung mit Hilfe automatisierter Verfahren durchführen will und dabei durchaus beabsichtigt, die Namen auf elektronischen Datenträgern zu speichern. Wohlgermerkt, darauf, ob eine solche Speicherung zulässig ist, kommt es zunächst überhaupt nicht an. Dem Bürger wurde ein bestimmter, in offenkundigem Gegensatz zu den bereits beschlossenen Durchführungsmaßnahmen stehender Eindruck vermittelt. Weder die seither, auf die Intervention der Datenschutzbeauftragten hin erfolgte Korrektur, noch die Feststellung, daß keine rechtlichen Bedenken gegen die Speicherung bestehen, können den Bürger wirklich zufriedenstellen. Er muß sich verständlicherweise fragen, was denn das Statistische Bundesamt veranlaßt hat, ihn falsch zu informieren und ob alle übrigen Auskünfte tatsächlich stimmen. Eben deshalb geht es nicht an, die administrativen Einzelheiten als vernachlässigungswerte Petitessen zu behandeln. Gewiß ist es nicht einfach, zu erklären, weshalb etwa die im Rahmen der Erhebung erforderliche Datenverarbeitung mit Hilfe der Kommunalen Gebietsrechenzentren erfolgt, von Rechenzentren also, die auch über eine Vielzahl anderer personenbezogener Angaben verfügen, oder Personal Computer in den Erhebungsstellen eingesetzt werden, die Automatisierung also mehr oder weniger den gesamten Verarbeitungsprozeß begleitet. Vor dem Hintergrund einer langen, gerade im Hinblick auf die Gefahren einer automatisierten Verarbeitung geführten Diskussion hat der Bürger nicht nur die verständliche Erwartung, sondern das Recht zu erfahren, wie sich die Erhebung und die weitere Verarbeitung genau abspielen werden und inwieweit alle notwendigen Vorkehrungen getroffen worden sind, um zweckwidrige Verwendungen seiner Daten auszuschließen.

Für den Datenschutzbeauftragten ergibt sich daraus: Er muß alle an der Volkszählung beteiligten Stellen immer wieder an ihre Verpflichtung erinnern, auch und gerade die administrativen Einzelheiten auf ihre Übereinstimmung mit den verfassungsrechtlichen Anforderungen zu prüfen und sich seinerseits vergewissern, wo noch Schwierigkeiten auftauchen. Er ist darüber hinaus dem Bürger gegenüber gehalten, ihn über den Vorbereitungsstand zu informieren und vor allem auf die Durchführungsmaßnahmen einzugehen, die im Hinblick auf die früheren Auseinandersetzungen und die damit verbundenen Anforderungen an die Volkszählung besondere Beachtung verdienen. Er muß und wird schließlich für eine den Erhebungs- und Verarbeitungsprozeß begleitende Kontrolle sorgen.

Eines sollte allerdings klar sein. Die Verpflichtung des Datenschutzbeauftragten, sich mit den administrativen Aspekten genauso auseinanderzusetzen, wie er es zuvor mit dem Volkszählungsgesetz getan hat, entlastet die an der Volkszählung beteiligten Stellen nicht von ihrer Verantwortung. Der Datenschutzbeauftragte kann nicht mehr als seinen Standpunkt darlegen, Vorschläge machen und das Parlament und die Öffentlichkeit informieren. Die Entscheidung und damit auch die Verantwortung liegt allein bei der öffentlichen Verwaltung.

1.4

Verdrängte und neue Probleme

1.4.1

Informationsverlangen der Europäischen Gemeinschaft

Die Tätigkeitsberichte der Datenschutzbeauftragten haben sich in der Vergangenheit mit den Informationserwartungen der verschiedensten Landes- und Bundesbehörden beschäftigt. Ein Bereich ist freilich weitgehend ausgespart geblieben: die Informationsanforderungen der Europäischen Gemeinschaft. Auf den ersten Blick mag dies überraschen. Schließlich ist es gar nicht so lange her, daß gerade im Zusammenhang mit einem der wichtigsten Anwendungsfälle des Datenschutzes, den statistischen Erhebungen, auf die Probleme hingewiesen wurde, die mit der auf die Europäische Gemeinschaft zurückzuführenden Stichprobenerhebung über Arbeitskräfte zusammenhängen (vgl. 13. Tätigkeitsbericht, Ziff. 3.2.4). Und auch sonst ist die Gemeinschaft immer wieder erwähnt worden. Es genügt an die Auseinandersetzung mit der von ihr geförderten Einrichtung internationaler Krankheitsregister zu erinnern.

So wichtig freilich jeder dieser Fälle für sich genommen sein mag, keiner von ihnen läßt den Umfang und die Bedeutung der von der Gemeinschaft veranlaßten Verarbeitung personenbezogener Daten wirklich erkennen. Beides wird erst in einem ganz anderen Zusammenhang sichtbar: dort, wo sie mit ihren Maßnahmen in den wirtschaftlichen Ablauf eingreift. Zwei Beispiele dafür: 1986 wurden vor dem Hintergrund der "Milchgarantiemengenverordnung" Fragebogen an die landwirtschaftlichen Haushalte verteilt. Ziel der Fragebogenaktion war es, den Haushaltsaufwand der landwirtschaftlichen Betriebe festzustellen, um die von der Verordnung vorgesehene Förderung zu bestimmen. Auf 19 Seiten wurde nicht nur nach den Wohnungsverhältnissen, dem Arbeitsablauf, der Freizeit oder der Aus- und Weiterbildung gefragt. Ähnlich detaillierte Angaben wurden unter anderem darüber erwartet, ob die Mahlzeiten aus zwei (Suppe u. Hauptgericht oder Hauptgericht u. Dessert) oder drei Gängen bestehen, wie viel Kalorien die einzelnen Haushaltsmitglieder (Name der Verpflegungsperson) zu sich nehmen, wie sich die Anschaffung für Möbel, Geschirr, Blumenschmuck, und zwar aufgeteilt in "Schnitt- und Topfblumen, Wohngarten und Grabstätten" konkret gestalten und was für Unterwäsche, Schlafanzüge, Socken, Zeitungen, Bücher und Kinobesuche ausgegeben wurde, um nur einige wenige Beispiele zu erwähnen.

Weit weniger detailliert, aber immer noch klar personenbezogen und recht substantiiert sind die Informationsanforderungen im Hinblick auf die von der Gemeinschaft beschlossene Einrichtung einer "Weinbaukartei". Und genauso wie bei dem im Zusammenhang mit der Milchmengenverordnung formulierten Fragebogen ist die Motivation klar: Im einen wie im anderen Fall geht es um eine verlässlichere, den Gemeinschaftsgrundsätzen entsprechende Zuteilung der Förderungsmittel und um eine bessere Kontrolle der Subventionsempfänger. Kurzum, die Informationsanforderungen sind die Kehrseite der Subvention, die Verpflichtung zur Offenlegung einer immer größeren Anzahl eindeutig personenbezogener Angaben der Preis für die Unterstützung.

Trotzdem kann und darf man es nicht bei dieser Feststellung belassen. Für die Europäische Gemeinschaft gilt zwar genauso wie für die nationalen Behörden: Die Inanspruchnahme öffentlicher Mittel ist an eine Überprüfung gebunden. So gesehen, gibt es keine Alternative zur Preisgabe bestimmter, um der Kontrolle willen notwendiger, unter Umständen auch und gerade personenbezogener Informationen. Aus der Vergabe von Subventionen folgt jedoch nicht das Recht, jede Information zu verlangen. Der Hinweis auf die Unterstützung erspart daher keineswegs Überlegungen über den Umfang und die Verwendung der angeforderten Angaben. Zugegeben, die Antwort fällt, sobald man sich auf die Ebene der Europäischen Gemeinschaft begibt, nicht leicht. Simplifizierte Schlüsse von der nationalen Regelung auf die supranationalen Informationsanforderungen verbieten sich. Anders ausgedrückt: Die vom Grundgesetz geforderte und vom Bundesverfassungsgericht bestätigte informationelle Selbstbestimmung ist keine ohne weiteres auf die Informationsverarbeitung der Gemeinschaft übertragbare Voraussetzung.

Bei jeder weiteren Überlegung gilt es vielmehr zweierlei zu berücksichtigen: Die früheren Tätigkeitsberichte haben wiederholt auf die Bemühungen des Europäischen Parlaments, den Datenschutz weiterzuentwickeln und eine einheitliche Regelung innerhalb der Gemeinschaft sicherzustellen, aber auch auf die immer wieder geäußerte Bereitschaft der EG-Kommission verwiesen, sich für den Datenschutz einzusetzen. Mag sein, daß es einstweilen zu nicht mehr gekommen ist, als zu einem Appell an die Mitgliedsländer, die Datenschutzkonvention des Europarates zu ratifizieren. Damit wird, wenigstens mittelbar, die Notwendigkeit akzeptiert, ein Mindestmaß an Datenschutz-

grundsätzen einzuhalten, angefangen bei der Zweckbindung, über eine Reihe konkreter Anforderungen an den Verarbeitungsprozeß bis hin zu einzelnen, den Betroffenen ausdrücklich eingeräumten Rechten. Die Kommission kann aber schlecht die Mitgliedsländer auffordern, den in der Konvention festgehaltenen Anforderungen zu entsprechen, genau diese Erwartungen jedoch in ihrem ureigenen Bereich gar nicht erst zur Kenntnis nehmen. Sicher, eine eigene, interne Regelung ist längst fällig. Man braucht nur an die Daten der Beschäftigten zu denken. Unabhängig davon muß sich jedoch die Kommission fragen, welche Konsequenzen ihre Informationserwartungen für die Verarbeitung personenbezogener Daten haben. Noch genauer: Überlegungen zu den verschiedenen Richtlinien lassen sich von einer Auseinandersetzung über die Art der jeweils verlangten Information, deren Umfang und deren Verwendung nicht trennen. Sicher ist es begrüßenswert, wenn sich der Hessische Minister für Landwirtschaft und Forsten bereit erklärt, die etwa im Zusammenhang mit der "Weinbaukartei" erhobenen Daten nur anonymisiert weiterzugeben. Doch kann und darf es nicht der Initiative der einzelnen nationalen Behörden überlassen bleiben, darüber zu entscheiden, wie der Verarbeitungsprozeß genau verlaufen muß. Schon deshalb, weil Meinungsverschiedenheiten und Komplikationen spätestens dann auftauchen dürften, wenn es um die konkret zu erhebenden Daten geht. Gemeinschaft und Kommission sind deshalb verpflichtet verbindliche Grundsätze zu formulieren und genauso wie die nationalen Instanzen die eigenen Informationserwartungen zu überprüfen, um die Verarbeitung personenbezogener Daten auf das wirklich erforderliche Maß zu beschränken.

Und noch etwas: Das Bundesverfassungsgericht hat erst jüngst klargestellt, daß es Aufgabe der Gemeinschaft, vor allem der Rechtsprechung des Europäischen Gerichtshofs ist, einen wirksamen Grundrechtsschutz im Rahmen der Gemeinschaftsaktivitäten zu gewährleisten. Das Bundesverfassungsgericht hat zur Begründung unter anderem darauf verwiesen, daß sich inzwischen alle Hauptorgane der Gemeinschaft dazu bekannt haben, die Grundrechte so wie sie sich insbesondere aus der Europäischen Menschenrechtskonvention ergeben, zu achten. Für die Anwendung der Konvention ist aber der Datenschutz nicht gleichgültig. Im Gegenteil, die Straßburger Rechtsprechung hat in letzter Zeit wiederholt bestätigt, daß eine korrekte Anwendung der Konvention gerade den Respekt vor den fundamentalen Datenschutzerfordernissen umfaßt, so wie sie etwa in der Konvention des Europarates zum Ausdruck kommen. Auch deshalb ist die Kommission verpflichtet, die bisherigen Verarbeitungsanforderungen zu revidieren und sich über datenschutzbedingte Einschränkungen ihrer Informationserwartungen klarzuwerden. Unabhängig davon gilt es, jetzt schon zu überlegen, wie sowohl die Betroffenen als auch die nationalen Behörden reagieren können, um die Verarbeitung personenbezogener Daten in Kenntnis des jeweiligen Verarbeitungszwecks und unter Berücksichtigung möglicher Alternativen zu beschränken. Dazu gehört auch die Frage, ob die Gemeinschaft wirklich alle jeweils erhobenen Angaben benötigt und ob ihren Anforderungen nicht doch in aller Regel mit anonymisierten Daten genügt werden kann.

1.4.2

Genomanalyse und Datenschutz

Spätestens seit den ersten, 1984 angestellten Überlegungen im Rahmen des Europarates, die auch durch den jüngst vorgelegten Bericht der Enquete-Kommission "Chancen und Risiken der Gentechnologie" bestätigt wurden, zeichnet sich ein neuer wichtiger Anwendungsbereich des Datenschutzes ab: die Verarbeitung der im Zusammenhang mit Genomanalysen erhobenen Daten. Sicher, die Diskussion über die genetischen Testverfahren ist in vielerlei Hinsicht noch in ihren Anfängen. Eines steht dennoch außer Frage: Genetische Testverfahren, gleichviel wie man sie im einzelnen beurteilen mag, sind eine personenbezogene Informationsquelle, ganz gleich ob man die pränatale Diagnostik, das Neugeborenenenscreening oder die Genomanalyse bei Arbeitnehmern nimmt. In dem Augenblick, in dem solche Verfahren entwickelt, akzeptiert und praktiziert werden, wird die Voraussetzung für die Verarbeitung zusätzlicher, überaus sensibler Informationen über den einzelnen geschaffen. Sie mag in einer Vielzahl von Fällen, etwa für die Früherkennung und die bessere Behandlung bestimmter Krankheiten, gerade aus der Perspektive des Betroffenen von großer Bedeutung sein. Sie eignet sich aber genauso gut als Grundlage für weitreichende, tief in die Existenz des einzelnen eingreifende Entscheidungen. Das Spektrum ist breit: Es reicht von einem Eingriff in die Beschäftigungsmöglichkeit von Arbeitsplatzbewerbern mit Hilfe der Genomanalyse bis hin zu generellen bevölkerungspolitischen Maßnahmen. Doch damit nicht genug. Die genetische Analyse wirft neue Probleme auch in Bereichen auf, in denen die Entwicklung der Informationstechnologie jetzt schon den Datenschutz vor immer kompliziertere Probleme stellt. Mit das beste Beispiel ist der Sicherheitsbereich. Über die "genetischen Fingerabdrücke" eröffnen sich ganz neue Möglichkeiten Straftäter zu überführen aber auch Dateien über Verdächtige zusammenzustellen. Und die genetische Analyse von Tatspuren verändert zutiefst den Inhalt und die Tragweite der polizeilichen Unterlagen.

Zudem: Gerade die Erfahrung mit der Informationstechnologie zeigt, daß sich schnell und leicht Gründe finden lassen, um neue Informationsmethoden, sei es auch nur "probeweise" zu nutzen. Wer will etwa ernsthaft bestreiten, daß eine Genomanalyse auch und gerade im Interesse der Beschäftigten in einem chemischen Werk liegt. Und wie lange wird man sich der Forderung entziehen können, nach gefährlichen Straftätern mit Hilfe genetischer Informationen zu fahnden? Im übrigen, das Argument, alles sei noch so ungewiß und abgesehen davon mit erheblichen Kosten verbunden, zieht hier genausowenig wie bei der Automatisierung der Datenverarbeitung.

Weder ist ein ganz bestimmtes Entwicklungsstadium erst abgewartet worden, noch hat man sich von den Kosten abschrecken lassen. Sie haben allenfalls dazu geführt, sich zunächst auf einzelne Anwendungsbereiche zu beschränken. Die Konsequenz kann unter diesen Umständen nur sein: Es darf nicht zu einer Diskussion kommen, die um einer angeblich besseren Information willen, zunächst die gleichsam technischen Aspekte aufgreift und die datenschutzrechtlichen Aspekte auf ein späteres Stadium verweist. Beides läßt sich nicht voneinander trennen und deshalb auch nicht sukzessiv diskutieren. Vielmehr gilt es, die "nur"-technischen Probleme von Anfang an unter Einbeziehung der möglichen Folgen einer Verarbeitung der genetischen Daten zu besprechen. Ganz zu Recht hat deshalb die Enquete-Kommission ausdrücklich auf die Datenschutzprobleme aufmerksam gemacht und jetzt schon eine eingehende Erörterung gefordert. Jede Verschiebung verändert die Chancen auch und gerade im Hinblick auf die Verarbeitung genetischer Angaben die Anwendung der verfassungsrechtlich begründeten Anforderungen an den Zugriff und die Verwendung personenbezogener Daten sicherzustellen. Noch einmal: Es bereitet keine Schwierigkeiten, Gründe dafür anzugeben, warum alle Nutzungsmöglichkeiten der Gentechnologie offengehalten, ja tendenziell in Anspruch genommen werden müssen. Sehr viel schwieriger ist es dagegen, der Faszination einer Technologie zu widerstehen, die scheinbar alle Voraussetzungen mit sich bringt, um gesundheitliche und soziale Risiken in einem nie dagewesenen Maß zu verringern.

So wenig sich freilich die Diskussion über die Datenschutzvorkehrungen verschieben läßt, so sehr gilt es, sich von Anfang an davor zu hüten, die Probleme zu unterschätzen. Sicher können viele der bisherigen Erfahrungen und Regelungen verwertet werden. Die Verarbeitung genetischer Angaben bringt aber auch Fragen mit sich, die sich jedenfalls in dieser Form bisher nicht gestellt haben. So dürften sich die einzelnen Daten sehr oft auf mehrere Personen beziehen. Weder die Informationspflichten noch die Entscheidungsrechte können deshalb so einfach wie bisher zugeordnet werden. Von der Benachrichtigung, über die Auskunft bis hin zur Sperrung und Löschung müssen Verfahren entwickelt werden, die auf die Pluralität der Betroffenen Rücksicht nehmen und zudem flexibel genug sind, um differenzierte Reaktionen zuzulassen. Darüber hinaus darf die Belastung, die mit der Erhebung und Kenntnis vieler dieser Daten einhergeht, nicht übersehen werden. Genetische Testverfahren konfrontieren den Betroffenen, wie sich etwa am Beispiel der Untersuchung von Neugeborenen zeigt, zu einem sehr frühen Zeitpunkt mit einer für ihn unter Umständen sehr nachteiligen Information und verändern schon deshalb seine gesamte Lebensperspektive. In mancher Beziehung wiederholen sich insoweit die im Zusammenhang mit der Aids-Infektion sichtbar gewordenen Probleme. Einmal mehr geht es daher nicht an, sich mit den mittlerweile üblichen Datenschutzvorkehrungen zufriedenzugeben. Vielmehr gilt es die Gefahr sowie die Folgen einer sozialen Isolierung und Stigmatisierung offen anzusprechen und sich von Anfang an eingehend mit möglichen Gegenmaßnahmen auseinanderzusetzen.

Kurzum, mehr noch als die ständige Verfeinerung der Datenverarbeitung zwingt die gentechnische Analyse zu der Einsicht, daß die gegenwärtigen Datenschutzvorkehrungen nur eine Durchgangsregelung sind, die Glaubwürdigkeit und die Wirksamkeit des Datenschutzes also von der Fähigkeit abhängen, rechtzeitig auf die Probleme der gentechnischen Analyse zu reagieren und auch in Anbetracht ihrer Konsequenzen eine Regelung sicherzustellen, die eine transparente, kontrollierbare und die Manipulation des einzelnen ausschließende Verarbeitung gewährleistet.

2. Novellierung der Datenschutzgesetze

2.1

Die Vorgaben des Bundesverfassungsgerichts

Das neue Hessische Datenschutzgesetz ist am 6. November 1986 vom Landtag verabschiedet worden. Es trat am 1. Januar 1987 in Kraft (Gesetz vom 11. November 1986, GVBl. I S. 309). Damit ist Hessen das erste Bundesland, das nicht nur in Teilbereichen, sondern für das gesamte Gebiet seines Datenschutzrechts Konsequenzen aus dem Volkszählungsurteil des Bundesverfassungsgerichts vom 15. Dezember 1983 gezogen hat. Kernpunkt dieser Entscheidung war die Bekräftigung, daß dem Bürger von Verfassungs wegen ein "informationelles Selbstbestimmungsrecht" zusteht, daß der einzelne die Befugnis hat, grundsätzlich selbst über die Preisgabe und Verwendung seiner Daten zu bestimmen. Für Eingriffe in dieses Recht, die aufgrund überwiegender Interessen der Allgemeinheit notwendig sind, verlangte das Bundesverfassungsgericht präzise, klar gefaßte gesetzliche Regelungen, die Umfang und Zweck der Erhebung und Verwendung persönlicher Daten im einzelnen festlegen. Besonderes Gewicht legte das höchste deutsche Gericht auch auf die Verbesserung der Aufklärungs-, Auskunfts- und Lösungsrechte.

Einigkeit besteht in der Datenschutzdiskussion darüber, daß der Schwerpunkt der Gesetzgebungsarbeit auf den bereichsspezifischen Regelungen liegen muß, die zugeschnitten auf die spezifischen Verarbeitungsbedingungen in den unterschiedlichen Bereichen von Verwaltung und Wirtschaft die Zulässigkeit des Umgangs mit personenbezogenen Daten bestimmen. Dementsprechend ist in den letzten drei Jahren in Bund und Ländern eine Fülle einschlägiger Rechtsvorschriften für Teilgebiete der Verwaltung verabschiedet und sind für andere Bereiche Gesetz- und Verordnungsentwürfe vorgelegt worden (vgl. beispielsweise Ziff. 5.1, 6.4, 8.1).

Legt man das Schwergewicht auf die Verbesserung des bereichsspezifischen Datenschutzes, bedeutet dies keineswegs, die Rolle und Bedeutung der allgemeinen Datenschutzgesetze des Bundes und der Länder bei den Novellierungsbemühungen zu unterschätzen. Zum einen deshalb, weil sie als Auffang- oder Rahmengesetze ergänzend die Punkte regeln, die generell alle Verarbeitungsbereiche betreffen, wie etwa die Kontrollbefugnisse der Datenschutzbeauftragten oder die technischen und organisatorischen Maßnahmen der Datensicherung.

Die Schaffung bereichseigener Verarbeitungsvorschriften ist außerdem ein allmählicher Prozeß, der sich noch über Jahre hinziehen wird; in dieser Zeit muß nach wie vor auf die Bestimmungen der allgemeinen Datenschutzgesetze der Länder und des Bundes zurückgegriffen werden. Für Hessen heißt dies konkret: Krankenhäuser, Statistik und Polizei sind die Verarbeitungsbereiche, bei denen nicht nur die Notwendigkeit einer besonderen Regelung feststeht, sondern schon Gesetzentwürfe der Ressorts vorliegen (zum Krankenhausgesetz vgl. Ziff. 4.1, zum Landesstatistikgesetz vgl. Ziff. 8.1, zur Änderung des Hessischen Gesetzes über die öffentliche Sicherheit und Ordnung vgl. Ziff. 4.3 des 14. Tätigkeitsberichts). Ganz gleich aber, wie die Gesetzgebung weiter verläuft, das Hessische Datenschutzgesetz legt auch für diese Bereiche das verbindliche Mindestmaß an Datenschutz fest.

Schließlich enthalten die Datenschutzgesetze ohnehin nicht nur Normen, die quer durch die Verarbeitungsbereiche Anwendung finden, sondern auch eine Vielzahl von Bestimmungen, die Ergänzungen oder Ausnahmen für bestimmte Zweige der öffentlichen Verwaltung vorsehen, wie etwa die Beschränkung des Einsichtsrechts des Bürgers in das Dateienregister bei gewissen Datensammlungen der Sicherheitsbehörden oder Sonderregelungen für den Rundfunk und die Sparkassen (vgl. Ziff. 2.2.3).

2.2

Das neue Hessische Datenschutzgesetz

2.2.1

Gesetzgebungsverfahren

Beratungsgrundlage für den Hessischen Landtag war der Gesetzentwurf der Landesregierung vom 26. November 1985 (Landtags-Drucks. 11/4749). Ihm vorausgegangen war der Referentenentwurf des Hessischen Ministers des Innern vom 5. Februar 1985, zu dem eine große Zahl von Stellungnahmen von Behörden und Interessenverbänden eingegangen war. Am 4. Juni 1985 hatte ich eine Fülle von Korrektur-, Ergänzungs- und Gegenvorschlägen unterbreitet und in meinem 14. Tätigkeitsbericht in synoptischer Darstellung zum Regierungsentwurf veröffentlicht (Ziff. 10).

Von meinen Anregungen sind im Gesetzgebungsverfahren die meisten berücksichtigt worden. Einige für mich zentrale Punkte sind allerdings nicht in das Gesetz aufgenommen worden. So sollten etwa nach meinen Vorstellungen der Verwaltung weniger Möglichkeiten zur Datenerhebung ohne Kenntnis und Mitwirkung des Betroffenen eingeräumt werden, als dies jetzt in § 12 geregelt ist. Auch hatte ich eine verschärfte Zweckbindung bei der Datenverwendung befürwortet, die eine Abweichung vom ursprünglichen Erhebungszweck nur bei Vorliegen einer entsprechenden gesetzlichen Regelung zugelassen hätte.

Insgesamt ist der Gesetzestext gegenüber der Regierungsvorlage grundlegend umgestaltet worden, wobei die zahlreichen Änderungen in den intensiven Ausschußberatungen zum großen Teil von allen Fraktionen akzeptiert wurden. Auch wenn eine Reihe weitergehender Vorstellungen in den parlamentarischen Beratungen nicht realisiert werden konnte, verbessert das neue Hessische Datenschutzgesetz in der Gesamtbewertung zweifellos ganz entscheidend die Rechtsstellung des Bürgers gegenüber den Behörden, die Angaben über ihn verarbeiten, was sicherlich auch über die Landesgrenzen hinweg Vorbildwirkung haben wird.

Für die Verwaltung bringt das novellierte Gesetz eine Reihe neuer Pflichten, die sie beim Umgang mit personenbezogenen Daten zu beachten hat. Dafür sind andere Verpflichtungen, die sich nicht bewährt haben, wie etwa die zur Veröffentlichung von Dateien, weggefallen. Bei den Gesetzesberatungen wurde großer Wert darauf gelegt, daß das HDSG auch in seiner neuen Fassung für die Verwaltung praktikabel bleibt und damit die Voraussetzungen für Akzeptanz und Anwendungsbereitschaft beim einzelnen Sachbearbeiter erhalten bleiben. Um die hessischen

Behörden und ihre Bediensteten rechtzeitig über die neue Rechtslage zu informieren, hat der Hessische Minister des Innern am 1. Dezember 1986 einen Einführungserlaß zum novellierten Hessischen Datenschutzgesetz herausgegeben (StAnz. 1986 S. 2382). Dem gleichen Zweck dient auch die von mir Ende November herausgegebene HDSG-Broschüre (vgl. Ziff. 2.2.6).

2.2.2

Leitprinzipien

Die wichtigsten Leitprinzipien der Neuregelung sind:

- die Transparenz der Datenverarbeitung,
- die Zweckbindung der Datenverwendung und
- die Einbeziehung der Akten in den Anwendungsbereich des Gesetzes.

Um die Transparenz der Datenverarbeitung für den Bürger, aber auch für die datenverarbeitenden Stellen selbst und den Hessischen Datenschutzbeauftragten herzustellen, sieht das novellierte Hessische Datenschutzgesetz eine Reihe neuer Maßnahmen vor. Einige Beispiele: Bei der Datenerhebung gilt der Vorrang der direkten Befragung des Bürgers vor der Informationsermittlung bei dritten Personen oder Stellen. Die Ansprüche auf Auskunft und Akteneinsicht werden erweitert. Von der erstmaligen Computerspeicherung wird jeder Bürger benachrichtigt. In einer ausführlichen Beschreibung wird für jede Datei der Verarbeitungsrahmen festgelegt. Über alle Verfahrensentwicklungen ist der Hessische Datenschutzbeauftragte rechtzeitig und umfassend zu unterrichten.

Zweckbindung bedeutet, daß sich die Datenverwendung prinzipiell an den von der Behörde vorher festgelegten, dem Bürger bei der Erhebung offengelegten Zweck halten muß. Werden vom Bürger Daten verlangt, ist er über den Zweck der Erhebung aufzuklären. Für jede Datei muß vor der Errichtung die Zweckbestimmung festgeschrieben werden. Nur so viele Daten dürfen verarbeitet werden, wie nicht nur allgemein zur Erfüllung der behördlichen Aufgabe, sondern - enger - zur Erfüllung des spezifischen Zwecks erforderlich sind. Für die Fälle, in denen abweichend vom Zweckbindungsgrundsatz die Datenverwendung auch für andere oder erweiterte Zwecke möglich sein muß, stellt das Gesetz einen abschließenden Katalog auf.

Mit der Einbeziehung der Akten schließlich wird der für den Bürger völlig unverständliche, unhaltbare Zustand beseitigt, daß wichtige Zulässigkeitsvorschriften ebenso wie Rechte des Betroffenen von der Verarbeitungsform abhängen, und der einzelne nur deshalb einen geringeren Schutz seiner Daten gewärtigen muß, weil diese sich in Unterlagen zwischen Aktendeckeln und nicht in manuellen oder automatisierten Dateien befinden.

2.2.3

Anwendungsbereich

2.2.3.1

Sonderregelungen für bestimmte öffentliche Stellen

Für eine Reihe datenverarbeitender Stellen auf Landes- wie auf Kommunalebene gelten einzelne Bestimmungen oder ganze Teile des HDSG nicht. Für Sozialleistungsträger nach dem Sozialgesetzbuch bleibt es dabei, daß die Zulässigkeit der Datenverarbeitung sich nach den speziellen Vorschriften über das Sozialgeheimnis sowie ergänzend dazu nach den Normen des 1. und 2. Abschnitts des Bundesdatenschutzgesetzes richtet (§ 79 Abs. 1 und 3 SGB X). Der völlig neugefaßte Erste Teil des HDSG (§§ 1 - 20) findet mit anderen Worten auf die gesetzlichen Krankenkassen, die Sozial- und Jugendämter usw. keine Anwendung, wohl aber der Zweite Teil, der die Stellung und Befugnisse des Hessischen Datenschutzbeauftragten - und zwar jetzt erweitert - festlegt. Zur Verdeutlichung nur zwei Konsequenzen: Die Sozialleistungsträger trifft keine Benachrichtigungspflicht nach § 18 Abs. 2 HDSG; sie müssen auch kein Geräteverzeichnis anlegen (§ 6 Abs. 3 HDSG). Auf der anderen Seite unterliegen die Sozialbehörden des Landes und der Gemeinden bzw. Kreise wie bisher der Kontrollbefugnis des Hessischen Datenschutzbeauftragten. Dementsprechend muß die Meldung zum Dateienregister in der erweiterten Form des § 6 Abs. 1 HDSG erfolgen (§ 26 Abs. 1 Satz 1 HDSG).

Soweit öffentlich-rechtliche Unternehmen am Wettbewerb teilnehmen, gelten für sie nur der Zweite Teil sowie die §§ 34 bis 36 des HDSG (§ 3 Abs. 7 HDSG). Es bleibt also wie bisher bei dem Prinzip, daß im Hinblick auf die Zulässigkeit der Datenverarbeitung und die Rechte des Betroffenen öffentlich-rechtliche Unternehmen und solche der Privatwirtschaft gleichgestellt und einheitlich nach dem Bundesdatenschutzgesetz behandelt werden sollen. Allerdings ist für die Überwachung der Einhaltung des Datenschutzes jetzt durchgängig der Hessische Datenschutzbeauftragte zuständig. Die Anwendbarkeit des Zweiten Teils des Gesetzes hat zur Folge, daß auch die öffentlich-rechtlichen Wettbewerbsunternehmen - dazu gehören etwa die Stadt- und Kreissparkassen - ausnahmslos zum Dateienregister des Hessischen Datenschutzbeauftragten melden müssen, und zwar mit dem gegenüber der bisherigen Rechtslage erweiterten Inhalt des § 6 Abs. 1 HDSG.

2.2.3.2

Vorrang bereichsspezifischer Datenschutzvorschriften

Für alle hessischen datenverarbeitenden Stellen gilt darüber hinaus generell das Prinzip, daß besondere Rechtsvorschriften über den Datenschutz in Einzelgesetzen den Bestimmungen des HDSG vorgehen (§ 3 Abs. 3 Satz 1 HDSG). Dabei ist in jedem Einzelfall genau zu prüfen, welche Normen des HDSG durch die speziellere Vorschrift verdrängt werden.

Für die Meldebehörden etwa legt das Landesmeldegesetz im einzelnen fest, welche Daten über den Bürger sie erheben und speichern dürfen; insoweit bedarf es mithin keiner Prüfung des Datenkatalogs an Hand des Maßstabs der Erforderlichkeit zur Aufgaben- bzw. Zweckerfüllung (§ 11 Abs. 1 HDSG). Ein anderes Beispiel: Hat der Gesetzgeber die Information des Bürgers über die Verarbeitung seiner Daten im Spezialgesetz bereits ausdrücklich geregelt (vgl. etwa §§ 9, 34 Abs. 2 Satz 2 Hessisches Meldegesetz), treten insoweit das Auskunftsrecht und die Benachrichtigungspflicht nach § 18 HDSG zurück.

2.2.4

Verbesserung der Bürgerrechte

2.2.4.1

Erhebung beim Betroffenen (§ 12)

Personenbezogene Daten sind grundsätzlich beim Betroffenen mit seiner Kenntnis zu erheben. Dabei ist er über den Zweck der Datenerhebung sowie ggf. über die Empfänger der Angaben aufzuklären. Der Betroffene ist darauf hinzuweisen, daß die Offenbarung seiner Angaben auf einer Rechtspflicht beruht oder freiwillig geschieht. Dieses Prinzip soll dem einzelnen transparent machen, welche Behörde was und aus welchem Grund über ihn weiß.

Die Ausnahmen von diesem Grundsatz sind abschließend in Fallgruppen aufgeführt, etwa wenn sich Anhaltspunkte für Straftaten oder Ordnungswidrigkeiten ergeben oder Angaben eines Bürgers in einem von ihm gestellten Antrag überprüft werden müssen. Auch wenn jedoch ein solcher Ausnahmefall vorliegt, in dem eine Behörde bei einer anderen öffentlichen Stelle Informationen ohne Kenntnis des Betroffenen einholen darf, muß sie immer erst prüfen, ob sie diese Erkenntnisse nicht durch direkte Befragung des Bürgers beschaffen kann.

Diese Prüfungspflicht gilt erst recht in den Ausnahmesituationen, in denen es um eine gleichsam "verdeckte" Datenerhebung geht, in denen ohne Kenntnis des Bürgers beispielsweise seine Nachbarn befragt oder sein Grundstück bzw. Geschäftsbetrieb kontrolliert werden. Das Gesetz läßt sie nur zu, wenn eine Rechtsvorschrift dies vorsieht oder der Schutz von Leben und Gesundheit oder die Abwehr einer erheblichen Gefährdung der natürlichen Lebensgrundlagen es gebieten. Eine solche Konstellation ist allerdings nur denkbar, wenn der Betroffene durch eine direkte Befragung gewarnt würde und belastende Vorgänge oder Tatsachen dann verschleiern bzw. beseitigen könnte. Auch dann jedoch muß er nachträglich benachrichtigt werden, sobald dies ohne Gefährdung des Erhebungszwecks möglich ist.

2.2.4.2

Auskunft (§ 18 Abs. 1)

Jedermann kann nicht nur wie bisher kostenlos von jeder datenverarbeitenden Stelle Auskunft darüber verlangen, welche Daten sie zu seiner Person in manuellen oder automatisierten Dateien gespeichert hat. Das neue Gesetz erweitert das Auskunftsrecht auch auf den Zweck und die Rechtsgrundlage der Datenspeicherung. Ist auch die Herkunft der Daten gespeichert, also die Person oder Stelle, die die Information weitergegeben hat, ist auch diese mitzuteilen.

2.2.4.3

Akteneinsicht (§ 18 Abs. 4)

Erstmals wird dem Bürger grundsätzlich ein Einsichtsrecht in alle Akten zugebilligt, die entweder namensbezogen zu seiner Person geführt werden oder als Sachakten oder Vorgangsakten Unterlagen über ihn enthalten. Bisher galt das Akteneinsichtsrecht nur im Rahmen eines Verwaltungsverfahrens und bei Nachweis eines rechtlichen Interesses (vgl. § 29 Hessisches Verwaltungsverfahrensgesetz). Allerdings ist dieses Akteneinsichtsrecht in mehrfacher Hinsicht abgeschwächt: So kann z.B. der Betroffene dann keinen direkten Einblick in die Akten nehmen und muß sich mit einer Auskunft begnügen, wenn in der Akte Angaben über Dritte enthalten sind, deren Abtrennung nicht möglich ist.

2.2.4.4

Begründung der Auskunftsverweigerung (§ 18 Abs. 5)

Das Auskunftsrecht für in Dateien gespeicherte Daten (vgl. Ziff. 2.2.4.2) besteht im Prinzip gegenüber jeder Behörde, also im Gegensatz zur bisherigen Rechtslage (vgl. § 18 Abs. 2 des alten HDSG) auch gegenüber Polizei, Finanzämtern und Verfassungsschutz. Zwar besteht für diese - ebenso wie für alle anderen - datenverarbeitenden Stellen die Möglichkeit, nach Abwägung zwischen dem Informationsinteresse des Bürgers und dem öffentlichen Interesse an der Geheimhaltung letzteres für vorrangig zu erklären und die Auskunft zu verweigern. Dann müssen jedoch dem Betroffenen die wesentlichen Gründe für die Ablehnung mitgeteilt und muß er auf die Tatsache hingewiesen werden, daß er sich zur Überprüfung der Ablehnung an den Hessischen Datenschutzbeauftragten wenden kann. Entsprechendes gilt für den Anspruch auf Akteneinsicht, wobei hier zusätzlich die generelle Ausnahme für die Gerichte und Staatsanwaltschaften (vgl. § 3 Abs. 3) zu beachten ist, die dem Vorrang bundesgesetzlicher Vorschriften Rechnung trägt. Die Regelung des § 18 Abs. 5 bedeutet den Abschied von der unbegründeten und pauschalen Datenabschottung bestimmter Behörden - vor allem im Sicherheitsbereich - gegenüber dem Bürger.

2.2.4.5

Benachrichtigung (§ 18 Abs. 2)

Werden erstmals Daten einer Person in einer automatisierten Datei gespeichert, erhält sie künftig darüber eine schriftliche Benachrichtigung. In dieser Benachrichtigung wird der Betroffene u.a. darüber informiert, welche Datenarten zu welchem Zweck und auf welcher Rechtsgrundlage wie lange gespeichert werden. Diese Unterrichtung gibt dem Bürger Gelegenheit, mit Hilfe seines Auskunftsrechts die über ihn registrierten Einzeldaten zu erfragen und ggf. die Berichtigung und Löschung von der datenverarbeitenden Stelle zu verlangen.

2.2.4.6

Berichtigung bei Datenempfängern (§ 19 Abs. 5)

Sind falsche Daten berichtigt worden, sind unverzüglich alle Stellen zu unterrichten, denen die Daten übermittelt wurden. Gleiches gilt für Angaben, die ohne Rechtsgrundlage oder in sonstiger Weise unzulässig verarbeitet wurden und deshalb gelöscht werden mußten. Damit soll verhindert werden, daß die Rechte des Bürgers zwar gegenüber der datenverarbeitenden Stelle selbst greifen, die Falschinformationen über ihn jedoch in den Akten oder Dateien anderer Stellen weiter aufgezeichnet bleiben und verwendet werden.

2.2.4.7

Schadensersatz (§ 20)

Der Anspruch auf Schadensersatz in Fällen unzulässiger Datenverarbeitung geht jetzt bis zu dem Maximalbetrag von DM 500.000,-. Nach dem alten Gesetz konnten höchstens DM 250.000,- geltend gemacht werden.

2.2.4.8

Anrufung des Hessischen Datenschutzbeauftragten (§ 28)

Was die Möglichkeit des einzelnen angeht, den Hessischen Datenschutzbeauftragten zur Klärung von Zweifelsfragen und zur Überprüfung von Beschwerden einzuschalten, enthält das Gesetz zwei wichtige Neuerungen. Zunächst wird klargestellt, daß kein Bürger deshalb benachteiligt werden darf, weil er sich an den Datenschutzbeauftragten gewandt hat. Für Behördenmitarbeiter wird bekräftigt, daß sie ohne die häufig umständliche und zeitraubende Einhaltung des Dienstwegs direkt mit dem Datenschutzbeauftragten in Kontakt treten können. Nur so läßt sich sicherstellen, daß der Datenschutzbeauftragte schnell und unbürokratisch auf allen Verwaltungsebenen effizient beraten und Hilfestellung geben kann.

2.2.5

Konsequenzen für die hessischen Behörden

2.2.5.1

Akten (§ 2 Abs. 2,6)

Das neue Hessische Datenschutzgesetz bezieht die Akten in seinen Anwendungsbereich ein und zielt damit auf einen im Prinzip einheitlichen Datenschutz ab, gleich ob die Daten des Bürgers bei den Behörden in schriftlichen Unterlagen oder in Computern aufgezeichnet sind. Das bisherige Hessische Datenschutzgesetz galt nur für die dateimäßige Verarbeitung, selbst wenn eine Reihe von Geheimhaltungsbestimmungen aus anderen Gesetzen auch

bisher schon für in Akten enthaltene Angaben anzuwenden war, wie etwa das Arzt- oder das Statistikgeheimnis oder die allgemeine Amtsverschwiegenheit. Allerdings trifft das Gesetz für Behördenakten Sonderregelungen dort, wo die praktische Durchführbarkeit dies erfordert, etwa beim Einsichtsrecht oder bei der Löschung (§§ 18 Abs. 4, 19 Abs. 6).

2.2.5.2

Behördlicher Datenschutzbeauftragter (§ 5 Abs. 2, 3)

Jede datenverarbeitende Stelle hat künftig von Gesetzes wegen einen behördeninternen Beauftragten für den Datenschutz zu bestellen. Er soll die Behördenleitung bei der Durchführung des Datenschutzes innerhalb der Dienststelle unterstützen. Zu seinen Aufgaben gehört u.a. die Mitwirkung bei der Aufstellung des Geräteverzeichnisses, der Meldung zum Dateienregister des Hessischen Datenschutzbeauftragten und bei der Überwachung der Datensicherungsmaßnahmen. Bisher galt die Bestellungspflicht nur für Landesbehörden und nur aufgrund eines Erlasses; Kommunen konnten freiwillig einen Beauftragten benennen. Eine Sonderregelung ist für kleine Behörden, insbesondere kleine Kommunen, getroffen worden. Der behördeninterne Beauftragte darf in keinem Interessenkonflikt mit sonstigen dienstlichen Aufgaben stehen. Diese Bedingung schließt beispielsweise den Leiter des Rechenzentrums sowie alle sonstigen Bediensteten, die maßgebliche Entscheidungsbefugnisse über die Verarbeitung von personenbezogenen Daten aufgrund ihrer Funktion oder ihrer hierarchischen Stellung innerhalb der Behörde haben, von dieser Aufgabe aus.

2.2.5.3

Geräteverzeichnis (§ 6 Abs. 3)

Jede öffentliche Stelle muß ein Verzeichnis der Geräte, mit denen personenbezogene Daten verarbeitet werden, führen und auf dem neuesten Stand halten. Dieses Verzeichnis enthält u.a. Typ, Art und Anzahl der eingesetzten DV-Geräte sowie die Möglichkeiten zur Datenübertragung und -fernverarbeitung. Dieses Register bietet zum einen der Amtsleitung selbst eine Übersicht über die ihr zur Verfügung stehende DV-technische Infrastruktur, zum anderen dem Hessischen Datenschutzbeauftragten ein wichtiges Hilfsmittel für die Datenschutzkontrolle.

2.2.5.4

Unterrichtungspflicht (§ 9)

Bisher mußte jede bei der Datenverarbeitung beschäftigte Person förmlich auf das Datengeheimnis verpflichtet werden (§ 9 Abs. 2 des alten HDSG). Diese Verpflichtung ist abgeschafft; sie war vielfach zur leeren Förmlichkeit geworden. Dafür ist jede Behörde gehalten, ihre Bediensteten über die bei deren Tätigkeit zu beachtenden Datenschutzvorschriften zu unterrichten. Diese Information soll sich vor allem auf die konkreten Auswirkungen des Hessischen Datenschutzgesetzes und der bereichsspezifischen Bestimmungen auf den speziellen Arbeitsplatz des jeweiligen Beschäftigten beziehen, muß also je nach inhaltlichem Arbeitsbereich und Stellung in der Behördenhierarchie unterschiedlich ausgestaltet sein.

2.2.5.5

Erhebung beim Betroffenen (§ 12)

Einer der Kernpunkte des neuen Hessischen Datenschutzgesetzes ist der Grundsatz, daß Daten beim Betroffenen mit seiner Kenntnis zu erheben sind. In allen Fällen der Informationsbeschaffung bei Dritten, ob bei anderen Behörden oder privaten Stellen und Personen, ist zunächst zu prüfen, ob die erwünschten Angaben nicht direkt beim betroffenen Bürger erfragt werden können (vgl. oben Ziff. 2.2.4.1). Formulare sind so zu gestalten, daß nicht nur - wie bisher - auf die die Auskunftspflicht begründende Rechtsvorschrift hingewiesen wird, sondern auch der Zweck der Datenerhebung sowie bei beabsichtigten Übermittlungen die Datenempfänger angegeben werden. Werden Informationen zulässigerweise am Betroffenen vorbei ermittelt, muß er nachträglich informiert werden.

2.2.5.6

Zweckbindung (§ 13)

Personenbezogene Daten dürfen grundsätzlich nur für den Zweck weiterverarbeitet werden, für den sie erhoben oder gespeichert worden sind. Die Zweckbindung greift nicht nur bei der Übermittlung nach außen, sondern auch bei der Datenverwendung durch die speichernde Stelle selbst und bei der Datenweitergabe innerhalb von Behörden. Doch gilt die Zweckbindung nicht ausnahmslos; das Gesetz enthält einen Katalog von Abweichungsfällen, etwa wenn dies zur Überprüfung von gestellten Anträgen notwendig ist oder Anhaltspunkte für Straftaten oder Ordnungswidrigkeiten vorliegen, die eine Benachrichtigung der Strafverfolgungsbehörden geboten erscheinen lassen. Als Konsequenz des Zweckbindungsgebots müssen alle Informationsbeziehungen und -flüsse innerhalb und zwischen den datenverarbeitenden Stellen daraufhin überprüft werden, ob die Datenverwendung dem Erhebungszweck entspricht oder die Zweckänderung die Voraussetzungen eines der in § 12 Abs. 2 aufgeführten Ausnahmefälle erfüllt.

2.2.5.7

Benachrichtigung (§ 18 Abs. 2)

Die Pflicht, den Betroffenen über Tatsache, Umfang, Zweck und Rechtsgrundlage der erstmaligen automatisierten Speicherung seiner Daten schriftlich zu benachrichtigen (vgl. oben Ziff. 2.2.4.5), gilt zunächst für alle Speicherrängefälle nach Inkrafttreten des Gesetzes. Zur Verwaltungsvereinfachung kann diese Benachrichtigung zusammen mit der Erhebung erfolgen, d.h. z.B. als Hinweis auf dem Antragsvordruck, der dem Bürger zur Ausfüllung ausgehändigt wird. Darüber hinaus ist jedoch innerhalb von zwei Jahren, also bis Ende 1988, auch über den gesamten gespeicherten "Altbestand" zu informieren (§ 42 Abs. 1).

2.2.5.8

Registermeldung/Veröffentlichung (§ 26)

Wie bisher ist jede speichernde Stelle verpflichtet, ihre personenbezogenen Dateien zum Dateienregister des Hessischen Datenschutzbeauftragten zu melden. Die meldepflichtigen Angaben wurden etwas erweitert; mitzuteilen sind beispielsweise jetzt auch die vorgesehenen Lösungsfristen und die technischen und organisatorischen Datensicherungsvorkehrungen. Dieses Dateienregister wird publiziert. Dafür ist die Veröffentlichungspflicht der Behörden selbst (vgl. § 17 des alten HDSG) entfallen.

2.2.5.9

Auskunftsrecht des Hessischen Datenschutzbeauftragten (§ 29)

§ 29 Abs. 1 HDSG enthält die Klarstellung, daß neben den datenverarbeitenden Stellen auch ihre Auftragnehmer verpflichtet sind, dem Hessischen Datenschutzbeauftragten Auskunft, Akteneinsicht und Zutritt zu den Diensträumen zu gewähren. In der Praxis betrifft diese Formulierung vor allem die Kommunalen Gebietsrechenzentren und die Hessische Zentrale für Datenverarbeitung. Die Klarstellung hatte sich nicht zuletzt deshalb als notwendig erwiesen, weil im Berichtsjahr zwei KGRZen meine Kontrolltätigkeit unter Berufung auf die auch nach dem bisherigen HDSG irriige Rechtsauffassung behindert hatten, wonach sie mir zu Überwachungszwecken angeforderte Ausdrücke mit personenbezogenen Daten nur nach Zustimmung der jeweiligen auftraggebenden Gemeinden überlassen wollten.

2.2.5.10

Information des Hessischen Datenschutzbeauftragten (§ 29 Abs. 3)

Jede datenverarbeitende Stelle muß sicherstellen, daß der Hessische Datenschutzbeauftragte über Verfahrensentwicklungen und Gesetzesvorhaben im Zusammenhang mit der automatisierten Verarbeitung personenbezogener Daten rechtzeitig und umfassend unterrichtet wird. Nur so kann der Datenschutzbeauftragte seine Beratungs- und Kontrollaufgaben wirksam erfüllen, nur so können aber auch die Behörden bei ihren DV-Planungen frühzeitig Datenschutzaspekte einbeziehen und spätere kostspielige Verfahrenskorrekturen vermeiden.

2.2.6

Besonderer Datenschutz

2.2.6.1

Datenverarbeitung für wissenschaftliche Zwecke (§ 33)

Auch der Dritte Teil des neuen Hessischen Datenschutzgesetzes über den "Besonderen Datenschutz" enthält Neuerungen, die bisher bundesweit einmalig sind. Bei der Datenverarbeitung für wissenschaftliche Zwecke (§ 33) galt es, die schwierige Konkordanz von grundgesetzlich garantierter Forschungsfreiheit - einschließlich des dafür notwendigen Zugangs auch zu personenbezogenen Daten - einerseits und dem ebenfalls verfassungsrechtlich verankerten informationellen Selbstbestimmungsrecht andererseits herzustellen und in Gesetzesform zu fassen. Dementsprechend bleibt es zwar bei dem Grundsatz, daß die Datenverwendung und -übermittlung zu Forschungszwecken die Zustimmung der Betroffenen voraussetzt. Wie im bisherigen Gesetz besteht jedoch nach wie vor die Möglichkeit, von der Einwilligung abzusehen, wenn die schutzwürdigen Belange der Betroffenen wegen der Art der Daten oder der Art ihrer Verwendung nicht beeinträchtigt werden (Abs. 1 Satz 1). Diese Voraussetzung kann insbesondere bei frühzeitiger Anonymisierung der Forschungsdaten gegeben sein.

Hinzugekommen ist im neuen Gesetz der weitere Ausnahmefall, daß der Zweck des Forschungsvorhabens überhaupt nicht erreicht werden kann, wenn Einwilligungen der Betroffenen beschafft werden müßten, und zusätzlich das öffentliche Interesse an der Durchführung des Forschungsvorhabens die mögliche Beeinträchtigung schutzwürdiger Belange der Betroffenen erheblich überwiegt (Abs. 1 Satz 2). Gedacht ist mit dieser Vorschrift beispielsweise an die Konstellation, daß der Aufenthalt von Personen, denen eine wichtige wissenschaftliche

Untersuchung gilt, nicht ermittelt werden kann und somit ihre Zustimmung nicht oder nur mit unverhältnismäßigem Ermittlungsaufwand beschafft werden kann (z.B. ins Heimatland zurückgekehrte ausländische Arbeitnehmer).

Den Ausnahmecharakter der Abweichung vom Grundsatz der Einwilligung unterstreicht, soweit Landesbehörden betroffen sind, die Pflicht zur Genehmigung durch das Ministerium mit genauer Festlegung der Einzelheiten und deren Mitteilung an den Hessischen Datenschutzbeauftragten (Abs. 1 Sätze 3 und 4). Darüber hinaus wird generell vorgeschrieben, die Personalien der Betroffenen bei der forschenden Einrichtung so schnell wie möglich getrennt von den eigentlichen Forschungsdaten zu speichern und sie zu löschen, sobald der Forschungszweck erreicht ist, sobald also auf die Herstellung des Personenbezugs verzichtet werden kann (Abs. 2).

2.2.6.2

Arbeitnehmerdatenschutz (§ 34)

2.2.6.2.1

Regelungsinhalt

Sondervorschriften für den Arbeitnehmerdatenschutz, die der besonderen Risikosituation der abhängig Beschäftigten gegenüber der Verarbeitung ihrer Daten durch den Arbeitgeber bzw. Dienstherrn Rechnung tragen, habe ich zu wiederholten Malen angemahnt (vgl. u.a. 12. Tätigkeitsbericht, Ziff. 1.1.3.2 und 3.3; 13. Tätigkeitsbericht, Ziff. 3.3). Dieses Thema bildete auch einen Schwerpunkt des Datenschutz-Symposiums der Hessischen Landesregierung vom September 1984 (dazu 13. Tätigkeitsbericht, Ziff. 3.3.1.2). Der hessische Gesetzgeber hat in diesem Bereich weitreichende Konsequenzen gezogen.

Der neue § 34 verschärft die Zweckbindung für die Verwendung der Daten der im hessischen öffentlichen Dienst Beschäftigten (Abs. 1). Bei Personalinformations- und -datensystemen wird das Auskunftsrecht des einzelnen auf die Art der automatisierten Auswertung ausgeweitet (Abs. 3); der Bedienstete kann also z.B. erfahren, welche Auswertungsläufe auf Veranlassung des Dienstherrn "gefährdet" werden. Nicht mehr benötigte Arbeitnehmerdaten müssen nicht nur gesperrt, sondern gelöscht werden, wenn nicht schutzwürdige Belange für eine weitere Speicherung sprechen (Abs. 4). Medizinische und psychologische Befunde, wie sie etwa bei ärztlichen Untersuchungen in dienst- und arbeitsrechtlichen Angelegenheiten anfallen, dürfen überhaupt nicht in Personaldateisysteme eingespeichert werden, sondern nur wie bisher als Unterlagen in den Personalakten aufbewahrt werden (Abs. 6).

Von großer Bedeutung ist schließlich die strenge Zweckbindung für die Bediener- und Protokolldaten, die an Bildschirmarbeitsplätzen anfallen. Sie dürfen nur zu Zwecken der Datensicherungskontrolle genutzt werden, also beispielsweise um festzustellen, ob ein und ggf. welcher Mitarbeiter unberechtigt auf Datenbestände zugegriffen hat. Der Arbeitgeber bzw. Dienstherr darf diese Informationen jedoch nicht dazu verwenden, durch Vergleich von Zeitpunkt, Dauer und Häufigkeit der Bildschirmnutzung das Verhalten oder die Leistung der Bediensteten zu kontrollieren (Abs. 7).

2.2.6.2.2

Konsequenzen

Mit dem neuen § 34 sind die datenschutzrechtlichen Rahmenbedingungen abgesteckt, nach denen sich jede Planung für eine Automatisierung der Personalverwaltung, gleich ob in Rechenzentren oder mit Hilfe von PC's, richten muß. Was die Landesverwaltung angeht, erinnere ich noch einmal an den Beschluß des Hessischen Landtags zu meinem 12. Tätigkeitsbericht (vgl. Nr. 4 der Beschlußempfehlung des Innenausschusses, Drucks. 11/1551), wonach "der Landtag erwartet, daß ... der weitere Ausbau (von Personalinformationssystemen in der hessischen Landesverwaltung) mit dem Innenausschuß bzw. den Gremien des Landtags diskutiert wird". Der neue § 34 bietet ausreichend Anlaß, daß jedes Ressort eventuelle Automationspläne im Personalbereich gründlich prüft und sich darüber klar wird, wie es sich im einzelnen den Technikeinsatz und die damit zusammenhängenden Datenschutzvorkehrungen vorstellt. In jedem Fall besteht nach § 34 Abs. 5 für alle datenverarbeitenden Stellen die Pflicht, vor Einführung oder Erweiterung von automatisierter Verarbeitung von Bedienstetendaten dem Hessischen Datenschutzbeauftragten u.a. die Art, die Zweckbestimmung, den Umfang und die Sicherung der vorgesehenen Dateien mitzuteilen und ihm Gelegenheit zur Stellungnahme zur vorgelegten Dateibeschreibung zu geben.

2.2.7

Informationsbroschüre

Wie nicht anders zu erwarten, war und ist der Bedarf an detaillierten Informationen über das neue Hessische Datenschutzgesetz innerhalb und außerhalb der Landesgrenzen groß. Ich habe daher Ende November 1986 in größerer Auflage eine Broschüre vorgelegt, die den Text des neuen Gesetzes und eine Übersicht über die

wichtigsten Änderungen gegenüber dem bisherigen Hessischen Datenschutzgesetz enthält. Dieses Heft habe ich einer Vielzahl von Behörden, insbesondere allen Kommunen, aber auch auf Anfrage zahlreichen Einzelpersonen zugesandt. Solange der Vorrat reicht, besteht für jeden Interessierten die Möglichkeit, diese Broschüre bei mir anzufordern (Postfach 31 63, 6200 Wiesbaden).

2.3

Novellierung des Bundesdatenschutzgesetzes (BDSG)

2.3.1

Kritik

Im Gegensatz zu Hessen ist der Regelungsauftrag des Bundesverfassungsgerichts auf Bundesebene, d.h. in bezug auf das Bundesdatenschutzgesetz (BDSG), bislang nicht umgesetzt worden. Sicher, der Gesetzentwurf der Koalition (Entwurf der Fraktionen von CDU/CSU und F.D.P., Bundestags-Drucks. 10/4737, S. 5 ff.; textgleich der Entwurf der Bundesregierung, Bundestags-Drucks. 10/5343) enthält eine Reihe positiver Ansätze zu längst fälligen Korrekturen des Datenschutzrechts. So wird wenigstens im Grundsatz die Zweckbindung der Verarbeitung personenbezogener Daten aufgenommen. Die Auskunft über die gespeicherten Angaben soll nach diesen Vorschlägen kostenfrei sein. Die Aufsichtsbehörden für den Datenschutz in der Privatwirtschaft erhalten verbesserte Überwachungsrechte. Das schwierige Sonderproblem der Datenverarbeitung im Zusammenhang mit der wissenschaftlichen Forschung wird aufgegriffen.

Diese positiven Regelungsansätze können jedoch die gravierenden inhaltlichen Mängel des Entwurfs nicht überdecken. Meine Kritik habe ich schriftlich wie mündlich dem Innenausschuß des Deutschen Bundestages auf seiner öffentlichen Anhörung am 21. April 1986 vorgetragen (vgl. Stenografisches Protokoll der 110. Sitzung des Innenausschusses sowie Ausschußdrucksache 10/153, S. 14 ff.). Auch die Konferenz der Datenschutzbeauftragten hat in ihrer Entschließung vom 14. März 1986 Bedenken geäußert und Gegenvorschläge unterbreitet (vgl. Ziff. 12.2 dieses Berichts).

Kernpunkt meiner Kritik am Entwurf ist die im ganzen gesehen bruchlose Übernahme des bisherigen, überholten Regelungskonzepts. Der Entwurf der Koalition versäumt es, die einschneidenden technologischen Veränderungen der letzten Jahre - wie etwa offene Kommunikationssysteme, die Dezentralisierung der Verarbeitung usw. - angemessen, d.h. soweit dies mit den juristischen Mitteln der Gesetzgebung überhaupt möglich ist, zu berücksichtigen. Dazu ein Beispiel: Anders als im neuen Hessischen Datenschutzgesetz (§ 15) gibt es keinen besonderen Regelungsvorbehalt für on-line-Verfahren, vielmehr können sich die beteiligten Behörden unter Zustimmung ihrer jeweiligen obersten Bundesbehörden selbst über die Details des Direktabrufs einigen.

Ein zweites Beispiel: Die Datenverarbeitung für private Zwecke und zum persönlichen Gebrauch wird pauschal aus dem Anwendungsbereich des Gesetzes herausgenommen. Dies kann mit dazu beitragen, einer in ihren Konsequenzen für das informationelle Selbstbestimmungsrecht der Bürger unabsehbaren und unkontrollierbaren Ausbreitung und Nutzung von Personal- und Heim-Computern Tür und Tor zu öffnen.

Ein weiterer grundlegender Einwand trifft die im Entwurf beabsichtigte Festschreibung der künstlichen, spätestens seit dem Volkszählungsurteil so nicht mehr hinnehmbaren Unterscheidung des Datenschutzniveaus je nachdem, ob von Akten oder Dateien die Rede ist. Wer den Anwendungsbereich eines Datenschutzgesetzes immer noch auf die Verarbeitung in Dateien reduziert und den Datenumgang in Akten nur mit wenigen, darüber hinaus unzulänglichen Bestimmungen im Verwaltungsverfahrensgesetz regeln will (vgl. Bundestags-Drucks. 10/4737, S. 18 ff.), hält an einem dem Bürger unverständlichen und der Wahrung seiner Rechtspositionen abträglichen "Zwei-Klassen-Schutz" fest.

Weitere Kritikpunkte ließen sich hinzufügen: Der Zweckbindungsgrundsatz ist durch zu viele und zu weit gefaßte Ausnahmeregelungen durchlöchert. Nach wie vor bleiben die Nachrichtendienste ohne Einzelfallabwägung pauschal aus der Auskunftspflicht herausgenommen. Die Kontrollmöglichkeiten des Bundesbeauftragten für den Datenschutz werden in wichtigen Punkten beschnitten. Dringend notwendige Sondervorschriften für Kredit- und Personalinformationssysteme sind nicht enthalten.

2.3.2

Konsequenzen

Der BDSG-Entwurf der Koalition ist über die erste Lesung im Deutschen Bundestag, die am 24. April 1986 stattfand, nicht hinausgekommen. Ursache hierfür ist sicherlich vor allem die vielfältige Kritik, die von den Sachverständigen und Verbandsvertretern in der genannten Ausschußanhörung, wenn auch in teilweise völlig

unterschiedlicher Zielrichtung und Interessengewichtung, geäußert worden ist. Mit eine Rolle gespielt hat auch die Einbindung des BDSG-Entwurfs in das Paket von "Sicherheitsgesetzen" (u. a. mit Entwürfen zur Änderung des Bundesverfassungsschutzgesetzes und für ein Gesetz über den Militärischen Abschirmdienst), die in Regelungsabsicht und -inhalt teilweise noch umstrittener waren als das Bundesdatenschutzgesetz selbst und die daher ebenfalls - mit Ausnahme der Änderung des Straßenverkehrsgesetzes zur Regelung des Datenzugriffs auf das Zentrale Verkehrsinformationssystem - ZEVIS (BGBl. I 1987, S. 486) - in der 10. Legislaturperiode nicht mehr verabschiedet wurden (vgl. auch Ziff. 6.4).

In der kommenden Parlamentsperiode sollte die dann erneut anstehende Neufassung des Bundesdatenschutzgesetzes als Chance begriffen werden, ein Gesetzgebungswerk vorzulegen, das weniger kompliziert formuliert ist und gleichzeitig sowohl die verfassungsrechtlichen Vorgaben für einen wirksamen Schutz des informationellen Selbstbestimmungsrechts des Bürgers erfüllt als auch der ständig fortschreitenden Entwicklung der Datenverarbeitungs- und Kommunikationstechnik Rechnung trägt.

Als Vorarbeit für die BDSG-Novellierung kann und sollte in vielen Punkten das neue Hessische Datenschutzgesetz herangezogen werden. Nicht ganz so weitgehende, aber in wichtigen Fragen ebenfalls weiterführende Regelungen enthält auch der gemeinsame Gesetzentwurf der Bundesländer Bremen, Hamburg, Hessen, Nordrhein-Westfalen und Saarland, der im Bundesrat vorgelegt worden ist (vgl. Bundesrats-Drucks. 121/86), von diesem jedoch nicht im Bundestag eingebracht worden ist (Beschluß des Bundesrates vom 16. Mai 1986, Bundesrats-Drucks. 121/86-Beschluß). Eine Fülle von Anregungen findet sich auch im nordrhein-westfälischen Gesetzentwurf zur Fortentwicklung des Datenschutzes vom 25. November 1986 (Landtags-Drucks. 10/1565), der die ursprüngliche Regierungsvorlage (Landtags-Drucks. 9/4075) erheblich revidiert hat.

3. Kommunen

3.1

Beratung von Kommunen

Neben der Kontrolltätigkeit ist ein weiterer Schwerpunkt meiner Aufgaben die Beratung öffentlicher Stellen. Durch den kontinuierlichen Informationsaustausch mit der Verwaltung konnten auch im vergangenen Jahr wieder eine Vielzahl datenschutzrechtlicher Konflikte frühzeitig erkannt und vermieden oder beseitigt werden. So werden beispielsweise in einer Gemeinde künftig Kreditinstitute die Anschriften möglicher Kunden nicht mehr aus dem sogenannten Baubuch erhalten, in das die kommunale Baubehörde die Bauanträge und Baugenehmigungen einträgt. Zu den Ergebnissen meiner Beratungstätigkeit zählen auch, daß Behörden in den Adressen ihrer Schreiben nicht mehr das Geburtsdatum des Empfängers angeben und die Polizei nicht mehr unabhängig von der Schwere des Delikts ihre Erkenntnisse längstmöglich, nämlich zehn Jahre, speichert. In all diesen Fällen war es möglich, recht schnell und einfach mit den jeweiligen Behörden die den datenschutzrechtlichen Anforderungen entsprechende Lösung zu finden. Wie die beiden folgenden Fälle zeigen, gestaltet sich die Beratungstätigkeit jedoch häufig weitaus langwieriger und komplexer und setzt eine detaillierte Analyse des Verwaltungsverfahrens voraus. Mitunter - auch das zeigt einer der Fälle - macht dabei die Verwaltung sogar überraschende Erfahrungen.

3.1.1

Gewerberegister

Um der Verwaltung einen Überblick zu geben, wie viele und welche Gewerbebetriebe in ihrem Zuständigkeitsbereich vorhanden sind sowie zur Überwachung der Einhaltung der gewerbe- und steuerrechtlichen Vorschriften, führen die Kommunen ein Gewerberegister. Dabei handelt es sich um ein "Zwangsregister", denn die Gewerbetreibenden sind verpflichtet, ihre gewerbliche Tätigkeit dem Gemeindevorstand zu melden (§§ 14, 15 und 55c Gewerbeordnung i.V.m. dem Vollzugserlaß des Hessischen Ministers für Wirtschaft und Technik vom 30. Mai 1980 - StAnz. 1980 S. 1111). Aus dem Gewerberegister erhalten unter den im Erlaß des Wirtschaftsministers näher bestimmten Bedingungen sowohl Behörden, wie etwa das Finanzamt oder das Staatliche Gewerbeaufsichtsamt, als auch z.B. Adreßbuchverlage, Versicherungsvertreter oder Markt- und Meinungsforschungsinstitute Auskunft (zur Auskunftspraxis vgl. Ziff. 3.2.2 dieses Berichts).

Nach einer genauen Prüfung der vielfältigen Auskünfte, die die Gewerbemeldestelle einer hessischen Großstadt aus dem Gewerberegister erteilte, ergab sich, daß eine Reihe von Übermittlungen teilweise oder ganz unzulässig waren. So wurde die regelmäßige Übermittlung der Daten aller Gewerbetreibenden an das Städtische Bauamt und an die Kriminalabteilung des Polizeipräsidenten eingestellt. Die Handwerkskammer erhält regelmäßig nur noch Angaben über handwerkliche Betriebe, und die Industrie- und Handelskammer muß sich auf die Daten der Handelsbetriebe beschränken. Privatpersonen bekommen in Zukunft nur noch einen Datensatz mit geringerem Umfang.

Meine Beratung hatte in diesem Fall jedoch nicht nur eine Änderung der Übermittlungspraxis zur Folge, sondern auch Konsequenzen für das automatisierte Datenverarbeitungsverfahren. Vereinbart wurden mit der Gemeinde zusätzliche Datensicherungsmaßnahmen sowie ein Auswertungsprogramm, mit dem Gewerbetreibende in kurzer Zeit über die zu ihrer Person im Gewerbeverzeichnis gespeicherten Daten informiert werden können. Die Durchführung dieser Maßnahmen werde ich zu gegebener Zeit überprüfen.

3.1.2

Paßdaten

In einem anderen Fall plante eine Gemeinde die Speicherung von Ausweisdaten in der automatisierten Datei des kommunalen Finanzwesens. Dagegen bestanden gleich zwei schwerwiegende Einwände. Zum einen sollte ein für einen völlig anderen Zweck entwickeltes Datenverarbeitungsprogramm ohne weiteres für die Verarbeitung von Ausweisdaten verwendet werden. Auch wenn ein solches Vorgehen auf den ersten Blick kostengünstig und naheliegend erscheint, bleibt dagegen zu bedenken, daß ein für eine bestimmte Aufgabe entwickeltes und datenschutzrechtlich überprüftes Verarbeitungsverfahren nicht unbedingt auch die Anforderungen eines anderen Verarbeitungszwecks erfüllt. Außerdem sollten bei dem Vorhaben Daten, die zur Erfüllung vollkommen verschiedener Aufgaben erhoben worden waren, in einer Datei zusammengeführt werden, was dem Grundsatz der funktionalen Trennung der Datenverarbeitung innerhalb einer Gemeinde widersprochen hätte.

Die von mir gemeinsam mit der Gemeinde durchgeführte Untersuchung der Situation der Paßstelle ließ die Notwendigkeit einer umfassenden Reorganisation der Ausweiskartei erkennen: Die Aufbewahrungskapazität war mit den vorhandenen 35.000 Karteikarten erschöpft. Nicht mehr benötigte Karten wurden nur aussortiert, wenn ein abgelaufener Ausweis ersetzt wurde. Die Paßstelle hätte unter den gegebenen Bedingungen die mit den neuen Ausweisgesetzen auf sie zukommenden Aufgaben kaum bewältigen können. Die in den nächsten Jahren zu erwartenden ca. 15.000 Anträge auf Ausstellungen von Personalausweisen und Reisepässen wären in der vorhandenen Kartei nicht unterzubringen gewesen. Schwierigkeiten hätte die lediglich alphabetisch geordnete Kartei bei Einhaltung der Lösungsfristen bereitet, wonach die Daten des Paßregisters und des Personalausweisregisters künftig spätestens fünf Jahre nach Ablauf der Gültigkeit des Ausweises zu löschen sind.

Ich habe daher der Gemeinde vorgeschlagen, die Altkartei zwar alphabetisch, aber nach Jahrgängen umzusortieren, alle über 15 Jahre alten Karten auszusondern und zu vernichten sowie die Ausstellungsdaten in einem Zusatzdatensatz des ADV-Verfahrens "Grundstufe Einwohnerwesen" zu erfassen. Die Möglichkeit, in diesem Verfahren einen Zusatzdatensatz anzufertigen, ist u.a. zum Speichern von Ausweisdaten landesweit geschaffen worden.

Durch diese organisatorischen und technischen Maßnahmen wird es der Paßstelle möglich, die Anforderungen der neuen Ausweisgesetze zu erfüllen. Mit den automatisiert in der Datei "Grundstufe Einwohnerwesen" gespeicherten Ausweisdaten dürften die Auskunftersuchen dritter Stellen in der Regel zu erfüllen sein. Sollte ausnahmsweise für die Auskunftserteilung die Karteikarte benötigt werden, etwa zum Vergleich von Lichtbildern, könnte diese ohne großen Aufwand gefunden werden, da das Ausstellungsdatum und damit auch die Fundstelle automatisiert gespeichert sind. Da die Kartei nach Jahrgängen sortiert ist, kann zum Jahreswechsel der jeweils 15 Jahre alte Jahrgang vernichtet werden, so daß sich die Lösungsfristen problemlos erfüllen lassen.

Auf meine Empfehlung hin hat die Gemeinde ihr Vorhaben, Ausweisdaten in der Datei des kommunalen Finanzwesens zu speichern, aufgegeben. Dort teilweise gespeicherte Daten wurden gelöscht. Die Ausweisdaten werden künftig in der Datei des Einwohnerwesens gespeichert. Die Ausweiskartei wird umsortiert und kann ausgelagert werden, da auf sie nicht mehr ständig zur Erfüllung von Auskunftersuchen zugegriffen werden muß. Der Erfassungsaufwand für die automatisierte Datenverarbeitung wird erheblich reduziert, weil nicht der gesamte Datensatz der Karteikarte, sondern nur die nicht bereits in der Meldedatei gespeicherten Angaben für die Ausstellung des Ausweises erfaßt werden müssen. Zur Überraschung der Gemeinde werden mit dem von mir vorgeschlagenen Verfahren jährlich ca. 25.000 DM gegenüber der ursprünglich geplanten Speicherung der Ausweisdaten in der Datei des kommunalen Finanzwesens eingespart - womit einmal mehr bewiesen ist, daß sich Datenschutz entgegen einer verbreiteten Ansicht keineswegs kostentreibend auswirken muß.

3.2

Datenübermittlung an private Personen oder Stellen

In meinem 14. Tätigkeitsbericht sind die typischen Dateien im kommunalen Bereich im einzelnen aufgelistet worden (vgl. dort Ziff. 9). Zwar dürfte weitgehend bekannt sein, daß aus einigen dieser Dateien personenbezogene Daten auch an private Stellen übermittelt werden, dagegen ist vermutlich weniger bekannt, in welchem Umfang dies geschieht. Wie unterschiedlich die Übermittlungspraxis nach Datei und Gemeinde sein kann, lassen beispielsweise die Zahlen erkennen, die mir auf Anfrage von verschiedenen Kommunen für die Bereiche Einwohnermeldeamt und Gewerbemeldestelle mitgeteilt worden sind.

3.2.1

Einwohnermeldeämter

Die Übermittlung von Daten aus dem Melderegister an private Personen oder Einrichtungen regelt das Hessische Meldegesetz (§§ 34, 35 HMG). Neben der sogenannten einfachen und der erweiterten Melderegisterauskunft sieht es als weitere praktisch bedeutsame Auskunftformen die Gruppenauskunft und die Auskunft an Adreßbuchverlage vor. Während die am häufigsten gewünschte einfache Melderegisterauskunft, bei der Name und Anschrift einzelner bestimmter Einwohner übermittelt werden, jeder ohne weiteres erhalten kann, muß der Empfänger für die erweiterte Registerauskunft ein berechtigtes Interesse glaubhaft machen. Nur insoweit können ihm zusätzlich Geburtsdatum und -ort, frühere Namen, Familienstand, Staatsangehörigkeit, frühere Anschriften, Tag des Ein- und Auszugs, gesetzlicher Vertreter sowie Sterbetag und -ort des Einwohners mitgeteilt werden. Ein solches Interesse besteht nicht nur, wenn die zusätzlichen Angaben zur Durchsetzung eines Rechtsanspruchs benötigt werden, sondern z.B. auch, wenn sie journalistischen oder Forschungszwecken dienen sollen. Die Gruppenauskunft wird nur erteilt, soweit sie im öffentlichen Interesse liegt. In diesem Fall erfolgt die Auskunft nicht über eine vom Empfänger namentlich bezeichnete Person, sondern über eine Mehrzahl von Personen mit gemeinsamen Merkmalen, wie ein bestimmtes Lebensalter oder Wohngebiet. Da ein "öffentliches Interesse" nur in wenigen Fällen bejaht werden kann, gehen derartige Auskünfte fast ausschließlich an Forschungsinstitute, die im Auftrag öffentlich-rechtlicher Körperschaften tätig werden.

Die folgende Übersicht zeigt die Anzahl der Auskünfte, die von den Einwohnermeldeämtern vier befragter Gemeinden von September 1985 bis September 1986 erteilt wurden.

Gemeinde	Einwohner	Grundauskünfte	Grundauskünfte pro 1.000 Einwohner	erweiterte Auskünfte	erweiterte auskünfte pro 1.000 Einwohner	Gruppenauskünfte
Frankfurt	600.000	190.000	317	2.750	5,0	3
Wiesbaden	270.000	38.000	140	450	2,0	145
Wetzlar	50.000	14.000	280	15	0,3	1
Stadtallendorf	20.000	2.070	100	87	4,0	12

Die vergleichsweise häufigen Gruppenauskünfte in Wiesbaden und Stadtallendorf beruhen hauptsächlich auf Anfragen eines im Auftrag der Bundesregierung tätigen Forschungsinstitutes, das in den beiden Städten regelmäßig Erhebungen durchführt.

Auskünfte aus dem Melderegister müssen von den Betroffenen keineswegs immer hingenommen werden, sondern lassen sich ganz oder teilweise verhindern. Das reicht von der totalen Auskunftssperre, die besonders gefährdete Personen verlangen können, über die bei berechtigtem Interesse gewährte Teilauskunftssperre, mit der die erweiterte Melderegisterauskunft unterbunden wird, bis zum Widerspruch gegen die Übermittlung von Namen und Anschrift an Adreßbuchverlage.

Wie sich die verschiedenen Auskunftssperren in den befragten Gemeinden verteilen, ist der folgenden Tabelle zu entnehmen (Stand September 1986):

Gemeinde	Einwohner	totale Auskunfts-sperren	pro 1.000 Einwohner	Teilauskunfts-sperren	pro 1.000 Einwohner	Adreßbuchauskünfte sperren	pro 1.000 Einwohner
Frankfurt	600.000	764	1,3	192	0,3	20.800	34,7
Wiesbaden	270.000	1.420	5,3	392	1,5	6.748	25,0
Wetzlar	50.000	13	0,3	—	—	333	6,7
Stadtallendorf	20.000	32	1,6	32	1,6	48	2,4

Die hohe Zahl der Adreßbuchauskunftssperren in Frankfurt beruht vermutlich darauf, daß die Stadtverwaltung vor jeder Neuauflage eines Adreßbuchs in vorbildlicher Weise öffentlich auf das Widerspruchsrecht der Betroffenen hinweist. Die große Anzahl der Totalauskunftssperren in Wiesbaden ist auf die relativ vielen, bei Sicherheitsbehörden (Bundeskriminalamt, Landeskriminalamt und Landesamt für Verfassungsschutz) beschäftigten Einwohner zurückzuführen.

3.2.2

Gewerbemeldestellen

Wie bereits dargestellt (vgl. Ziff. 3.1.1), führen die Kommunen eine Datei aller Gewerbetreibenden, das sogenannte Gewereregister. In seinem Vollzugserlaß vom 30. Mai 1980 zu den §§ 14, 15 und 55c der Gewerbeordnung (StAnz. 1980 S. 1111) hat der Hessische Minister für Wirtschaft und Technik näher bestimmt, unter welchen Voraussetzungen und in welchem Umfang die Gewerbemeldestellen Daten an Privatpersonen weitergeben dürfen. Unterschieden wird dort - ähnlich wie im Melderecht - zwischen einfachen und erweiterten Einzelauskünften sowie Gruppenauskünften. Nach dem Erlaß kann in der Regel die einfache Einzelauskunft, bei der Namen des Gewerbebetriebes, Vor- und Familiennamen des Gewerbetreibenden, Anschrift des Gewerbebetriebes und angemeldete Tätigkeiten mitgeteilt werden, ohne weiteres gewährt werden. Bei der erweiterten Einzelauskunft muß dagegen für jedes zusätzliche Datum ein berechtigtes Interesse glaubhaft gemacht werden. Gruppenauskünfte, die insbesondere für Zwecke der Werbung und Meinungsforschung erteilt werden, dürfen nur erteilt werden, wenn der Gewerbetreibende bereits bei der Anmeldung darin eingewilligt hat.

Die folgende Zusammenstellung zeigt die Auskunftspraxis in vier befragten Gemeinden im Zeitraum September 1985 bis September 1986:

Gemeinde	gemeldete Gewerbe- betriebe	ein- fache Auskünfte	ein- fache Auskünfte pro 100 Gewerbe- betriebe	erwei- terte Auskünfte	erwei- terte Auskünfte pro 100 Gewerbe- betriebe	Grup- pen- aus- künfte	Einwil- ligung in Grup- penaus- künften
Frankfurt	43.785	4.135	9,4	10.440	23,8	0	unter 1 %
Wiesbaden	16.300	1.507	9,3	3.689	22,6	60	10 %
Gießen	3.996	75	1,9	1.344	33,6	6	25 %
Stadtallendorf	800	0	—	83	10,4	0	2 %

3.3

Meldedaten von psychisch Kranken im Adreßbuch

3.3.1

Vorfall

Im Frühjahr 1986 gab ein Spezialverlag ein Adreßbuch für die Stadt Marburg heraus. Der Verlag hatte dafür Meldedaten verwendet, die ihm von der Stadt überlassen worden waren. Bei Durchsicht eines der ersten ausgelieferten Exemplare bemerkte der Direktor einer örtlichen psychiatrischen Klinik, daß die Namen von mehreren hundert Patienten seiner Klinik unter der Krankenhausadresse eingetragen waren. Die Namen standen dort zwar zusammen mit denen der Beschäftigten, die in der Klinik wohnten; dennoch konnten Außenstehende mit geringem Zusatzwissen leicht feststellen, in welchen Fällen es sich um Patientendaten handelte.

Die Stadt beschloß deshalb im Einvernehmen mit dem Verlag, das Buch zurückzuziehen und einzustampfen. Vor der Neuauflage wurden alle Patienten oder ihre gesetzlichen Vertreter um Mitteilung gebeten, ob die Namen im Adreßbuch erscheinen sollten. Daraufhin beantragten nahezu alle Betroffenen eine Übermittlungssperre, so daß in dem jetzigen Adreßbuch fast keine Patientendaten mehr enthalten sind.

Das Verhalten von Stadt und Verlag ist umso lobenswerter, als beide dazu keineswegs gesetzlich verpflichtet waren: Nach § 28 Abs. 1 des Hessischen Meldegesetzes sind Personen, die in Krankenhäuser, Sanatorien, Heil- und Pflegeanstalten oder ähnlichen Einrichtungen aufgenommen werden, dann meldepflichtig, wenn sie über keine andere Wohnung verfügen und der Aufenthalt in dieser Einrichtung die Dauer von zwei Monaten überschreitet. Wie bei jeder anderen Person wird im Melderegister natürlich nicht das Datum "psychisch krank" oder "krank" gespeichert. Lediglich aus der Adresse, die für Eingeweihte als Anschrift einer bestimmten Pflegeeinrichtung erkennbar ist, kann unter Umständen auf den Patientenstatus der gemeldeten Personen geschlossen werden. Wie jedem anderen Bürger stand es natürlich auch den betroffenen Patienten frei, gem. § 35 Abs. 5 des Hessischen Meldegesetzes ohne jede Begründung die Übermittlung ihrer Anschrift an Adreßbuchverlage sperren zu lassen. Offensichtlich hatten die Betroffenen dies jedoch nicht gewußt.

Da die Bürger häufig über die Möglichkeit der Auskunftssperre nicht Bescheid wissen, kommt es immer wieder nach erfolgter Datenübermittlung und Veröffentlichung zu Vorwürfen gegenüber der Verwaltung. Mehrfach habe ich deshalb bereits die Meldebehörden darauf hingewiesen, daß sie durch besondere Maßnahmen die Betroffenen informieren müssen.

In diesem Fall hatte der Magistrat vor der Veröffentlichung das bevorstehende Erscheinen des Adreßbuchs und die vorgesehenen Datenübermittlungen amtlich bekanntgemacht und ergänzend auf Informationsveranstaltungen hingewiesen. Außerdem stand ein besonderes Informationsblatt zur Verfügung. Vor der zweiten Ausgabe des Adreßbuchs wurden interessierte Bürger noch einmal durch Hinweise in der Presse aufgefordert, einen Sperrvermerk im Einwohnermelderegister eintragen zu lassen und bei allen Ämtern Informationsblätter ausgelegt. Darüber hinaus wurden - wie bereits erwähnt - die Patienten oder ihre gesetzlichen Vertreter besonders angesprochen. Erst danach wurde das Adreßbuch erneut und mit korrigiertem Datensatz herausgegeben.

3.3.2

Konsequenzen

Der Vorfall macht zweierlei deutlich:

Nur wenige der Einwohner wissen, daß nach dem Hessischen Meldegesetz (§ 35) insbesondere Parteien vor Wahlen zum Zweck der Wahlwerbung, Adreßbuchverlage zur Herstellung eines Adreßbuchs, aber auch Mitglieder der staatlichen und kommunalen Parlamente, sowie Presse und Rundfunk zu bestimmten Zwecken Daten aus dem Melderegister anfordern können, die Auskunft allerdings durch einen zu beantragenden Sperrvermerk verhindert werden kann. Die Gemeinden sollten deshalb regelmäßig und in nicht zu langen Abständen in der Presse und den amtlichen Bekanntmachungen auf dieses Verfahren hinweisen.

Besondere Sorgfalt erfordern Adreßbücher. Vor der Übermittlung der Daten an den Verlag sollte die Gemeinde die Betroffenen auf die Möglichkeit des Widerspruchs hinweisen. Empfehlenswert ist auch die Praxis einiger Kommunen, die bei Krankenanstalten, Justizvollzugsanstalten, Heimen oder ähnlichen Einrichtungen entweder die Namen der dort gemeldeten Personen von vornherein nicht übermitteln oder die Betroffenen vorher fragen. Die Ereignisse um das Marburger Adreßbuch sollten die Landesregierung veranlassen, zu prüfen, ob diese Praxis einiger Gemeinden verwaltungsintern nicht generell eingeführt werden sollte.

4. Gesundheit

4.1

Datenverarbeitung im Krankenhaus

4.1.1

Allgemeine Entwicklung

In den Krankenhäusern ist generell eine erhebliche Zunahme der automatisierten Datenverarbeitung festzustellen. Dies gilt sowohl für die Verwaltung als auch für den medizinischen Bereich der Krankenhäuser. Nahezu immer geht es dabei auch um die Verarbeitung personenbezogener Daten, vielfach um die Verarbeitung sensibler medizinischer Daten der Patienten.

Hintergrund dieser Entwicklung sind vor allem die steigenden Erwartungen an die von den Krankenhäusern zu erbringenden medizinischen Leistungen und - zum Teil damit zusammenhängend - die ständig zunehmenden Kosten der Krankenhäuser sowie die daraus resultierende Forderung nach einer Begrenzung der Kostensteigerung. Gegenwärtig bildet die Krankenhauspflege einen hohen und durch überdurchschnittlichen Kostenzuwachs noch steigenden Anteil an den Ausgaben der gesetzlichen Krankenversicherung. Es wächst daher der Druck auf die Krankenhäuser, Kosten einzusparen oder sie mit nachprüfbaren Daten zu begründen.

Die Forderung nach Kostendämpfung hat bereits zu gesetzgeberischen Maßnahmen geführt. So wurde 1984 vom Bundestag das Krankenhausfinanzierungsgesetz durch das Krankenhaus-Neuordnungsgesetz (BGBl. I 1984, S. 1716) geändert und damit die Krankenhausfinanzierung neu geordnet. Wesentliche auch für den Datenschutz wichtige Änderung: Bei der Bemessung der Pflegesätze sind künftig auch die Kosten und Leistungen vergleichbarer Krankenhäuser zu berücksichtigen. Die Krankenhäuser müssen grundsätzlich alle für die Ermittlung der Pflegesätze erforderlichen Kosten- und Leistungsnachweise erbringen.

Umgesetzt werden die pflegesatzrechtlichen Vorgaben des Gesetzes durch die neue Bundespflegesatzverordnung (BpflV) vom 21. April 1985 (BGBl. I, S. 1666). Die seit dem 1. Januar 1986 geltende Verordnung stellt neue Anforderungen an die Aufstellung des Haushalts der Krankenhäuser und verlangt u.a. auch die Anfertigung von Diagnosestatistiken. Dadurch müssen die Krankenhäuser neben ihren Kosten erstmals auch ihre Leistungen im medizinischen Bereich offenlegen.

Vor diesem Hintergrund verwundert das gegenwärtig festzustellende breite Spektrum angewandter oder geplanter automatisierter Datenverarbeitungsverfahren im Krankenhausbereich kaum. Um nur einige Beispiele zu nennen:

So werden im Verwaltungsbereich der Krankenhäuser z.B. DV-Verfahren zur Abwicklung der Patientenaufnahme, -verlegung und -entlassung, Abrechnung mit dem Kostenträger, Leistungserfassung, Personalabrechnung und Personaldisposition eingesetzt. Im medizinischen Bereich werden zum Teil DV-Verfahren z.B. für die Befunddokumentation und das Schreiben von Arztbriefen sowie für die Labordatenverarbeitung (vgl. dazu Ziff. 4.3 dieses Berichts) verwendet. Erwogen wird derzeit, daß der Hessische DV-Verbund in sein Angebot für die hessischen Krankenhäuser ein Radiologiesystem aufnimmt, das der Steuerung und Verwaltung von Radiologieabteilungen dienen soll. Das gleiche gilt für ein DV-gestütztes Verfahren, mit dessen Hilfe u.a. außerplanmäßige Entwicklungen im Kosten- und Leistungsbereich schnell erkannt werden sollen. Des weiteren ist die Aufnahme eines Krankenhaus- Kommunikationssystems in das Angebot des DV-Verbundes vorgesehen, das als Bindeglied zwischen den einzelnen Krankenhausbereichen dienen und einen reibungslosen Informationsaustausch innerhalb des Krankenhauses gewährleisten soll. Schließlich ist noch auf den fortschreitenden Ausbau klinischer Krebsregister in einigen hessischen Krankenhäusern hinzuweisen (vgl. hierzu Ziff. 4.2.3).

4.1.2

Konkrete Regelungen sind notwendig

Konsequenzen müssen auf verschiedenen Ebenen gezogen werden. Zunächst einmal bedarf es konkreter gesetzlicher Regelungen. Hierauf hat auch die Konferenz der Datenschutzbeauftragten des Bundes und der Länder in ihrer Entschließung vom 14. März 1986 hingewiesen (vgl. hierzu Ziff. 12.4). Infolge des Krankenhaus-Neuordnungsgesetzes ist in Hessen eine darauf abgestimmte Neufassung des Krankenhausgesetzes geplant. Dem Hessischen Sozialminister habe ich in diesem Zusammenhang bereits Ende 1985 bereichsspezifische Datenschutzvorschriften für die Datenverarbeitung im Krankenhaus vorgeschlagen, die im vergangenen Jahr mehrfach zwischen dem Sozialminister wie auch weiteren Ressorts und mir erörtert worden sind.

Wichtig sind insbesondere:

- eine umfassende Regelung der Verarbeitung von Patientendaten, unabhängig von der Form ihrer Verarbeitung,
- eine präzise Regelung der Erhebung und Speicherung von Patientendaten im Krankenhaus. Unterschieden werden muß hierbei zwischen der Erhebung und Speicherung zur Erfüllung des mit dem Patienten oder zu seinen Gunsten abgeschlossenen Behandlungsvertrages und zur Erfüllung einer gesetzlichen Erhebungs- und Speicherungspflicht sowie der Erhebung und Speicherung von Daten aufgrund einer Einwilligung des Patienten. Angesichts der besonderen Situation des Patienten im Krankenhaus sollte im Gesetz der zulässige Umfang und die Form der Einwilligung des Patienten in die Verarbeitung seiner Daten festgelegt werden. Die Einwilligung sollte im Regelfall schriftlich erfolgen und der Patient über Art, Umfang und Zweck der beabsichtigten Erhebung und Speicherung schriftlich unterrichtet werden. Aus der Verweigerung der Einwilligung dürfen dem Patienten keine Nachteile entstehen. Unzumutbare oder sachfremde Angaben dürfen auch mit Einwilligung des Patienten nicht verarbeitet werden,
- eine Vorschrift zur Abschottung personenbezogener Daten innerhalb des Krankenhauses, die sicherstellt, daß die Beschäftigten Patientendaten nur für den zu ihrer jeweiligen rechtmäßigen Aufgabenerfüllung gehörenden Zweck verarbeiten,
- eine konkrete Regelung der Übermittlung von personenbezogenen Daten an Personen oder Stellen außerhalb des Krankenhauses. Für eine Übermittlung von Daten zwischen verschiedenen Behandlungseinheiten innerhalb eines Krankenhauses muß diese Regelung entsprechend Anwendung finden,
- eine detaillierte Regelung der Verarbeitung von Patientendaten für Forschungszwecke, die einerseits das informationelle Selbstbestimmungsrecht des Patienten berücksichtigt, andererseits aber auch der besonderen Bedeutung der Forschung im medizinischen Bereich Rechnung trägt. Notwendig ist in jedem Fall eine präzise Unterscheidung der einzelnen Verarbeitungssituationen und eine daran anknüpfende sorgfältige Abwägung der tangierten Rechtspositionen, die von folgenden Prämissen ausgehen sollte:
 Eine Verwendung der für die Behandlung gespeicherten Patientendaten für eigene wissenschaftliche medizinische Forschungsvorhaben von Ärzten der Behandlungseinheit - nicht von allen Ärzten des gesamten Krankenhauses - ist ohne Einwilligung des Patienten zulässig. Patientendaten dürfen an andere Behandlungseinheiten oder an Stellen außerhalb des Krankenhauses für bestimmte Forschungsvorhaben übermittelt werden, wenn der Patient einwilligt. Ohne Einwilligung ist die Übermittlung nur zulässig, soweit sie erforderlich ist zur Durchführung eines bestimmten medizinischen Forschungsvorhabens, es nicht zumutbar ist, die Einwilligung beim Patienten einzuholen, und das öffentliche Interesse an der Durchführung des Forschungsvorhabens die schutzwürdigen Belange des Patienten überwiegt,
- die Bestellung eines Datenschutzbeauftragten für jedes Krankenhaus,

- ein umfassendes Recht des Patienten auf Auskunft über die zu seiner Person gespeicherten Daten und Einsicht in seine Krankenakte, wobei der Inhalt im Einzelfall durch einen Arzt vermittelt werden kann, sofern anderenfalls ein gesundheitlicher Schaden für den Patienten zu befürchten ist. Die Rechte des Patienten dürfen hierdurch jedoch nicht eingeschränkt werden.

Bei den im vergangenen Jahr geführten Diskussionen hat sich eine weitgehende Übereinstimmung zwischen dem Hessischen Sozialminister und mir ergeben. Ich hoffe daher, daß eine gesetzliche Regelung sobald wie möglich erfolgt.

4.1.3 Interne Abschottungen

4.1.3.1

Datengeheimnis und ärztliche Schweigepflicht - Auswirkungen im Krankenhaus

Von besonderer Bedeutung für den Datenschutz und bereits heute rechtlich geboten ist die interne Abschottung der personenbezogenen Daten in den Krankenhäusern.

Das Datengeheimnis, das den Beschäftigten in Krankenhäusern die Verarbeitung personenbezogener Daten nur zu den zur rechtmäßigen Aufgabenerfüllung gehörenden Zwecken gestattet (§ 5 Bundesdatenschutzgesetz) und die ärztliche Schweigepflicht (§ 203 Abs. 1 Nr. 1 Strafgesetzbuch) verbieten es, das Krankenhaus als eine Einheit anzusehen, in der Informationen uneingeschränkt ausgetauscht und verwendet werden dürfen. Rechtlich geboten ist vielmehr zum einen eine weitgehende Abschottung der medizinischen Daten von dem Verwaltungsbereich des Krankenhauses: Das Personal der Aufnahme- und Abrechnungsabteilungen darf nur Zugriff auf Verwaltungsdaten erhalten. Hierzu zählen z.B. die Patientenaufnahmenummer, Name und Adresse der Patienten, Kostenträger der Behandlung, Aufnahmeart (Einweisung, Notfall, Verlegung usw.), Aufnahme- und Entlassungstag. In gewissem Umfang können hierzu auch medizinische Daten gehören, wie beispielsweise die bei der Einweisung gestellte Diagnose und die Entlassungsdiagnose, soweit sie für den Antrag auf Kostenübernahme durch die Krankenkassen erforderlich sind. Zum anderen muß darüber hinaus sichergestellt werden, daß jeder im Krankenhaus Beschäftigte auch nur die für seine jeweilige Aufgabenerfüllung erforderlichen Daten zur Kenntnis nehmen kann.

Diese Anforderungen gewinnen im Zuge der zunehmenden Automatisierung der Datenverarbeitung und des Einsatzes komplexer Systeme, wie z.B. bereichsübergreifender Kommunikationssysteme, besondere Bedeutung. Hier bedarf es einer sorgfältigen Analyse, welche Informationsflüsse im Krankenhaus tatsächlich erforderlich sind, und einer entsprechenden Ausgestaltung der DV-Systeme sowie der jeweiligen konkreten Zugriffsmöglichkeiten.

4.1.3.2

Beispiel: Diagnosestatistik

Im letzten Jahr waren diese Anforderungen für die Festlegung des Verfahrens zur Erstellung der Diagnosestatistik von Bedeutung. Die bereits erwähnte Bundespflegesatzverordnung verpflichtet seit dem 1. Januar 1986 die Krankenhäuser, eine Diagnosestatistik mit Angaben zur Diagnose sowie zur Anzahl der durchgeführten Operationen zu erstellen (§§ 16 Abs. 4, 24 Abs. 2 BpflV). Ab 1. Januar 1988 sind darüber hinaus auch die Verweildauer im Krankenhaus und die Altersgruppe der Patienten zu erfassen. Diese Statistik ist ab 1987 von den Krankenhäusern für die Pflegesatzverhandlungen vorzulegen.

Die Krankenhäuser sind zwar lediglich zur Vorlage einer statistischen Übersicht verpflichtet, zur Erstellung dieser Statistik werden jedoch personenbezogene medizinische Daten des ärztlichen Bereichs benötigt, die der ärztlichen Schweigepflicht unterfallen. Vorgesehen war, die Statistik von der Krankenhausverwaltung erstellen zu lassen. Damit ergab sich die Frage, ob eine Weitergabe der benötigten Daten an die Krankenhausverwaltung zulässig ist.

Eine Weitergabe der Daten an die Krankenhausverwaltung ist eine Offenbarung von medizinischen Daten i.S.v. § 203 Strafgesetzbuch, die nur dann nicht strafbar ist, wenn eine gesetzliche Regelung dies erlaubt oder das Einverständnis des Patienten vorliegt.

Eine gesetzliche Regelung, die eine Befugnis zur Durchbrechung der ärztlichen Schweigepflicht zum Zwecke der Erstellung der Diagnosestatistik enthält, gibt es nicht. In den §§ 16 Abs. 4 Satz 2 Nr. 1, 24 Abs. 2 BpflV ist lediglich die Pflicht der Krankenhäuser festgelegt, eine Diagnosestatistik zu erstellen und vorzulegen. Das Verfahren ist nicht geregelt. Theoretisch ist es z.B. auch denkbar, daß die Statistik im ärztlichen Bereich erstellt wird oder vom ärztlichen Bereich nur anonymisierte Daten an die Krankenhausverwaltung zur Erstellung der Statistik weitergegeben werden.

Eine Offenbarung der Daten an die Krankenhausverwaltung könnte allenfalls aufgrund einer sog. "konkludenten" Einwilligung der Patienten zulässig sein; d.h., aus dem Verhalten des Betroffenen, nämlich daß er sich in ein Krankenhaus zur Behandlung begibt, könnte auf die Einwilligung in die Offenbarung seiner Daten für die Diagnosestatistik zu schließen sein. Eine konkludente Einwilligung setzt jedoch nach allgemeiner Auffassung voraus, daß der Betroffene die Tragweite seiner Einwilligung im wesentlichen zu überblicken vermag. Sicherlich weiß jeder Patient, daß ein Krankenhaus arbeitsteilig aufgebaut ist und Daten aus dem ärztlichen Bereich für Verwaltungsaufgaben, insbesondere für Abrechnungen, an die Krankenhausverwaltung weitergegeben werden und dies auch unumgänglich ist. Ob allerdings auch noch davon ausgegangen werden kann, daß er mit einer Übermittlung seiner Diagnosen an die Krankenhausverwaltung für die Erstellung einer Diagnosestatistik rechnet, ist zweifelhaft.

Da es sich um einen Grenzfall handelt, habe ich den Hessischen Sozialminister aufgefordert, eingehend zu überprüfen, ob nicht eine Verfahrensweise für die Erstellung der Diagnosestatistik gefunden werden kann, die eine Offenbarung der medizinischen Daten an die Krankenhausverwaltung vermeidet. Sollte dies nicht möglich sein, ist in jedem Fall folgendes zu beachten:

- Eine Offenbarung weiterer, in den §§ 16 Abs. 4 Satz 2 Nr. 1, 24 Abs. 2 BpflV nicht vorgesehenen Daten an die Krankenhausverwaltung - wie sie zum Teil diskutiert wird - ist nicht zulässig. Dies gilt insbesondere für Nebendiagnosen.
- Die offenbarten personenbezogenen Daten dürfen nur für die Erstellung der Diagnosestatistik verwendet werden. Eine konkludente Einwilligung der Patienten umfaßt allenfalls eine Offenbarung der medizinischen Daten gegenüber der Krankenhausverwaltung zum Zwecke der Erstellung der Diagnosestatistik. Keinesfalls dürfen die Daten der gesamten Krankenhausverwaltung für die verschiedensten Zwecke auf Dauer zur Verfügung gestellt werden, wie dies offenbar erwogen wird. Die Daten sind so schnell wie möglich zu anonymisieren.
- Sofern die Daten in einer anonymisierten Datei gespeichert werden und Rückschlüsse auf einzelne Patienten nicht mehr möglich sind, dürfen sie mit anderen bereits in der Krankenhausverwaltung vorhandenen Daten zu statistischen Zwecken zusammengeführt werden. Dies gilt allerdings nur, soweit sich dadurch das Reidentifikationsrisiko nicht entscheidend erhöht.

Auch bei meiner Prüfung des neuen Laborsystems des DV-Verbundes hat der Gesichtspunkt der internen Abschottung eine wichtige Rolle gespielt (s. hierzu 4.3).

4.1.4

Aufnahmeformulare

Angesichts der zunehmenden automatisierten Datenverarbeitung in den Krankenhäusern ist besonders darauf zu achten, daß die Verarbeitung der personenbezogenen Daten für den Patienten transparent wird und seine Entscheidungsfreiheit so weit wie möglich sichergestellt wird.

Konkret geht es vor allem um die Ausgestaltung der von den Krankenhäusern verwendeten Aufnahmeformulare. Die gegenwärtig benutzten Aufnahmeformulare sind zum Teil sehr pauschal gefaßt. Auf das Problem wird auch im Beschluß der Konferenz der Datenschutzbeauftragten hingewiesen (vgl. Ziff. 12.3 dieses Berichts). So soll sich der Patient z.B. damit einverstanden erklären, daß seine Daten "im Rahmen des Aufnahmevertrags" gespeichert und -soweit dadurch nicht "offenkundig seine Interessen verletzt werden" - übermittelt werden. Eine solche Klausel ist zu undifferenziert. Insbesondere wird nicht klar unterschieden zwischen der Verarbeitung derjenigen Daten, die zur Durchführung der Behandlung erforderlich sind, und der Verarbeitung weiterer Daten, die bei Vorliegen einer Einwilligung verarbeitet werden können. Für den Patienten werden Art und Umfang der Verarbeitung seiner Daten in keiner Weise transparent. Eine Klausel, derzufolge jede Übermittlung zulässig ist, soweit sie nicht "offenkundig" die Interessen des Betroffenen verletzt, setzt sich zudem über die geltende Rechtslage hinweg.

Für das vergangene Jahr habe ich die Zurückstellung der Überarbeitung der Aufnahmeformulare noch akzeptiert, weil zunächst einmal die konkreten Regelungen für das Krankenhausgesetz verabschiedet werden sollten. Im Jahr 1987 kann die Überarbeitung jedoch nicht weiter aufgeschoben werden. Es ist für die Patienten nicht mehr länger zumutbar, diese formularmäßigen Erklärungen zu unterschreiben.

4.2

Krebsregister

4.2.1

Registerarten

Die datenschutzrechtliche Diskussion um Krebsregister kann sich nicht mehr nur auf die in der Öffentlichkeit weitgehend bekannten epidemiologischen Register beschränken, sondern muß auch die im Aufbau befindlichen klinischen Tumorregister einbeziehen.

Epidemiologische Inzidenzregister kennzeichnet die Landesregierung in ihrer in der Antwort vom 11. April 1985 auf die Große Anfrage der SPD-Fraktion betreffend Krebsregister enthaltenen Funktionsbeschreibung der beiden Register als Basisinstrument der epidemiologischen Krebsforschung und Krebsursachenbekämpfung. In ihnen sollen alle Krebserkrankungen einer bestimmten Region erfaßt werden, damit Häufigkeit (Inzidenz) und Verteilung innerhalb der Region genau bestimmt werden können. Auf diese Weise kann das Krebsgeschehen beispielsweise innerhalb der hessischen Bevölkerung abgebildet und auf umweltbezogene sowie individuelle Krebsrisiken untersucht werden. Klinische Krebsregister (Nachsorgeregister), so die Landesregierung, dienen der Verbesserung der Krebsbehandlung im Erkrankungsfall, indem die Vielzahl der dabei anfallenden Daten automatisch erfaßt, verarbeitet und im Interesse einer interdisziplinären Zusammenarbeit den verschiedenen behandelnden Ärzten als solide Informationsbasis zugänglich gemacht werden. Darüber hinaus sollen diese Register Arzt und Patient an die Einhaltung von Kontrolluntersuchungen und Nachsorgeterminen erinnern (Drucks. 11/3565).

4.2.1.1

Epidemiologisches Krebsregister

In den letzten Jahren war die Frage der Errichtung eines epidemiologischen Krebsregisters zur Erfassung und Beobachtung von Krebserkrankungen und zur Krebsforschung immer wieder Gegenstand eingehender Diskussionen. Allerdings zeichnete sich auf dem Gebiet der Gesetzgebung hierzu in Hessen kein Fortschritt ab, seit die Landesregierung 1982 die Arbeiten an einer gesetzlichen Grundlage für epidemiologische Krebsregister weitgehend eingestellt hat (vgl. 11. Tätigkeitsbericht, Ziff. 2.1.4.4). Dies scheint sich nunmehr zu ändern. Im September 1986 teilte mir der Sozialminister mit, das Kabinett habe anlässlich des Reaktorunfalls in Tschernobyl beschlossen, der Entwurf eines Krebsregistergesetzes vom 25. Mai 1982 solle unter besonderer Berücksichtigung des Datenschutzes überarbeitet werden und bat mich um Beratung. Ein erstes Gespräch hat inzwischen stattgefunden.

Bei der Diskussion über epidemiologische Krebsregister müssen verschiedene Fragenbereiche unterschieden werden. Die letzten Jahre haben deutlich gezeigt, daß bei der Auseinandersetzung um solche Register auch Kontroversen innerhalb der Ärzteschaft über den Stellenwert der medizinischen Forschung eine wichtige Rolle spielen. In neuerer Zeit ist darüber hinaus auch zum Teil die grundsätzliche Frage aufgeworfen worden, in welchem Umfang epidemiologische Krebsregister überhaupt in der Vergangenheit zur Bekämpfung von Krebserkrankungen beigetragen haben bzw. prinzipiell beitragen können. Während einerseits immer wieder auf konkrete Beispiele hingewiesen wird, die den Nutzen von Krebsregistern belegen, wird andererseits dagegen argumentiert, daß z.B. die in der Bundesrepublik in verschiedenen Bundesländern bereits seit vielen Jahren geführten Krebsregister bisher nur sehr begrenzte konkrete Ergebnisse erbracht haben und die vorhandenen Erkenntnisse nicht weiter verfolgt bzw. nicht politisch umgesetzt wurden. Angeführt wird auch, daß sich die im Zusammenhang mit Krebsregistern durchgeführte Forschung in unangemessener Weise auf individuelle Faktoren wie z.B. das Rauchen konzentrierte und bedeutsame allgemeine gesellschaftliche Ursachen der Krebsentstehung zu sehr ausblende. Schließlich wird zum Teil auch in Frage gestellt, ob ein Krebsregister mit standardisierten Datenerhebungen den komplexen Ursachen von Krebserkrankungen hinreichend Rechnung tragen kann. Diese Fragen gehen - auch wenn sie vielfach unter dem Stichwort "Datenschutz" erörtert werden - über datenschutzrechtliche Aspekte hinaus und müssen vorrangig von den zuständigen politischen Gremien überprüft und bewertet werden.

Hinsichtlich der datenschutzrechtlichen Fragen konnte bereits im 12. Tätigkeitsbericht (Ziff. 2.1.4.1) eine deutliche Annäherung der Positionen der Datenschutzbeauftragten und der zuständigen Gesundheitsministerien festgestellt werden. Zu dem gleichen Fazit gelangt auch die Landesregierung in ihrer Antwort vom 11. April 1985 auf die Große Anfrage der SPD-Fraktion betreffend Krebsregister (Drucks. 11/3565). Der Hessische Sozialminister hat sich meiner Auffassung angeschlossen, daß für die Errichtung eines epidemiologischen Krebsregisters angesichts der damit verbundenen Gefährdung des informationellen Selbstbestimmungsrechts auch dann, wenn die Meldungen an das Register auf einer Einwilligung des Patienten beruhen, eine umfassende gesetzliche Regelung der Verarbeitungsbedingungen der im Register enthaltenen Daten erforderlich ist (vgl. die Antwort der Landesregierung auf die Große Anfrage). Konsens besteht auch darüber, daß grundsätzlich die Einwilligung des Patienten für eine Meldung an das Register notwendig ist. Eine entsprechende Regelung hat der Sozialminister 1982 nach der von der Arbeitsgruppe Datenschutz und Datenverarbeitung des Innenausschusses des Landtags durchgeführten Anhörung in seinen Entwurf aufgenommen.

Ungeachtet der grundsätzlichen Annäherung der Standpunkte wird allerdings die konkrete Ausgestaltung einer gesetzlichen Regelung sorgfältig zu diskutieren sein. Insbesondere ist zu berücksichtigen, daß sich seit der Vorlage eines Gesetzentwurfs durch den Hessischen Sozialminister im Jahre 1982 die datenschutzrechtliche Diskussion weiter entwickelt hat. Ein Krebsregistergesetz gibt es inzwischen in Hamburg, seit 1984, und Nordrhein-Westfalen, seit 1985. Beide Gesetze enthalten zwar eine Reihe unterschiedlicher Vorschriften, gehen aber gemeinsam von dem Erfordernis einer Einwilligung des Patienten in die Meldung an das Register aus und lassen nur ausnahmsweise eine Übermittlung ohne Einwilligung zu. Vor einer weiteren Diskussion sollte zunächst geklärt werden, wie sich die verschiedenen Regelungen in den beiden Bundesländern in der Praxis ausgewirkt haben, nicht zuletzt auch deshalb, weil zum Teil Vermutungen geäußert werden, die Einwilligungslösungen würden in der Praxis unterlaufen und die vorgesehenen Ausnahmen zur Regel gemacht, d.h. die Einwilligung des Patienten werde regelmäßig nicht eingeholt. Ich habe daher den Sozialminister aufgefordert, mir konkrete Zahlen zur praktischen Handhabung der vorhandenen Einwilligungslösungen zur Verfügung zu stellen.

4.2.1.2

Klinische Krebsregister

Im Gegensatz zu den epidemiologischen Krebsregistern haben die klinischen Krebsregister bisher in der öffentlichen Diskussion kaum eine Rolle gespielt. Nichtsdestoweniger wird ihr Aufbau seit Jahren konsequent betrieben. So führt etwa die Deutsche Krebshilfe in einer 1984 gezogenen Bilanz ihrer 10jährigen Tätigkeit als wesentlichen Teil ihrer Projektförderung die klinischen Krebsregister an: Um Aufschluß darüber zu erhalten, ob eine Therapie oder Nachsorgephase erfolgreich verläuft, sei die Kontrolle des Patienten über ein klinisches Krebsregister "unerlässlich". An Tumorzentren und onkologischen Schwerpunktkrankenhäusern bildeten diese Dokumentationen das "Herzstück der medizinischen Überwachung".

Der Bundesminister für Arbeit und Sozialordnung mißt in seinem Bericht vom August 1985 über die Förderung von Modellmaßnahmen zum Aufbau von Tumorzentren und onkologischen Schwerpunkten in den Jahren 1981-1985 den klinischen Krebsregistern ebenfalls einen zentralen Stellenwert bei. Dem Bericht zufolge fördert der Bundesarbeitsminister seit 1981 schwerpunktmäßig sieben Bereiche, darunter:

- den Aufbau einer rechnergestützten Krankendokumentation (klinisches Krebsregister) durch die Bereitstellung von Mitteln zum Ausbau von Rechnern und Betriebssystemen sowie für Personalstellen;
- den Aufbau einer bundeseinheitlichen und vergleichbaren Dokumentation in Form einer rechnergestützten Krankendokumentation, um die Vergleichbarkeit der diagnostischen und therapeutischen Verfahren und ihrer Ergebnisse sicherzustellen.

Nach dem Bericht des Bundesarbeitsministers sind bis 1985 in der Bundesrepublik bereits 23 Tumorzentren und 20 onkologische Schwerpunktkrankenhäuser aufgebaut worden.

Auf den zunehmenden Aufbau klinischer Krebsregister auch in Hessen habe ich bereits in meinem 12. Tätigkeitsbericht (Ziff. 2.1.4.2) aufmerksam gemacht. In der Zwischenzeit hat sich diese Entwicklung verstärkt. Dies gilt insbesondere auch hinsichtlich klinikübergreifender zentraler Nachsorgedokumentationen. Im September 1986 haben die Vertreter der hessischen Tumorzentren Rhein-Main und Marburg-Gießen sowie die onkologischen Schwerpunktkrankenhäuser in Darmstadt, Fulda, Kassel, Limburg und Offenbach mit Vertretern der Kassenärztlichen Vereinigung Hessen, der Hessischen Krebsgesellschaft und des Sozialministers vereinbart, gemeinsam eine flächendeckende "kooperative Nachsorge" in Hessen zu organisieren. Alle Nachsorgeaktivitäten der Kassenärzte und der klinischen Fachabteilungen sollen im Rahmen dieser kooperativen Nachsorge zentral an den jeweiligen Tumorzentren bzw. Schwerpunktkrankenhäusern gespeichert und allen an der Nachsorge beteiligten Ärzten zugänglich gemacht werden. Damit soll auch eine breite empirische Basis für die wissenschaftliche Forschung geschaffen werden.

Die Landesregierung geht in ihrer Antwort auf die Große Anfrage betreffend Krebsregister (Drucks. 11/3565) auf die klinischen Krebsregister nur beiläufig ein, indem sie, wie eingangs erwähnt, die Funktionen epidemiologischer Krebsregister einerseits und klinischer Krebsregister andererseits voneinander abgrenzt. Im übrigen weist die Landesregierung nur kurz auf den Aufbau klinischer Krebsregister hin, Ausführungen zu den mit diesen Registern verbundenen datenschutzrechtlichen Fragen erfolgen nicht.

Demgegenüber habe ich in meiner von der Arbeitsgruppe Datenschutz und Datenverarbeitung des Innenausschusses angeforderten Stellungnahme vom 19. November 1985 zu der Antwort der Landesregierung betont, daß die aktuelle Entwicklung dieser Register ihre Einbeziehung in die datenschutzrechtliche Diskussion über Krebsregistrierungen erfordert und auf die Gefahr hingewiesen, daß der Behandlungsbezug der Datenspeicherungen weitgehend verlorengeht und sich die klinischen Register in eine verselbständigte Form der Patientendokumentation verwandeln. Auch um hierüber genauer Aufschluß zu erhalten, habe ich 1986 in dem onkologischen

Schwerpunktkrankenhäus Darmstadt sowie im Tumorzentrum Rhein-Main den Stand der Datenverarbeitung in den dort vorhandenen klinischen Krebsregistern, die Zweckbestimmung dieser beiden Register und die jeweils zur Gewährleistung des informationellen Selbstbestimmungsrechts der Patienten getroffenen Vorkehrungen überprüft.

4.2.2

Prüfung des klinischen Tumorregisters in den Städtischen Kliniken Darmstadt

Bei meiner Überprüfung des Tumorregisters der Städtischen Kliniken Darmstadt im Jahr 1986 haben mich sowohl die Städtischen Kliniken als auch die Kassenärztliche Vereinigung Hessen in konstruktiver Weise unterstützt. Die Städtischen Kliniken Darmstadt sind seit 1981 onkologischer Schwerpunkt im Sinne der 1980 ergangenen Empfehlungen der Arbeitsgemeinschaft Deutscher Tumorzentren (ADT) zur regionalen onkologischen Versorgung in der Bundesrepublik Deutschland.

4.2.2.1

Datenbestand

Das in den Kliniken geführte Tumorregister erfüllt zwei verschiedene Funktionen, weshalb auch zwei Datenbestände zu unterscheiden sind.

1.

Es ist ein klinisches Register einschließlich der sogenannten "Aktiv-Nachsorge". Gespeichert sind in diesem Datenbestand Daten über Patienten mit Tumorerkrankungen, die mindestens einmal in den Städtischen Kliniken behandelt wurden. Ferner sind hier auch die Daten von Patienten eines weiteren Krankenhauses, des Elisabethenstifts in Darmstadt, registriert. Zum Zeitpunkt meiner Prüfung waren die Daten von etwa 4000 Patienten in diesem Datenbestand. Den weiteren Kliniken der Region steht die Beteiligung an dem Register offen. Längerfristig ist daher mit einer erheblichen Zunahme des Datenbestandes zu rechnen.

2.

Das Tumorregister umfaßt ferner das "Darmstädter Nachsorgemodell", einen 1984 begonnenen Modellversuch der Städtischen Kliniken Darmstadt und der Kassenärztlichen Vereinigung Hessen zur EDV-gestützten passiven Tumornachsorge. Grundlage des Modells ist ein Vertrag zwischen der Kassenärztlichen Vereinigung und den Städtischen Kliniken, aufgrund dessen die Kliniken bestimmte Leistungen für die niedergelassenen Ärzte erbringen. Der Modellbeschreibung zufolge soll die Nachsorgedokumentation die patientenbezogene Dokumentation durch den Arzt ergänzen und allen Ärzten, die für die Behandlung eines Patienten zuständig sind, die vollständige Information über den Krankheitsverlauf sichern sowie die Prüfung der Effektivität der Primärbehandlung gewährleisten.

Gespeichert waren in diesem Datenbestand zum Zeitpunkt meiner Prüfung die Daten von etwa 400 kliniksexternen Patienten. Die Daten werden von den niedergelassenen Ärzten, die an dem Modell teilnehmen, auf Formblättern an das Tumorregister weitergegeben und anschließend dort in die Nachsorgedokumentation eingespeichert. Zum Zeitpunkt der Prüfung beteiligten sich 116 niedergelassene Ärzte aus der Darmstädter Region sowie 30 niedergelassene Ärzte außerhalb dieser Region an dem Modell. Angestrebt wird, alle Tumorpatienten der Region in der Nachsorgedokumentation zu erfassen.

Eine zeitliche Begrenzung der Datenspeicherung ist nicht vorgesehen. Für die Erfassung der Patientendaten wurden standardisierte Erkrankungs-, Behandlungs- und Nachsorgebögen entwickelt, die je nach Erkrankungsart variieren. Bei der Ausgestaltung des Datenkataloges werden die Empfehlungen der ADT berücksichtigt, die die Vergleichbarkeit der bundesdeutschen Dokumentationen untereinander sowie mit internationalen Dokumentationen sicherstellen sollen. Für die 4400 Patienten wurden insgesamt etwa 20.000 Bögen angelegt.

4.2.2.2

Rechtsgrundlage für die Speicherung im Register

4.2.2.2.1

Behandlungsvertrag

Gegenwärtig ist vorgesehen, daß eine Speicherung von Patientendaten im Tumorregister nur dann erfolgt, wenn der betroffene Patient eine Erklärung unterschrieben hat, daß er mit der "EDV-mäßigen" Speicherung seiner Daten einverstanden ist. Zweifelsohne haben die beteiligten Stellen mit dieser Verfahrensweise angestrebt, dem informationellen Selbstbestimmungsrecht der Patienten Rechnung zu tragen, dennoch wirft diese Praxis bislang ungelöste Rechtsfragen auf.

Die Datenspeicherung in einem klinischen Register soll der Behandlung der Patienten dienen. Dieser Zusammenhang wird gerade im Gegensatz zu der Speicherung in epidemiologischen Registern immer wieder hervorgehoben. Eine gesonderte ausdrückliche Einwilligung in die Speicherung ist nicht erforderlich, wenn und soweit die Speicherung vom Behandlungsvertrag gedeckt ist. Es stellt sich daher hier zunächst einmal die Frage, inwieweit überhaupt für eine Speicherung von Patientendaten im Tumorregister eine Einwilligung der Patienten notwendig ist. Eine Frage, die jedoch erst dann beantwortet werden kann, wenn - was bislang nicht der Fall ist - die künftige Verwendung der Registerdaten umfassend geklärt ist. Die gegenwärtige pauschale Verfahrensweise bei allen Patienten bedarf einer Abänderung. Unterschieden werden muß zwischen der Speicherung der Daten von Patienten der Städtischen Kliniken selbst, weiterer Kliniken sowie der niedergelassenen Ärzte. Auf jeden Fall muß von den externen Patienten eine Einwilligung eingeholt werden.

Klärungsbedürftig ist zudem, wie das informationelle Selbstbestimmungsrecht des Patienten im Rahmen der Nachsorgedokumentation praktisch gewährleistet werden kann. So ist zwar derzeit die Verwendung eines bestimmten Einwilligungsformulars vorgesehen, es bleibt jedoch letztlich dem niedergelassenen Arzt überlassen, ob und auf welche Weise er die Einwilligung des Patienten in die Speicherung einholt. Vor der Einspeicherung der von ihm gemeldeten Patientendaten in das Tumorregister wird nicht geprüft, ob eine wirksame Einwilligungserklärung des Patienten vorliegt.

4.2.2.2

Wortlaut der Einwilligungserklärung

Der Wortlaut des derzeit verwandten pauschalen Einwilligungsformulars trägt dem informationellen Selbstbestimmungsrecht nicht hinreichend Rechnung.

Dem Formular zufolge willigt der Patient in die "EDV-mäßige" Speicherung seiner Daten ein. Er erhält darüber hinaus lediglich den Hinweis, daß durch diese Speicherung "alle mitbehandelnden Ärzte in Klinik und Praxis schnell und vollständig über den Krankheits- und Behandlungsverlauf informiert werden" sollen. Durch diesen allgemein gehaltenen Text wird der Patient nicht hinreichend darüber informiert, daß seine Daten in einem zentralen Tumorregister gespeichert werden sollen, welches die Daten der Patienten nicht nur verschiedener Kliniken innerhalb der Städtischen Kliniken, sondern auch weiterer Krankenhäuser und darüber hinaus auch von niedergelassenen Ärzten enthält. Er wird auch nicht darüber unterrichtet, wo seine Daten gespeichert werden sollen. Aufgrund des Formulartextes dürften die Patienten der niedergelassenen Ärzte regelmäßig annehmen, der Arzt selbst werde ihre Daten speichern.

Der im Formular hinzugefügte Hinweis, daß die Speicherung der Daten ausschließlich der persönlichen medizinischen Betreuung dient, ist zudem so nicht zutreffend. Zum einen sollen die Daten in einem weiteren Behandlungszusammenhang, so z.B. für Verlaufskontrollen für ganze Patientengruppen, verwendet werden, zum anderen ist längerfristig eine wissenschaftliche Nutzung der Datenbestände vorgesehen. Dies ergibt sich auch aus dem Text der auf dem Formular enthaltenen folgenden Anmerkung: "Sollen diese Daten auch für wissenschaftliche Zwecke Anwendung finden, so wird dies streng anonymisiert erfolgen". Die auf dem Vordruck mitgeteilten Informationen sind damit insgesamt auch widersprüchlich. Die wiedergegebene Anmerkung begegnet zudem unter einem weiteren Gesichtspunkt Bedenken: Eine Übermittlung ohne Namen und Anschrift wird als "streng anonym" bezeichnet. Dies trifft jedoch keinesfalls zu.

4.2.2.3

Verantwortlichkeit für die Datenspeicherung im Register

Im Tumorregister werden zum Teil die eigenen Daten der Städtischen Kliniken, zum Teil die Daten Dritter - weiterer Krankenhäuser sowie niedergelassener Ärzte - in deren Auftrag verarbeitet. Durch die zentrale Zusammenführung dieser verschiedenen Datenarten in einem Register ergeben sich Risiken für den Datenschutz, weil die Gefahr einer unklaren Vermengung der rechtlichen Verantwortlichkeiten für die Rechtmäßigkeit und Richtigkeit der Datenverarbeitung nicht von der Hand zu weisen ist. In jedem Fall ist es unerlässlich, daß die Verantwortlichkeiten und die hierauf abgestimmten konkreten Verfahrensweisen zur Kontrolle der Datenverarbeitung klar festgelegt werden. Eine solche Festlegung liegt gegenwärtig nicht vor.

4.2.2.4

Online-Zugriff auf Daten des Tumorregisters

Derzeit steht bereits verschiedenen Kliniken innerhalb der Städtischen Kliniken Darmstadt sowie einem weiteren Krankenhaus ein Online-Zugriff (Direktzugriff) auf die Daten des Tumorregisters zur Verfügung. Eine Beteiligung weiterer Krankenhäuser aus der Region ist vorgesehen. Eine am Behandlungszusammenhang orientierte Ausge-

startung der Online-Zugriffsmöglichkeiten ist besonders wichtig, damit es zu keiner Veralterung der Datenspeicherungen im Register kommt. Konkret: Es muß sichergestellt werden, daß die Kliniken jeweils nur auf die Daten der von ihnen (mit-)behandelten Patienten Zugriff haben.

Bei meinem Prüfbesuch im Juni 1986 hatte mir das Tumorzentrum mitgeteilt, jeder Benutzer könne nur auf Daten der Patienten, für die er (bzw. seine Klinik, sein Oberarzt) als "mitbehandelnd" im Datensatz eingetragen sei, zugreifen. Damit wäre der Behandlungszusammenhang gewahrt gewesen. Spätere Nachfragen haben jedoch ergeben, daß der Zugriff nicht in der beschriebenen Weise beschränkt ist:

Alle Zugriffsberechtigten (Sekretärinnen und Ärzte) der online- angeschlossenen Kliniken haben Online-Zugriff auf einen Teil der Stammdaten aller Patienten, die im Tumorregister gespeichert sind (Ärzte nur lesend, Sekretärinnen auch schreibend/verändernd): auf Nachname, Vorname, Geburtsdatum und einen Teil der Anschrift. Als "Suchkriterium" ist jedes der vier Merkmale Name, Vorname, Geburtsname und Geburtsdatum verwendbar sowie Teile davon. Wenn es mehrere Patienten gibt, die das Suchkriterium erfüllen, werden alle fortlaufend nummeriert angezeigt. Zum Beispiel: Alle Patienten, deren Nachname mit "S" beginnt. Alle Patienten, deren Nachname mit "Schneider" beginnt. Alle Patienten, die "Schneider, Wilhelm" heißen. Alle Patienten, die "1940" oder im "September" (irgendeines Jahres) oder am "3. Oktober" geboren sind.

Gegen diese Ausgestaltung der Zugriffsmöglichkeiten bestehen erhebliche Bedenken. Insbesondere geht ein Online-Zugriff eines Krankenhauses auf einen Teil der Patientendaten eines anderen Krankenhauses über den Behandlungszusammenhang hinaus und steht mit dem Gebot der ärztlichen Schweigepflicht nicht in Einklang. Darüber hinaus kann nach meinen Feststellungen die Begrenzung der Zugriffsberechtigung für medizinische Daten auf diejenigen Patienten, die von der Klinik (mit-)behandelt werden, leicht umgangen werden. Die Ausgestaltung der Online-Zugriffsberechtigungen muß daher so verändert werden, daß der Behandlungszusammenhang der Speicherungen gewahrt wird.

4.2.2.5

Auswertung der Registerdatenbestände

Angesichts der besonderen Sensibilität der im Tumorregister gespeicherten Daten und der Gefahr der Herauslösung des Registers aus dem Behandlungszusammenhang halte ich es für erforderlich, daß verbindlich festgelegt wird, wer welche Arten von Auswertungen aus dem Tumorregister erhalten darf und wer im Einzelfall in welchem Verfahren über eine Verwendung der Datenbestände und die Anforderungen an die Anonymisierung entscheidet. Darüber hinaus muß im Tumorregister protokolliert werden, wer wann auf wessen Aufforderung welche Auswertungen vorgenommen hat und wem sie zugeleitet wurden. Klärungsbedürftig ist ferner - wie auch der Text der derzeit benutzten Einwilligungserklärung zeigt -, welche Anforderungen an eine faktische Anonymisierung gestellt werden.

4.2.2.6

Datensicherung

Bei meiner Prüfung habe ich auch Mängel bei der Datensicherung festgestellt und folgende Maßnahmen vorgeschlagen:

- Die Schließzylinder für den ADV-Bereich sollten aus dem Schließsystem herausgenommen und die Schlüsselvergabe restriktiv gehandhabt werden.
- Im Rechenzentrum sollte das Führen eines Besucherbuchs festgelegt werden.
- Die Schutzmöglichkeiten des Betriebssystems und der Software sollten optimal ausgenutzt werden, um eine größtmögliche Abschottung der Benutzer des Tumorregisters, des Kraztur- System-Managers und der übrigen Rechner-Benutzer zu erreichen. Dasselbe gilt für die Abschottung des Datenbestandes und der Programme. Eine einzige Benutzererkennung auf Betriebssystemebene für alle Benutzer des Tumorregister-Datenbestandes mit einer Paßwort-Änderung alle 180 Tage ist in jedem Fall unzureichend. Neben solchen Maßnahmen auf der jeweiligen Systemebene sollten auch Hardware-Änderungen (z.B. eigene Festplatte für das Tumorregister) in die Überlegungen einbezogen werden.
- Der Betriebssystemzugang sollte auf das unbedingt notwendige Maß beschränkt werden, d.h. wenn irgend möglich Durchschalten auf Anwenderprogramm-Ebene mittels LOGIN-Prozedur. Positiv aufgefallen ist mir die Verwendung von LOGIN- Prozeduren, die dem Benutzer bei der Anmeldung den Zeitpunkt des letzten LOGONS und die Anzahl der inzwischen erfolgten Fehlversuche am Bildschirm anzeigen. Wünschenswert ist eine Änderung dahingehend, daß der Benutzer diese Angaben in Ruhe zur Kenntnis nehmen und überprüfen kann, bevor dieser Bildschirminhalt gelöscht wird.

- Auch wenn aus personellen Gründen eine strikte Trennung von Test und Produktion und von Operating und Programmierung nicht durchhaltbar ist, sollte diese Trennung doch soweit als möglich durchgeführt werden.

Darüber hinaus habe ich empfohlen, bei der Beratungsstelle der zuständigen örtlichen Kriminalpolizeidienststelle bzw. beim Landeskriminalamt in Wiesbaden - falls noch nicht geschehen - eine Schwachstellenanalyse und ein Gutachten über die erforderlichen Bausicherungsmaßnahmen für die Gebäude des Rechenzentrums und des Datenträgerarchivs in Auftrag zu geben und auf dieser Grundlage die erforderlichen Maßnahmen unverzüglich einzuleiten.

Wegen der besonderen Sensibilität des Datenbestandes des Tumorregisters und der Besonderheiten eines klinikübergreifenden zentralen Registers ist überdies eine präzise Dienstanweisung für die Mitarbeiter des Tumorregisters unerlässlich.

4.2.2.7

Zusammenfassung der wichtigsten Prüfergebnisse

- Die ausschließliche Verarbeitung der Registerdaten im Rahmen der Behandlung ist gegenwärtig nicht hinreichend sichergestellt. Zwar ist der Inhalt der Daten und ihre bisherige Verwendung im wesentlichen auf die Behandlung zugeschnitten. Es sind jedoch Ansätze für eine Lockerung des Zusammenhangs der Datenspeicherung im Tumorregister mit der Behandlung des Patienten, d.h. für eine Verselbständigung des Registers, zu verzeichnen. Weder ist eine zeitliche Begrenzung der Datenspeicherung vorgesehen, noch sind beispielsweise die Online-Zugriffsmöglichkeiten (Direktzugriffsmöglichkeiten) hinreichend am Behandlungszusammenhang orientiert. Indiz für eine tendenzielle Verselbständigung ist auch, daß es keine eindeutige rechtliche Verantwortlichkeit der jeweiligen behandelnden Ärzte bzw. Kliniken für die Rechtmäßigkeit und Richtigkeit der Speicherung ihrer Patientendaten gibt. Ferner ist die Verfahrensweise bei Auswertungen des Registers nicht hinreichend geklärt und festgelegt.
- Für die Speicherung der Daten externer Patienten ist in jedem Fall eine Einwilligung erforderlich. Das gegenwärtig verwandte pauschale Einwilligungsformular bedarf einer Überarbeitung.
- Schließlich sind eine Reihe zusätzlicher Maßnahmen zur Verbesserung der Datensicherung notwendig.

4.2.2.8

Letzter Stand des Verfahrens

Die Städtischen Kliniken Darmstadt, den Hessischen Sozialminister sowie die Kassenärztliche Vereinigung habe ich über die von mir festgestellten Probleme unterrichtet. Im November ist mir ein Antwortschreiben der Städtischen Kliniken Darmstadt zugegangen. Die von mir dargelegten Problempunkte sind jedoch bisher in keiner Weise zufriedenstellend geklärt. Zur Frage des Behandlungszusammenhangs der Datenspeicherungen haben die Kliniken nicht Stellung genommen. Hinsichtlich der Formulierung der Einwilligungserklärung wird von den Kliniken auf die Kassenärztliche Vereinigung verwiesen. Demgegenüber muß betont werden, daß die Kliniken in jedem Fall für die Fragen der Rechtmäßigkeit der Verarbeitung der Daten ihrer eigenen Patienten verantwortlich sind. Es zeigt sich hier bereits sehr deutlich die mit der Zusammenführung der Daten der Städtischen Kliniken Darmstadt, weiterer Kliniken sowie der niedergelassenen Ärzte in einem zentralen Register verbundene Gefahr der Vermengung von Verantwortlichkeiten für die Datenverarbeitung. Auch die weiteren von mir aufgeführten Punkte sind nach wie vor klärungsbedürftig.

4.2.3

Prüfung des klinischen Tumorregisters im Klinikum der Frankfurter Universität

Im Jahr 1986 habe ich außerdem das klinische Tumorregister im Klinikum der Frankfurter Universität überprüft. Das Register wird vom Tumorzentrum Rhein-Main geführt. Dieses Tumorzentrum - ein eingetragener Verein - wurde 1979 gegründet. Es entstand aus der Zusammenfassung der onkologisch tätigen Abteilungen im Universitätsklinikum. Seiner Satzung zufolge soll es die sachgebietsbezogene und interdisziplinäre Zusammenarbeit aller an der Tumorbekämpfung beteiligten Ärzte und Institutionen fördern und hat außerdem die Aufgabe, "die diagnostischen und therapeutischen Maßnahmen, ihre Durchführung und ihre Ergebnisse sachgerecht und nach einheitlichen Gesichtspunkten zu dokumentieren und ein Tumorregister aufzubauen, dabei die Datennutzung nicht auf das Tumorzentrum Rhein-Main zu beschränken, sondern regional übergreifende Verwendung im Rahmen kooperativer Studien einzuschließen".

4.2.3.1

Umfang der Datenverarbeitung

Im Unterschied zum Darmstädter Register werden gegenwärtig im Frankfurter Register ausschließlich die Daten der eigenen Patienten des Klinikums gespeichert. Eine Übernahme des "Darmstädter Nachsorgemodells" und damit auch die Beteiligung weiterer Kliniken sowie niedergelassener Ärzte an dem Register ist jedoch bereits mit der Kassenärztlichen Vereinigung abgeprochen und soll in Kürze realisiert werden. Einzelheiten sind derzeit jedoch noch nicht geklärt. Die verschiedenen Abteilungen der Universitätskliniken, die sich mit Onkologie befassen, werden erst nach und nach in die Tätigkeit des Tumorzentrums integriert. Insofern befindet sich auch die Datensammlung des Tumorregisters gegenwärtig noch im Aufbau. Zum Zeitpunkt meiner Prüfung waren im Register die Daten von ca. 2000 Patienten aus verschiedenen Abteilungen gespeichert. Eine Einwilligung der Patienten wird - im Gegensatz zu Darmstadt - nicht eingeholt, weil davon ausgegangen wird, daß die Speicherung im Rahmen der Behandlung erfolgt. Von einer erheblichen Zunahme des Registerumfangs in den nächsten Jahren ist auszugehen. Bei der Ausgestaltung des Datenkataloges werden auch in Frankfurt die Empfehlungen der ADT berücksichtigt, die die Vergleichbarkeit mit anderen Dokumentationen sicherstellen sollen.

4.2.3.2

Die wichtigsten Prüfergebnisse

Die Prüfung, bei der mich das Universitätsklinikum sehr unterstützt hat, hat eine Reihe klärungsbedürftiger Probleme ergeben. Zum Teil handelt es sich um strukturelle Fragen des Aufbaus eines klinischen Krebsregisters, wie sie sich auch in Darmstadt stellen, zum Teil um klinikspezifische Probleme.

4.2.3.2.1

Rechtsgrundlage der Datenspeicherung

Von zentraler Bedeutung war für mich auch bei der Prüfung des Frankfurter Registers die Frage, ob der Zusammenhang der Datenspeicherungen mit der Behandlung der Patienten gesichert ist. Die Prüfung hat gezeigt, daß die Verarbeitung der Daten im Register derzeit im wesentlichen auf die Behandlung der Patienten zugeschnitten ist. Dies gilt insbesondere für den Inhalt der Datenspeicherungen, die konkrete Ausgestaltung der Online-Zugriffsberechtigungen für die medizinischen Daten und die bisherige Verwendung der Registerdaten. Andererseits ist festzustellen, daß auch in Frankfurt keine an dem Behandlungszeitraum orientierten Lösungsfristen für die Datenspeicherungen vorgesehen sind. Ferner ist langfristig eine Erweiterung des Datensatzes auf Anamnesedaten geplant, so daß hier die Unterscheidung zwischen klinischem Register und Inzidenzregister zu verwischen beginnt. Vor allem aber bedarf es im Hinblick auf die geplante Übernahme des sogenannten "Darmstädter Nachsorgemodells" sowie auf die in der Satzung vorgesehene überregionale Verwendung des Datenbestandes einer Klärung, wie der Behandlungszusammenhang der Datenspeicherung auf Dauer konkret gesichert werden soll und ob, wenn ja, in welchem Umfang und in welcher Form künftig eine Einwilligung der Patienten in die Datenspeicherung im Register eingeholt werden muß.

4.2.3.2.2

Verantwortlichkeit für die Datenspeicherung im Register

Ebenso wie für das Darmstädter Register ist auch für das Frankfurter Register unerlässlich, daß die Verantwortlichkeit für die Rechtmäßigkeit und Richtigkeit der Datenverarbeitungen und die dementsprechend konkreten Verfahrensweisen zur Kontrolle klar festgelegt werden.

4.2.3.2.3

Auswertungen des Registerdatenbestandes

Für das Frankfurter Register gilt wie für das Darmstädter Register, daß angesichts der besonderen Sensibilität der gespeicherten Daten sowie der Gefahr der Herauslösung des Registers aus dem Behandlungszusammenhang eine präzise Festlegung der Verwendungszwecke der Daten unerlässlich ist. Es bedarf eines klaren Konzepts, wer welche Arten von Auswertung aus dem Tumorregister erhalten darf und wer im Einzelfall in welchem Verfahren über eine Verwendung der Datenbestände und die Anforderungen an die faktische Anonymisierung entscheidet. Dies gilt um so mehr, als in offiziellen Darstellungen immer wieder auf die Bedeutung des Frankfurter Tumorregisters für Forschungszwecke hingewiesen wird.

Auf meine Anfrage hin hat das Universitätsklinikum in der Zwischenzeit ein Konzept für die Auswertungen des Registerdatenbestandes vorgelegt. Daraus geht hervor, daß Auswertungen des Registers in erheblichem Umfang auch externen Stellen zur Verfügung gestellt werden sollen. Neben den Ärzten der dem Tumorzentrum angeschlos-

senen Zentren bzw. Abteilungen sollen auch das Bundesministerium für Arbeit und Sozialordnung oder von ihm beauftragte Institute Auswertungen erhalten können, ferner "andere Personen oder Institute, die ein berechtigtes Interesse nachweisen können". Zur Verfügung gestellt werden sollen nur anonymisierte Daten.

Dieses Konzept ist in jedem Fall noch konkretisierungsbedürftig. Dies gilt zum einen hinsichtlich der konkreten Verfahrensweise bei der Durchführung und Weitergabe von Auswertungen, zum anderen auch hinsichtlich der Anforderungen an eine faktische Anonymisierung der Patientendaten. Gegenwärtig wird davon ausgegangen, daß ein Datensatz, der u.a. die Kliniknummer, die klinikspezifische Patientenidentifikationsnummer, das vollständige Geburtsdatum des Patienten, das Geschlecht, den Wohnort, die Staatsangehörigkeit, den derzeitigen sowie den am längsten ausgeübten Beruf, das Datum der ersten ärztlichen Diagnose sowie detaillierte medizinische Angaben über die Erkrankung enthält, als anonymisiert anzusehen ist. Dieser Auffassung kann ich keinesfalls zustimmen. Es handelt sich vielmehr eindeutig um personenbezogene Daten, da ein Rückbezug auf den betreffenden Patienten mit geringem Zusatzwissen und ohne großen Aufwand hergestellt werden kann. Wenn eine hinreichende Anonymisierung der Daten nicht sichergestellt wird, bedeutet dies, daß eine Verwendung der Patientendaten außerhalb des Behandlungszusammenhangs und damit ohne Rechtsgrundlage erfolgt.

4.2.3.2.4

Datensicherung

Zur Verbesserung der Datensicherheit halte ich folgende Maßnahmen für notwendig:

- Das "Datenschutzkonzept RZ" sollte zur Dienstanweisung und damit für alle Mitarbeiter zur verbindlichen Regelung erklärt werden.
- Regelmäßige Paßwortänderungen am Schnittstellenverteiler PACX und Verbesserung der Kontrolle bei Fehlversuchen.
- Regelmäßige Änderung der Paßwörter zum Zugriff auf die Tumorzentrumssoftware.
- Verbesserungen der Benutzer- und Zugriffskontrolle, wie sie für die verwendete BAIK-Software (BAIK Befunddokumentation und Arztbriefschreibung im Krankenhaus) geplant sind, sollten für die Tumorzentrum-Software unverzüglich und umfassend genutzt werden.

Das Universitätsklinikum Frankfurt sowie den Hessischen Sozialminister und den Hessischen Minister für Wissenschaft und Kunst habe ich über die von mir festgestellten Problempunkte unterrichtet.

4.2.4

Konsequenzen

Meine Prüfungen in Darmstadt und Frankfurt haben eindeutig bestätigt, daß die klinischen Krebsregister verstärkt in eine öffentliche Diskussion einbezogen werden müssen. Der Aufbau dieser Register ist in Hessen bereits weit fortgeschritten. Den datenschutzrechtlichen Fragen ist dabei bisher zu wenig Beachtung geschenkt worden. Neben klinikspezifischen Einzelfragen habe ich eine Reihe von Problempunkten festgestellt, die grundsätzliche strukturelle Fragen der klinischen Krebsregister betreffen und einer einheitlichen Lösung für alle klinischen Register in Hessen bedürfen. Zentral geht es dabei darum, wie der Behandlungszusammenhang dieser Datenspeicherungen dauerhaft gewährleistet werden und der Gefahr einer Verselbständigung der klinischen Register entgegengewirkt werden kann. Die Funktionen der epidemiologischen Register einerseits und der klinischen Register andererseits beginnen sich zu vermischen. Die von der Landesregierung in ihrer Antwort auf die Große Anfrage betreffend Krebsregister dargelegte Abgrenzung der beiden Registerarten (vgl. oben Ziff. 2.1) muß daher im Hinblick auf die sich abzeichnende weitere Entwicklung der klinischen Register in Frage gestellt werden.

Angesichts dieser Sachlage habe ich die Hessische Landesregierung aufgefordert, darauf hinzuwirken, daß die beteiligten Stellen ein Datenschutzkonzept für die klinischen Krebsregister vorlegen. In dem Konzept muß insbesondere präzise zwischen kliniksinternen Dokumentationen und Nachsorgedokumentationen mit Beteiligung externer Stellen unterschieden werden. Bereits in ihrem Beschluß vom 4. November 1983 (vgl. 12. Tätigkeitsbericht, Ziff. 2.1.4.2.2) hat die Konferenz der Datenschutzbeauftragten darauf hingewiesen, daß die Einrichtung klinischer Krebsregister durch Datenschutzkonzeptionen ergänzt werden muß, die der besonderen Sensitivität dieser Datensammlungen gerecht werden. Ein solches Konzept besteht in Hessen gegenwärtig nicht. Für die einzelnen datenschutzrechtlichen Fragen sind verschiedene Ansprechpartner vorhanden. Angesichts des fortschreitenden Ausbaus der klinischen Register halte ich es für dringend geboten, daß die datenschutzrechtlichen Fragen in einem Gesamtzusammenhang erörtert, bewertet und entschieden werden und ein einheitliches Konzept vorgelegt wird, wie dem informationellen Selbstbestimmungsrecht der Patienten in Zukunft Rechnung getragen werden soll. Das vorzulegende Konzept sollte insbesondere Ausführungen zu den folgenden Punkten enthalten:

- Eine Präzisierung der Funktionen der klinischen Krebsregister in Abgrenzung zu epidemiologischen Krebsregistern;
- strukturelle Maßnahmen zur Sicherstellung des Behandlungszusammenhangs der Datenspeicherungen in den klinischen Registern sowie der Verantwortlichkeit der jeweiligen speichernden Stellen oder Personen einschließlich der konkreten Kontrollmöglichkeiten;
- Ausgestaltung der Online-Zugriffsmöglichkeiten;
- Umfang der Verwendung und konkrete Ausgestaltung einer dem Patienten vorzulegenden Einwilligungserklärung für die Datenspeicherung im Register;
- Nutzung der Datenbestände, insbesondere Umfang und Art und Weise der Nutzung der Datenbestände zu wissenschaftlicher Forschung;
- Rechte der Patienten einschließlich der Unterrichtung über die Registrierung. In ihrem Beschluß von 1983 haben die Datenschutzbeauftragten darauf hingewiesen, daß sich die subjektiven Rechte der Patienten gegen die behandelnde Einrichtung oder Person richten müssen. Wenn allerdings der Patient überhaupt nichts von der Existenz eines klinischen Krebsregisters erfährt, laufen seine Rechte - z.B. auf Berichtigung, Löschung oder Auskunft über seine Daten - leer, und die Gefahr einer Verselbständigung des Registers verstärkt sich.
- Technische und organisatorische Maßnahmen zur Datensicherheit.

Angesichts der Vielzahl der an dem Aufbau der klinischen Register beteiligten Einrichtungen und Personen müssen in dem Konzept auch Ausführungen darüber enthalten sein, auf welche Weise die konkrete Umsetzung der Datenschutzkonzeption gewährleistet werden soll. Sollte es sich zeigen, daß das informationelle Selbstbestimmungsrecht der Patienten mit Hilfe einer solchen Datenschutzkonzeption nicht hinreichend und dauerhaft sichergestellt werden kann, so muß eine gesetzliche Regelung der klinischen Krebsregister erfolgen.

4.3

Prüfung des Laborsystems LABOSYS des DV-Verbundes

4.3.1

Ziel und Verfahren der Prüfung

In diesem Bericht habe ich die rapide Zunahme der Automatisierung der Datenverarbeitung in den Krankenhäusern beschrieben, die sich nicht nur auf den Verwaltungsbereich beschränkt, sondern auch im ärztlichen Bereich zu verzeichnen ist (vgl. Ziff. 4.1.1). Ein Beispiel für den Einsatz von DV-Verfahren im medizinischen Bereich ist das Laborverfahren LABOSYS, das der Hessische DV-Verbund seit Anfang 1986 anbietet. Pilotanwender waren die Städtischen Kliniken Wiesbaden, die am 5. März 1986, nachdem die Software im Routine-Betrieb lief, zu einer Demonstration eingeladen hatten.

Dieses Laborsystem, mit dem in den Städtischen Kliniken drei Laborärzte und über 30 medizinisch-technische Assistentinnen arbeiten, habe ich in diesem Jahr überprüft. Dabei ging es zum einen um Fragen der Datensicherheit, zum anderen aber auch um die interne Abschottung des Systems innerhalb der Kliniken, denn die ärztliche Schweigepflicht und das in § 5 Bundesdatenschutzgesetz normierte Datengeheimnis verbieten es, das Krankenhaus als eine Einheit anzusehen, innerhalb der Daten uneingeschränkt genutzt werden dürfen. Es muß vielmehr sichergestellt werden, daß jeder der im Krankenhaus Beschäftigten nur die für seine Aufgabenerfüllung erforderlichen personenbezogenen Daten zur Kenntnis nehmen kann (vgl. hierzu auch Ziff. 4.1.3). In LABOSYS werden in erheblichem Umfang personenbezogene Daten verarbeitet: Gespeichert werden die Daten aller stationär aufgenommenen Patienten - pro Jahr etwa 24.000 - sowie ein Teil der pro Jahr etwa 30.000 ambulant behandelten Patienten.

LABOSYS ist kein festes, unveränderliches System. Vielmehr kann und muß das vom Hersteller gelieferte Programmsystem an die (teilweise unterschiedlichen) Anforderungen der jeweiligen Klinik und ihres Labors angepaßt werden. Diese Anpassung beinhaltet sowohl rein medizinische (z.B. Eingeben von Normalwerten) als auch technische und organisatorische Aspekte (z.B. welche Analysegeräte, wie viele Bildschirme und Drucker werden angeschlossen, welche Formulare sind zu benutzen, wie sollen verschiedene Listen ausgedruckt werden). Sie beinhaltet aber auch Fragen, die aus der Sicht des Datenschutzes wichtig sind, wie z.B.:

- wer kann das Laborsystem von welchen Endgeräten aus benutzen;

- welche Abstufungen der Benutzungsberechtigung gibt es etwa bezüglich des Umfangs, in dem auf personenbezogene Daten zugegriffen werden kann oder hinsichtlich der Funktionen, die genutzt werden können (z.B. Eingabe von Labordaten, Ändern von Stammdaten, Zulassung neuer Systembenutzer, Änderung der Zugriffsberechtigung vorhandener Benutzer, Änderung von Kennwörtern, mit denen die Zugriffsberechtigung überprüft wird).

Damit wird deutlich, daß eine datenschutzrechtliche Bewertung einer Pilotinstallation sich sinnvollerweise auf zwei verschiedenen Ebenen bewegen sollte:

1. Prüfung der Möglichkeiten, die das System, so wie es vom Hersteller geliefert wird, bietet.
2. Prüfung, welche der Möglichkeiten von der konkreten Installation wie genutzt werden.

Nun stellte sich heraus, daß es weder eine allgemeine Verfahrensbeschreibung des Laborsystems und seines Aufbaus noch eine konkrete Beschreibung der Installation bei den Städtischen Kliniken Wiesbaden gibt. Erstere sollte zumindest für den/die für ein solches System beim Anwender Verantwortlichen zur Verfügung stehen, letztere sollte als Ergebnis der Installation vorliegen und auch spätere Änderungen dokumentieren.

Wohlgemerkt: Es handelt sich bei diesen Unterlagen nicht um eine datenschutzspezifische Darstellung - eine solche existiert ebenfalls nicht -, sondern um allgemeine Unterlagen, die ein - doch recht umfangreiches und komplexes - Programmsystem und seine konkrete Installation beschreiben. Solche Unterlagen sind üblicherweise Grundlage zunächst für die Einführung des Systems und die Anwenderschulung und später für Wartung und Pflege des Systems.

4.3.2

Das System LABOSYS

Der Aufbau des Laborsystems LABOSYS und die für den Datenschutz verwendbaren Komponenten lassen sich wie folgt skizzieren:

- Die Software ist in der Form eines sogenannten Menübaums aufgebaut, d.h. der Bediener wird mit einem Inhaltsverzeichnis und Bedienerhinweisen, die auf dem Bildschirm erscheinen, in dem Programm geführt. So erscheint nach der Eingabe eines Kennwortes, mit dem die Berechtigung des Benutzers überprüft wird, am Bildschirm ein Ausgangsmenü, nach Wahl eines Menüpunktes das zu diesem gehörige Menü etc. Dabei werden - mit einer Ausnahme - jeweils nur solche Menüpunkte angezeigt, zu denen die dem Kennwort zugeordnete Benutzergruppe berechtigt ist.
- Es gibt verschiedene Benutzergruppen für LABOSYS mit jeweils unterschiedlichen Berechtigungsprofilen. Die umfassendste Berechtigung haben die Systemspezialisten, d.h. die für die Betreuung und Programmierung des Laborsystems verantwortlichen Mitarbeiter des Kommunalen Gebietsrechenzentrums Gießen, das das System vertreibt und wartet, und des Softwareherstellers. Nach Angaben des Kommunalen Gebietsrechenzentrums sollte der für das Laborsystem in der Klinik Verantwortliche weder Benutzer dieser Gruppe neu zuordnen noch Kennwörter oder Berechtigungsprofile von Benutzern dieser Gruppe ändern können. Er kann aber weitere Berechtigungsprofile definieren (z.B. für die medizinisch-technischen Assistentinnen oder die Laborärzte), Personen zu einer solchen Benutzergruppe zulassen und ihnen hierfür ein persönliches Kennwort zuordnen.

Zur Nutzung dieser Funktion "Kennwort-Dialog", mit der Kennwörter eingerichtet, geändert und zu Benutzergruppen zugeordnet werden können, muß der Systemverantwortliche der Klinik selbst durch sein Berechtigungsprofil berechtigt sein, und er muß das zugehörige "Funktionsschlüsselwort" kennen, das vor dem Aufruf dieser Funktion abgefragt wird.

- Wenn bis zum Ablauf einer Zeitschranke (sogenanntes time-out), die für jede Installation einstellbar ist, keine Eingabe am Terminal erfolgt, schaltet das System automatisch auf das nächst höhere Menü zurück; beim Ausgangsmenü wird die Verbindung zum Programm unterbrochen, so daß erst nach erneuter Eingabe eines Kennwortes weitergearbeitet werden kann.
- Sämtliche Patientendaten stehen nicht unter der Benutzer-/Anwendungskennung des Laborsystems, sondern zentral unter der Systemkennung, das betrifft sowohl den Datenbestand mit den Patienten-Stamm- und Abrechnungsdaten, der auch von anderen Softwaresystemen der Herstellerfirma (wie z.B. dem Radiologiesystem RADOS) genutzt werden soll, als auch die anwendungsspezifischen Patientendaten, also etwa die eigentlichen Labordaten oder die Radiologiedaten, die von der entsprechenden Anwendung, beispielsweise von LABOSYS oder von RADOS, verwaltet werden sollen. Alle diese Daten sind ohne große Programmierkenntnisse mit wenigen festen Informationen abrufbar. Damit wird deutlich, daß verschiedene Programme der Herstellerfirma auf demselben Rechner untereinander nicht hinreichend abgeschottet sind.

Ich habe daher das Kommunale Gebietsrechenzentrum Gießen aufgefordert sicherzustellen, daß jeder Beschäftigte nur die für seine jeweilige Aufgabenerfüllung erforderlichen Daten zur Kenntnis nehmen kann, auch wenn auf dem Laborrechner weitere Anwendungen laufen.

Wünschenswert ist darüber hinaus, das Programmsystem so zu ändern, daß nach Ablauf der Zeitschranke nicht auf das nächsthöhere Menü zurückgeschaltet, sondern direkt die Verbindung zum Programm unterbrochen wird. Damit würde verhindert, daß bis zum Abschalten des Programms ein Vielfaches der Zeitschranke vergehen muß, falls der Benutzer auf einem logisch tieferen Menü sein Gerät verlassen hat.

4.3.3

Realisierung in den Städtischen Kliniken Wiesbaden

4.3.3.1

Zugriffsberechtigung

Im zweiten Halbjahr 1986 habe ich das in den Städtischen Kliniken Wiesbaden installierte Laborsystem überprüft. Als ein Vertreter des Kommunalen Gebietsrechenzentrums Gießen im September die verschiedenen Schutzmechanismen demonstrieren wollte, gab es allerdings Überraschungen:

- Er konnte mehrmals hintereinander den "Kennwort-Dialog" aufrufen, ohne nach dem genannten Funktionsschlüsselwort gefragt zu werden;
- er konnte Benutzer zur Gruppe der Systemspezialisten neu zulassen;
- beim Anlisten der bereits zugelassenen Benutzer fiel ein Benutzer mit dem Namen "HACKER" auf, der der Benutzergruppe der Systemspezialisten angehörte. Das Kommunale Gebietsrechenzentrum hat diesen Benutzer sofort aus dem System gelöscht, weil es unter den Benutzern von LABOSYS niemand mit diesem Namen gibt und falsch benannte Benutzer, insbesondere mit dieser höchsten Berechtigungsstufe, in einem solchen System nichts zu suchen haben. Es ließ sich nachträglich nicht feststellen, wer diesen Benutzer zugelassen hatte;
- beim erneuten Aufruf des "Kennwort-Dialogs" wurde jetzt plötzlich ein Funktionsschlüsselwort verlangt. Im Kommunalen Gebietsrechenzentrum hat man als Erklärung dafür entweder einen Programmfehler (der mehrfach hintereinander und dann plötzlich gar nicht mehr auftrat!) oder die kurzfristige Einrichtung eines Funktionsschlüsselwortes für diese Funktion.

Da es keine automatische Protokollierung der von den Benutzern des Rechners veranlaßten Aktivitäten gibt, ist auch nicht nachvollziehbar, wann und von wem welche Änderungen an Programmen, Schlüsselwörtern etc. vorgenommen wurden. Auch eine manuelle Dokumentation vorgenommener Änderungen existiert nicht. Hinzu kommt, daß der Laborleiter der Systemverantwortliche für LABOSYS ist, während der Rechenzentrumsleiter der Klinik nur für den technischen Betrieb des Rechners verantwortlich ist. Diese formale Zuständigkeit verkennt das Problem, daß der Rechenzentrumsleiter, das Kommunale Gebietsrechenzentrum Gießen und der Software-Hersteller nicht nur mindestens ebensoviel über das DV-System wissen, sondern auch mit ihrer Programmierberechtigung umfassend Zugriff haben, ohne daß der Laborleiter, dessen Zugriffsmöglichkeiten auf das System im Vergleich stark beschränkt sind (er hat keine Programmierberechtigung), über eine entsprechende Kontrollmöglichkeit verfügt, die selbstverständlich von den übrigen Beteiligten nicht manipulierbar sein dürfte.

Eine Nachprüfung im Dezember ergab, daß nicht der "Kennwort-Dialog" selbst, wohl aber seine übergeordnete Funktion beim Aufruf durch ein Funktionsschlüsselwort geschützt ist. Auch der Bestand der zugelassenen Benutzer war inzwischen bereinigt worden: Es waren keine Benutzer mehr mehrfach zugelassen, und es gab keine offensichtlich unzulässigen Benutzereinträge mehr, wie den "HACKER" im September. Zusätzlich stellte sich heraus, daß der Betriebssystemzugang zum Laborrechner inzwischen nur noch im Rechenzentrum und über den Wählanschluß möglich ist, während alle übrigen Bildschirme direkt auf ein Anwendungsprogramm geschaltet sind.

Notwendig ist allerdings noch eine Reihe weiterer Maßnahmen:

- Es muß ein Systemverantwortlicher in den Kliniken benannt werden, der sowohl von seinen Befugnissen/Berechtigungen als auch von seiner Systemkenntnis und mit der vom System geleisteten Unterstützung (letztere muß evtl. geändert/erweitert werden) in der Lage ist, die Nutzung des Systems unter dem Aspekt des Datenschutzes und der Datensicherheit optimal zu gestalten und Änderungen am System oder seiner Benutzung festzustellen, zu prüfen und evtl. erforderliche Maßnahmen zu ergreifen bzw. zu veranlassen.

- Es ist ein häufiger Kennwortwechsel erforderlich, insbesondere für die Laborärzte. In diesem Zusammenhang ist eine Softwareunterstützung für automatischen Kennwortwechsel wünschenswert.
- Für den "Kennwort-Dialog" ist ein eigenes Funktionsschlüsselwort zu definieren und regelmäßig zu ändern.
- Die Weitergabe der regelmäßig zu ändernden Programmierererkennung muß eingeschränkt und kontrolliert werden.

4.3.3.2

Schnittstellen

Unter Ziff. 4.3.2 wurde bereits beschrieben, daß die Patientenstammdaten des Laborsystems ggf. von Anwendern anderer Systeme des Laborsystemherstellers mitbenutzt werden können. Diese sogenannte Datenschnittstelle wird derzeit in Wiesbaden von keinem anderen Bereich genutzt.

In den Städtischen Kliniken Wiesbaden existiert aber eine andere Schnittstelle zwischen dem Laborrechner und der Patienten-Stamm- und Abrechnungsdatei des Krankenhausverwaltungssystems INKAS auf dem Verwaltungsrechner. Von INKAS (Informations- und Kommunikationssystem) wird ein Teil der Patientenstammdaten an das Laborsystem übertragen. Im Labor werden dann diese Stammdaten redundant gespeichert. Dies gilt auch hinsichtlich der in der chirurgischen Ambulanz behandelten Patienten. Gespeichert werden hierbei u.a. auch Angaben zur Versicherungsart und zum Wohnort des Patienten. Diese Angaben werden nach Auskunft des Laborleiters zur Abrechnung benötigt. Nach meinen Feststellungen werden jedoch die Abrechnungen für die stationären und die ambulanten Kassenpatienten - das sind nach Auskunft der Kliniken etwa 92-94 % der Patienten - nicht vom Labor erledigt und die Angaben daher dort auch nicht benötigt. Das Labor erhält somit mehr Daten, als die Beschäftigten zur Erfüllung ihrer Aufgaben benötigen, denn für alle Kassenpatienten würden diejenigen Daten völlig ausreichen, die ihre sichere Identifizierung ermöglichen.

4.3.3.3

Löschung

Bedenken habe ich auch hinsichtlich der derzeitigen Lösungspraxis. Die Löschung der personenbezogenen Labordaten erfolgt generell erst etwa 5-6 Monate nach der Entlassung der Patienten. Entscheidend für diese Frist ist die Kapazität der Magnetplatten. Danach werden die personenbezogenen Daten gelöscht. Selbstverständlich sind die Laborbefunde dann noch in der Krankenakte des Patienten enthalten.

Die Speicherdauer darf sich nicht an der Plattenkapazität orientieren. Ich habe daher vorgeschlagen, die Labordaten nach Entlassung des Patienten zu löschen, da sie nach diesem Zeitpunkt von den Beschäftigten für ihre Aufgabenerfüllung nicht mehr benötigt werden und sie daher für den ständigen Zugriff nicht mehr zur Verfügung stehen sollten. Von den Kliniken ist dagegen eingewandt worden, die Daten könnten im Einzelfall - so z.B. in bestimmten Krankheitsfällen bei Wiederaufnahme des Patienten - nützlich sein. Es ist jedoch unverhältnismäßig, die Speicherdauer für die Daten von mehr als 24.000 Patienten an solchen etwaigen Einzelfällen zu orientieren. Sollten die alten Laborbefunde tatsächlich noch einmal benötigt werden, kann auf die in der Krankenakte enthaltenen Laborbefunde zurückgegriffen werden - wie dies ohnehin derzeit schon nach Ausschöpfung der Plattenkapazität geschehen muß.

Ich habe daher die Kliniken aufgefordert, Umfang und Dauer der Datenspeicherungen noch einmal zu überprüfen.

4.3.3.4

Müllbeseitigung

Im Labor befinden sich verschließbare Behälter für Papiermüll mit personenbezogenen Daten. Die Kontrolle des Labordruckers einer Intensivstation machte allerdings deutlich, daß auf den Stationen keine getrennte Sammlung und Vernichtung von personenbezogenem (Papier-)Müll erfolgt: Nicht nur Labordaten, auch fehlerhafte, nicht verschickte Arztbriefe, Durchschläge u.a.m. gelangen in einfache Papierkörbe und von dort aus in den Krankenhausmüll. Meines Erachtens ist es für den gesamten Klinikbereich unbedingt erforderlich, daß Müll mit personenbezogenen Daten in verschlossenen Behältern aufbewahrt und transportiert sowie datenschutzgerecht vernichtet wird.

4.4 AIDS

Auch 1986 war Aids wieder ein zentrales Thema der gesundheitspolitischen Diskussion. Die Krankheit breitet sich weiter aus und verbunden damit mehren sich die Fälle offener Diskriminierung von Aids-Virusträgern oder -Kranken: So konnte sich z.B. ein Mieter nach Bekanntwerden seiner Infektion nur mit Hilfe einer gerichtlichen Verfügung Zugang zu seiner Wohnung verschaffen. Von Kündigungen des Arbeitsverhältnisses durch den Arbeitgeber, Belästigungen durch Telefonanrufe, Schmierereien auf der Haustür oder Lokalverbote berichtet die Deutsche Aids-Hilfe.

Angesichts solcher Reaktionen gewinnen neben Aspekten wie insbesondere der Notwendigkeit einer verstärkten Aufklärung über Umfang und Grenzen der Ansteckungsgefahr datenschutzrechtliche Fragen besondere Bedeutung. Es ist sorgfältig zu prüfen, unter welchen Voraussetzungen und zu welchen Zwecken Daten über Aids-Infektionen und -Erkrankungen erhoben, gespeichert und weitergegeben werden dürfen. Forderungen nach Beschränkungen gibt es bereits. Auf der letztjährigen Tagung der Weltgesundheitsorganisation in Graz zum Thema "Aids in Europa" wurde die besondere Rolle des Datenschutzes betont und u.a. verlangt, die Weitergabe von Testergebnissen an Arbeitgeber oder Versicherungen zu untersagen sowie die Speicherung von Aids-Daten und den Zugang zu ihnen strikten Beschränkungen zu unterwerfen (vgl. den in Aids-Forschung 1986, S. 505 ff. abgedruckten Bericht).

Zu den mit Aids zusammenhängenden datenschutzrechtlichen Fragen zählt sicherlich die Einführung einer personenbezogenen Meldepflicht, über die auch im vergangenen Jahr wieder intensiv diskutiert wurde. Daß aber bereits der derzeitige Umgang mit Aids-Daten in der öffentlichen Verwaltung Anlaß zu Kritik gibt, wird an den unten geschilderten Beispielen "Aids-Tests" und "Aids in Justizvollzugsanstalten" deutlich.

4.4.1 Personenbezogene Meldepflicht

4.4.1.1 Grundvoraussetzung

Grundsätzlich ist bei jeder gesetzgeberischen Maßnahme zur Bekämpfung von Aids genau zu überprüfen, ob sie den Anforderungen des Verhältnismäßigkeitsgrundsatzes entspricht, d.h. ob sie geeignet ist zur Bekämpfung der Krankheit und die Bürger nicht in einem Ausmaß belastet, das außer Verhältnis zu dem angestrebten Erfolg steht. Besonders zu bedenken ist hierbei auch, daß diese Krankheit in erster Linie durch sexuelle Kontakte übertragen wird und daher alle potentiellen Maßnahmen in engem Zusammenhang mit Fragen des Schutzes der persönlichen Intimsphäre stehen und zugleich auch die Grenzen der Regulationsmöglichkeiten durch Gesetze erkannt werden müssen. Kaum verwunderlich ist daher, daß auf der erwähnten Tagung der Weltgesundheitsorganisation als Ergebnis einer Bestandsaufnahme der gesetzgeberischen Aktivitäten in Europa festgestellt wurde: Generell werde in Europa gezögert, gesetzgeberische Maßnahmen zu ergreifen. Ganz überwiegend werde vielmehr auf die Selbstregulationsfähigkeit der Gesellschaft gesetzt, da auf diese Weise eine bessere Kooperation der Risikogruppen erwartet werden könne und generell die Information, Beratung und Anleitung jedes Bürgers zu verantwortlichem Handeln erfolgversprechender sei.

Diese Grundüberlegungen sind auch für die Frage der Einführung einer personenbezogenen Meldepflicht von Bedeutung. Eine gesetzlich auferlegte personenbezogene Meldepflicht würde das informationelle Selbstbestimmungsrecht der von Aids Betroffenen einschränken. In meinem 14. Tätigkeitsbericht habe ich darauf hingewiesen, daß ein derartiger Eingriff in das informationelle Selbstbestimmungsrecht verfassungsrechtlich nur zulässig ist, wenn er dem Verhältnismäßigkeitsgrundsatz entspricht, und diese Voraussetzung derzeit nicht erfüllt ist. Dieser Auffassung waren auch die wichtigsten politischen Entscheidungsträger (vgl. 14. Tätigkeitsbericht, Ziff. 3.1.3).

Nichtsdestoweniger wurde im vergangenen Jahr in der Bundesrepublik in öffentlichen Diskussionen wieder verschiedentlich die Meldepflicht gefordert. Dabei wurde regelmäßig sehr pauschal von der - nicht zu bestreitenden - Gefährlichkeit der Krankheit Aids und ihrer zunehmenden Verbreitung auf die Notwendigkeit einer Meldepflicht geschlossen. Eine derartige Argumentation spricht die in der Bevölkerung verständlicherweise vorhandene Angst vor Aids an, und es erscheint keineswegs ausgeschlossen, daß sie zunehmend Anhänger findet. Sie läßt jedoch die unbedingt gebotene präzise Auseinandersetzung mit der Frage des Ziels einer Meldepflicht und ihrer konkreten Auswirkungen vermissen und begegnet daher größten Bedenken. Die Meldepflicht darf auf keinen Fall aus dem Bedürfnis nach oberflächlichem Aktionismus heraus eingeführt werden. Eine solche Handlungsweise würde im Endeffekt dem Ziel der Bekämpfung von Aids eher schaden als nützen. Im folgenden werden daher die bei der Frage einer Meldepflicht zu berücksichtigenden Aspekte noch einmal eingehend dargelegt.

4.4.1.2

Überprüfungskriterien

Im Hinblick auf den verfassungsrechtlichen Grundsatz der Verhältnismäßigkeit muß die Frage der Einführung einer Meldepflicht unter einer Reihe von Gesichtspunkten überprüft werden. Zunächst stellt sich die Frage, ob eine gesetzliche Verpflichtung der Ärzte zur Meldung überhaupt praktisch durchsetzbar wäre. Die Erfahrungen mit bisher eingeführten Meldepflichten haben gezeigt, daß regelmäßig mit hohen Dunkelziffern zu rechnen ist, d.h. eine Meldepflicht nur in Grenzen durchsetzbar ist. Andererseits wird vermutet, die Verlässlichkeit der derzeit erfolgenden Meldungen von Aids-Erkrankungen durch Ärzte auf freiwilliger Basis liege bereits über den für andere Krankheiten gesetzlich vorgeschriebenen Meldungen, so daß die Einführung einer Verpflichtung keinen Gewinn bringe.

Die entscheidende Frage ist jedoch, ob mit der personenbezogenen Meldepflicht das zentrale Ziel - ein verbesserter Schutz Dritter - erreicht werden kann, und ob dieses Ziel nicht mit weniger einschneidenden Maßnahmen erreichbar ist.

Eine zentrale Registrierung der Daten von Aids-Kranken (oder auch zusätzlich von Aids-Virusträgern) allein kann sicherlich keinen verbesserten Schutz Dritter gewährleisten. Entscheidend ist daher, wie im Anschluß an eine Registrierung weiter verfahren werden soll, welche Stellen diese Daten zu welchen Zwecken erhalten sollen, welche weiteren Ermittlungen angestellt und welche Folgemaßnahmen möglicherweise getroffen werden sollen. Darauf sind freilich die Befürworter einer Meldepflicht bisher die Antworten schuldig geblieben. Eine Klärung dieser Fragen wäre indes vor jeder konkreteren Erwägung einer Meldepflicht unerlässlich. Nicht zuletzt müßte auch geklärt werden, auf welche Art und Weise dann bei dem Ausmaß der zu erwartenden Datenströme der Datenschutz praktisch sichergestellt werden könnte.

Zu berücksichtigen ist ferner, welche unerwünschten Auswirkungen die Einführung einer personenbezogenen Meldepflicht haben kann. Vielfach wird eine Verstärkung der Diskriminierung Aids-Kranker befürchtet. Eine Meldepflicht, so die Annahme, könnte zudem bei den besonders gefährdeten Personen Angst und Panik erzeugen und sie von der Nutzung der vorhandenen Informations-, Beratungs- und Untersuchungsangebote abhalten. Aus dem Ausland liegen inzwischen erste Ergebnisse der Einführung einer Meldepflicht vor, die diese Befürchtungen bestätigen: Auf der Internationalen Aids-Konferenz in Paris im Juni 1986 berichtete ein Vertreter der schwedischen Gesundheitsverwaltung, daß in Schweden seit der Einführung der Meldepflicht die Nutzung der Informations- und Untersuchungsmöglichkeiten erheblich zurückgegangen, ein positiver Effekt dagegen bisher nicht zu erkennen sei.

Ein Klima der Angst kann auch einen rationalen Umgang mit der Krankheit verhindern und damit die bisher erreichten gesundheitspolitischen Erfolge mindern. Schließlich ist auch zu bedenken, daß sich die Einführung einer Meldepflicht negativ auf das Vertrauensverhältnis zwischen Arzt und Patient auswirken kann, dieses Vertrauensverhältnis jedoch gerade bei dieser Krankheit von besonderer Bedeutung ist und sich auch auf den Schutz Dritter auswirkt.

4.4.1.3

Konsequenzen

Festzustellen bleibt: Die Einführung einer Meldepflicht ist ein schwerer Eingriff in die Rechte der von Aids Betroffenen, dessen Eignung zur Bekämpfung der Krankheit bisher in keiner Weise überzeugend dargetan wurde. Solange sich dies nicht ändert, sind Aufklärung und Beratung sowie Anleitung zu selbstverantwortlichem Handeln absolut vorrangig.

Dies ist wohl auch immer noch die herrschende Ansicht. Bei einer öffentlichen Anhörung des Bundestagsausschusses für Jugend, Familie und Gesundheit am 19. März 1986 hat sich nur eine Minderheit von Sachverständigen für eine Meldepflicht ausgesprochen. In seiner Antwort vom 25. April 1986 auf eine kleine Anfrage hat das Bundesgesundheitsministerium die Auffassung geäußert, das in der Bundesrepublik geübte Verfahren der freiwilligen anonymen Meldung (s. hierzu noch unten Ziff. 4.4.2) gebe einen ausreichenden Überblick über die epidemiologische Situation, sonstige Gründe für die Einführung einer Meldepflicht seien nicht ersichtlich (Bundestags-Drucks. 10/5430). An dieser Meinung hat das Ministerium auch auf dem Internationalen Aids-Kongreß im November 1986 in Berlin festgehalten.

Ähnlich ist die Situation in Hessen:

Der Hessische Sozialminister hat sich gegen eine Meldepflicht ausgesprochen und der Hessische Landtag hat anläßlich der Beratung meines 14. Tätigkeitsberichts folgenden Beschluß gefaßt:

“Der Landtag lehnt eine generelle Meldepflicht für Aids-Kranke ab.

Es soll weiterhin sichergestellt werden, daß ausschließlich anonymisierte Daten in Aids-Register übermittelt werden.“ (Vgl. Nr. 2 der Beschlußempfehlung des Innenausschusses, Drucks. 11/6231 i.V.m. Protokoll der 84. Plenarsitzung vom 19. Juni 1986, S. 4979)

4.4.2

Meldungen an das Aids-Register des Bundesgesundheitsamts

Von einer gesetzlich angeordneten personenbezogenen Meldepflicht ist eine von den Ärzten auf freiwilliger Basis vorgenommene Meldung anonymisierter Patientendaten strikt zu unterscheiden. In der Bundesrepublik werden bereits seit einiger Zeit von Ärzten freiwillig Aids-Krankheitsfälle (nicht alle positiven Testergebnisse) an ein vom Bundesgesundheitsamt (BGA) geführtes Register gemeldet, das der Gewinnung epidemiologischer Erkenntnisse dienen soll. Soweit diese Meldungen keine personenbezogenen Daten der Patienten enthalten, sind die Ärzte hierzu ohne weiteres berechtigt.

1985 hatte das BGA zur Erleichterung und Standardisierung solcher freiwilligen Meldungen einen Fallberichtsbogen entwickelt, der den Ärzten für ihre Meldungen zur Verfügung gestellt werden sollte. Vorgesehen war, daß die Ärzte nur anonymisierte Patientendaten melden. Die konkrete Ausgestaltung des Fallberichts bogens stieß jedoch auf datenschutzrechtliche Bedenken, weil durch die vorgesehene Art der Verschlüsselung der Patientendaten eine Anonymisierung nicht hinreichend sichergestellt war (vgl. hierzu 14. Tätigkeitsbericht, Ziff. 3.1.4).

Der Fallberichtsbogen wurde daraufhin überarbeitet. Dabei mußte sichergestellt werden, daß trotz der anonymisierten Meldung das BGA Mehrfachmeldungen für denselben Patienten erkennen und aussondern kann, da andernfalls die statistischen Ergebnisse verfälscht würden. Vorgesehen ist jetzt:

- Auf dem Bogen wird klar und deutlich darauf hingewiesen, daß es sich um eine freiwillige Meldung des Arztes handelt und nur anonymisierte Patientendaten gemeldet werden.
- Es wird eine neue anonymisierte Kennzeichnung der Patientendaten verwendet. Insbesondere der Name des Patienten wird umfassender verschlüsselt. Ferner wird auf eine Ortsangabe des Wohnsitzes des Patienten verzichtet. Neben dem Bundesland sollen nur die beiden ersten Ziffern der Postleitzahl angegeben werden. Schließlich wird beim Geburtsdatum auf die Angabe von Tag und Monat, beim Sterbedatum auf die Angabe des Tages verzichtet.

Die neue Gestaltung des Fallberichts bogens gewährleistet nunmehr eine hinreichende Anonymisierung der Patientendaten. Zugleich berücksichtigt sie die Notwendigkeit der Gewinnung epidemiologischer Kenntnisse. Hier zeigt sich wieder einmal, daß der Datenschutz notwendigen Maßnahmen keineswegs im Wege steht, sondern durch eine sorgfältige Auswahl der konkreten Verfahrensweise beides miteinander in Einklang gebracht werden kann.

4.4.3

Durchführung und Verwendung von Aids-Tests

Seit 1984 kann durch Testverfahren einigermaßen sicher festgestellt werden, ob ein Kontakt mit dem Aids-Virus stattgefunden hat. Diese Tests wurden zunächst entwickelt zur Sicherung von Blutprodukten und Transplantaten, ferner auch zur Präzision der Diagnose bei unklaren Krankheitsbildern. In diesem Zusammenhang sind sie auch ohne Zweifel hilfreich und notwendig.

In der Zwischenzeit zeichnet sich jedoch im Ausland und zum Teil auch bereits in der Bundesrepublik eine zunehmende Durchführung der Tests an größeren Gruppen von symptomlosen Personen ab. Um nur einige Beispiele zu nennen: Die US-Armee verlangt seit Oktober 1985 ein negatives Testergebnis als Aufnahmevoraussetzung. In Deutschland müssen Stipendiaten aus bestimmten Ländern seit 1985 ein negatives Testergebnis vorweisen. Häftlingen wird nahegelegt, sich einem Test freiwillig zu unterziehen. In der öffentlichen Diskussion werden zum Teil sogar regelmäßige Zwangsuntersuchungen aller Angehörigen von Risikogruppen oder gar der gesamten Bevölkerung gefordert.

Solche Aids-Tests werfen zahlreiche sehr schwierige und weit über das Datenschutzrecht hinausgehende Fragen auf. Zu bedenken ist beispielsweise die begrenzte Verlässlichkeit der vorhandenen Tests. Ferner: Symptomlose Bürger, die sich einem Test unterziehen, sind gesund. Die Mitteilung eines positiven Testergebnisses bedeutet für sie eine ganz erhebliche psychische Belastung, die zu erheblichen sozialen Problemen führen kann. Andererseits sagt das Testergebnis nichts darüber aus, ob und gegebenenfalls wann und in welchem Umfang sie an Aids erkranken. Medizinische Maßnahmen zur Verhinderung eines evtl. Krankheitsausbruchs stehen nicht zur Verfügung. Mit anderen Worten: Ein positives Testergebnis führt zu einer äußerst schwierigen Situation für den Betroffenen.

Ebenso wie die Einführung einer Meldepflicht bedarf daher die Frage nach dem Umfang der Durchführung und Verwendung von Aids-Tests einer sorgfältigen Analyse. Konkret ist insbesondere zu überdenken, welchem Ziel die Tests dienen sollen, ob dieses Ziel, vor allem auch der Schutz Dritter, durch sie erreicht werden kann, und ob weniger einschneidende Maßnahmen denkbar sind. Es ist außerdem zu prüfen, ob mit unerwünschten Auswirkungen gerechnet werden muß und wie diese zu bewerten sind. Eine Diskussion all dieser Fragen hat bisher nicht in ausreichendem Maße stattgefunden.

4.4.4

Aids-Tests des Gesundheitsamtes Frankfurt

Im September 1986 erhob die Frankfurter Aids-Hilfe gegen das Gesundheitsamt der Stadt den Vorwurf, es führe Aids-Zwangstests an männlichen Homosexuellen, die sich prostituieren, durch. Das Amt reagierte Anfang Oktober 1986 mit einer Presseerklärung, in der die grundsätzlich vorgesehenen Maßnahmen zur Aids-Bekämpfung geschildert wurden. Vorrang räumte das Gesundheitsamt in seiner Erklärung der Informations- und Beratungstätigkeit ein, schloß aber für Risiko- und Hochrisikogruppen unter bestimmten Bedingungen Zwangsmaßnahmen nach dem Bundesseuchengesetz nicht aus.

Es ist kaum zu bestreiten, daß jemand, der im Verdacht steht, Aids-Virusträger zu sein, nach dem Bundesseuchengesetz u.U. zwangsuntersucht werden kann und evtl. auch seine Daten zur Einleitung eines Bußgeldverfahrens vom Gesundheitsamt an das Ordnungsamt weitergeleitet werden können. Eine Anwendung dieser Vorschriften kommt allerdings nur dann in Betracht, wenn im Einzelfall die im Gesetz aufgeführten Voraussetzungen gegeben sind und ferner auch der Grundsatz der Verhältnismäßigkeit gewahrt ist.

Ich habe mich daher Anfang November eingehend im Gesundheitsamt Frankfurt über die derzeitige Praxis der Verarbeitung personenbezogener Aids-Daten informiert. Anhaltspunkte für eine datenschutzrechtliche Beanstandung ließen sich nicht finden. Mein Gespräch hat vielmehr ergeben, daß der Gesichtspunkt der Verhältnismäßigkeit bei den internen Überlegungen des Amtes durchaus eine wichtige Rolle spielt. Nach Auskunft des Amtsleiters sind Aids-Tests bisher ausschließlich auf freiwilliger Basis durchgeführt worden. Alle Untersuchungsunterlagen verbleiben in dem speziellen Sachgebiet des Gesundheitsamtes und sind darüber hinaus für niemanden zugänglich. An das Ordnungsamt sind bislang keine personenbezogenen Daten von Aids-Virusträgern übermittelt worden. Diese Maßnahme will das Gesundheitsamt nur in Betracht ziehen, wenn alle sonstigen zur Verfügung stehenden Mittel erfolglos geblieben sind. Einvernehmen bestand zwischen dem Gesundheitsamt und mir darüber, daß jeder Einzelfall einer Übermittlung von Daten an das Ordnungsamt im Gesundheitsamt zu dokumentieren wäre.

4.4.5

Aids in Justizvollzugsanstalten

Im letzten Jahr ist zwischen dem Justizminister und mir mehrfach kontrovers diskutiert worden, welcher Personenkreis genau in den Haftanstalten von Aids-Erkrankungen der Gefangenen Kenntnis erhalten soll. Leider sind die Probleme noch immer nicht hinreichend gelöst.

4.4.5.1

Ausgangspunkt

Unstreitig unterliegen beamtete oder angestellte Anstaltsärzte ebenso wie ihre übrigen Kollegen der strafrechtlich gesicherten beruflichen Schweigepflicht (§ 203 Abs. 1 Nr. 1 Strafgesetzbuch). Unter die ärztliche Schweigepflicht fallen selbstverständlich auch die Ergebnisse der den Gefangenen auf freiwilliger Basis angebotenen Aids-Tests. Zwischen dem Justizminister und mir besteht Einigkeit darüber, daß eine Durchbrechung der ärztlichen Schweigepflicht durch die in der Anstalt tätigen Ärzte gerechtfertigt ist, wenn und soweit die Offenbarung der medizinischen Daten der Abwehr einer Lebensgefahr bzw. einer erheblichen Gesundheitsgefahr für die Anstaltsbediensteten oder die Mitgefangenen dient. Meines Erachtens kann eine für die Durchbrechung der ärztlichen Schweigepflicht erforderliche Lebensgefahr bzw. erhebliche Gesundheitsgefährdung jedoch nicht pauschal für alle Bediensteten der Anstalt bejaht werden, sondern ist eine Differenzierung nach Risikogruppen innerhalb des Personals erforderlich. Nur diejenigen Bediensteten, die tatsächlich gefährdet sind, dürfen über die festgestellten Infektionen informiert werden. Im Grundsatz teilt diese Position auch der Justizminister. Durch seinen Erlaß vom 8. August 1985 ist dies allerdings nicht hinreichend sichergestellt worden (vgl. hierzu 14. Tätigkeitsbericht, Ziff. 3.1.5).

4.4.5.2

Der neue Erlaß

Anfang 1986 hat mich der Justizminister über einen neuen Erlaß vom 5. Dezember 1985 (AZ 4450 SH 1-IV/5-1655/85) informiert. Der Erlaß enthält in erster Linie Verfahrensregeln: Danach berichtet der Anstaltsarzt dem

Anstaltsleiter, bei welchem Gefangenen das Untersuchungsergebnis positiv war. Dem Anstaltsleiter obliegt es anschließend, unter Berücksichtigung der örtlichen Verhältnisse zu entscheiden, welche weiteren Bediensteten zu unterrichten sind.

In ihrer Stellungnahme zu meinem 14. Tätigkeitsbericht (Drucks. 11/6120, S. 10 f.) vertritt die Landesregierung dazu die Auffassung, eine generelle Festlegung der Personengruppen, die zu unterrichten sind, sei in einem für alle hessischen Vollzugsanstalten gültigen Runderlaß wenig sinnvoll und im Hinblick auf die unterschiedliche Größe und Zweckbestimmung der einzelnen Anstalten auch undurchführbar. Im übrigen sei der Datenschutz hinreichend gewährleistet, da eine Eintragung über die Krankheit in die Gefangenenpersonalakte nicht erfolge.

Der neue Erlaß ist zwar eine datenschutzrechtliche Verbesserung, insbesondere auch deshalb, weil die Verantwortlichkeit des Anstaltsleiters eindeutig zum Ausdruck kommt und die Notwendigkeit einer klaren Begrenzung des Kreises der zu informierenden Bediensteten anerkannt wird. Im übrigen ist jedoch die Frage, welche Bediensteten informiert werden sollen, auf die Ebene der einzelnen Anstalten verschoben worden. Wie die Bediensteten informiert werden sollen, und ob und gegebenenfalls in welcher Weise die medizinischen Daten in den verschiedenen Arbeitsbereichen innerhalb der Anstalten gespeichert werden dürfen, regelt der Erlaß gleichfalls nicht.

Bei den Beratungen des Landtags zu meinem 14. Tätigkeitsbericht habe ich meine Bedenken nochmals bekräftigt, aber aufgrund von Ausführungen des Justizministers zur restriktiven Praxis in den Anstalten zunächst zurückgestellt und eine Überprüfung der Praxis angekündigt. Der Landtag hat hierzu folgenden Beschluß gefaßt:

„Der Landtag sieht in dem Erlaß des Hessischen Ministers der Justiz vom 5. Dezember 1985 betreffend Gesundheitsfürsorge in den Justizvollzugsanstalten einen ersten Schritt in die richtige Richtung zur Regelung der Übermittlung von positiven Untersuchungsbefunden an Anstaltsbedienstete.“ (Vgl. Nr. 2 der Beschlussempfehlung des Innenausschusses, Drucks. 11/6231 i.V.m. Protokoll der 84. Plenarsitzung vom 19. Juni 1986, S. 4979).

4.4.5.3

Überprüfung der Praxis in verschiedenen Anstalten

Im Sommer habe ich mich in vier Haftanstalten über die dort praktizierten Verfahrensweisen informiert. Dabei hat sich herausgestellt, daß der Kreis derjenigen Bediensteten, die über festgestellte Aids-Infektionen unterrichtet werden, zum Teil sehr unterschiedlich eingegrenzt wird. Die Praxis ist keineswegs immer restriktiv, zudem konnte mir die vorgesehene Verfahrensweise nicht in jedem Fall klar dargelegt werden.

In den Anstalten bestehen insbesondere unterschiedliche Auffassungen darüber, ob und gegebenenfalls in welchem Umfang Bedienstete der Kleiderkammer, der Arbeitsverwaltung, der einzelnen Arbeitsbereiche und der Zentrale sowie der Sozialdienst Informationen über die Infektionen erhalten sollen, und ob diese Bediensteten die Informationen an ihrem Arbeitsplatz speichern dürfen. Die von mir festgestellten unterschiedlichen Verfahrensweisen in den einzelnen Anstalten sind keineswegs durch die verschiedenen örtlichen Verhältnisse oder etwa durch besondere Zweckbestimmungen der jeweiligen Anstalten bedingt.

Ein anschauliches Beispiel für die unterschiedlichen Verfahrensweisen ist die Frage der Unterrichtung der Mitarbeiter der Kleiderkammern: In einer Anstalt informieren sich der Leiter der Kleiderkammer und sein Vertreter in der Zentrale über diejenigen Gefangenen, die infiziert sind, vermerken diese Daten in ihrer Kartei und halten es darüber hinaus für erforderlich, daß jeder der in der Kleiderkammer arbeitenden Gefangenen ebenfalls darüber informiert wird, welche Gefangenen infiziert sind. In einer anderen Anstalt hingegen wird der Kreis der zu informierenden Bediensteten eng begrenzt. Eine Unterrichtung des Leiters der Kleiderkammer bzw. der weiteren in der Kleiderkammer Beschäftigten wird nicht für erforderlich gehalten.

Im übrigen sind die getroffenen Maßnahmen innerhalb der Anstalten zum Teil nicht konsequent aufeinander abgestimmt. Ein Beispiel: So wird in einer Anstalt einerseits der Anstaltsleiter vom Anstaltsarzt in einem verschlossenen Umschlag über die Infektionen unterrichtet und die Information dann beim Anstaltsleiter in einem Panzerschrank aufbewahrt. Andererseits wird die Information aber zugleich in ganz erheblichem Umfang weiterverbreitet: Der Anstaltsleiter informiert den Sicherheitsdienstleiter, der Sicherheitsdienstleiter die Zentrale, die Vollzugsgeschäftsstelle, die Arbeitseinsatzleiter und den Sozialdienst. In der Zentrale und zum Teil auch auf den einzelnen Stationen werden die Informationen über die Infektionen an die Belegungstafel angeschlagen, von der wiederum jeder Bedienstete Kenntnis nehmen kann. Kenntnis nimmt u.a. auch auf diesem Wege der Leiter der Kleiderkammer, der seinerseits die dort beschäftigten Mitgefangenen informiert. Hier werden somit einerseits sorgfältige Maßnahmen zur Gewährleistung des Datenschutzes getroffen, andererseits aber wird deren Wirkung durch weitere Maßnahmen verhindert.

Problematisch sind auch Ausgestaltung und Verwendung der Begleitscheine für den Häftlingstransport. Die Begleitscheine Aids-infizierter Häftlinge enthalten den Vermerk "Blutkontakt vermeiden". Bedenken bestehen vor allem dagegen, daß die Transportbegleitscheine zum Teil zur Personalakte genommen werden, in die wiederum alle Bediensteten Einsicht nehmen können. Diese Verfahrensweise läuft der angestrebten differenzierten Unterrichtung der Bediensteten über Aids-Erkrankungen zuwider. In der Stellungnahme der Landesregierung zu meinem 14. Tätigkeitsbericht wird betont, die Ergebnisse der Aids-Untersuchungen würden nicht in der Gefangenenpersonalakte vermerkt, was nach meinen Feststellungen auch zutrifft. Wenn allerdings der Transportbegleitschein mit dem Vermerk "Blutkontakt vermeiden" in die Gefangenenpersonalakte aufgenommen wird, so kommt dies letztlich einem ausdrücklichen Vermerk gleich.

Der Hinweis in der Stellungnahme der Landesregierung, der Vermerk "Blutkontakt vermeiden" gelte auch für andere Infektionskrankheiten und lasse daher keine individuellen Schlußfolgerungen hinsichtlich des Gesundheitszustandes eines Gefangenen zu, überzeugt nicht. Wenn die Offenlegung der konkreten Diagnose dem Betroffenen Nachteile bringt, so gilt dies entsprechend im Fall einer derartigen teilweisen Offenbarung der Daten. Es bedarf keiner großen Phantasie, zu vermuten, daß es sich bei den betroffenen Gefangenen größtenteils um Aids-Infizierte handelt; im übrigen wird der Vermerk nach den mir vorliegenden Informationen derzeit fast nur bei Aids-Infizierten verwandt. Aus diesem Grund dürfen Transportbegleitscheine nicht in die Gefangenenpersonalakte aufgenommen werden, sondern sind gesondert aufzubewahren und nur denjenigen Bediensteten zugänglich zu machen, die diese Information benötigen.

4.4.5.4

Forderungen

Als Ergebnis der Überprüfungen bleibt festzuhalten: Der Erlaß des Hessischen Justizministers vom 5. Dezember 1985 gewährleistet keinen ausreichenden Datenschutz. Das Verfahren zur Unterrichtung der Bediensteten muß von der Anstaltsleitung schriftlich detailliert festgelegt werden. Dies betrifft die Fragen, welche Bediensteten in welcher Form informiert werden, ob und gegebenenfalls in welcher Weise sie diese Informationen in ihrem Arbeitsbereich speichern dürfen und ob und gegebenenfalls welche Bediensteten wiederum diese in den einzelnen Arbeitsbereichen gespeicherten Informationen zur Kenntnis nehmen dürfen.

Dazu bedarf es aber Vorgaben des Justizministers. Ich bezweifle, daß eine generelle Regelung der Verfahrensweise für alle Anstalten "wenig sinnvoll" und "undurchführbar" ist, wie dies in der Stellungnahme der Landesregierung zu meinem 14. Tätigkeitsbericht dargestellt ist. In jedem Fall sollten zumindestens einige einheitliche Kriterien für die schriftliche Festlegung der Verfahrensweise in den einzelnen Anstalten generell vorgegeben werden. Eine Aufbewahrung der Daten an einer Stelle, an der jeder Bedienstete davon Kenntnis nehmen kann, ist nicht akzeptabel.

Was die zu informierenden Personengruppen anbelangt, halte ich insbesondere eine Unterrichtung bzw. eine Möglichkeit der Kenntnisnahme der gesamten Vollzugsgeschäftsstelle, der Kleiderkammer und der Pfarrer nicht für erforderlich. Die Arbeitseinsatzleiter benötigen die Informationen über Infektionen nur dann, wenn sie bei der Arbeitszuteilung eine selbständige Entscheidung treffen müssen, für die eine Aids-Infektion von Bedeutung ist. Für die Betriebsleiter sind die Informationen nur erforderlich, wenn es sich um Bereiche mit besonderer Verletzungsgefahr handelt.

Sollte auf den Vermerk "Blutkontakt vermeiden" beim Transport von Aids-infizierten Häftlingen nicht verzichtet werden können, ist in jedem Fall klar und einheitlich zu regeln, wer diesen Vermerk verfügt und wo die Transportbegleitscheine aufbewahrt werden.

Im Sommer habe ich den Justizminister über das Ergebnis der Überprüfung unterrichtet. Ende Dezember hat mir der Justizminister in seinem Antwortschreiben mitgeteilt, der Erlaß vom 5. Dezember 1985 sei unter Berücksichtigung meines Schreibens geändert worden. Nunmehr hat der Anstaltsleiter "in der Regel" seinen ständigen Vertreter, den Vollzugsabteilungsleiter, die Vollzugsdienstleitung, die betroffenen Stationsbediensteten und die betroffenen Werkbediensteten zu unterrichten. Die Unterrichtung erfolgt mündlich. Die Bediensteten sind ausdrücklich auf ihre Amtsverschwiegenheit und das Erfordernis einer zweckgebundenen Verwendung der Daten hinzuweisen. Erforderliche schriftliche Aufzeichnungen am jeweiligen Arbeitsplatz des zu informierenden Bediensteten sind so aufzubewahren, daß unbefugte Dritte keine Einsicht nehmen können.

Damit liegen jetzt zwar einige für alle hessischen Haftanstalten verbindliche Regelungen vor. Diese sind jedoch sehr allgemein gehalten und lassen eine Reihe der von mir angesprochenen Fragen völlig offen.

5. Justiz

5.1

Justizmitteilungsgesetz

Nicht nur in Strafsachen, sondern auch in Zivilverfahren haben die Gerichte anderen Gerichten oder Behörden Mitteilungen zu machen. Mitteilungspflichten haben allerdings nicht nur die Gerichte, sondern z.B. auch die Staatsanwaltschaften, die etwa die Polizei über den Ausgang eines Strafverfahrens unterrichten müssen. Wer wem was zu welchem Zeitpunkt mitzuteilen hat, regeln gegenwärtig die bundeseinheitlichen Verwaltungsanordnungen des Bundes und der Länder über Mitteilungen in Strafsachen (MiStra) in der ab 1. April 1985 geltenden Fassung und über die Mitteilungen in Zivilsachen (MiZi) in der Fassung der Bekanntmachung vom 11. November 1985. Nach der mehrfach geäußerten Kritik der Datenschutzbeauftragten des Bundes und der Länder an der mangelhaften Rechtsgrundlage dieser Übermittlungspraxis (vgl. etwa 9. Tätigkeitsbericht, Ziff. 4.2.3 und 12. Tätigkeitsbericht, Ziff. 2.2.1) hat nunmehr der Bundesjustizminister im Dezember 1986 den Entwurf eines "Gesetzes über Mitteilungen der Justiz von Amts wegen in Zivil- und Strafsachen (Justizmitteilungsgesetz)" vorgelegt.

5.1.1

Kritische Punkte

Im Vergleich zu MiStra und MiZi verfolgt der Entwurf eine abweichende Konzeption. Während die beiden Verwaltungsvorschriften Gegenstand, Zeitpunkt und Empfänger der einzelnen Mitteilungsverfahren festlegen, sieht der Entwurf lediglich zwei Grundvorschriften für den Bereich der MiStra und der MiZi vor, die durch einige wenige Regelungen über besondere Probleme ergänzt werden. Ausdrückliches Ziel der Verfasser ist es, mit dem vorgesehenen Justizmitteilungsgesetz relativ abstrakt die Merkmale für die Weitergabe von Informationen zu regeln, und die Bestimmungen durch eine Verwaltungsvorschrift des Bundes (Art. 84 Abs. 2 Grundgesetz), ggf. zusätzlich durch Länderverwaltungsvorschriften, zu konkretisieren. Das Gesetz würde demnach lediglich die formale Grundlage der bereits geltenden MiStra und MiZi sein.

Diese Konzeption ist kaum geeignet, den Anforderungen des Bundesverfassungsgerichts zu entsprechen. Der Bestimmtheitsgrundsatz und das Gesetz der Normenklarheit verlangen vielmehr, daß bereits im Mitteilungsgesetz selbst Anlaß, Datenarten, Zweck und Empfänger der Übermittlungen genau bestimmt werden.

Auch der Inhalt der Übermittlung muß näher qualifiziert werden als durch die Formel "soweit sie zur Erfüllung gesetzlicher Aufgaben des Empfängers erforderlich ist". So sollte entsprechend einer langjährigen Forderung der Datenschutzbeauftragten bei Straftaten mit geringem Schuldehalt, in der Regel auch bei Fahrlässigkeitstaten, von einer Übermittlung abgesehen werden. Außerdem sollte, wenn kein Zusammenhang mit der beruflichen Tätigkeit des Betroffenen besteht, eine Mitteilung an Institutionen, die die Aufsicht über bestimmte Berufe ausüben, unterbleiben. Derartige Einschränkungen fehlen jedoch im Entwurf.

Der Inhalt der Mitteilung ist auf das Notwendige zu begrenzen. In der Regel dürfen daher nur Strafvorwurf (kurze Zusammenfassung), Anklagesatz oder Urteilsformel übermittelt werden. Eine Weitergabe ganzer Urteilstexte wäre damit ausgeschlossen bzw. nur im besonderen Ausnahmefall zulässig.

Bereits im Gesetz selbst sollte klargestellt werden, daß eine Mitteilung im Regelfall erst nach Rechtskraft der ergangenen Entscheidung ergehen darf. Sollte ausnahmsweise vorher eine Mitteilung notwendig sein, so darf sie grundsätzlich erst zum Zeitpunkt der Erhebung der öffentlichen Klage vorgenommen werden. Es müssen in jedem Fall begründete Anhaltspunkte vorliegen, daß die zu benachrichtigende Behörde bereits zu diesem frühen Zeitpunkt unaufschiebbare Maßnahmen treffen muß und deshalb auf die frühzeitige Benachrichtigung angewiesen ist.

Der Entwurf sieht vor, daß für einige wenige Bereiche die Mitteilungen dem Richter oder Staatsanwalt vorbehalten sind. Betroffen sind die Verfahren, für die der Gesetzentwurf besonders allgemeine Bestimmungen enthält. Darüber hinaus sollte dies jedoch auch für die übrigen Fälle gelten, soweit sich die Entscheidung über die Mitteilung nicht bereits direkt aus dem Gesetz ergibt.

Vor jeder einzelnen Mitteilung ist zu überprüfen, ob die Information für den Empfänger und dessen Aufgabenerfüllung tatsächlich erforderlich ist. Eine solche Prüfungspflicht enthält der Entwurf jedoch nicht.

5.1.2

Positive Ansätze

Der Gesetzentwurf greift eine Reihe von Punkten auf, die von den Datenschutzbeauftragten bereits seit längerer Zeit gefordert werden.

Leider nur zum Teil folgt der Entwurf dem Vorschlag, daß bei einer Mitteilung, die durch nachträgliche Informationen des Versenders sich als inhaltlich unrichtig, unvollständig oder überholt erwiesen hat, der Empfänger hiervon unverzüglich zu unterrichten ist. Für Mitteilungen aus öffentlichen Registern wird dies pauschal abgelehnt. Hier wäre eine differenziertere Regelung, die auf den Zeitpunkt der Übermittlung abstellt, sinnvoll.

Ebenso wichtig ist die vorgesehene Unterrichtung des Betroffenen über die Mitteilung. Nach dem Entwurf soll die Mitteilung grundsätzlich zugleich mit der Benachrichtigung erfolgen. Aus der Sicht des Rechtsschutzes des Betroffenen ist dagegen eine vorherige Unterrichtung vorzuziehen. Auf die Einschränkung, daß eine solche Benachrichtigung grundsätzlich dann unterbleibt, wenn die Mitteilung gesetzlich angeordnet ist, der mitgeteilte Vorgang rechtmäßig öffentlich verkündet oder bekannt gemacht oder in einem öffentlichen Register eingetragen ist, der Zweck des Verfahrens durch die Unterrichtung gefährdet würde oder der Betroffene eine Unterrichtung vernünftigerweise nicht erwartet, sollte verzichtet werden. Kaum ein Bürger wird diese alternativen Informationswege ohne weiteres erkennen können.

Positiv zu bewerten ist die Regelung, wonach der Empfänger die Mitteilung nur zu dem Zweck verwenden darf, zu dessen rechtmäßiger Erfüllung sie übermittelt worden ist. Damit wird dem Grundsatz der Zweckbindung Rechnung getragen.

Nach dem Entwurf sind die Empfänger zur Löschung der mitgeteilten personenbezogenen Daten verpflichtet, sobald der Verwendungszweck entfallen ist. Dieser Grundsatz wird insoweit eingeschränkt, als die Speicherung oder Aufbewahrung der mitgeteilten personenbezogenen Daten "Teil der gesetzlichen Aufgabe des Empfängers" sind. Die hiervon erfaßten Register haben in der Regel sicherlich keinen selbständigen Registerzweck, so daß "der Zweck der Verwendung der Daten" nicht eindeutig festgelegt werden kann. Andererseits wäre es möglich, in diesen Fällen an die Tilgungsbestimmungen der bestehenden Registergesetze - insbesondere des Bundeszentralregistergesetzes - anzuknüpfen oder entsprechende Gesetzesvorbehalte vorzusehen.

5.2

Reform der Strafprozeßordnung

5.2.1

Neue Regelungsvorschläge

Durch das Urteil des Bundesverfassungsgerichts zur Volkszählung 1983 wurden die Forderungen nach konkreten, bereichsspezifischen Regelungen für die personenbezogene Datenverarbeitung gerade in den Bereichen, die mit Sanktionen gegenüber den Betroffenen verbunden sind, ausdrücklich bestätigt. Niemand bezweifelt mehr ernsthaft, daß sowohl für die polizeiliche Tätigkeit zum Zweck der Gefahrenabwehr als auch für die Datenverarbeitung zu Strafermittlungszwecken die bestehenden gesetzlichen Regelungen einer umfassenden Revision unterzogen und ergänzt werden müssen.

Dies gilt insbesondere für die Strafprozeßordnung. Nachdem mit der Regelung der sog. Schleppnetzfahndung in § 163d StPO im Frühjahr 1986 (BGBl. I S. 537) im Zusammenhang mit der Novellierung der Paß- und Ausweisgesetze (BGBl. I S. 537, 545 und 548) bereits ein erster und isolierter Schritt getan wurde, sind sich alle Beteiligten darüber einig, daß weitere Schritte folgen müssen. Ungeachtet der berechtigten Kritik an § 163d StPO ist deshalb der vom Bundesminister der Justiz vorgelegte "Arbeitsentwurf eines Gesetzes zur Regelung der rechtlichen Grundlagen für Fahndungsmaßnahmen, Fahndungshilfsmittel und für die Akteneinsicht im Strafverfahren" zu begrüßen. Wie sich bereits dem Titel entnehmen läßt, enthält er keineswegs die geforderte Gesamtrevision der Strafprozeßordnung. Vielmehr geht es um einzelne Bereiche der Fahndung, die besonders intensiv das Recht auf informationelle Selbstbestimmung der Betroffenen beeinträchtigen können, wie etwa die sogenannte Rasterfahndung, die Ausschreibung zur Festnahme und den Erlaß eines Steckbriefs, die Ausschreibung zur Aufenthaltsermittlung, oder die Erteilung von Auskünften und Akteneinsicht aus Unterlagen der Strafverfolgungsbehörden. Hinzu kommen Vorschläge für die Befugnis der Staatsanwaltschaften, von allen öffentlichen Behörden Auskünfte zu verlangen, und Regelungen für die Ausschreibung von Personen zur "polizeilichen Beobachtung" sowie zur "planmäßigen Überwachung".

Ausdrückliches Ziel des Entwurfs ist, sowohl neuartige als auch hergebrachte Fahndungsmethoden neu, umfassend und klar zu regeln; gleichzeitig weist er unmißverständlich darauf hin, daß weitere Regelungen zum Einsatz sogenannter "verdeckter Ermittler" sowie allgemeine Bestimmungen über die Erhebung, Speicherung und Übermittlung personenbezogener Daten durch die Ermittlungsbehörden erforderlich sind und lediglich aus technischen Gründen nicht gleichzeitig vorgelegt wurden. Allgemeine Regelungen über die Datenverarbeitung zum Zwecke der Straftatenaufklärung bilden die Grundlage für die Datenverwertung in diesem Bereich überhaupt. Es wäre deshalb sinnvoll, entsprechende Überlegungen möglichst frühzeitig vorzulegen, so daß ein Gesamtbild der vorgeschlagenen Konzeption gewonnen werden kann.

5.2.2

Kritik einzelner Vorschläge

5.2.2.1

Rasterfahndung (§ 98a und b E)

Sicherlich handelt es sich bei der Rasterfahndung um eine der meistdiskutierten neuen Fahndungsmethoden der Polizei. Der Entwurf legt den Rahmen für den Einsatz dieser Methode fest. Demnach können die Strafermittlungsbehörden bei einem durch bestimmte Tatsachen begründeten Verdacht, eine der aufgezählten Straftaten sei begangen worden, von jedem Dritten Datenträger mit elektronisch oder sonst nicht unmittelbar wahrnehmbar gespeicherten Daten anfordern.

Zu bemängeln ist einmal, daß die Straftaten, bei denen eine Rasterfahndung zulässig sein soll, nicht vollständig in den beiden Vorschriften über die Rasterfahndung aufgelistet sind, sondern auch auf den Straftatenkatalog des § 163d StPO verwiesen wird. Dies trägt nicht zur Normenklarheit bei. Darüber hinaus ist nicht ausreichend geprüft worden, ob und in welchem Umfang hier wirklich nur Straftaten erfaßt werden, deren Schwere einen solchen Eingriff verhältnismäßig erscheinen lassen.

Außerdem bestimmt § 98a E, daß die Datenträger mit automatisiert gespeicherten Datensätzen von - im Regelfall einer Vielzahl betroffener und nichtbetroffener - Personen an die Strafermittlungsbehörde herausgegeben werden müssen. Vorgesehen ist, daß "die Datenträger (...) zur Aussonderung der Daten dieser Personen abgefragt oder mit anderen gespeicherten Daten abgeglichen werden (können)". Mit anderen Worten: Aus einer großen Anzahl von Datensätzen werden entweder durch Abfrage oder Verknüpfung bestimmter Merkmale eine Reihe von Datensätzen herausgefiltert, oder dieser Filtervorgang ergibt sich aus dem Abgleich mit bereits bei den Strafermittlungsbehörden vorhandenen Datensätzen aus anderen Quellen. Der Entwurf legt nicht eindeutig fest, ob vor der Weitergabe an die Polizei die Datensätze bereits sortiert und vorgefiltert werden dürfen oder sollen, oder ob dieser Vorgang erst bei der Polizei im Rahmen der Gesamtüberprüfung stattfindet.

Da auch die Daten einer Vielzahl nicht Betroffener einbezogen werden, ist das Verfahren nur zulässig, wenn eine Aufklärung der Straftat oder die Ergreifung des Täters auf andere Weise aussichtslos oder wesentlich erschwert wäre.

Eine Rasterfahndung bedarf der schriftlichen Anordnung durch den Richter; erfolgt die Anordnung bei Gefahr im Verzug durch die Staatsanwaltschaft, muß sie innerhalb von drei Tagen vom Richter bestätigt werden.

Zwar sieht der Entwurf die Rückgabe bzw. Löschung der nicht mehr benötigten Daten vor. Allerdings lassen die Formulierungen "unverzüglich" bzw. "sobald und soweit sie (die Datenträger) für das Strafverfahren nicht mehr benötigt werden" auch eine sehr langfristige Auswertung der übermittelten Daten bei den Strafermittlungsbehörden zu. Das Gesetz sollte deshalb absolute Höchstfristen setzen.

5.2.2.2

Ausschreibung zur Festnahme und Erlaß eines Steckbriefs (§ 131 E)

Nach dem Entwurf kann die Staatsanwaltschaft oder der Richter eine Ausschreibung zur Festnahme anordnen und einen Steckbrief erlassen, wenn ein Haftbefehl oder ein Unterbringungsbeehl vorliegt, der Beschuldigte flüchtig ist, sich verborgen hält und andere Fahndungsmaßnahmen nicht ausreichend erscheinen. Damit handelt es sich auch hier um ein "letztes Mittel". Mit der Ausschreibung zur Festnahme werden die Daten des Betroffenen einer Vielzahl von Behörden bekannt; ein Steckbrief erreicht nahezu die gesamte Öffentlichkeit. Insofern ist es nicht unproblematisch, wenn unter bestimmten Voraussetzungen ("erhebliche Gefährdung des Fahndungserfolgs") die Staatsanwaltschaft oder sogar die Polizei ("wenn ein Festgenommener entweicht oder sich sonst der Bewachung entzieht") eine Ausschreibung bzw. steckbriefliche Verfolgung vornehmen kann. Ausdrücklich sieht der Entwurf die Möglichkeit vor, ein bundesweites automatisiertes Informationssystem zu verwenden, darin den Gesuchten zu bezeichnen, zu beschreiben, eine Abbildung weiterzuleiten und Tatverdacht, Ort und Zeit der Begehung anzugeben.

Schon das Verfahren des Erlasses eines Steckbriefs schließt aus, daß es sich um eine so dringende Maßnahme handeln kann, daß die Polizei die Maßnahme anordnen und erlassen können muß. Wichtiger jedoch ist die Kritik am Anwendungsbereich dieser Maßnahme. Steckbriefe werden nur in sehr seltenen Fällen und bei sehr schweren Delikten erlassen. Der Regelungsentwurf enthält keinerlei Vorgaben hierfür. Schon die Erfahrungen der Praxis sollten deshalb zu einer erheblichen Einschränkung des Anwendungsbereichs führen.

5.2.2.3

Polizeiliche Beobachtung (§ 163e E)

Die polizeiliche Beobachtung wird bisher bei einem wesentlich kleineren Katalog bestimmter Straftaten praktiziert, als im Entwurf vorgesehen. Dazu zählen etwa der bandenmäßige Rauschgifthandel oder Verstöße gegen das Waffengesetz. Es ist unbedingt notwendig, den im Entwurf enthaltenen Katalog der betroffenen Straftaten erheblich einzuschränken.

Die Vorschrift verdient allerdings auch grundsätzliche Kritik. Bei der polizeilichen Beobachtung handelt es sich um Vorfelderhebungen, bei denen eine konkrete Straftat keinesfalls feststeht, sondern lediglich die Vermutung vorliegt, die kontrollierten Personen würden ständig Straftaten eines bestimmten Typus planen oder ausführen. Als "Verdachtsverdichtungsinstrument" kommt der polizeilichen Beobachtung damit hauptsächlich präventiv-polizeiliche Funktion zu, d.h. in erster Linie eine Bedeutung zur Abwehr zukünftiger Straftaten. Zweifel sind deshalb berechtigt, ob die Vorschrift nicht in das Polizeirecht übernommen werden sollte und in der Strafprozeßordnung fehl am Platze ist.

Da dieses Instrument als Vorfeldinstrument auch ohne einen konkreten Tatverdacht eingesetzt werden kann - zudem können nicht nur Beschuldigte, sondern auch andere Personen zur Beobachtung ausgeschrieben werden - ist seine Anwendung, wenn überhaupt, nur sehr restriktiv denkbar. Es kann nur letztes Mittel sein, um an Straftatenkomplexe heranzukommen, die mit den übrigen Ermittlungsmethoden nicht aufgeklärt werden können. Eine örtliche und räumliche Begrenzung der Maßnahme ist unabdingbar; ebenso die unverzügliche Vernichtung der gewonnenen Unterlagen, soweit sie für den ursprünglich angestrebten Zweck nicht verwendet werden können.

5.2.2.4

Planmäßige Überwachung (§ 163f E)

Merkt der Betroffene bei der polizeilichen Beobachtung von dieser Maßnahme in der Regel nichts, so wird dies bei der "planmäßigen Überwachung" umgekehrt sein. Sie soll zulässig sein, "soweit bestimmte Tatsachen den Verdacht begründen, daß eine erhebliche Straftat begangen worden ist, und tatsächliche Anhaltspunkte die Annahme rechtfertigen, daß die Überwachung zur Aufklärung der Straftat oder zur Ergreifung des Täters führen kann, und wenn dies auf andere Weise aussichtslos oder wesentlich erschwert wäre". In gleichem Umfang wie bei der polizeilichen Beobachtung kann sich diese Maßnahme auch gegen eine "andere Person", die im Kontakt mit dem Beschuldigten steht, richten.

Absolut unzureichend ist die Zulässigkeitsvoraussetzung "erhebliche Straftat". Damit ist kaum eine Einschränkung verbunden; der Grundrechtseingriff einer totalen Überwachung bzw. Beschattung kann aber allenfalls im Zusammenhang mit der Aufklärung bestimmter, weniger Straftaten gerechtfertigt sein. Dies wird insbesondere dann deutlich, wenn, wie § 163f Abs. 2 E vorsieht, auch "verdeckt" Lichtbilder aufgenommen und, soweit bestimmte Tatsachen den Verdacht begründen, daß eine erhebliche Straftat begangen worden ist, sonstige technische Mittel, namentlich zur Anfertigung von Bildaufzeichnungen sowie zum Abhören oder Aufzeichnen des gesprochenen Wortes auf Tonträger, eingesetzt werden dürfen. Zwar sieht § 163f Abs. 3 E vor, daß die erwähnten Maßnahmen der Überwachung überhaupt ebenso wie der technischen Überwachung "nicht innerhalb einer Wohnung und von außen her nicht mit technischen Mitteln durchgeführt werden, deren Wirkung in die Wohnung eindringt". Für den Betroffenen macht es im Ergebnis wohl kaum einen Unterschied, ob sein Gespräch mittels einer Wanze in der Wohnung oder von außen mit einem Richtmikrofon abgehört wird.

5.2.2.5

Ermittlungen und Auskunftsverlangen der Staatsanwaltschaften gegenüber allen öffentlichen Behörden (§ 161 E)

Die vorgeschlagene Änderung des bereits existierenden § 161 StPO soll diesen lediglich insoweit modifizieren, als die staatsanwaltschaftlichen Ermittlungshandlungen im Hinblick auf die Aufklärung der Straftat oder die Ergreifung des Täters an den Erforderlichkeitsgrundsatz gebunden werden, die staatsanwaltschaftliche Ermittlungstätigkeit nicht gegen "besondere gesetzliche Übermittlungsregelungen" verstoßen darf und andere gesetzliche Vorschriften die Befugnisse der Strafverfolgungsbehörde nicht besonders regeln. Damit sollen in die Strafprozeßordnung einzelne Grundsätze aus dem Datenschutzrecht übernommen werden, die bisher aufgrund der verfassungsrechtlichen Vorgaben eigentlich schon galten. Insoweit würde sich an der Praxis nichts ändern. Von wesentlich größerer Bedeutung wäre es, wenn die staatsanwaltschaftliche Datenverarbeitung in all ihren Phasen umfassend und konkret aufgegriffen würde und der Bürger damit genauer feststellen könnte, was mit seinen, bei der Staatsanwaltschaft befindlichen Daten geschieht. Die vorgeschlagene Vorschrift stellt allenfalls eine Rumpfregelung mit geringer Aussagekraft dar.

5.2.3

Resümee

Die Vorschläge des Bundesjustizministers enthalten bewußt nur eine Teilregelung. Aber selbst als Teilregelung stecken sie den Rahmen der Datenverarbeitung der Ermittlungsbehörden in den aufgegriffenen Bereichen zu vorsichtig, zu unklar ab. Dies kann um so weniger hingenommen werden, als bei einigen Bereichen - der polizeilichen Beobachtung und der Fahndung durch Steckbrief - die vorgeschlagenen Bestimmungen weit über die Bedürfnisse der Praxis hinaus Möglichkeiten der Datenverarbeitung eröffnen.

5.3

Auskünfte aus dem Grundbuch

Bekanntlich enthalten Grundbücher nicht nur Angaben über Grundstückseigentümer, sondern auch über Belastungen des Grundstücks, beispielsweise mit Nutzungsrechten Dritter oder Hypotheken. Auch wenn diese Angaben nicht immer auf dem neuesten Stand sind und der Umfang der Sicherung der Kreditgeber nicht stets der tatsächlichen Schuldenlast entspricht, so ist mit den Informationen des Grundbuchs insbesondere kurz nach Eintragung der Belastungen doch ein recht guter Überblick über den Schuldenstand zu gewinnen. Deshalb kommen die meisten Anfragen verständlicherweise von Kreditinstituten. Es kann daher aber auch nicht überraschen, daß Beschwerden von Betroffenen gegen die Auskunftspraxis der Grundbuchämter hauptsächlich Auskünfte an Kreditinstitute betreffen. In zwei Fällen, die ich im vergangenen Jahr überprüft habe, waren die Beschwerden durchaus berechtigt.

5.3.1

Auskünfte

Ein Gesellschafter hatte für einen Überziehungskredit, den eine Großbank seiner GmbH gewährt hatte, die private Bürgschaft übernommen. Durch Zufall erfuhr er, daß die Bank seit einiger Zeit Grundbuchauszüge sowohl über sein Privathaus als auch über seine privaten Büroräume besaß. Seine Nachfragen bei den zwei betreffenden Grundbuchämtern ergab, daß der Bank die Auskünfte ohne weiteres erteilt worden waren. Einen besonderen Grund für ihre Auskunftswünsche hatte sie nicht angegeben.

Im zweiten Fall wollte sich ein Grundstückseigentümer unverbindlich über die Kreditbedingungen einer Bank erkundigen und war erstaunt, als der Direktor sein Angebot auf einen Grundbuchauszug stützte, den er sich ohne Wissen des Betroffenen zur Vorbereitung des Gesprächs vom Grundbuchamt besorgt hatte. Auch hier hatte die Bank, ohne einen besonderen Grund anzugeben, die Auskunft erhalten.

5.3.2

Prüfungspflicht des Grundbuchamtes

Nach der Grundbuchordnung ist die Einsicht des Grundbuchs jedem gestattet, der ein berechtigtes Interesse darlegt (§ 12 GBO). In beiden Fällen hatten die Grundbuchämter nicht ausreichend geprüft, ob ein solches Interesse dargelegt worden war. Ein Grundbuchamt teilte im ersten Fall dem Betroffenen vielmehr mit: "Fordert eine Bank eine Grundbuchauskunft an, wird vorausgesetzt, daß Geschäftsverbindungen zum Eigentümer bestehen und somit das berechtigte Interesse gegeben ist." Das widerspricht jedoch dem Gesetz, das die Darlegung eines berechtigten Interesses verlangt. Das Grundbuchamt hat bei jeder Anfrage die Erfüllung dieser Voraussetzung zu prüfen. An die Darlegung des berechtigten Interesses werden zwar keine hohen Anforderungen gestellt, wirtschaftliche Interessen genügen, mit dem Briefkopf alleine kann aber keineswegs das berechtigte Interesse dargelegt werden.

Einen wesentlich strengeren Maßstab legen die Grundbuchämter im übrigen bei Anfragen von einzelnen Privatpersonen an. Dort genügt es nicht, wenn etwa ein Kaufinteresse lediglich behauptet wird, sondern es werden zumeist schriftliche Unterlagen verlangt, aus denen sich Kaufverhandlungen zwischen dem Auskunftssuchenden und dem Grundstückseigentümer erkennen lassen.

Meine Kritik an der Praxis der Grundbuchämter bei Auskünften an Kreditinstitute habe ich dem Hessischen Minister der Justiz mitgeteilt. Nach Ansicht des Justizministers ist die Auskunftspraxis jedoch unbedenklich. Auch er gehe davon aus, so der Minister in seinem Antwortschreiben, daß bei einer Bank, die eine Grundbuchauskunft beantrage, Kreditbeziehungen zu dem Grundbuchberechtigten bestünden und nicht sonstige, nicht berechtigende Gründe, etwa private Neugier, ausschlaggebend für den Antrag seien. Bei bestimmten Bankinstituten könne der Grundbuchbeamte auch ohne nähere Prüfung Anhaltspunkte für einen Mißbrauch des Einsichtsrechts verneinen.

6. Sicherheitsbehörden

6.1

Polizeilicher Zugriff auf Meldedaten

6.1.1

Trennung von Polizei und Melderegister

Eine wesentliche Erkenntnisquelle für die polizeiliche Überprüfung personenbezogener Daten oder auch Nachforschungen nach der derzeitigen Wohnung einer einzelnen Person sind die Melderegister der Gemeinden. Während die Polizei rund um die Uhr tätig ist und gerade an Wochenenden und zur Nachtzeit Überprüfungen notwendig werden können, sind die Meldeämter nur während der üblichen Bürozeiten besetzt. Die Folge liegt auf der Hand: Die Polizei fordert Möglichkeiten des Zugriffs auf die Meldedaten, die ihr unabhängig von den Bürozeiten der Meldebehörden einen ständigen Datenzugang gewährleisten. Ein Ausweg bleibt freilich rechtlich versperrt: Die Integration des Melderegisters in den polizeilichen Bereich würde verkennen, daß mit dem Melderegister eine Vielzahl von nichtpolizeilichen Aufgaben verknüpft sind, die mit der Tätigkeit der Polizeidienststellen nicht vermengt werden dürfen. Konsequenterweise hat deshalb das Bundesland Berlin, in dem das Melderegister früher als Aufgabe der Vollzugspolizei angesehen wurde, in den letzten Jahren bewußt eine Trennung beider Aufgabenbereiche einschließlich der Behördenorganisation vorgenommen.

6.1.2

Übergangsregelung

Art und Umfang des Zugangs einer Behörde zu den Daten einer anderen datenverarbeitenden Stelle hängen nicht zuletzt davon ab, wie die Daten gespeichert und verwertet werden, insbesondere ob dies automatisiert erfolgt oder nicht. Der Bundesgesetzgeber hat deshalb in § 24 des Melderechtsrahmengesetzes bewußt nur zeitlich befristet bis zum 31. Dezember 1985 zugelassen, daß nach den Landesmeldegesetzen - § 45 des Hessischen Meldegesetzes hat diese Bestimmung aufgegriffen und umgesetzt - die Polizei außerhalb der Dienstzeiten der Meldebehörde mit einem eigenen Schlüssel deren Räume betreten und Einsicht in die Meldeunterlagen nehmen kann. Die zeitliche Befristung hatte zwei Gründe: Zum einen sollte sich die Datenweitergabe auf Dauer nur auf die jeweils für die Polizei erforderlichen Daten beschränken, während bei einer Einsichtnahme der Blick in weitere Informationen kaum verhindert werden kann. Zum anderen kann lediglich bei einem automatisierten Zugriff der Polizei der erschließbare Datensatz von vorneherein eingegrenzt und über die Protokollierung jedes Einzelzugriffs eine wirksame nachträgliche Kontrolle ausgeübt werden, welche Angaben tatsächlich abgerufen wurden. Ein solcher automatisierter Zugriff war nach den Feststellungen des Gesetzgebers faktisch nicht vor dem 1. Januar 1986 allgemein realisierbar, da erst zu diesem Zeitpunkt eine automatisierte Meldedatenverarbeitung bei den Gemeinden die Regel sein würde.

Zu Beginn des Jahres 1986 bestand damit keine Möglichkeit mehr für die Polizei, an Wochenenden und während der Nachtzeit selbst die Meldeunterlagen einzusehen. Mit anderen Worten: Die Schlüssel mußten abgegeben werden. Nur soweit die Gemeinden entsprechend einem Erlaß des Hessischen Ministers des Innern einen Notdienst auf Abruf bereitstellten, konnte während dieser Zeit eine Datenübermittlung an die Polizei stattfinden.

6.1.3

Meldedaten-Übermittlungsverordnung

Mit der am 3. Juli 1986 in Kraft getretenen Verordnung über regelmäßige Datenübermittlungen der Meldebehörden (Meldedaten-Übermittlungsverordnung - MeldDÜVO - GVBl. I S. 210) wurde generell der Datenaustausch zwischen Meldebehörden und Polizei auf eine neue Grundlage gestellt. Die Verordnung sieht in § 13 vor, daß ein bestimmter Datenkatalog für die Polizeidienststellen zum automatisierten Abruf bereitgehalten wird. Genauer: Die Kommunalen Gebietsrechenzentren "öffnen" im gesetzlichen Auftrag der Gemeinden jeweils für einzelne Regierungspräsidenten, Polizeipräsidenten und Polizeidirektionen innerhalb ihres Zuständigkeitsbereichs die Meldedatenbestände, die sie im Auftrag der Gemeinde verarbeiten. Mit dieser "dezentralen Lösung" ist auf meine Initiative die frühere technische Konzeption einer zentralen Anbindung des Landeskriminalamts an alle Kommunalen Gebietsrechenzentren aufgegeben worden. Der ursprünglich geplante "Rechner-Rechner-Verbund" und die beabsichtigte Errichtung eines "SNI-Netzes" (System Network Architecture Integration) hätten jeder hessischen Polizeidienststelle ermöglicht, einen Grundkatalog von Daten jedes hessischen Bürgers abzurufen - faktisch wäre damit für den Sicherheitsbereich ein erweitertes Landesadreßregister eingerichtet worden.

Ein Rechner-Rechner-Verbund hätte die technische Verwertbarkeit der Daten in vielerlei Hinsicht erweitert - möglich gewesen wären gezielte Auswertungen nach bestimmten Merkmalen, Datenabgleiche auch im Sinne der Rasterfahndung, temporäre oder dauernde Verknüpfungen mit kriminalpolizeilichen Informationen. Damit wäre der gesamte hessische Meldedatenbestand in das polizeiliche Informationssystem integriert worden.

Eine stichprobenhafte Überprüfung bei Meldebehörden unterschiedlicher Größen, die ich Ende 1985 durchgeführt hatte, ergab, daß die Polizeibehörden unter der früheren, die Einsicht zu bestimmten Zeiten erlaubenden Regelung faktisch nur in einigen größeren Städten von ihrem "Schlüssel" Gebrauch gemacht hatten. Mein darauf gründender Vorschlag, den Direktzugriff nur in diesen "Kriminalitätsschwerpunkten" und bezogen auf die dortigen Gemeinden einzurichten, wurde jedoch von der Landesregierung nicht aufgegriffen.

6.1.4

"Datenfernverarbeitung im Einwohnerwesen - Polizeiauskunftssystem - EWOTP"

Nachdem die Verordnung in Kraft getreten war, ließ der Hessische Minister des Innern vom Kommunalen Gebietsrechenzentrum Wiesbaden ein Konzept "Datenfernverarbeitung im Einwohnerwesen - Polizeiauskunftssystem - EWOTP" entwickeln. Meine Überprüfung dieses Systems kam zu einem überraschenden Ergebnis, das gerade deswegen ein besonderes Interesse verdient, weil es sich bei anderen Formen des Direktzugriffs einer Behörde auf Daten einer anderen Dienststelle wiederholen kann:

Während bei der traditionellen Datenübermittlung der Empfänger der übermittelnden Stelle einen Teil des Datensatzes nennt und diesen ergänzt erhält, sollte das geplante Auskunftsverfahren wesentlich mehr Möglichkeiten enthalten. Die Konzeption sah weit über Einzelfallanfragen hinaus mehrstufige Recherche- und Auswertungsverfahren vor, die im Ergebnis wiederum die ursprünglich geplante weitgehende Eingliederung der Melderegister in das polizeiliche Informationssystem zur Folge gehabt hätten.

Im Gegensatz zum bisherigen Verfahren, bei dem die Polizei im Regelfall nur Daten einzelner bestimmter Personen aus dem Melderegister erhielt, war nach dem neuen Verfahren eine Auswertung des gesamten beim KGRZ verarbeiteten und allgemein nach der Verordnung übermittelbaren Einwohnerdatenbestandes durch verschiedene Raster möglich. Auch der Zugriff war nicht entsprechend der Vorschrift je nach dem Zuständigkeitsbereich der Polizeidienststelle beschränkt. Vielmehr erlaubte das Verfahren eine Direktverarbeitung der Daten aller Gemeinden im jeweilig angeschlossenen Rechenzentrumsbereich durch alle angeschlossenen Polizeibehörden. Die Abfrage konnte sich sowohl auf Daten einzelner Gemeinden beschränken, als auch den Gesamtbestand des Rechenzentrums einschließen. Über die Eingabe von Namen, Namensfragmenten oder Straßen konnten nach bestimmten Suchkriterien gemeindebezogen oder gemeindeübergreifend bestimmte Gruppen von Personen - ausgewählt etwa nach Alter, Geburtsdatum oder Geschlecht - ausgewählt werden. Selbst Abfragen nach Personen mit bestimmten Namensfragmenten - z. B. der Buchstabenkombination Sch... des Familiennamens - oder einfach eines bestimmten Alters unter Angabe einer bestimmten Straße waren möglich.

Das Abfragesystem sollte somit nicht nur zur Erschließung einzelner Daten einer im Grunde bekannten Person genutzt werden können, sondern im Sinne eines Recherchesystems sollten anhand einzelner Merkmale und zusätzlicher Auswahlkriterien ganze Personengruppen aus dem Einwohnermeldedatenbestand herausgefiltert werden. Damit hätten den Polizeibehörden bei weitem umfangreichere Auswertmöglichkeiten zur Verfügung gestanden als den Meldebehörden selbst. Nicht nur sämtliche Schranken der Datenverarbeitung zwischen Meldebehörden und der Polizei wären aufgehoben worden, auch der Grundsatz, daß Direktzugriffe lediglich der Abfrage dienen sollen und nicht zum Recherchesystem ausgebaut werden dürfen, wäre verletzt worden. Da außerdem der Direktzugriff keineswegs nur auf die dienstfreie Zeit der Meldebehörden beschränkt, sondern das Auskunftssystem rund um die Uhr genutzt werden sollte, war die Einführung dieses Verfahrens keinesfalls hinnehmbar.

Nach Gesprächen mit dem Minister des Innern wurden die Zugriffsmöglichkeiten erheblich eingeschränkt. Insbesondere wird grundsätzlich die Abfrage auf den Bestand einer bestimmten Gemeinde beschränkt, Zugriffe auf Daten einer Personengruppe unter Verwendung von Altersangaben sind nur ausnahmsweise zulässig. Schließlich ist in der Protokollierung des Abrufs nicht nur die Organisationseinheit der Polizeidienststelle, sondern auch die anfragende Person durch ein Namenskurzzeichen festzuhalten.

Der Innenminister will jedoch erst dann diese Einschränkungen auch programmtechnisch fixieren, wenn sich die Einschränkungen nach seiner Ansicht aus polizeilichen Gesichtspunkten vertreten lassen. Meines Erachtens haben die Einschränkungen aber lediglich dann einen Sinn, wenn über die gegenüber den Polizeidienststellen ausgesprochenen Verbote hinaus auch technisch lediglich eine eingegrenzte Auswertung möglich ist. Es widerspräche grundsätzlichen Erwägungen des Datenschutzes, wollte man eine technische Infrastruktur beibehalten, die eine Vielzahl von Auswertungen ermöglicht, die rechtlich nicht zulässig sind. Ich habe deshalb den Innenminister noch einmal aufgefordert, die Programme entsprechend zu ändern.

6.2

Sicherheitsüberprüfung in kerntechnischen Anlagen

In den letzten Jahren hat der Bundesminister des Innern - bzw. seit der Schaffung des neuen Ministeriums der Bundesminister für Umwelt, Naturschutz und Reaktorsicherheit - unter Mitwirkung des Länderausschusses für Kernenergie den Entwurf einer Richtlinie für die Durchführung von Sicherheitsüberprüfungen von Personal in kerntechnischen Anlagen und bei der Beförderung und Verwendung von Kernbrennstoffen erarbeitet. Über die geplante Richtlinie habe ich 1986 mit dem Hessischen Minister für Wirtschaft und Technik verschiedene Gespräche geführt, in denen ich dargelegt habe, in welchen Punkten Ergänzungen bzw. Abänderungen des Entwurfs geboten sind. Es liegt nunmehr eine neue Fassung des Entwurfs vor, die voraussichtlich 1987 ohne gravierende Änderungen in Kraft treten wird. Sie stellt zwar einen wesentlichen Schritt in die richtige Richtung dar, kann jedoch die bestehenden Probleme keineswegs hinreichend lösen.

6.2.1

Gegenwärtige Situation

Gegenwärtig ist die Sicherheitsüberprüfung von Personal in kerntechnischen Anlagen nur sehr lückenhaft festgelegt. Als Rechtsgrundlage für die Durchführung der Überprüfungen wird von den atomrechtlichen Behörden auf § 7 Abs. 2 Nr. 1 und 5 des Atomgesetzes hingewiesen. In diesen Vorschriften wird die Genehmigung von kerntechnischen Anlagen u.a. davon abhängig gemacht, daß "keine Tatsachen vorliegen, aus denen sich Bedenken gegen die Zuverlässigkeit des Antragstellers und der für die Errichtung, Leitung und Beaufsichtigung des Betriebs der Anlage verantwortlichen Personen ergeben", ferner, daß "der erforderliche Schutz gegen Störmaßnahmen oder sonstige Einwirkungen Dritter gewährleistet ist". Die konkrete Durchführung von Sicherheitsüberprüfungen, insbesondere der Kreis der zu überprüfenden Personen und die genaue Verfahrensweise, ist allerdings weder im Atomgesetz noch in anderen Vorschriften geregelt. Dies entspricht nicht rechtsstaatlichen Erfordernissen.

6.2.2

Die geplante Richtlinie

6.2.2.1

Übergangslösung

Vor diesem Hintergrund ist es grundsätzlich zu begrüßen, daß nunmehr die Durchführung von Sicherheitsüberprüfungen im einzelnen festgelegt werden soll. Es darf jedoch nicht verkannt werden, daß eine Festlegung in der Form einer Richtlinie nur eine vorübergehende Lösung sein kann. Ich halte es in jedem Fall für unerlässlich, daß der Kreis der zu überprüfenden Personen sowie die Grundzüge des Verfahrens - entweder im Atomgesetz oder in einem bereichsübergreifenden Gesetz über die allgemeine Durchführung von Sicherheitsüberprüfungen - gesetzlich geregelt wird. Dies insbesondere auch deshalb, weil die Sicherheitsüberprüfungen gravierende konkrete Auswirkungen für die Betroffenen haben können, so namentlich deren Nichteinstellung. Auch die Tatsache, daß die Durchführung einer Überprüfung stets von dem Einverständnis der Betroffenen abhängig gemacht wird, vermag an dem Erfordernis einer gesetzlichen Regelung nichts zu ändern: Der Zutritt zu einer kerntechnischen Anlage wird den Betroffenen in der Regel nur nach Durchführung einer Sicherheitsüberprüfung gestattet werden. Faktisch haben sie daher keine andere Wahl, als sich mit einer Überprüfung einverstanden zu erklären. Aus diesem Grund bedarf es in jedem Fall einer klaren und rechtsstaatlichen Regelung der Verfahrensweise.

6.2.2.2

Inhalt

Inhaltlich enthält der neue Richtlinienentwurf eine Reihe positiv zu bewertender Bestimmungen, an denen sich eine gesetzliche Regelung orientieren könnte. Es wird nach verschiedenen Personenkreisen differenziert und die jeweilige Verfahrensweise bei der Durchführung der Überprüfung im einzelnen festgelegt. Die Beteiligung weiterer Behörden (des Landesamtes für Verfassungsschutz, des Landeskriminalamts, des Bundeszentralregisters sowie in Einzelfällen auch des Gewerbezentralregisters) wird ebenfalls festgelegt. Ferner wird darauf hingewiesen, daß generell dem Grundsatz der Verhältnismäßigkeit Rechnung zu tragen ist. Hervorzuheben ist insbesondere, daß der Grundsatz der Zweckbindung personenbezogener Daten konkret umgesetzt wurde: Die im Rahmen der Sicherheitsüberprüfung von der zuständigen atomrechtlichen Behörde gesammelten Daten sollen ausschließlich für die Zwecke der Sicherheitsüberprüfung nach dem Atomgesetz verwendet und nicht an andere Stellen weitergeleitet werden. Schließlich ist es von zentraler Bedeutung, daß die Betroffenen bei Zweifeln an der Zuverlässigkeit Gelegenheit erhalten, sich zum Überprüfungsergebnis zu äußern.

Nichtsdestoweniger halte ich die Richtlinie in einigen Punkten noch für verbesserungsbedürftig. Die beteiligten Behörden sollten ausdrücklich verpflichtet werden, nur richtige, aktuelle und nicht zu löschende Daten zu

übermitteln. Von besonderer Bedeutung ist dies für die Sicherheitsbehörden: Es muß sichergestellt werden, daß bei der Übermittlung von Daten zu Ermittlungs- bzw. Strafverfahren in jedem Fall auch der Verfahrensausgang bzw. der aktuelle Ermittlungsstand mitgeteilt wird. Ferner sollte vorgesehen werden, daß dem Betroffenen auch das Endergebnis der Sicherheitsüberprüfung mitgeteilt wird, damit er z.B. erkennen kann, ob seine Nichteinstellung auf ungenügender Qualifikation oder auf Sicherheitsbedenken beruht. Dies ist eine wichtige Voraussetzung für die Schaffung von mehr Transparenz für die Betroffenen, wie sie von mir seit langem gefordert wird.

Besondere Probleme ergeben sich im Zusammenhang mit der vorgesehenen Beteiligung der Sicherheitsbehörden an der Überprüfung. Im Richtlinienentwurf wird ausdrücklich darauf hingewiesen, daß sich die Vorschriften lediglich auf die von der nach dem Atomgesetz zuständigen Genehmigungs- oder Aufsichtsbehörde zu veranlassenden Überprüfungsmaßnahmen erstrecken, nicht jedoch auf die Tätigkeiten der Sicherheitsbehörden. Zweifelsohne können die generellen Befugnisse der Sicherheitsbehörden nicht in diesem Zusammenhang geregelt werden, andererseits ist gerade die Tätigkeit der Sicherheitsbehörden im Rahmen der Sicherheitsüberprüfungen von besonderer Bedeutung und werden von ihnen besonders sensible Daten an die Atombehörde übermittelt. Solange die Verarbeitung personenbezogener Daten durch die Sicherheitsbehörden nicht in bereichsspezifischen Gesetzen präzise geregelt ist - wie es von mir bereits seit Jahren gefordert wird -, kann daher auch eine Regelung für die Sicherheitsüberprüfung von Personal in kerntechnischen Anlagen in keinem Fall zufriedenstellen. So muß insbesondere auch eine präzise Regelung der Mitwirkung des Verfassungsschutzes an Sicherheitsüberprüfungen erfolgen. Hierauf habe ich bereits in meinem 13. Tätigkeitsbericht (Ziff. 2.2.3) und 14. Tätigkeitsbericht (Ziff. 13.1.2) hingewiesen. Regelungsbedürftig ist dabei in jedem Fall auch die Frage der Zweckbindung und der Aufbewahrungsdauer der beim Verfassungsschutz im Zusammenhang mit Sicherheitsüberprüfungen vorhandenen Daten.

6.3

Sicherheitsgesetze

6.3.1

Verabschiedete und geplante Gesetze

Im Jahr 1986 standen sechs für die Tätigkeit der Sicherheitsbehörden wichtige Gesetzentwürfe der Bundesregierung bzw. der Koalitionsfraktionen zur Diskussion. Neben der Novellierung der Paß- und Personalausweisgesetze ging es um die Änderung des Straßenverkehrsgesetzes, der Strafprozeßordnung, des Bundesverfassungsschutzgesetzes, um Gesetze über die informationelle Zusammenarbeit der Sicherheits- und Strafverfolgungsbehörden und für den Militärischen Abschirmdienst. Ganz abgesehen von der inhaltlichen Kritik gab schon das Verfahren Anlaß zur Sorge. Die Eile, mit der formuliert, debattiert und die Entwürfe schließlich verabschiedet werden sollten, vertrug sich nicht mit der Relevanz der Themen und den umfassenden Auswirkungen auf die betroffenen Verwaltungsbehörden und den Bürger. Die Zusammenfassung so unterschiedlicher Vorhaben wie der Novellierung des Bundesverfassungsschutzgesetzes, der Neufassung des Bundesdatenschutzgesetzes und der Regelung der Datenverarbeitung für das Kfz-Register beim Kraftfahrt-Bundesamt in einem Gesetzgebungsverfahren (vgl. BR-Drucks. 65/86; BT-Drucks. 10/4737) ist für eine sorgfältige parlamentarische Debatte nicht unbedingt förderlich.

Vom Bundestag verabschiedet wurden schließlich nur das Paßgesetz und das Gesetz zur Änderung der Strafprozeßordnung, mit dem der § 163d StPO neu eingeführt wurde (BGBl. 1986 I S. 537), das Personalausweisgesetz (BGBl. 1986 I S. 545, Neubekanntmachung S. 548) sowie das Gesetz zur Änderung des Straßenverkehrsgesetzes (BGBl. 1986 I S. 486). Die weiteren geplanten Gesetze für den Bundesverfassungsschutz und den Militärischen Abschirmdienst (vgl. BT-Drucks. 10/4738 und BT-Drucks. 10/5342) sowie das Gesetz über die informationelle Zusammenarbeit der Sicherheits- und Strafverfolgungsbehörden des Bundes und der Länder in Angelegenheiten des Staats- und Verfassungsschutzes (ZAG - das das Stadium des nichtveröffentlichten Vorentwurfs nicht verließ), sind nicht zustande gekommen. Es ist allerdings zu erwarten, daß der Bundestag sich in der kommenden Legislaturperiode wieder mit diesen Themen befassen wird.

Anfang 1986 habe ich in verschiedenen Anhörungen des Innenausschusses des Deutschen Bundestages zu den Sicherheitsgesetzen Stellung genommen. Auch der Innenausschuß des Hessischen Landtags beabsichtigte, im Juni 1986 eine öffentliche Anhörung zu den Bonner Gesetzesprojekten und den damit verbundenen landesrechtlichen Auswirkungen durchzuführen. Verfahrensprobleme führten jedoch dazu, daß die Veranstaltung abgesagt wurde und die Stellungnahmen der Sachverständigen - ebenso wie mein Gutachten - lediglich in schriftlicher Form dem Landtag zugeleitet wurden.

6.3.2

Änderung des Straßenverkehrsgesetzes: Einführung des "Zentralen Verkehrsinformationssystems" (ZEVIS)

Den Entwurf einer Änderung des Straßenverkehrsgesetzes habe ich in meinem 13. Tätigkeitsbericht (Ziff. 3.5.4) und im 14. Tätigkeitsbericht (Ziff. 13.2.5) erörtert. Wesentliche Änderungen, die meine damals erhobenen

Einwände entkräften könnten, - insbesondere gegen die weitgehenden Zugriffsmöglichkeiten der Polizei und die umfassende Nutzung durch Justizbehörden und Nachrichtendienste - hat die im November 1986 vom Bundestag verabschiedete Fassung nicht vorgenommen. Das Gesetz entspricht in weiten Teilen nicht der Forderung nach einer Zweckbindung der bei den Zulassungsstellen und dem Kraftfahrtbundesamt gespeicherten Fahrzeug- und Halterdaten. Zunächst für verkehrsbezogene Maßnahmen erhobene Daten dürfen zu einer Vielzahl anderer Zwecke verwandt werden. Bedenken bestehen insbesondere gegen die Übermittlungsmöglichkeiten an die Nachrichtendienste. Diese können Fahrzeug- oder Halterdaten ohne jede Einschränkung erhalten, soweit dies zu ihrer Aufgabenerfüllung unerlässlich ist.

Diese Zweckentfremdung ist umso bedenklicher, als die Verarbeitung der personenbezogenen Daten durch die Nachrichtendienste bislang nicht an spezifische Datenschutzbestimmungen gebunden ist. Es bleibt also nach wie vor offen, in welchem Umfang und zu welchen Zwecken diese Behörden auf Fahrzeug- bzw. Halterdaten zugreifen. Besonders deutlich wird dieser Mangel bei der Informationsverarbeitung des Militärischen Abschirmdienstes und Bundesnachrichtendienstes. Für beide Dienste gibt es keinerlei Rechtsnormen, die deren Tätigkeit regeln. Soweit das Gesetz versucht, dadurch Abhilfe zu schaffen, daß es in einem besonderen Artikel die Aufgaben der Dienste umschreibt, für die eine Datenübermittlung zulässig sein soll, ist die Forderung nach einer bereichsspezifischen Regelung der Datenverarbeitung nur völlig unzureichend erfüllt: Eine bruchstückhafte, aus dem Zusammenhang gerissene Aufgabenbeschreibung im Straßenverkehrsgesetz verschafft nicht die nötige Transparenz. Erforderlich sind vielmehr eigene gesetzliche Regelungen für beide Dienste, die ihre Aufgaben und Befugnisse umfassend und präzise regeln. So lange solche Normen nicht vorliegen, sollte eine Übermittlung aus den Fahrzeugregistern an diese Stellen nicht erfolgen.

6.3.3

Personalausweisgesetz, Paßgesetz und § 163d Strafprozeßordnung

Die im Frühjahr dieses Jahres verkündeten Personalausweis- und Paßgesetze haben in den kritischen Bereichen identische Regelungen und weisen deshalb auch im wesentlichen dieselben Probleme auf.

Personalausweis und Paß sind nach Wortlaut und Zweck der Gesetze austauschbare Dokumente. Der Paß verliert damit zum großen Teil seine ursprüngliche Bedeutung als Grenzdokument. Je mehr er aber im Inland den Personalausweis ersetzt, desto deutlicher stellen sich auch bei seiner Benutzung die Fragen, die bereits die Diskussion über den Ausweis beherrscht haben.

Zu den Entwürfen für ein Personalausweisgesetz habe ich mich in den letzten Tätigkeitsberichten (14. Tätigkeitsbericht, Ziff. 13.2.4, 13. Tätigkeitsbericht, Ziff. 3.5.3, 12. Tätigkeitsbericht, Ziff. 3.1.) ausführlich geäußert. Die im Zusammenhang mit dem Personalausweis geäußerten Bedenken gelten gleichermaßen für das Paßgesetz.

6.3.3.1

Maschinenlesbarkeit

Nach wie vor ist die Notwendigkeit für die Maschinenlesbarkeit des Personalausweises und des Passes nicht ausreichend begründet. Vermehrte und beschleunigte Kontrollen im Inland und an der Grenze, die das einzige Motiv sein könnten, sind weder vom Bundesministerium des Innern noch von den Innenbehörden in ausreichendem Maße in Aussicht gestellt worden.

Die in den Entwürfen vorgesehene Befugnis der Polizei zur Speicherung der mit Hilfe des maschinenlesbaren Ausweises gewonnenen Daten ist nicht übernommen worden. Gegen diese Vorschriften hatte ich Bedenken geäußert, unter anderem wegen des schwer abgrenzbaren Personenkreises, der von einer solchen Maßnahme betroffen wäre. Vor allem aber deswegen, weil die für eine solche Regelung erforderlichen bereichsspezifischen gesetzlichen Grundlagen für die Sicherheitsbehörden fehlen. So gibt es für die Polizeibehörden des Bundes und der Länder - mit Ausnahme von Bremen - nach wie vor keine bereichsspezifischen Datenverarbeitungsvorschriften. Das gleiche gilt für die Nachrichtendienste.

Um diesen Mangel zu beheben, verfiel der Gesetzgeber auf folgende Lösung: Die Voraussetzungen, unter denen im Zusammenhang mit der Nutzung des maschinenlesbaren Ausweises, bzw. des Passes Dateien errichtet werden dürfen, werden bereichsspezifisch, also außerhalb der Personalausweis- und Paßgesetze geregelt. Als solche Regelung wurde § 163 d in die Strafprozeßordnung aufgenommen, der die Speicherung personenbezogener Daten für Strafverfolgungszwecke, und zwar nicht mehr ausschließlich im Zusammenhang mit der Nutzung des maschinenlesbaren Ausweises, sondern ganz allgemein regelt.

Eines wurde mit der endgültigen Fassung der Gesetze immerhin erreicht: Daten, die für präventivpolizeiliche Zwecke im Zusammenhang mit dem maschinenlesbaren Ausweis erhoben wurden, dürfen nicht gespeichert werden, bis entsprechende gesetzliche Regelungen vorliegen. Wie diese Verarbeitungsbestimmungen aussehen werden, ist jedoch vollkommen ungewiß. Der allgemein gehaltene Gesetzesvorbehalt eröffnet die Möglichkeit, weitere Verwertungen ohne jede erkennbare Schranke zu formulieren.

Zudem ist mit § 163 d StPO keinesfalls eine aus datenschutzrechtlicher Sicht beispielhafte Regelung gelungen. Es erscheint kaum möglich, mit Hilfe isolierter Einzelbestimmungen wichtige Grundfragen der Datenverarbeitung der Polizei und Staatsanwaltschaft zu regeln. Dazu bedarf es vielmehr eines geschlossenen Konzepts von Regelungen über die Datenverarbeitung im Zusammenhang mit Maßnahmen der Strafverfolgung (siehe hierzu Ziff. 5.2).

6.3.3.2

Andere Einwände

Bedenken bestehen nach wie vor gegen die mangelnde Zweckbindung der in den örtlichen Personalausweis- bzw. Paßregistern gespeicherten Daten. Die viel zu allgemein formulierten, über das generelle Erforderlichkeitsprinzip kaum hinausgehenden Übermittlungsvoraussetzungen sind unschwer von allen öffentlichen Stellen zu erfüllen. In den Gesetzen hätte vielmehr festgelegt werden müssen, daß die Paß- bzw. Personalausweisregister lediglich im Zusammenhang mit der Ausstellung von Pässen oder zur Identifikation ihrer Träger durch die Sicherheitsbehörden herangezogen werden dürfen.

Zu kritisieren ist auch, daß die im Paß- bzw. Personalausweisregister einerseits und in den Melderegistern andererseits enthaltenen Daten zur wechselseitigen Registerberichtigung verwendet werden dürfen. Damit werden die Grenzen der Verarbeitung dieser zwei unterschiedlichen Zwecken dienenden Dateien verwischt.

Erhebliche Einwände habe ich bereits früher gegen die nunmehr beschlossene Regelung erhoben, nach der nur die die Ausweisbehörde um Informationen ersuchende Behörde die Verantwortung für die Rechtmäßigkeit der Übermittlung trägt. Damit wird ein datenschutzrechtliches Grundprinzip aufgegeben: die geteilte und damit doppelte Verantwortung von Absender und Empfänger für die rechtlich einwandfreie Weitergabe von Daten.

6.3.4

Entwurf eines Gesetzes zu Änderung des Bundesverfassungsschutzgesetzes

6.3.4.1

Ungenügende Regelung der Aufgaben und Befugnisse der Verfassungsschutzbehörden

Der Entwurf (Bundestags-Drucks. 10/4737, Bundesrats-Drucks. 65/86) genügt nicht den im Volkszählungsgesetzurteil entwickelten Grundsätzen des Bundesverfassungsgerichts für die Verarbeitung personenbezogener Daten. Auch und gerade für die personenbezogene Datenverarbeitung der Nachrichtendienste sind bereichsspezifische Regelungen erforderlich, die präzise und in einer für den Bürger nachvollziehbaren Weise die Aufgaben der verarbeitenden Behörde umschreiben und klar zu erkennen geben, für welche Zwecke die Daten verwendet werden sollen.

So übernimmt der Vorschlag weitgehend die Aufgabenbeschreibung des geltenden Gesetzes. Die einzelnen Haupttätigkeitsbereiche der Verfassungsschutzbehörden - die Abwehr des politischen Extremismus, die Bekämpfung der Spionage und des Terrorismus sowie die Mitwirkung bei Sicherheitsüberprüfungen - werden lediglich generalklauselartig umschrieben. Nicht beantwortet wird die Frage, wann eine Person oder Organisation Objekt nachrichtendienstlicher Aktivität werden kann. Mit der Verwendung von Formeln wie "Bestrebungen, die gegen die freiheitlich-demokratische Grundordnung gerichtet sind" bleibt ungeklärt, in welchem Ausmaß im Umfeld extremistischer und terroristischer Bestrebungen personenbezogene Beobachtungen vorgenommen werden können, welches Ausmaß an organisatorischer Verfestigung die "Bestrebung" aufweisen muß, wo die Schwelle zwischen verfassungsfeindlicher Aktivität und regierungskritischer Gesinnung liegt. Ungeklärt bleibt auch, welcher Grad an verfassungsfeindlichem Einfluß auf demokratische Gruppen erforderlich ist, um nicht nur die Infiltranten, sondern die Gruppe selbst zur "Bestrebung" werden zu lassen.

Die jeweilige, dem Verfassungsschutz zugewiesene Aufgabe muß Maßstab sein für die gesetzliche Festlegung der einzelnen Befugnisse. Maßnahmen, die zur Abwehr von Spionen vertretbar sind, lassen sich nicht ohne weiteres auf die Beobachtung extremistischer Bestrebungen und erst recht nicht auf die Überprüfungen von Personen, die an sicherheitsempfindlichen Stellen tätig sind, übertragen. Der Entwurf differenziert jedoch nicht nach den einzelnen Aufgaben; selbst für den Einsatz "nachrichtendienstlicher Mittel" - d.h. etwa der Einschleusung von Vertrauensleuten, für Abhörmaßnahmen und Observationen, auch mit fototechnischen Mitteln - differenziert er nicht nach dem Objekt der nachrichtendienstlichen Tätigkeit. Angesichts der Schwere des mit der Anwendung des nachrichtendienstlichen Mittels verbundenen Eingriffs in das Persönlichkeitsrecht ist sicherzustellen, daß sich der Einsatz nur gegen konkret verdächtige Personen richtet und nicht gegen Dritte, die keinen Anlaß zur Beobachtung gegeben haben. Sobald beim Einsatz dieser Mittel "zufällig" Informationen über Personen anfallen, bei denen diese Voraussetzungen nicht vorliegen, sind diese zu löschen oder müssen einem Verwertungsverbot unterliegen.

6.3.4.2

Unzulässiger Informationsaustausch

Der Entwurf sieht einen weitreichenden Informationsaustausch zwischen dem Bundesamt für Verfassungsschutz und anderen Behörden, insbesondere den Polizeibehörden, vor, der nicht dem Gebot der Trennung von Verfassungsschutz und Polizei entspricht. Dieser vom Gesetzgeber zu beachtende Grundsatz gebietet zunächst die organisatorische und funktionelle Trennung von Polizei und Geheimdiensten. Unzulässig wäre also eine Angliederung des Verfassungsschutzes an eine polizeiliche Dienststelle, aber auch die Zuweisung von polizeilichen Eingriffsbefugnissen oder von Weisungsbefugnissen gegenüber Polizeidienststellen an den Verfassungsschutz. Der Entwurf stellt zwar klar, daß der Verfassungsschutz die Polizei auch nicht im Wege der Amtshilfe um Maßnahmen ersuchen darf, zu denen er selbst nicht befugt ist. Dies genügt jedoch nicht. Sinn des Trennungsgebots ist es, eine Zusammenballung von nachrichtendienstlichen und polizeilichen Befugnissen in der Hand einer Behörde zu verhindern. Würden nun die Ergebnisse aus dem Einsatz dieser speziellen Befugnisse - nämlich die dabei gewonnenen personenbezogenen Daten - zwischen Polizei und Verfassungsschutz frei ausgetauscht, so hätte man über den Umweg des Informationsaustausches das erreicht, was das Trennungsgebot verhindern will: Behörden mit dem konzentrierten "Wissen" eines im geheimen und mit nachrichtendienstlichen Mitteln arbeitenden Dienstes und zugleich den auch Zwang einschließenden Befugnissen der Vollzugspolizei. Dessen ungeachtet erlaubt der Entwurf einen umfassenden Datenaustausch zwischen Bundesamt für Verfassungsschutz und Polizeibehörden.

Auch das dem Bundesamt für Verfassungsschutz eingeräumte Recht, verfassungsschutzrechtliche Erkenntnisse an andere Behörden bereits dann weitergeben zu dürfen, wenn der Empfänger die Informationen "für Zwecke der öffentlichen Sicherheit" benötigt, geht zu weit. Damit gelangen Informationen, die mit den besonderen Befugnissen des Verfassungsschutzes beschafft wurden, in erheblichem Umfang zur Polizei. Der Zweckbindungsgrundsatz verlangt jedoch, daß Angaben, die der Verfassungsschutz für eigene Zwecke erhoben hat, allenfalls zur Verfolgung von Staatsschutzdelikten weitergeleitet werden dürfen. Ausnahmen von diesem Grundsatz - z.B. wenn klare Anhaltspunkte für eine schwere Straftat bestehen - müssen gesetzlich geregelt werden.

Die Übermittlungsregelungen des Bundesverfassungsschutzgesetzes sollen durch ein "Zusammenarbeitengesetz" (ZAG) ergänzt werden; dazu Ziff. 6.3.5.

6.3.4.3

Sicherheitsüberprüfungen

Der Verfassungsschutz wirkt bei der Überprüfung von Personen, die in sicherheitsempfindlichen Bereichen beschäftigt werden sollen, mit. Die Bedingungen für die Verarbeitung dieser Daten unterscheiden sich von der übrigen Tätigkeit der Behörde: Der Betroffene liefert weitgehend seine Daten selbst - einschließlich der Angaben über Angehörige. Er ist in der Regel über den Überprüfungsvorgang informiert, weiß z.B., daß Referenzpersonen, die er angegeben hat, angesprochen werden. Bei Sicherheitsüberprüfungen werden besonders viele und sensible Daten erfaßt. Die besonderen Umstände dieser Verarbeitung erlauben und erfordern eine genaue Festlegung des Umfangs der zu speichernden Daten, der zulässigen Datenübermittlungen und des Verfahrensablaufs. So viel Transparenz für den Betroffenen wie möglich ist zu gewähren. Daten, die im Zusammenhang mit der Sicherheitsüberprüfung bei dem Betroffenen oder anderen Stellen erhoben wurden, dürfen nur für die Sicherheitsüberprüfung verwendet werden. Soweit Ausnahmen davon notwendig erscheinen sollten, müssen sie sich ausdrücklich aus der gesetzlichen Regelung ergeben. (Zur Sicherheitsüberprüfung vgl. auch Ziff. 6.2).

6.3.4.4

Ausbau des nachrichtendienstlichen Informationssystems (NADIS)

Der geplante Entwurf soll die Rechtsgrundlage für das automatisierte nachrichtendienstliche Informationssystem (NADIS) schaffen. Ursprünglich wurde NADIS als bloßes Aktenhinweissystem eingerichtet und gerechtfertigt. Hinweissysteme belassen es grundsätzlich bei der Informationsverarbeitung in Akten, sie setzen den Zugriff auf die schriftliche Unterlage als notwendigen Schritt voraus. Der Entwurf legalisiert demgegenüber die schon teilweise praktizierte Aufnahme von Textzusätzen aus Akten der Verfassungsschutzbehörden in automatisierte Dateien. Akteninhalte werden dadurch verkürzt, aus ihrem Entstehungszusammenhang herausgenommen; die Gefahr einer Informationsverzerrung und einer Vervielfältigung von Fehlern nimmt zu. Die Ausweitung von Dateien mit Textzusätzen verändert die Qualität und Quantität der Informationstätigkeit, insbesondere den Umfang der Datenspeicherung und die Verknüpfungs- und Recherchemöglichkeiten. Das Potential für mögliche Gefährdungen des Rechts auf informationelle Selbstbestimmung steigt an. Aus diesen Gründen sollten gerade im sensiblen Bereich des Verfassungsschutzes Dateien mit Textzusätzen nicht zugelassen werden.

6.3.5

Vor-Entwurf eines "Gesetzes über die informationelle Zusammenarbeit der Sicherheits- und Strafverfolgungsbehörden des Bundes und der Länder in Angelegenheiten des Staats- und Verfassungsschutzes und nachrichtendienstlicher Tätigkeit" (Zusammenarbeitsgesetz - ZAG)

Während sich der Entwurf des Bundesverfassungsschutzgesetzes mit dem Datenaustausch zwischen dem Bundesamt für Verfassungsschutz und anderen Bundesstellen, ausländischen Stellen sowie privaten Adressaten beschäftigt, befaßt sich der Vorentwurf des Zusammenarbeitsgesetzes (ZAG) mit dem Datenaustausch zwischen Polizeibehörden und Strafverfolgungsbehörden einerseits und den Nachrichtendiensten andererseits sowie der Datenweitergabe der Nachrichtendienste untereinander.

Schon der Ansatzpunkt dieses Entwurfs verdient Kritik: Ausgehend von einer einheitlichen Aufgabe "Schutz der freiheitlichen demokratischen Grundordnung, des Bestandes und der Sicherheit des Bundes oder eines Landes und des Schutzes auswärtiger Belange der Bundesrepublik Deutschland" wird die Datenübermittlung zwischen Landes- und Bundesbehörden, Polizei und Nachrichtendiensten zum Selbstzweck. Der Grundsatz der Zweckbindung verlangt hingegen die Orientierung an der jeweiligen Aufgabe der Behörde und dem unmittelbaren Verwendungszusammenhang der Daten. Die Konzeption des ZAG widerspricht zudem dem Gebot der Trennung auch der informationellen Aktivitäten von Polizei und Nachrichtendiensten. Die unterschiedlichen Befugnisse - bei der Polizei ausgerichtet an der konkreten Straftat und unter Einschluß von Zwangsmitteln, bei den Nachrichtendiensten "nachrichtendienstliche Mittel" zur Aufklärung von Sachverhalten auch im Vorfeld von Straftaten, aber ohne die Möglichkeit des Einsatzes von Zwangsmitteln - läßt eine Vermengung der Datenverarbeitung beider Bereiche nicht zu. Das ZAG setzt aber punktuell die Polizei als Erhebungshelfer der Nachrichtendienste ein. "Zufallsfunde", die für die eigentliche polizeiliche Arbeit keine Bedeutung haben, sollen an die Nachrichtendienste weitergeleitet werden. Damit wird gegen den datenschutzrechtlichen Grundsatz verstoßen, daß allenfalls eine Übermittlung solcher Daten in Betracht kommt, die schon für die Aufgaben der weitergebenden Stelle gespeichert werden durften.

Denkbar sind allenfalls Datenübermittlungen zwischen den beteiligten Behörden aufgrund von spezifischen, ihre jeweilige Tätigkeit regelnden gesetzlichen Bestimmungen unter Berücksichtigung des Verhältnismäßigkeitsgrundsatzes.

6.3.6

Vorgaben für Hessen

Meine Kritik an den vorliegenden Entwürfen für ein Bundesverfassungsschutzgesetz und ein Zusammenarbeitsgesetz erhält zusätzliche Bedeutung dadurch, daß die Vorschläge, sollten sie Gesetzeskraft erhalten, die Arbeit des hessischen Gesetzgebers an einem Verfassungsschutzgesetz präjudizieren. Mache der Bund in der geplanten Weise von seiner Gesetzgebungskompetenz Gebrauch, so hätte der hessische Gesetzgeber nach der Kompetenz-Regelung des Grundgesetzes seine Vorgaben zu beachten: Eindeutig gebunden wäre der Landesgesetzgeber durch jene Regelungen des Entwurfs, die hessische Behörden in die verschiedenen Übermittlungskonstellationen einbeziehen. Einschränkungen für den hessischen Gesetzgeber ergeben sich aber auch aus Bestimmungen, die die Zusammenarbeit des Bundes mit den Ländern bzw. der Länder untereinander betreffen. In gewissem Maße gilt dies auch für die Beschreibung der Aufgaben des Bundesamtes für Verfassungsschutz; denn die in den Entwürfen vorgesehene Verpflichtung zur Zusammenarbeit zwischen Bundes- und Landesbehörden setzt die Festlegung - zumindest eines Mindestmaßes - an gemeinsamen Aufgaben voraus.

7. Ausländerzentralregister

Im Ausländerzentralregister (AZR), das vom Bundesverwaltungsamt in Köln geführt wird, sind Daten über Ausländer gespeichert, die sich im Bundesgebiet nicht nur vorübergehend aufhalten oder einen anderen Bezug zur Bundesrepublik Deutschland haben. Übermittelt werden diese Daten vorwiegend von den Ausländerbehörden der Länder. Gegenwärtig sind weit über 100 Millionen Daten von etwa 10 Millionen Ausländern gespeichert, die sich im Bundesgebiet aufhalten oder aufgehalten haben.

7.1

Überlegungen zur Neukonzeption

Nicht nur der große Umfang der beim Ausländerzentralregister gespeicherten Datenmenge, sondern auch der Wunsch, die Nutzungsmöglichkeiten des Registers zu verbessern, gaben Anlaß, beim Bundesminister des Innern eine Arbeitsgruppe einzurichten, die das Register mit dem Ziel einer Effizienzsteigerung überprüft hat. Die

Arbeitsgruppe, in der auch der Bundesbeauftragte für den Datenschutz beratend mitwirkte, hat 1986 einen umfassenden Bericht über die Neukonzeption des AZR vorgelegt, der als Grundlage für eine gesetzliche Regelung der Speicherung und Nutzung von Daten des AZR dienen soll. Im Rahmen einer Arbeitsgruppe der Datenschutzbeauftragten des Bundes und der Länder habe ich mich eingehend mit dem Register befaßt.

7.2

Bewertung

Von entscheidender Bedeutung für die datenschutzrechtliche Bewertung sind die Funktionen, die das Register erfüllen soll.

7.2.1

Indexregister

Problemlos ist die Verwendung des Registers als Indexregister zur Feststellung, ob eine - und wenn ja, welche - Ausländerbehörde Unterlagen über einen bestimmten Ausländer besitzt. Damit erleichtert das Register den Zugang zu den eigentlichen, bei Ausländer- und Meldebehörden gespeicherten Daten. Es ersetzt nicht den Rückgriff auf die bei den örtlichen Dienststellen gesammelten Informationen.

7.2.2

Datenverwendung

7.2.2.1

Novellierung des Ausländergesetzes, der Strafprozeßordnung und der Polizeigesetze

Schwieriger ist dagegen die Frage, in welchem Umfang die vorgesehene Datenverwendung gesetzlich geregelt werden soll. Wenn die Hauptfunktion des Registers nach der Novellierung die Unterstützung der Tätigkeit der Ausländerbehörden und der Polizei ist, so muß der Gesetzgeber diesen größeren Verwendungszusammenhang aufgreifen. Deswegen ist es folgerichtig, daß nicht nur die Verwendung der Daten im Register, sondern auch ihre Übermittlung an das Register und Weitergabe an andere Dienststellen in die gesetzliche Regelung aufgenommen werden. Nur auf diese Weise ist gewährleistet, daß die Betroffenen klar und eindeutig erkennen können, in welchem Umfang in ihr Recht auf informationelle Selbstbestimmung eingegriffen wird. Konkret bedeutet dies: Ein Registergesetz allein genügt solchen Anforderungen nicht. Die zeitlich parallele Novellierung des Ausländergesetzes ist unabdingbar. Gleichzeitig muß außerdem der Datenaustausch zu Fahndungszwecken und zur Erfüllung anderer polizeilicher Aufgaben in der Strafprozeßordnung und in den Polizeigesetzen des Bundes und der Länder geregelt werden.

7.2.2.2

Datensatz

Wie auch bei anderen Registergesetzen ist vorgesehen, den zu speichernden Datensatz ausdrücklich festzulegen. Natürlich hängen Umfang und Inhalt des Datensatzes davon ab, welche Funktionen das Register zu erfüllen hat. Es ist deshalb folgerichtig, daß Anschriften der betroffenen Ausländer nicht gespeichert werden sollen; diese hat nur die örtliche Ausländerbehörde, ebenso wie zusätzliche, nicht in das Raster des Zentralregisters passende Daten. Damit ist jede anfragende Behörde gehalten, für ihre Entscheidungen in Kontakt mit der zuständigen Ausländerbehörde zu treten. Nur auf diese Weise kann eine umfassende, alle Aspekte des konkreten Falls einbeziehende, Entscheidung getroffen werden.

7.2.2.3

Nutzungsbeschränkungen

Allerdings ist unverkennbar, daß verschiedene Benutzer Daten aus dem AZR für konkrete Entscheidungen gegenüber dem Betroffenen nutzen wollen. Da in diesen Fällen nur ein Ausschnitt aus den gesamten, den Ausländerbehörden zur Verfügung stehenden Daten genutzt wird, ist dieses Verfahren nicht unproblematisch. Bedenken ergeben sich insbesondere dann, wenn das Datum selbst einer Wertung entspringt. Dies gilt insbesondere für das Merkmal "Einreisebedenken". Unter diesem Datum werden belastende Vorgänge im Umfeld des Ausländers erfaßt, die noch keine ausländerrechtlichen Maßnahmen ausgelöst haben. Konkret handelt es sich dabei um im Einzelfall oft unpräzise Angaben über ein vermutetes (Fehl-) Verhalten des Ausländers selbst. Als Beispiel für solche Bedenken werden genannt: "Stellung von offensichtlich unbegründeten oder unbeachtlichen Asylanträgen", "Einreise in das Bundesgebiet mit dem Ziel der Inanspruchnahme sozialer Leistungen", "alle Sachverhalte, die in den im § 10 des Ausländergesetzes beschriebenen Ausweisungsgründen enthalten sind", ohne daß bei diesen sehr vagen Formulierungen jeweils der Einzelfall geprüft wird, oder "ein nicht unerheblicher Verstoß

gegen die öffentliche Sicherheit oder Ordnung". Ohne Zweifel sind mit diesem Datum oberflächliche Einschätzungen und Bewertungen verbunden, die im Einzelfall jeweils der weiteren Überprüfung bedürfen, um eine rechtsstaatlich haltbare Entscheidung treffen zu können. Aufgrund dieses Datenfeldes dürfen deshalb ohne Hinzuziehen der Akten und damit der Prüfung des Gesamtsachverhalts nur für den Ausländer positive Entscheidungen getroffen werden.

Ebenso problematisch ist die geplante Aufnahme von Daten aus dem INPOL-Fahndungsbestand in das AZR. Ziel dieser Aufnahme ist es, die mit dem Datensatz des einzelnen Ausländers befaßten Ausländerbehörden vor Erteilung oder Verlängerung einer Aufenthaltserlaubnis zur Prüfung zu veranlassen, ob nach dem Ausländer gefahndet wird. Die polizeilichen Daten werden damit unmittelbar mit den Daten der Ausländerüberwachung verknüpft. Eine solche Verknüpfung ist problematisch, da sie nicht die unterschiedlichen Zweckbestimmungen beider Bereiche berücksichtigt. Die Notwendigkeit dieser Maßnahme ist angesichts möglicher Alternativen, z.B. eines regelmäßigen Datenabgleichs beider Datenbestände, bisher nicht ausreichend dargelegt worden.

7.2.2.4

Übermittlungsvorschriften

Nach dem Bericht der Arbeitsgruppe beim Bundesinnenminister soll eine Vielzahl von Behörden Auskünfte aus dem Ausländerzentralregister erhalten. Neben den Ausländerbehörden, den Grenzpolizeibehörden und den verschiedenen mit dem Flüchtlingsasyl befaßten Behörden zählen dazu Polizeibehörden, das Zollkriminalinstitut und die Bundesanstalt für Arbeit. Aber auch Staatsanwaltschaften und ganz allgemein sonstige Behörden und öffentliche Stellen sind anfrageberechtigt. Daneben kommen noch eine Reihe von privaten Institutionen wie das Deutsche Rote Kreuz oder der Internationale Suchdienst sowie ausländische diplomatische und konsularische Missionen als Datenempfänger in Frage. Die enger mit Ausländerfragen befaßten Behörden sowie die Polizeibehörden und die Bundesanstalt für Arbeit sollen überdies einen automatisierten Zugriff auf die Daten erhalten. Der Bericht sieht lediglich vor, daß diese Empfänger Daten erhalten sollen und legt die technische Form der Übermittlung fest. Die gesetzliche Regelung wäre jedoch nicht ausreichend, solange nicht präzise festgelegt wird, für welche konkreten Zwecke die Behörden Daten abrufen dürfen bzw. das Ausländerzentralregister an sie übermitteln darf. Nur eine solche Regelung macht den Verwendungszusammenhang transparent und würde den Anforderungen des Bundesverfassungsgerichts genügen. In keinem Fall reicht es aus, wenn gesetzlich allein festgelegt wird, daß die Behörden die gewünschte Information bekommen können, sofern sie sie "zu ihrer Aufgabenerfüllung benötigen".

8. Statistik

8.1

Landesstatistikgesetz

8.1.1

Bedeutung

Nachdem der Landtag in Reaktion auf meinen 13. und 14. Tätigkeitsbericht zweimal die Landesregierung einstimmig aufgefordert hat, ihm einen Entwurf eines Landesstatistikgesetzes vorzulegen (vgl. Nr. 4 der Beschlußempfehlung des Innenausschusses, Drucks. 11/4696 i.V.m. Protokoll der 63. Plenarsitzung vom 14. November 1985, S. 3615 und Nr. 8 der Beschlußempfehlung des Innenausschusses, Drucks. 11/6231 i.V.m. Protokoll der 84. Plenarsitzung vom 19. Juni 1986, S. 4979), hat die Landesregierung nunmehr am 24. Dezember 1986 dem Landtag den Entwurf für ein Gesetz über die Statistik im Land Hessen (Hessisches Landesstatistikgesetz - HessLStatG-) zugeleitet (Drucks. 11/7087). Einen Vorentwurf hatte mir die Landesregierung Ende September 1986 zur Stellungnahme übersandt.

In meiner Stellungnahme habe ich nochmals nachdrücklich auf die Bedeutung des Landesstatistikgesetzes hingewiesen: Das Landesstatistikgesetz ist die für den Landes- und Kommunalstatistikbereich notwendige bereichsspezifische Ergänzung des gerade verabschiedeten neuen Hessischen Datenschutzgesetzes. Mit dem neuen HDSG hat der Landtag als erster die allgemeinen Datenschutzvorschriften den Anforderungen aus dem Volkszählungsurteil des Bundesverfassungsgerichts angepaßt und damit - wie auch zuvor schon - entscheidende Weichenstellungen für die Entwicklung des Datenschutzes vorgenommen. Das Landesstatistikgesetz bietet angesichts der Situation in den anderen Bundesländern die Chance, die Bemühungen des Landes Hessen um eine Pionierrolle im Datenschutz konsequent fortzusetzen.

8.1.2.

Regelungsinhalt

Das Gesetz soll sowohl die allgemeinen materiell-rechtlichen Bedingungen, wie etwa das Statistikgeheimnis, als auch Organisation und Verfahren der Landes- und Kommunalstatistik sowie, ergänzend zum Bundesstatistikgesetz, die in der Regel dem Land obliegende Durchführung von Bundes- und EG-Statistiken regeln.

Zwei bereits bestehende Einrichtungen werden im Landesstatistikgesetz endlich eine gesetzliche Basis erhalten: Erstmals soll die Tätigkeit des Statistischen Landesamtes, das gegenwärtig auf Grund der Organisationsverordnung Nr. 15 des Office of Military Government for Greater Hesse vom 14. Januar 1946 und der Anordnung der Landesregierung über die zuständige Behörde für Bundesstatistiken vom 1. April 1977 (GVBl I S. 157) agiert, gesetzlich geregelt werden. Außerdem ist beabsichtigt, den Statistischen Koordinierungsausschuß, ein Beratungsgremium für die amtliche Statistik in Hessen, in dem unter anderem die obersten Landesbehörden, die kommunalen Spitzenverbände und der Hessische Datenschutzbeauftragte vertreten sind, gesetzlich zu institutionalisieren.

Ein großer Teil der Vorschriften des Entwurfs der Landesregierung entspricht, häufig wortgleich, den Bestimmungen des am 4. Dezember 1986 vom Bundestag verabschiedeten und am 30. Januar 1987 in Kraft getretenen neuen Bundesstatistikgesetzes (BGBl. I 1987 S. 462). Übernommen wurden beispielsweise die Regelung über Erhebungsbeauftragte, der Gesetzesvorbehalt für Landesstatistiken und entsprechend der Satzungs Vorbehalt für Kommunalstatistiken sowie die Regelungsvorgaben für landes- und kommunalstatistische Rechtsvorschriften, die Vorschrift zur Nutzung allgemein zugänglicher Quellen für Landesstatistiken und die Bestimmungen zum Schutz vor Deanonymisierung statistischer Angaben. Übereinstimmungen mit dem Bundesstatistikgesetz gibt es zum Teil bei der Ermächtigung der Landesregierung zur Anordnung von Statistiken mit Auskunftspflicht und zur Änderung von Statistiken, den Vorschriften über Hilfs- und Erhebungsmerkmale oder den Regelungen zur Übermittlung statistischer Einzelangaben vom Statistischen Landesamt an Dritte.

8.1.3

Auskunftspflicht

Nach dem Entwurf dürfen Landesstatistiken grundsätzlich nur mit freiwilliger Beteiligung der Befragten durchgeführt werden. Lediglich ausnahmsweise, wenn Geeignetheit und Erforderlichkeit zuvor festgestellt worden sind, können in einem Gesetz, das eine Landesstatistik anordnet, die Bürger zur Auskunft verpflichtet werden.

Angesichts der Tatsache, daß gegenwärtig von den wenigen Landesstatistiken keine einzige mit Auskunftspflicht durchgeführt wird, sollte dem Gesetzgeber die Entscheidung für dieses Regel-Ausnahmeverhältnis nicht allzu schwer fallen. Er würde damit die Konsequenz ziehen aus der in der Diskussion um Volkszählungs- und Mikrozensusgesetz gewonnenen Erkenntnis, daß nicht staatlicher Zwang der wirksamste Garant der Funktionsfähigkeit der amtlichen Statistik ist, sondern die Kooperationsbereitschaft der Befragten und diese sich am ehesten bei einer auf der Basis freiwilliger Beteiligung der Befragten durchgeführten Datenerhebung gewinnen läßt. Das beabsichtigte Regelungsverhältnis entspricht auch der vom Bundesverfassungsgericht im Volkszählungsurteil (BVerfGE 65, 55) aus dem Verhältnismäßigkeitsprinzip abgeleiteten Forderung, wonach der Gesetzgeber für jede Einzelstatistik kontinuierlich und unter Berücksichtigung des jeweiligen Standes der Methodendiskussion die Methoden der Informationserhebung und -verarbeitung und damit auch die Geeignetheit und Erforderlichkeit der Auskunftspflicht zu prüfen hat. Anders als noch die Bundesregierung in ihrem Bundesstatistikgesetzentwurf vom 17. April 1986 hat dies inzwischen auch der Bundestag anerkannt und in dem am 4. Dezember 1986 verabschiedeten neuen Bundesstatistikgesetz in § 15 Abs. 1 bestimmt, daß die eine Bundesstatistik anordnende Rechtsvorschrift festzulegen hat, ob und in welchem Umfang die Erhebung mit oder ohne Auskunftspflicht erfolgen soll.

Die Forderung des Bundesverfassungsgerichts hat außerdem zur Folge, daß der parlamentarische Gesetzgeber bedenkenfrei nur solche Kommunalstatistiken der Satzungsgewalt der Kommunen überlassen kann, die auf freiwilliger Basis durchgeführt werden. Die Gemeindevertretung müßte - wie der Parlamentsgesetzgeber - unter Berücksichtigung des Standes der Methodendiskussion für die jeweilige eigene Datenerhebung die Notwendigkeit der Auskunftspflicht feststellen. Dies setzt jedoch eine gründliche Kenntnis der Methoden der Statistik und der empirischen Sozialforschung voraus, die in der Regel auf kommunaler Ebene nicht vorhanden sein dürfte. Auch aus rechtlichen Gründen und nicht nur aus den in der Begründung zum Vorentwurf angeführten Akzeptanzgründen empfiehlt sich daher die im Vorentwurf vorgesehene Regelung, die den Gemeinden die Durchführung eigener Erhebungen nur auf der Grundlage einer freiwilligen Beteiligung der Befragten erlaubt.

8.1.4

Kommunalstatistik

Über die Notwendigkeit einer landesgesetzlichen Regelung der Kommunalstatistik kann es spätestens seit dem Volkszählungsurteil des Bundesverfassungsgerichts keinen Zweifel mehr geben (vgl. BVerfGE 65, 68 f). Folgerichtig enthält daher der Entwurf spezifische Vorschriften zu diesem Bereich.

Positiv hervorzuheben ist zunächst, daß Kommunalstatistiken durch gemeindliche Satzung geregelt werden müssen und der Regelungsinhalt der Satzung die gleichen Anforderungen zu erfüllen hat wie Gesetze, die Landesstatistiken anordnen.

Dagegen hat die Landesregierung das im Vorentwurf enthaltene und von mir begrüßte Verbot der Auskunftspflicht bei Kommunalstatistiken (vgl. hierzu oben Ziff. 8.1.3) in dem dem Landtag zugeleiteten Entwurf nicht mehr vorgesehen.

Sollte sich der Gesetzgeber für ein Verbot der Auskunftspflicht entscheiden, bestehen Bedenken gegen die bereits im Vorentwurf enthaltene Übermittlungsregelung, die den Verwaltungsstellen erlaubt, unregelmäßig oder regelmäßig Einzelangaben an die Statistikstelle der Gemeinden weiterzugeben. Die Vorschrift würde die Umgehung des Verbots der Auskunftspflicht für Kommunalstatistiken ermöglichen. Soweit keine spezialgesetzlichen Übermittlungsverbote bestehen, könnten auch solche Daten weitergegeben werden, die die Verwaltungsstellen im Wege der Auskunftspflicht oder eines faktischen Auskunftszwanges (weil z.B. bei Verweigerung der Auskunft bestimmte Leistungen vorenthalten werden) erlangt haben.

Es fragt sich, ob bei dieser Übermittlungsvorschrift für die Gemeinden überhaupt noch die Notwendigkeit besteht, eigene statistische Primärerhebungen durchzuführen, denn der Statistikbedarf der Gemeinden dürfte weitgehend mit aus Verwaltungsdaten erstellten Statistiken zu decken sein. Zwar ist es rechtlich grundsätzlich möglich, daß die Gemeinde Sekundärstatistiken durch die Statistikstelle erstellen läßt (vgl. aber die kritischen Anmerkungen des Bundesverfassungsgerichts zur Übernahme von Daten aus verschiedenen bereits vorhandenen Dateien der Verwaltung, BVerfGE 65, 56 f.). Dies kann jedoch nicht auf der Grundlage einer pauschalen Ermächtigung geschehen, wie sie der Entwurf vorsieht, sondern erfordert eine einzelgesetzliche Regelung.

8.1.5

Übermittlung statistischer Einzelangaben

8.1.5.1

Übermittlung zu wissenschaftlichen Zwecken

Der Vorentwurf der Landesregierung, der mir zur Stellungnahme vorlag, sah eine unnötig restriktive Regelung der Weitergabe statistischer Einzelangaben zu wissenschaftlichen Zwecken vor. Er gestattete die Übermittlung von lediglich faktisch anonymisierten, d.h. nicht vollständig anonymisierten, statistischen Einzelangaben nur an Amtsträger oder für den öffentlichen Dienst besonders Verpflichtete in Hochschulen und sonstigen Einrichtungen mit der Aufgabe unabhängiger wissenschaftlicher Forschung. Faktisch anonymisiert sind statistische Einzelangaben, wenn sie nur mit unverhältnismäßig hohem Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten Person zugeordnet werden können. Durch die Anknüpfung an den Status des Amtsträgers oder des für den öffentlichen Dienst besonders Verpflichteten werden jedoch Forscher privatrechtlich organisierter Forschungseinrichtungen von dem Übermittlungsprivileg ausgeschlossen. Der Vorentwurf folgte hier fast wortgleich der Regelung des § 16 Abs. 4 Bundesstatistikgesetzentwurf. Bereits in meiner Stellungnahme im Rahmen der vom Bundestagsinnenausschuß am 8. September 1986 zum Bundesstatistikgesetzentwurf der Bundesregierung durchgeführten Anhörung habe ich darauf hingewiesen, daß ich diese Einschränkung aus datenschutzrechtlicher Sicht nicht für erforderlich halte (Protokoll der 124. Sitzung des Innenausschusses).

Eine Einschränkung, wie sie im Vorentwurf vorgesehen war, läßt die Forschungsorganisation in der Bundesrepublik unberücksichtigt. Gerade auf den Gebieten der Wirtschaftsforschung und der empirischen Sozialforschung mit einem besonders hohen Bedarf an statistischen Einzelangaben sind bedeutende Forschungseinrichtungen - obgleich öffentlich gefördert - oft privatrechtlich organisiert. Beispielhaft seien hier nur erwähnt das Deutsche Institut für Wirtschaftsforschung in Berlin, die Institute der Max-Planck-Gesellschaft oder das Wissenschaftszentrum Berlin. Auch das landeseigene Institut Wohnen und Umwelt GmbH in Darmstadt hätte nach der geplanten Regelung, entgegen der in der Begründung des Vorentwurfs vertretenen Ansicht, keine faktisch anonymisierten Einzeldatensätze erhalten dürfen, denn die Voraussetzungen "Amtsträger und für den öffentlichen Dienst besonderes Verpflichtete" sowie "in Hochschulen und sonstigen Einrichtungen" mußten nach dem Vorentwurf kumulativ erfüllt sein.

Zweifellos ist es notwendig, im Hinblick auf das verbleibende Deanonymisierungsrisiko bei faktisch anonymisierten Einzelangaben die privilegierte Übermittlung auf Personen zu beschränken, die in Einrichtungen mit der Aufgabe unabhängiger wissenschaftlicher Forschung tätig sind. Die mit der Beschränkung auf Amtsträger und für den öffentlichen Dienst besonders verpflichtete Personen beabsichtigte Sicherung läßt sich jedoch auch bei Übermittlungen an Forscher in privatrechtlich organisierten Einrichtungen erzielen: In der Erläuterung zum Entwurf wurde die Beschränkung mit dem Geltungsbereich der Strafvorschriften des § 203 Strafgesetzbuch begründet. Sicherlich ist es erforderlich, daß alle Empfänger bei Mißbrauch der nicht vollständig anonymisierten Daten dieselben Sanktionen zu befürchten haben. Dies läßt sich aber durch Aufnahme einer eigenständigen Strafvorschrift in das Landesstatistikgesetz auch für Forscher in privatrechtlich organisierten Einrichtungen erreichen. Empfänger, die an privatrechtlich organisierten unabhängigen wissenschaftlichen Forschungseinrichtungen tätig sind, müssen allerdings nicht nur die zweckgebundene Verwendung der übermittelten Daten garantieren, sondern die Übermittlung sollte auch davon abhängig gemacht werden, daß sich der Empfänger der Kontrolle des Hessischen Datenschutzbeauftragten unterwirft. Dies sieht im übrigen § 33 Abs. 4 des neuen Hessischen Datenschutzgesetzes als Zulässigkeitsvoraussetzung für Übermittlungen zu Forschungszwecken an Empfänger, die nicht der Kontrolle des Hessischen Datenschutzbeauftragten unterliegen, vor.

Nachdem sich der Bundestag den gegen § 16 Abs. 4 des Bundesstatistikgesetzentwurfs der Bundesregierung geäußerten Einwänden angeschlossen hat und in § 16 Abs. 6 und 7 des neuen Bundesstatistikgesetzes eine Regelung vorgesehen hat, die auch die Übermittlung statistischer Einzelangaben an Forscher in privatrechtlich organisierten unabhängigen Forschungseinrichtungen zuläßt, ist auch die Landesregierung von ihrer restriktiven Haltung abgerückt (vgl. § 16 Abs. 3 und 4 HessLStatGE).

8.1.5.2

Übermittlung an Gemeinden und Oberste Landesbehörden

Nach dem Entwurf der Landesregierung soll das Statistische Landesamt die pauschale Befugnis erhalten, statistische Einzelangaben an die Gemeinden und Landkreise für deren eigene statistische Aufbereitung zu übermitteln. Außerdem wird dem Statistischen Landesamt ebenfalls pauschal die Übermittlung von statistischen Einzelangaben an die für Landesplanung zuständige oberste Landesbehörde zu planerischen Zwecken gestattet. Gegen beide Übermittlungsvorschriften bestehen erhebliche Bedenken.

Die erstgenannte Regelung entspricht teilweise dem vom Bundesrat zum Bundesstatistikgesetzentwurf der Bundesregierung vorgeschlagenen § 16a, der von der Bundesregierung in ihrer Gegenäußerung wegen Unvereinbarkeit mit den im Volkszählungsurteil des Bundesverfassungsgerichts gestellten Anforderungen an die Gewährleistung des Statistikgeheimnisses abgelehnt worden ist (Bundestags-Drucks. 10/5345, S. 26 und 29 f.). Mit der zweiten Vorschrift geht der Entwurf noch über den vom Bundesrat zum Bundesstatistikgesetzentwurf vorgeschlagenen § 16a hinaus, der seinerseits bereits großzügigere Übermittlungsmöglichkeiten als das alte Bundesstatistikgesetz vorsieht.

Grundsätzlich sind Übermittlungen statistischer Einzelangaben vom Statistischen Landesamt an die Gemeinden oder obersten Landesbehörden zu statistischen Zwecken datenschutzrechtlich nicht ausgeschlossen (vgl. BVerfGE 65, 61). Als Rechtsgrundlage genügt allerdings nicht eine derart pauschale Befugnisnorm, wie sie der Entwurf vorsieht. Zur Gewährleistung des Statistikgeheimnisses ist nicht nur die strikte Trennung von Statistik und Verwaltungsvollzug erforderlich, sondern auch, daß grundsätzlich nur das Statistische Landesamt Zugang zu nicht anonymisierten Einzelangaben aus Landesstatistiken hat. Das entspricht dem einfachen Erfahrungssatz, wonach die Mißbrauchsgefahr um so geringer ist, je weniger Stellen die Einzelangaben kennen. Eine Übermittlung statistischer Einzelangaben an Gemeinden und Landkreise sowie oberste Landesbehörden kommt daher nur ausnahmsweise in Betracht und bedarf einer spezialgesetzlichen Regelung in der die Einzelstatistik anordnenden Rechtsvorschrift. Folgerichtig sieht daher das Volkszählungsgesetz 1987 in § 14 Abs. 1 eine detaillierte und eng begrenzte Vorschrift zur Übermittlung statistischer Einzelangaben aus der Volkszählung an Gemeinden und Gemeindeverbände vor.

Dieser Ansicht war offensichtlich auch der Bundestag. Zwar hat er nicht die gleiche ablehnende Haltung wie die Bundesregierung gegenüber dem Bundesratsvorschlag eingenommen und in dem am 4. Dezember 1986 verabschiedeten neuen Bundesstatistikgesetz die Übermittlung von Einzelangaben an die statistischen Ämter der Gemeinden und Gemeindeverbände gestattet, dies aber von der Bedingung abhängig gemacht, daß die Übermittlung in einem eine Bundesstatistik anordnenden Gesetz vorgesehen ist sowie Art und Umfang der zu übermittelnden Einzelangaben bestimmt sind (§ 16 Abs. 5).

Gegen die Vorschrift, wonach an die für Landesplanung zuständige oberste Landesbehörde Einzelangaben übermittelt werden dürfen, bestehen noch zusätzliche Bedenken: Werden der Landesbehörde vom Statistischen Landesamt nicht-anonymisierte Einzelangaben zu Planungszwecken übermittelt, so bedeutet das eine Durchbrechung des Grundsatzes der Zweckbindung, wonach zu statistischen Zwecken erhobene Daten grundsätzlich nur für statistische Zwecke verwendet werden dürfen. Das Bundesverfassungsgericht hat im Volkszählungsurteil offengelassen, ob statistische Einzelangaben aufgrund einer ausdrücklichen gesetzlichen Regelung zu anderen Zwecken verwendet werden dürfen, allerdings Bedenken insbesondere hinsichtlich der Verwendung statistischer Einzelangaben zu Verwaltungsvollzugszwecken anklingen lassen (BVerfGE 65, 61). Das Gericht hat jedoch ausdrücklich § 9 Abs. 3 Volkszählungsgesetz 1983, der die Übermittlung statistischer Einzelangaben an Gemeinden und Gemeindeverbände für Zwecke der Regionalplanung, des Vermessungswesens, der gemeindlichen Planung und des Umweltschutzes gestattete, für verfassungswidrig erklärt (BVerfGE 65, 66 ff). Unter diesen Voraussetzungen ist die im Entwurf vorgeschlagene Befugnis zur Übermittlung von statistischen Einzelangaben zu Planungszwecken mit einem weiteren verfassungsrechtlichen Risiko behaftet. Auf beide Übermittlungsvorschriften sollte verzichtet werden.

8.2

Volkszählung 1987

Mit dem Näherrücken des Volkszählungstermins, Zählungstichtag ist der 25. Mai 1987, sind auch die Vorbereitungsarbeiten in ihre letzte Phase gegangen. Der Bundesgesetzgeber hat mit dem Gesetz über eine Volks-, Berufs-, Gebäude-, Wohnungs- und Arbeitsstättenzählung (Volkszählungsgesetz 1987), das am 15. November 1985 in Kraft getreten ist (BGBl. I S. 2078), die vom Bundesverfassungsgericht im Volkszählungsurteil an eine solche Totalerhebung gestellten Anforderungen erfüllt (vgl. hierzu Ziff. 5.3.1 meines 14. Tätigkeitsberichts). Dagegen hat der Landesgesetzgeber seinen Regelungsauftrag aus dem Volkszählungsgesetz 1987 derzeit noch nicht erledigt, denn ohne ein Landesstatistikgesetz sind Übermittlungen von Einzelangaben aus der Volkszählung an die Gemeinden unzulässig. Das Volkszählungsgesetz 1987 hat allerdings auch die Landesregierung vor eine Reihe von Regelungsaufgaben gestellt.

8.2.1

Ausführungsverordnung zu § 9 Abs. 3 Volkszählungsgesetz 1987

Eine dieser Regelungsaufgaben bestand in der Bestimmung der Erhebungsstellen und der Festlegung der konkreten Anforderungen an die räumliche, organisatorische und personelle Abschottung dieser Stellen von anderen Verwaltungsstellen. Die Landesregierung hat hierzu am 26. Juni 1986 die Hessische Ausführungsverordnung zu § 9 Abs. 3 des Volkszählungsgesetzes 1987 über die Erhebungsstellen und deren Aufgaben erlassen, die am 15. Juli 1986 in Kraft getreten ist (GVBl. I S. 229).

8.2.1.1

Erhebungsstellen

In der Verordnung wird das Hessische Statistische Landesamt zur obersten Erhebungsstelle des Landes bestimmt und ermächtigt, den örtlichen Erhebungsstellen die technischen und organisatorischen Anweisungen zu erteilen. Die örtliche Durchführung der Volkszählung 1987 erfolgt grundsätzlich durch die Gemeinden, die zu diesem Zweck Erhebungsstellen einzurichten haben. Eine Ausnahmeregelung besteht lediglich für kleine Gemeinden: Das Volkszählungsgesetz läßt den Ländern die Wahl, die Aufgaben der Erhebungsstellen auch Gemeindeverbänden zu übertragen. Von dieser Möglichkeit hat die Landesregierung Gebrauch gemacht und den Landkreisen die Durchführung der Volkszählung in Gemeinden mit weniger als 3.000 Einwohnern übertragen. Damit ist sie meinem Vorschlag gefolgt, angesichts der knappen personellen und räumlichen Ressourcen und der beschränkten organisatorischen Möglichkeiten der kleinen Gemeinden zur Gewährleistung der vom Volkszählungsgesetz geforderten Trennung der Erhebungsstellen von anderen Verwaltungsstellen, für diese Gemeinden grundsätzlich die Errichtung der örtlichen Erhebungsstellen bei den Landkreisen anzuordnen. Nur wenn sie der Kommunalaufsichtsbehörde nachweisen können, daß die Trennung gewährleistet ist, erlaubt die Verordnung Gemeinden mit weniger als 3.000 Einwohnern die örtliche Durchführung der Volkszählung. Von den 42 betroffenen Gemeinden beabsichtigen nach den Ermittlungen des Statistischen Landesamtes zumindest 18 die Erhebung selbst durchzuführen, während 20 Gemeinden die örtliche Zählungsdurchführung den Landkreisen überlassen wollen (Stand: 29. Oktober 1986).

8.2.1.2

Personal der örtlichen Erhebungsstellen

Von entscheidender Bedeutung für die Gewährleistung des Trennungsgebots und die Sicherung der statistischen Geheimhaltung sind die Auswahlkriterien und Verhaltenspflichten für die in den Erhebungsstellen tätigen Personen. Einige Vorgaben enthält bereits das Volkszählungsgesetz 1987. Es verbietet den Bediensteten der Erhebungs-

stelle, die aus ihrer Tätigkeit gewonnenen Erkenntnisse über Auskunftspflichtige in anderen Verfahren oder für andere Zwecke zu verwenden und verlangt außerdem, daß die in den Erhebungsstellen tätigen Personen auf die Wahrung des strafrechtlich gesicherten Statistikgeheimnisses und zur Verschwiegenheit verpflichtet werden (§ 9 Abs. 2). Die Ausführungsverordnung wiederholt dies und ordnet ergänzend an, daß Bedienstete der Erhebungsstelle die Gewähr für Zuverlässigkeit und Verschwiegenheit bieten müssen und während des Zeitraums, in dem sie der Erhebungsstelle zugeteilt sind, keine anderen Aufgaben des Verwaltungsvollzugs wahrnehmen dürfen.

Mit Verwertungsverbot, Statistikgeheimnis, Zuverlässigkeitsgewähr und Tätigkeitsbeschränkung sind zweifelsohne wichtige Sicherungen vorhanden. Zu berücksichtigen ist jedoch, daß die sensibelste Phase der Volkszählung die Datenerhebung ist. In den Erhebungsstellen werden die ausgefüllten Erhebungsbogen personenbezogen gesammelt und auf Vollständigkeit und Vollzähligkeit überprüft, bevor sie an das Statistische Landesamt weitergegeben werden. Wegen der Nähe zum Auskunftspflichtigen ist in den örtlichen Erhebungsstellen am ehesten mit Zusatzwissen über den Befragten zu rechnen. Die Bediensteten in den Erhebungsstellen üben zum Teil auch Zählertätigkeiten aus, da die Auskunftspflichtigen die Erhebungsbogen unmittelbar bei der Erhebungsstelle abgeben und dorthin übersenden können. Besonders aus Akzeptanzgründen hätte deshalb die Landesregierung meine Forderung, entsprechend der im Volkszählungsgesetz für Zähler getroffenen Regelung, solche Personen von der Tätigkeit in der Erhebungsstelle auszuschließen, bei denen die Gefahr einer Interessenkollision besteht, aufgreifen müssen. Die Gefahr dürfte insbesondere für Personen aus den Ordnungs-, Steuer-, Sozial- und Einwohnermeldeämtern in Betracht kommen.

Die Landesregierung kann sich auch nicht darauf berufen, die Ablehnung meiner Forderung sei in Übereinstimmung mit den anderen Bundesländern erfolgt - im Gegenteil: Die Berliner Ausführungsvorschriften zum Volkszählungsgesetz 1987 vom 2. September 1986 schließen in Ziffer 4.1 Personen, bei denen eine Interessenkollision mit ihren sonstigen dienstlichen Tätigkeiten eintreten kann, vom Einsatz in der Erhebungsstelle aus. Nach § 5 Abs. 1 der rheinland-pfälzischen Landesverordnung zur Durchführung des Volkszählungsgesetzes 1987 vom 24. Juni 1986 sollen Personen, bei denen aufgrund ihrer beruflichen Tätigkeit oder aus anderen Gründen zu besorgen ist, daß Erkenntnisse aus ihrer Tätigkeit in der Erhebungsstelle zu Lasten eines Auskunftspflichtigen verwendet werden, in der Erhebungsstelle nicht eingesetzt werden. Die bayerische Prüfungsanleitung für die Einrichtung örtlicher Erhebungsstellen für die Volkszählung 1987 empfiehlt schließlich "dringend", Bedienstete des Einwohnermeldeamtes und aus anderen sensiblen Bereichen, wie z.B. aus der gemeindlichen Finanzverwaltung, nicht in der Erhebungsstelle einzusetzen.

8.2.2

Verwaltungsvorschrift

Die Landesregierung hat in dem Erlaß zur Durchführung der Volkszählung 1987 vom 2. September 1986 (StAnz. 1986, S. 1774) noch einmal ihre Auffassung betont, nach der jeder Angehörige der Verwaltung, der die Gewähr für Zuverlässigkeit und Verschwiegenheit bietet, als Mitarbeiter in der Erhebungsstelle eingesetzt werden kann. In der Verwaltungsvorschrift werden im übrigen ergänzend zur Ausführungsverordnung die Aufgaben des Zählungsleiters und dessen Stellvertreters, die Zählerbestellung, die organisatorische, räumliche und personelle Trennung der Erhebungsstelle von anderen Verwaltungsaufgaben und einige besondere Aufgaben der Gemeinde zur Durchführung der Zählung geregelt. Danach dürfen Angehörige der Steuerverwaltung, Polizeibeamte im Vollzugsdienst, Bedienstete des Landesamtes für Verfassungsschutz sowie Staats- und Anwälte nicht als Zähler eingesetzt werden. Der Verzicht auf Bedienstete aus dem Bereich des Einwohnermeldewesens wird hingegen lediglich empfohlen.

Hervorzuheben ist die auf meinen Vorschlag hin aufgenommene Zugangsregelung für die Erhebungsstellen. Sie legt fest, wer neben den Bediensteten der Erhebungsstelle Zugang zur Erhebungsstelle hat und stellt ausdrücklich klar, daß zu den Zugangsberechtigten auch der Hessische Datenschutzbeauftragte und seine Beauftragten zählen. Begrenzt wird zudem der Kreis der Personen, die die Erhebungsunterlagen einsehen dürfen, wobei wiederum ausdrücklich der Hessische Datenschutzbeauftragte und seine Beauftragten eingeschlossen werden. Diese auf meinen Wunsch hin erfolgten Klarstellungen sind gleichzeitig ein deutlicher Hinweis auf das von mir im Zusammenhang mit der Volkszählung 1987 geplante Prüfprogramm: Ein Teil dieses Programms wird aus genauen datenschutzrechtlichen Kontrollen der Datenverarbeitung in den Erhebungsstellen bestehen.

8.2.3

ADV in den örtlichen Erhebungsstellen

Keineswegs gelöst sind bislang sämtliche mit der Datenverarbeitung der örtlichen Erhebungsstellen zusammenhängenden datenschutzrechtlichen Probleme. Dabei geht es allerdings primär nicht um die Angaben der Befragten in den Erhebungsbogen, sondern um die zur Organisation der Volkszählung erforderliche Datenverarbeitung. Zu diesem Zweck übermitteln gemäß § 11 Volkszählungsgesetz die Meldeämter den Erhebungsstellen auf Verlangen

im Melderegister gespeicherte Daten der Einwohner, und zwar im einzelnen: Vor- und Familiennamen, Anschrift, Haupt- und Nebenwohnung, Geburtsjahr und -monat, Geschlecht und Staatsangehörigkeit. Aus diesem Registerauszug erstellt die Erhebungsstelle beispielsweise für jeden Zählbezirk eine Liste mit Namen und Anschrift der Auskunftspflichtigen, die dem Zähler ausgehändigt wird und ihm zur Durchführung der Zählung dient. Das kommunale Steueramt oder die öffentlich-rechtliche Gebäudebrandversicherung stellen der Erhebungsstelle Namen und Anschrift der Eigentümer der Wohngebäude zur Verfügung, während die für die Entgegennahme von Gewerbeanzeigen zuständige Stelle der Gemeinde der Erhebungsstelle Namen und Anschrift der Arbeitsstätten mitteilt. In jedem Fall muß sichergestellt sein, daß nur die im Gesetz genannten Daten übermittelt werden. Gegenwärtig überprüfe ich, ob dies in den Fällen, in denen die Kommunalen Gebietsrechenzentren Datenverarbeitung für die Erhebungsstellen durchführen, gewährleistet ist.

Soweit sich die Erhebungsstellen für ihre Datenverarbeitung der Kommunalen Gebietsrechenzentren bedienen, tritt jedoch noch ein gravierenderes Problem auf, nämlich die Gewährleistung der Abschottung der Erhebungsstelle. Das Bundesverfassungsgericht hat zur Sicherung des informationellen Selbstbestimmungsrechts für die Volkszählung besondere Vorkehrungen für Durchführung und Organisation der Datenerhebung verlangt und in diesem Zusammenhang "wirksamen Abschottungsregelungen nach außen" entscheidende Bedeutung beigemessen (BVerfGE 65, 2, 49). Der Gesetzgeber hat daraus die Konsequenzen gezogen und in § 9 Abs. 1 Volkszählungsgesetz 1987 die räumliche, organisatorische und personelle Trennung der Erhebungsstellen von anderen Verwaltungsstellen angeordnet. Wenngleich das Gesetz nur die Trennung von anderen Verwaltungsstellen erwähnt, so ist doch selbstverständlich, daß dieses Abschottungsgebot generell, also auch gegenüber anderen Stellen, die nicht Verwaltungsstellen sind, gilt. Das schließt zwar nicht aus, daß die Erhebungsstelle ein Kommunales Gebietsrechenzentrum mit Datenverarbeitungsaufgaben beauftragt, wenngleich unter Akzeptanzgesichtspunkten sicherlich die Datenverarbeitung auf einem ohne Kommunikationsanschluß in der räumlich abgeschotteten Erhebungsstelle befindlichen Personalcomputer die empfehlenswertere Lösung ist.

Die Nutzung externer Datenverarbeitungsanlagen durch die Erhebungsstellen darf nicht zu einer Verletzung des strikten Abschottungsgebots des Bundesverfassungsgerichts und des Volkszählungsgesetzes 1987 führen. Das läßt sich bei der DV-Unterstützung der Erhebungsstellen durch die Kommunalen Gebietsrechenzentren nur erreichen, wenn u.a. zusätzliche technische, organisatorische und personelle Abschottungsmaßnahmen auch innerhalb der Kommunalen Gebietsrechenzentren getroffen werden. Je nach Umfang des nicht einheitlichen Leistungsangebots der fünf Kommunalen Gebietsrechenzentren werden nicht nur die nach § 11 Volkszählungsgesetz 1987 zu übermittelnden Daten in den Kommunalen Gebietsrechenzentren zur Herstellung von Adreßaufklebern und Namenslisten verwendet, sondern auch zur eventuell später notwendigen Vervollständigung der Angaben der Volks- und Berufszählung - und damit als Erhebungsmerkmale - gespeichert. Denn in allen Fällen, in denen es den Zählern oder der Erhebungsstelle nicht gelingt, innerhalb von sechs Wochen nach dem Zählungstichtag Angaben vom Auskunftspflichtigen zu erhalten, erlaubt das Volkszählungsgesetz den Erhebungsstellen, die Daten für die betreffende Person aus dem Melderegisterauszug mit Ausnahme von Vor- und Familiennamen in den Haushaltsmantelbogen und den Personenbogen zu übertragen. Einige Kommunale Gebietsrechenzentren offerieren den Erhebungsstellen auch die Möglichkeit der automatisierten Rücklaufkontrolle, d.h. die Erhebungsstellen können die Kontrolle des Rücklaufs der Erhebungsbogen mit Angaben über Ausgabezeitpunkt, Rückgabedatum, erfolgte Mahnungen oder Einleitung eines Bußgeldverfahrens im Wege der Datenfernverarbeitung auf dem Rechner des Kommunalen Gebietsrechenzentrums durchführen.

Gegenwärtig sind die Gespräche zwischen mir, der Staatskanzlei und den Kommunalen Gebietsrechenzentren mit dem Ziel, hier eine datenschutzrechtlich akzeptable Lösung zu finden, noch nicht abgeschlossen.

8.2.4

Zentrale Volkszählungsstelle für Hessen

Das Statistische Landesamt richtet in Korbach eine Außenstelle ein, in der nach Abschluß der Erhebung in den Gemeinden die manuelle Datenaufbereitung vorgenommen wird. Anschließend werden die Daten dann automatisiert in der Hessischen Zentrale für Datenverarbeitung in Wiesbaden verarbeitet. Die Außenstelle soll ihre Arbeit am 1. Mai 1987 aufnehmen. Nach einer Besichtigung des vorgesehenen Dienstgebäudes in Korbach habe ich im September 1986 auf der Grundlage eines kriminalpolizeilichen Gutachtens dem Statistischen Landesamt einen Katalog ergänzender Datensicherungsmaßnahmen empfohlen. Die Durchführung der Maßnahmen werde ich, bevor die Außenstelle ihre Arbeit aufnimmt, überprüfen.

9. Individuelle Datenverarbeitung mit Personal-Computer (PC)

9.1

Technologischer Fortschritt

Der Technologiesprung bei der Entwicklung immer kleinerer und leistungsfähigerer elektronischer Bausteine der Mikroelektronik hat völlig neue, vor einigen Jahren noch undenkbar Möglichkeiten der Kommunikationstechnik eröffnet und die Strukturen herkömmlicher Datenverarbeitung grundlegend verändert.

Ich habe den sich abzeichnenden Technologiewandel und seine denkbaren Folgen für den Datenschutz bereits im 11. Tätigkeitsbericht für 1982 beschrieben (vgl. dort, Ziff. 3.1).

Der erreichte Stand der Technik jetzt nach nur vier Jahren und die aus den Sitzungsprotokollen der Automationsgremien des Landes und der Kommunen zu entnehmenden Beschaffungszahlen für Personal-Computer (allein für das Jahr 1986 weit über 100 Stück) zeigen auf, daß diese Entwicklung weitaus schneller vonstatten ging, als 1982 abzusehen war. Nicht nur, daß die Leistungsfähigkeit der PC der letzten Generation wie z.B. IBM AT 03 mit einem 16-Bit-Prozessor (CPU 80286) und 512 Kilo-Byte (KB) Hauptspeicher, Festplatte 40 Mega-Byte (MB) oder TANDON PCA 40 (Leistung w. oben, Festplatte 40 MB) die der in den KGRZ eingesetzten Großrechner der 70er Jahre erreicht hat, sie sind inzwischen auch so preiswert, daß ihre Anschaffung selbst für kleine Verwaltungseinheiten wirtschaftlich erscheint. Die zum Betrieb dieser Geräte erforderliche Software ist in Form von Standardprogrammen für die unterschiedlichsten Problemstellungen bis hin zum leistungsfähigen Datenbanksystem mit komfortabler Abfragesprache wie z.B. das Produkt dBase III kostengünstig, praktisch "von der Stange" in jedem Computerladen zu kaufen. Ich halte es deshalb für erforderlich, dieses Thema erneut aufzugreifen, an den gemachten Erfahrungen zu vertiefen und neue sich abzeichnende Problemlösungen aufzuzeigen.

9.2

Technische Ausstattung und Einsatzarten der Personal-Computer

PC verfügen heute in der Regel über einen Prozessor von mindest 128 KB an aufwärts. Als Massenspeicher für Daten und Programme werden flexible Datenträger (Floppy Disks) in den Abmessungen 3,5 Zoll (720 KB), 5,25 Zoll (0,16-2 MB) und 8 Zoll (max. 360 KB im "IBM-Standard" 3740) verwendet. Bei Geräten der Preisklasse zwischen ca. 6.000 DM und 20.000 DM sind bereits hermetisch gekapselte und damit ausfallsichere Festplatten (Winchesterlaufwerke) mit einer Speicherkapazität von 10 MB bis 70 MB eingebaut. Zusätzlich haben diese Geräte noch ein bis zwei Laufwerke für Floppy Disk.

Die vielfältigen technischen Möglichkeiten dieser Geräte erlauben deren Verwendung in fast jeder denkbaren Funktion und Betriebsart. Sie können sowohl als isoliertes System (Stand-Alone) als auch im Verbund (Netz) mit anderen PC oder Großrechnern (Host) eingesetzt werden. Begriffe wie Single-User- oder Multi-User-Betrieb bedeuten lediglich ob ein oder mehrere Benutzer Zugang zu einem System haben. Einzelplatzsysteme verfügen über einen Bildschirm, müssen also nacheinander benutzt werden, Mehrplatzsysteme haben mehrere Bildschirme, ermöglichen also den gleichzeitigen Zugriff mehrerer Mitarbeiter. Werden PC über ein Netz intern miteinander verbunden spricht man von einem Inhouse-System. Erfolgt ein externer Anschluß an einen Großrechner, behandelt dieser den PC wie ein intelligentes Terminal (z.B. 3278 Emulation). Ist bei dieser Anschlußart vereinbart, daß Dateien oder deren Teilmengen auf den PC zur eigenständigen Weiterverarbeitung übertragen werden (File Transfer), können alle technischen Möglichkeiten des PC genutzt werden, um diese Daten zu verändern, auszuwerten und auf die Datenbank des Großrechners zurück zu übertragen.

9.3

Stärken und Schwächen des Personal-Computers

9.3.1

Vorzüge

Der PC ist ein Produkt, das im Gegensatz zu den Systemen der Großrechner von der Industrie ganz spezifisch für die Belange der Anwender entwickelt wurde. Nur so ist das unglaubliche Tempo seiner Verbreitung zu erklären.

- Er ist ein leicht bedienbares und preisgünstiges Hilfsmittel der Büroorganisation, welches seinen Benutzer nicht durch übermäßige technische Zwänge in seiner Handlungsfreiheit einengt. Damit wird die Hemmschwelle zur Automatisierung gesenkt. Bisher manuell (und damit oft unzulänglich und wenig aktuell) geführte Karteien, Suchlisten und Verzeichnisse werden leicht in die Datenverarbeitung überführbar.

- Er erlaubt jederzeit den Zugriff auf die gespeicherten Daten ohne Abhängigkeit von einem zentralen Rechenzentrum. Als Folge davon sinkt der Bedarf an zahlreichen Computerlisten, deren Gefährdungspotential oft darin liegt, daß niemand weiß, welche Liste gerade auf einem aktuellen Stand ist und somit u.U. falsche Daten enthält. Es verringert sich die Gefahr der unberechtigten oder unnötigen Kopien, und es stellt sich nicht mehr das Problem der geordneten Vernichtung dieser Papierfluten (Datenmüll-Skandale).
- Die Verantwortung für eine ordnungsgemäße Datenverarbeitung liegt wieder weitgehend in der Hand des Sachbearbeiters (PC-Bedieners). Es entfällt damit die Gefährdung durch mangelnden Informationsfluß bei verteilten Zuständigkeiten.
- Er erlaubt die völlig abgeschottete Verarbeitung besonders schutzwürdiger Daten (z.B. im Gesundheitswesen). Ein unbefugter Zugriff Dritter kann unter Idealbedingungen (beispielsweise ausschließlich ein Bediener) mit einfachsten Vorkehrungen wie z.B. dem Verschuß des PC und/oder der Datenträger ausgeschlossen werden.

9.3.2

Die Stärken des Personal-Computers sind auch seine Schwächen

Die positiven Eigenschaften des PC sind aber auch zugleich seine Schwachpunkte. Denn die Kontrollmöglichkeiten, z.B. für den Datenschutzbeauftragten, sind bei dezentral eingesetzten PC weitaus geringer als bei zentraler Datenverarbeitung im Großrechenzentrum. Dies wird besonders deutlich, wenn man die technischen Möglichkeiten der PC, ihre geringe Größe, die Organisation ihrer Verwendung und die Funktionsweise ihrer Betriebssysteme betrachtet.

9.3.2.1

Organisation der DV mit Personal-Computer

PC werden fast ausschließlich vom Anwender "autonom", d.h. in eigener Verantwortlichkeit und allein an seinen spezifischen Bedürfnissen orientiert, ausgewählt und eingesetzt. Nur in wenigen Fällen erfolgt eine Beschränkung der eigenen Kreativität bei der Lösung eines Problems durch zentrale Vorgaben wie z.B. die Einhaltung bestimmter Standards bei der Auswahl und Zusammenstellung der Geräte (Konfiguration), der Zwang zur zentralen Datenspeicherung oder die Verwendung bestimmter Standardprogramme.

9.3.2.2

Die Betriebssysteme

Personal-Computer (aus dem engl. "persönlicher Computer") sind, wie ihr Name sagt, ursprünglich als Einzelplatzsysteme für den Single-User-Betrieb konzipiert. Sie benötigen zu ihrer Funktion genau wie Großrechner bestimmte Systemprogramme. Diese Betriebssysteme steuern den Ablauf der Anwendungsprogramme im Rechner, koordinieren und überwachen die Zusammenarbeit des Prozessors mit allen anderen Komponenten des Systems wie Arbeitsspeicher, Floppy Disk/Winchesterlaufwerk als Massenspeicher und Drucker oder Bildschirm als Ausgabeeinheiten.

Die gängigsten Betriebssysteme für PC wie z.B. CP/M (Control Program for Microprocessors) oder MS-DOS (Microsoft Disk Operating System) unterscheiden sich von den Betriebssystemen für Großrechner wie MVS (IBM) oder BS 2000 (Siemens) einmal dadurch, daß sie keine Eigenentwicklung der Gerätehersteller sind, sondern vielmehr Produkte von Software-Häusern, die lediglich bei Bedarf an neu auf den Markt kommende PC angepaßt werden. Aber, was viel gravierender ist: Sie sind von ihrer Konzeption her reine Single-User-Systeme. D.h. sie gehen davon aus, daß an einem PC nur ein Anwender tätig ist, dem es selbst überlassen bleibt, wie er seine Daten sichert. Die Betriebssysteme bieten dazu keinerlei Unterstützung wie z.B. User-ID, Paßworte oder Dateischutz an.

Eine Ausnahme ist das z.Zt. noch weniger verbreitete Multi-User und Multi-Tasking Betriebssystem UNIX-System III mit seinen Abkömmlingen XENIX und SINIX. Hier haben die Systementwickler bereits einige Möglichkeiten geschaffen, den Systemzugang über eine sogen. User-Directory zu kontrollieren, sowie Dateien gegen unbefugtes Lesen, Schreiben oder Löschen zu schützen. Dies geschieht durch das Setzen bestimmter Schutz-Bits in den Header-Sätzen.

9.3.2.3

Eingeschränkte Kontrolle durch fehlende Funktionstrennung

Die Kontrolle der ordnungsgemäßen Verwendung eines dezentral in der Verwaltung eingesetzten PC ist weitaus schwieriger als die Überwachung des Betriebsablaufs in einem Großrechenzentrum. Das liegt z.B. daran, daß eine Funktionstrennung zwischen Fachabteilung und DV nicht mehr vorhanden ist. Das Vier-Augen-Prinzip entfällt. Der Bediener des PC ist Sachbearbeiter, Arbeitsvorbereiter, Verwalter der Datenträger - einschließlich der Sicherungskopien -, Operator, Arbeitsnachbereiter und Programmierer in einer Person. Er gerät somit in die Rolle des Systemprogrammierers, der als "Super User" Zugriff auf alle Systemfunktionen und alle Daten hat. Somit werden Dienstanweisungen die seine Zuständigkeiten reglementieren immer dann auf Unverständnis stoßen, wenn sein Datenschutzbewußtsein gering ausgebildet ist.

9.3.2.4

Kein Schutz der sensitiven Systemfunktionen

Sensitive Funktionen der Betriebssysteme wie spezielle Dienstprogramme die das Kopieren von Datenträgern, das Anlegen oder Löschen von Dateien oder deren Umbenennung erlauben, sind nicht geschützt und stehen standardmäßig im freien Zugriff des PC-Bedieners.

9.3.2.5

Dateien werden nur logisch gelöscht und sind wiederauffindbar

Herkömmliche Betriebssysteme ändern bei einer Löschung von Dateien nur den Eintrag in das "Inhalts"verzeichnis des Datenträgers (Directory). Für ein "normales" Zugriffsprogramm ist die Datei nicht mehr auffindbar, also scheinbar gelöscht. Nur: Standardsoftware, die eben diese Daten wieder finden kann, gibt es in jedem Computerladen zu kaufen. Ein Schutz vor dieser Manipulation, nämlich das Überschreiben der zu löschenden Datensätze mit anderen Zeichen z.B. Nullen, ist in den Standardbetriebssystemen nicht vorhanden.

9.3.2.6

Systemaktivitäten werden nicht protokolliert; wer kontrolliert den privilegierten Benutzer?

PC-Betriebssysteme sehen keine Protokollierung von Systemaktivitäten und damit die Möglichkeit einer nachträglichen Kontrolle vor. Bei einigen Produkten kann allerdings der letzte Zugriff auf eine Datei mit Datum/Uhrzeit - und auch nur das - in deren Verzeichnis geschrieben werden. Das Problem der Kontrolle des privilegierten Benutzers ist deshalb beim PC-Einsatz ohne zusätzliche hardware- oder programmtechnische Eingriffe in das System nicht lösbar. Für einige wenige Systeme mit Winchesterlaufwerk sind seit kurzer Zeit solche Produkte im Handel. Einige von ihnen habe ich auf einem PC untersucht (siehe unten Ziff. 4.3.3.).

9.3.2.7

Gefahren durch selbstentwickelte, nicht freigegebene Programme; Abhängigkeit durch fehlende Dokumentation und Herrschaftswissen

Die Systeme können alle Programme verarbeiten die von der Maschinenlogik her fehlerfrei sind. Was aber nicht bedeutet, daß diese auch ausreichend getestet und freigegeben sind. Sie sind im Gegenteil oft selbst und manchmal auch laienhaft entwickelt. Es fehlen Abstimm- und Kontrollsysteme wie z.B. Prüfsummen, Fehlerausgänge und konkrete Fehlerhinweise und es mangelt an ausreichenden Plausibilitätsprüfungen. Eine ordnungsgemäße Programmdokumentation existiert in vielen Fällen nicht. Die Folgen sind: fehlerhafte Datenverarbeitung, Datenverlust und die drohende Abhängigkeit der Behörde von dem Wissen eines bestimmten Mitarbeiters.

Mir ist ein Fall bekannt, in welchem eine Behörde allein deshalb den PC eines bestimmten Herstellers anschaffte, weil ein Mitarbeiter diesen PC-Typ privat besaß und schon verschiedene Programme für dienstliche Zwecke auf dem System entwickelt hatte.

9.3.2.8

Empfindliche Systeme und Datenträger, mangelhafte Datensicherung durch umständliche Betriebsarten

Die meisten PC sind übermäßig empfindlich gegen Störungen in der Stromversorgung (Netzausfall). Standardmäßig sind meist keine Systemkomponenten vorhanden, die in solchen Fällen eine Zerstörung von Dateien verhindern (z.B. Netzpuffer). Flexible Datenträger (Floppy Disk) sind sehr empfindlich gegen Staub und Hitze oder das Berühren ihrer Speicheroberfläche in der Lese-/Schreiböffnung der Schutzhülle. Statische Aufladungen - bei den heute üblichen Textilbodenbelägen, Kunststoffoberflächen der Büromöbel oder Kunstfaseranteilen in der Bekleidung der Mitarbeiter keine Seltenheit - können zur Zerstörung von Datensammlungen führen. Abhilfe technischer Art, wie z.B. Schutzerdung der Bodenbeläge und Geräte ist aufwendig und teuer.

Deshalb sollte der Sicherung der Datenbestände größte Aufmerksamkeit gewidmet werden. PC mit Festplatte werden normalerweise auf Disketten gesichert. Ein überaus zeitraubendes Verfahren. So dauert das Sichern der 10 MB Festplatte eines verbreiteten Systems auf ca. 10 Disketten etwa 50 Minuten. Die Folge ist, der Benutzer scheut den Aufwand und wählt zu große Zeitabstände zwischen den einzelnen Sicherungsläufen. Er gerät damit in die Gefahr von größeren Datenverlusten bei Zerstörung einer Platte. Technische Einrichtungen, die eine schnelle Datensicherung erlauben, z.B. sogen. Streamer-Tapes, sind relativ teuer.

9.4

Datenschutz und Datensicherung bei Datenverarbeitung mit Personal-Computern

9.4.1

Problemdarstellung

Die Datenverarbeitung auf kleinen separaten DV-Systemen wie den PC unterscheidet sich in vielfältiger Weise von den Methoden der Groß-DV wie z.B. im Hessischen DV-Verbund oder den Universitätsrechenzentren. Bei meinen Prüfungen und Beratungen habe ich aber noch ein weiteres, längst vergessen geglaubtes Problem festgestellt: Als Stellen der öffentlichen Verwaltung in den Jahren ab 1965 erstmals in größerem Umfang mit der ADV konfrontiert wurden, sahen sie sich vor eine Fülle bisher unbekannter Fragen gestellt. Begriffe wie Datensicherung und Datenschutz tauchten auf und führten letztlich zu ersten gesetzlichen Regelungen. Die Erfahrungen im Umgang mit der Datenverarbeitung veränderten althergebrachte Organisationsabläufe und Strukturen der betroffenen Verwaltungen.

Mit dem Auftreten der PC als Mittel der IDV (Individuellen Datenverarbeitung) werden nun Bereiche der Verwaltung für die automatisierte Datenverarbeitung erschlossen, die bisher davon ausgenommen waren. Es gibt nun wiederum eine Gruppe von ADV-Neulingen, die den auf sie zukommenden Problemen des Datenschutzes ohne eigene Erfahrung gegenübersteht. Die nachfolgenden Hinweise sollen helfen, den Einstieg in die Materie zu erleichtern, Probleme aufzuzeigen und Lösungsansätze anzubieten.

9.4.2

Abgrenzung der Begriffe

Zur Erinnerung: Mit Individueller Datenverarbeitung (IDV) bezeichnet man den Einsatz von DV-Systemen die eine auf die speziellen Bedürfnisse einer Organisationseinheit der Verwaltung zugeschnittene autonome Verarbeitung von Daten in eigener Verantwortlichkeit ermöglichen. Die Größe des dabei eingesetzten DV-Systems ist nicht entscheidend, lediglich die Art der Verwendung. Nicht dazu gehören Geräte, denen folgende Mindesteigenschaften fehlen: Die Systeme müssen programmierbar sein, und sie müssen die Fähigkeit besitzen, Daten und Programme auf magnetisierbaren Datenträgern speichern zu können. Einfache Speicherschreibmaschinen - mit oder ohne Display -, Fernkopierer, Taschen- und Tischrechner erfüllen diese Anforderungen nicht.

Im Interesse einer kompakten Darstellung wird bei den nachfolgenden Ausführungen auf eine Trennung nach Geräten im Stand-Alone-Betrieb, gleich ob als Einzel- oder Mehrplatzsystem oder Geräte, die in einem Inhouse-Netz oder mit einem Host-Rechner verbunden sind, verzichtet. Wo aber z.B. durch den gleichzeitigen Zugriff mehrerer Bediener an Mehrplatzsystemen oder die Verarbeitung von Daten in Netzen besondere Probleme auftreten, sind diese gesondert gekennzeichnet. Probleme, die bei vereinbartem File-Transfer vom Host zum PC oder umgekehrt auftreten können oder die Risiken die entstehen, wenn zusammen mit anderen Teilnehmern die Verarbeitung von Daten in einem sog. Teilnehmersystem eines Groß-Rechenzentrums erfolgt, sollten vorzugsweise über die Nutzung der Schutzfunktionen der Betriebssysteme dieser Großsysteme oder der Verwendung besonderer Datenschutzprogramme wie RACF, SECURE oder TOP SECRET erfolgen.

9.4.3

Organisatorische Ansätze

9.4.3.1

Checklisten sind kein Allheilmittel; keine DV mit Personal-Computern ohne ausreichende Datensicherung

Es gibt eine Menge Versuche, Regularien für die Datenverarbeitung mit PC durch die Interpretation des Maßnahmenkatalogs der Anlage zu § 10 Hessisches Datenschutzgesetz bzw. § 6 Bundesdatenschutzgesetz zu schaffen. Diese Organisationshilfen, Hinweise oder Empfehlungen enthalten jedoch oft nur sehr allgemein gehaltene Zielsetzungen, die zudem nicht die speziellen Eigenheiten der DV mit PC berücksichtigen. Sie stoßen zum anderen auf das oft wenig ausgeprägte Datenschutzbewußtsein der PC-Anwender, die als privilegierte Benutzer mitunter wenig Bereitschaft zeigen, Vorschriften zum Datenschutz und zur Datensicherung zu akzeptieren.

Grundsätzlich gilt:

- keine Checkliste kann den konkreten Einzelfall lösen, sie muß sich auf generelle Ansätze beschränken und ist lediglich eine Hilfestellung bei der Entwicklung eigener Lösungen.
- Jeder Überlegung über Maßnahmen, die eine ordnungsgemäße DV mit PC sicherstellen sollen, muß eine Bestandsaufnahme und die Untersuchung der künftigen Arbeitsweise voraus gehen (Ist- und Soll-Zustand). Organisatorische oder technische Maßnahmen, die nicht in ein Gesamtkonzept eingepaßt sind, erhöhen bestenfalls den bürokratischen Aufwand und verfehlen ihren Zweck.
- Anweisungen und Verfügungen zur DV mit PC, die nicht schriftlich erfolgen und deren Einhaltung nicht regelmäßig überprüft wird, werden schnell vergessen.
- Technische Maßnahmen zur Gewährleistung des Datenschutzes und der Datensicherung, wie Eingriffe in die Hardware der PC und/oder besondere Datenschutzprogramme sind organisatorischen Lösungen immer überlegen, da sie nicht so leicht unterlaufen werden können.
- Wenn ausreichende Datensicherungsmaßnahmen bei einem bestimmten PC und den zur Verwendung auf diesem System vorgesehenen Programmen nicht erreicht werden können, dürfen keine personenbezogenen Daten auf diesem PC verarbeitet werden.

9.4.3.2

Planung des PC-Einsatzes durch sorgfältige Aufgabenuntersuchung und Festlegung eines Sollkonzepts

Im Gegensatz zur Datenverarbeitung auf zentralen Großrechnern ermöglicht der PC die Lösung fachspezifischer Probleme einschließlich der damit verbundenen Datenschutzfragen mit relativ einfachen Mitteln, denn er ist im Grunde genommen das Rechenzentrum in der Fachabteilung. Aber bereits die Entscheidung für ein bestimmtes System und eine bestimmte Betriebsart z.B. Stand-alone oder Netzbetrieb mit Mehrfachzugriff auf eine gemeinsame Festplatte hat gravierende Auswirkungen auf die Art und den Umfang der nach § 10 HDSG erforderlichen Maßnahmen. Eine sorgfältige Bestandsaufnahme und ein durchdachtes Soll-Konzept sind deshalb unabdingbare Voraussetzung für eine künftige ordnungsgemäße Datenverarbeitung.

9.4.3.2.1

Checkliste für die zu verarbeitenden Daten

Die Fragen nach Art und Menge der zu verarbeitenden Daten, ihrer Herkunft, ihrer Schutzbedürftigkeit - ganz besonders auch im Hinblick auf die geplante Verarbeitung -, sind nicht nur wesentliche Kriterien für die Systemauswahl und eine Datenschutzkonzeption, sie sind auch Grundlage der nach § 6 Hessisches Datenschutzgesetz vom 11. November 1986 (HDSG) durch die speichernde Stelle anzufertigenden Dateibeschriftung.

Ist der PC jedoch bereits vorhanden und die Verarbeitungsumgebung damit vorgegeben, hat dies Auswirkungen auf die Verarbeitungsweise. Mit einer aufgabenbezogenen Datei-Checkliste sollte ermittelt werden:

Datei-Checkliste

1. Welchem Zweck dient die Datei?
2. Welche Daten sollen gespeichert werden?
3. Welche Rechtsvorschrift erlaubt die geplante Verarbeitung?
4. Wessen Daten sollen verarbeitet werden (Betroffene)?
5. Sollen Daten regelmäßig an Dritte übermittelt werden?
Wenn ja: welche und an wen?
6. Werden Daten regelmäßig empfangen?
Wenn ja: welche und von wem?
7. Sind die Daten/Programme/Ergebnisse besonders schutzwürdig
(z.B. Gesundheitsdaten, Sozialdaten, Personaldaten)?
8. Sind zusätzliche bereichsspezifische Rechtsvorschriften zu beachten wie z.B. Sozialgesetzbuch Zehntes Buch (SGB X) oder Bestimmungen über die Verfahrenssicherheit bei der Verwendung automatischer Datenverarbeitungsanlagen im Haushalts-, Kassen- und Rechnungswesen und für die Übernahme des Inhalts auf Bildträger (HKR-ADV-Best)?

9.4.3.2.2

Das System; was leistet es, wo sind seine Schwachstellen?

Gäbe es für PC genormte Mindestanforderungen an deren technische Ausstattung und Leistungsvermögen oder gar eine amtliche Betriebserlaubnis (ABE) ähnlich der des Kraftfahrt-Bundesamtes für Automobile, ließe sich der Umfang der zu ergreifenden Datensicherungsmaßnahmen daran messen. Was ein PC aus der Sicht des Datenschutzes leisten kann bleibt aber leider allein der Phantasie oder der Marktstrategie des Herstellers (z.B. gewollte Inkompatibilität zu anderen Systemen und deren Betriebssoftware) überlassen. Das nachstehende Beispiel einer System-Checkliste soll es erleichtern, ein bereits vorhandenes System einzuschätzen, bzw. Hilfestellung für die an ein noch zu beschaffendes System zu stellenden Datenschutzanforderungen geben. Dazu müssen die gewünschten Schutzmaßnahmen (siehe Ziff. 9.4.4.2, Maßnahmenmatrix zu § 10 HDSG) aus der Matrix ausgesucht und geprüft werden, ob eine Antwort zu einer Frage aus der nachstehenden System-Checkliste diese Anforderung erfüllt bzw. ob eine durch eine andere Maßnahme (z.B. Objektschutz, besonderes Datenschutzprogramm o.ä.) zu schließende Lücke besteht.

System-Checkliste

1. Systemkonzept
 - 1.1 Einzelplatzbetrieb?
 - 1.2 Mehrplatzbetrieb mit getrennter Datenspeicherung (Disketten) oder gemeinsamer Datenspeicherung (Festplatte)?
 - 1.3 Vernetztes System mit anderen lokalen PC bzw. Terminals (Inhouse) oder externem System (Host)?
 - 1.4 Betriebsart (Stapelbetrieb/Dialog als Teilhaber oder Teilnehmer/File-Transfer oder lediglich Terminal-Emulation)?
2. Hardwareausstattung/Peripherie
 - 2.1 Zahl der Bildschirme?
 - 2.2 Zahl der Drucker?
 - 2.3 Betriebsart (Warteschlangenverwaltung-Spool/gewidmet-privat)?
 - 2.4 Zahl der Diskettenlaufwerke oder sonstiger Wechselplattenlaufwerke/Kapazität?
 - 2.5 Zahl der Festplatten bzw. der Winchesterlaufwerke/Kapazität?
 - 2.6 Sonstige Speichermedien (Band/Streamer-Tape)?
 - 2.7 Sonstige technische Schnittstellen (V/24, TELETEx, BTX, MAIL-BOX, Akustik-Koppler)?
3. Betriebssystem
 - 3.1 LOG-ON Prozedur

Wird die Systemsoftware über Diskettenlaufwerk oder Festplatte geladen?
Wahlweises Laden von einem beliebigen Laufwerk?
Bei vernetzten PC und Mehrplatzsystemen:
Ist ein spezielles Systemterminal/Masterplatz vorgesehen?
Kann dieses auch als Arbeitsplatz genutzt werden?
Sind Supervisor- bzw. Masterfunktionen auch von anderen Bildschirmen aufrufbar?
 - 3.2 Zugriffsschutz

Ist ein programmgesteuerter Zugriffsschutz vorgesehen (Paßwort/Benutzer-Identifikation)?
Ist die Abfrage des Paßwortes obligatorisch und wird dieses verdeckt eingegeben?
Bei Paßworten auf Systemebene:
Sind schutzbedürftige Dateien, Funktionen bzw. Dienstprogramme wie z.B. Paßwortdatei, Systemresidenz, Formatierprogramme, Kopierer, Datenträgerverzeichnisse geschützt?
Bei gemeinsam genutzten Programm- bzw. Datenbeständen oder zentraler Datenspeicherung: Zugriffsschutz auf Dateiebene gegen Lesen, Schreiben, Entfernen (Eigentümer, Gruppe, Andere)?
Speicherschutz gegen gleichzeitigen Zugriff? Paßwortformat und -behandlung (alfa, alfa-numerisch, Länge, Erkennung trivialer PW, verschlüsselte PW-Datei)?
Wieviel Fehlversuche sind beim LOG-ON erlaubt?
Folgen der Fehlversuche (autom. LOG-OFF, Systemstart wiederholen, Tastaturblockade)?
Technischer Zugriffsschutz vorhanden (Gehäuseschloß, Tastaturschloß, Laufwerkschloß)?
 - 3.3 Datensicherungsfunktionen

Back-Up unterstützt durch spez. Programme?
Auf welchem Datenträger erfolgt der Back-Up (Disketten, Festplatte, Streamer-Tape)?
Wieviele Generationen der Daten und des Betriebssystems sollen gesichert werden?
Wo und wie sollen diese aufbewahrt bzw. ausgelagert werden?

3.4 Protokollfunktionen

- Ist eine Protokollfunktion vorhanden?
- Speichermedium für die Protokolldatei?
- Zugriffsschutz vorhanden (nur Zugriff des Supervisors bzw. des Superusers)?
- Datensatzbeschreibung der Protokolldatei?
- Sind Auswertprogramme vorhanden?

4. Software-Ausstattung

- 4.1 Ist ausschließlich Standardsoftware eingesetzt, welche?
- 4.2 Ist eine Systemprogrammierung möglich/vorgesehen (welche Interpreter, Compiler)?
- 4.3 Sind die Arbeitsprogramme ständig im Zugriff (auf Festplatte) oder nur bei Bedarf (auf Diskette)?
- 4.4 Sind nur die Lademodule (Objectcode) vorhanden oder auch der Quellcode (Sourcecode)?
- 4.5 Ist Datenbanksoftware installiert wie z.B. dBase?
- 4.6 File-Transfer geplant/realisiert?
- 4.7 Besondere Datenschutz-Software (Zugriffsschutz/Protokolle) geplant bzw. vorhanden?

9.4.3.2.3

Die Systemumgebung - der Objektschutz

In einem verantwortungsbewußt geführten Großrechenzentrum sind konventionelle in der Praxis erprobte Maßnahmen zur Objektsicherung gängiger Standard. Sie schützen nicht nur die wertvolle Installation, sondern erfüllen auch einen Teil der Anforderungen, die § 10 HDSG stellt.

Diese Sicherungsmaßnahmen, wie z.B. die oft aufwendig geschützten Sicherheitszonen eines Closed-Shop-Betriebs lassen sich zweckmäßigerweise nicht ohne weiteres auf die arbeitsplatzorientierte Installation eines PC übertragen. Hier reichen oft einige wenige aber sinnvolle bauliche Maßnahmen der Zugangskontrolle aus, um den gewollten Schutz des Systems zu erreichen. Eine Übersicht über die baulichen Verhältnisse gibt die Gebäude-Checkliste.

Gebäude-Checkliste

- 1. Besondere Gefährdungen
 - 1.1 Gehen von Teilen des Gebäudes, insbesondere von dem PC-Standort benachbarten Räumen, besondere Gefährdungen aus?
 - 1.2 Wasser, Gas- oder sonstige Versorgungsleitungen?
 - 1.3 Lagerung feuergefährlicher Materialien wie Papier oder Chemikalien?
 - 1.4 Sind Staubemissionen z.B. von Offset-Druckern, sonstigen Druckern oder Kopierern (Tonerstaub) vorhanden?
- 2. Stromversorgung
 - 2.1 Ist das System an einen separaten Stromkreis des Gebäudes angeschlossen?
 - 2.2 Ist eine Notstromversorgung geplant/vorhanden (Pufferbatterie)?
- 3. Zugang zum Rechner/bzw. zum Arbeitsraum
 - 3.1 Wieviel Türen gibt es und wo führen diese hin?
 - 3.2 Welche Schlösser (Zylinder- oder Kastenschloß, nur Außenknauf mit autom. Türschließer oder Klinke, elektr. Türöffner) sind eingebaut?
 - 3.3 Ist ein Sichtfenster, Türspion, eine Videoüberwachung vorhanden?
 - 3.4 Ist das Gebäude mit einer Schließanlage mit Gruppen- und Hauptschlüsseln ausgestattet?
 - 3.5 Ist der Rechner-/Arbeitsraum in dieses System einbezogen?
 - 3.6 Wer hat Schlüssel und mit welchen Berechtigungen, Empfang quittiert, Kontrolle des Verbleibs?
 - 3.7 Notfallregelung, Telefon im Rechnerraum?
 - 3.8 Wie ist der Zutritt des Reinigungspersonals - insbesondere außerhalb der Dienstzeit - geregelt, Publikumsverkehr?
 - 3.9 Elektronische Sicherungsmaßnahmen (Einbruchmelder, Durchbruchmelder für Türen und bei ebenerdigem Raum oder möglichem Zugang über Vorbauten auch für die Fenster) geplant/vorhanden?
- 4. Sicherung durch Verschuß des Systems
 - 4.1 Sind Sicherheitsmöbel für Bildschirmarbeitsplätze vorhanden (Terminaltisch mit verschließbarem Tastatur- und Diskettenfach, Terminalschränk)?
 - 4.2 Sonstige verschlußsichere (Zylinderschloß) Möbel?
 - 4.3 Bei Anschluß an Netze:
 - Verschußmöglichkeit für MODEM/Anschlußbox/Akustik-Koppler/DFÜ-Steuereinheit?

9.4.3.3

Hard- und Softwaretechnische Lösungen - Beispiele für Lösungsansätze anhand untersuchter Projekte

Einige der auf dem Markt angebotenen Produkte habe ich auf einem PC installiert und auf ihre Wirksamkeit untersucht. Die Ergebnisse können nur eine Momentaufnahme eines sich täglich ändernden Marktes sein. Sie erheben keinen Anspruch auf Vollständigkeit und sollen lediglich der Information darüber dienen was z.Zt. machbar ist.

9.4.3.3.1

Schalt- und Tastaturschlösser

Schutzvorrichtungen, die mechanisch, elektromechanisch oder elektronisch in die Hardware des PC eingreifen, zielen vor allem darauf ab, die unbefugte Inbetriebnahme des PC zu verhindern. Dies kann z.B. durch den Einbau von Schaltschlössern geschehen oder durch die Verwendung zusätzlicher elektronischer Bauteile (intelligente Steckkarten). Die Verwendung von Chip-Karten zur sicheren Identifizierung und Authentifizierung eines Benutzers gegenüber dem System ist nicht Gegenstand dieser Betrachtungen. Dieses Problem habe ich bereits in meinem 12. Tätigkeitsbericht ausführlich dargestellt (vgl. dort, Ziff. 3.4.2.4)

Schaltschlösser bzw. Schlüsselschalter werden in die Stromversorgung des PC eingebaut (eingeschleift). Mit ihnen kann die Stromversorgung des Rechners blockiert werden. Nur der berechtigte Benutzer kann mit Hilfe seines Schlüssels das Gerät in Betrieb nehmen.

Diese Lösung ist zwar kostengünstig und relativ einfach zu installieren, hat aber auch Nachteile. Sofern der Benutzer das Gerät abschließt, nur weil er z.B. kurzfristig seinen Arbeitsplatz verläßt, wird der PC abgeschaltet. D.h. er muß erneut mit einem LOG-ON gestartet werden. Soll ein unbefugtes Überbrücken dieses Schlosses verhindert werden, muß das PC-Gehäuse zusätzlich mit speziellen Sicherungsschrauben verschraubt werden.

Ebenfalls zu den elektromechanischen Schutzmaßnahmen zählt das beispielsweise in PC der AT-Klasse eingebaute Schloß zur Verriegelung der Bedientastatur. Dieses Schloß unterbricht nicht den Stromkreis des gesamten PC sondern lediglich den der Tastatur. Gleichzeitig verriegelt ein Bolzen das Gehäuse gegen unbefugtes Öffnen. Im verschlossenen Zustand kann der PC nicht neu gestartet werden, da das Betriebssystem die Schalterstellung OFF/ON abfragt. Der Vorteil dieses Systems liegt darin, daß laufende Programme bei kurzfristiger Abwesenheit des Benutzers nicht unterbrochen werden und ein erneutes LOG-ON entfällt. Der mechanische Widerstandswert des Gehäusebolzens ist aber eher als gering einzustufen.

9.4.3.3.2

Die elektronische Sicherheitskarte

Besser sind in jedem Fall Sicherheitskarten auf der Basis elektronischer Schaltungen. Sie werden vom Fachhandel als Zusatzkarten angeboten, die in einen freien Steckplatz (Slot) des PC gesteckt werden. Sie sind von der Systemorganisation her vor dem Betriebssystem angeordnet. Sofort nach dem Systemstart fragen sie vom Benutzer ein persönliches Paßwort ab. Versucht dieser die Abfrage zu umgehen oder zu manipulieren, blockiert sich das System nach einer vorbestimmten Anzahl von Fehlversuchen oder nach Zeitablauf selbst und ist nur über einen erneuten LOG-ON Versuch (mit erneuter Paßwortabfrage) zu starten.

ELKEY-CARD (INFOSYS Computer Elektronik GmbH) ist ein Beispiel für eine elektronische Sicherheitskarte, die eine unbefugte Benutzung eines PC unabhängig von dessen Anwendersoftware zuverlässig verhindert. Sie wird z. Zt. für PC mit dem Betriebssystem MS-DOS (IBM-PC und alle zu diesen Geräten 100 Prozent kompatiblen PC) angeboten.

Das Produkt kann 99 Benutzer und zusätzlich einen Super-User (Master) verwalten. Mit dem von diesem zu vergebenden Paßwort kann die Benutzung des PC auf bestimmte Tage und Uhrzeiten beschränkt werden. Zusätzlich kann jedem Benutzer eine von 127 möglichen Sicherheitsstufen zugeordnet werden. Dieses in der ELKEY-CARD gespeicherte Benutzerprofil kann von jedem Anwenderprogramm abgefragt und somit die Befugnis des Benutzers überprüft werden. Außerdem ist die Einrichtung einer Protokolldatei möglich, in der für jeden Benutzer die letzten 25 eingegebenen Befehle festgehalten werden. Nicht möglich ist dagegen die feste Zuordnung von bestimmten Speicherbereichen oder Dateien zu einem bestimmten Benutzer.

Nach dem Einschalten des PC wird automatisch eine durch ELKEY-CARD eingerichtete Erweiterung des PC-Betriebssystems "LOGON" gestartet. Dieses Programm überprüft, ob der PC mit der Sicherheitskarte ausgerüstet ist und ob der Selbsttest ordnungsgemäß ausgeführt wurde. Danach wird der Benutzer aufgefordert sein Paßwort einzugeben. Wurde dieses gefunden und zugeordnet, kann der PC im durch das Benutzerprofil vorgegebenen Umfang genutzt werden. Wird bei installierter ELKEY-CARD das Programm "LOGON" nicht gefunden, weil

z.B. versucht wurde das Betriebssystem von einer normalen DOS-Diskette zu laden und nicht von der dafür vorgesehenen Festplatte oder es wird dreimal nacheinander ein falsches Paßwort eingegeben, blockiert sich der PC innerhalb weniger Sekunden. Soll der PC für unbestimmte Zeit unbeaufsichtigt bleiben, so kann er mit der Eingabe des Befehls "LOGOFF" geschützt werden. Beim ersten Betätigen einer Taste ruft das System dann wieder das Programm "LOGON" einschließlich der Paßwortabfrage auf.

Die Sicherheitskarte ermöglicht darüberhinaus das Kodieren und Dekodieren von Dateien und, soweit in einem PC-Verbund beim Sender und Empfänger die Karte installiert ist, eine Datenfernübertragung im geschützten Modus.

9.4.3.3.3

Datenschutzprogramme

Eine effektive Datenverarbeitung auf PC mit umfangreicheren Anwendungsprogrammen wird heute sinnvollerweise unter Verwendung einer Festplatte (Winchesterlaufwerk) realisiert. Das Problem für den Datenschutz liegt hierbei darin, daß die auf der Festplatte gespeicherten Daten (Betriebssystem, Anwendungsprogramme, Dateien) dem befugten Benutzer zur Verfügung stehen müssen. Dem Unbefugten aber, der das System z.B. von einem Diskettenlaufwerk gestartet hat, was ohne Probleme möglich ist, verborgen bleiben sollen. Datenschutzprogramme greifen an diesem Punkt ein. Sie schützen die Festplatte vor dem unbefugten Benutzer indem sie:

- die Dateizuordnungstabelle bei gleichzeitiger Veränderung bestimmter Teile des Betriebssystems (Device-Driver) verschlüsseln;
- die Einträge im Inhaltsverzeichnis (Directory) verschlüsseln;
- die Dateien verschlüsseln.

Diese Möglichkeiten werden je nach Produkt einzeln oder kombiniert angewandt.

9.4.3.3.3.1

PC+SOFTLOCK

PC+SOFTLOCK (Copyright PC-PLUS, Gesellschaft für Planung und Systementwicklung professioneller Computeranwendungen mbH), ist eine reine Software-Lösung, welche die auf der Festplatte eines PC gespeicherten Dateien und Programme vor unberechtigtem Zugriff schützt. Sie erlaubt es, unterschiedlichen Benutzern unterschiedliche Berechtigungen einzuräumen (z.B. Kopieren von Daten der Festplatte auf ein Diskettenlaufwerk nur in verschlüsselter Form, Zugriff nur auf genau definierte Daten und Programme). Die Anzahl der Benutzer ist unbegrenzt. Programme zum Kodieren bzw. Dekodieren von Dateien werden vom Hersteller angeboten. Alle Betriebssystemkommandos werden in einer Logdatei protokolliert. Auf Wunsch ist ein physikalisches Löschen von Ursprungsdateien möglich wenn der Kodiervorgang abgeschlossen ist.

Nach ordnungsgemäßem LOG-ON eines berechtigten Benutzers hat das Datenschutzprogramm keine negativen Auswirkungen auf das Systemverhalten (Performance). Es kann vor allem aber auch so installiert werden, daß Benutzer, die keinen Zugang zur Betriebssystemebene haben sollen (Menuetechnik), weiterhin von dieser ferngehalten werden und lediglich die für sie freigegebenen Programme benutzen können.

Im Gegensatz zu anderen Produkten verschlüsselt PC+SOFTLOCK nicht die Dateien, sondern setzt die Dateiattribute der Directory-Einträge auf "hidden" bzw. "system" (dies gilt nicht für Dateien die allgemein zugänglich sein müssen, z.B. den Kommandoprozessor). Die Folge ist, daß "normale" DOS-Befehle diese Dateien nicht erreichen. Die Informationen über die Zugehörigkeit von Dateien zu bestimmten Benutzern sind in einer Konfigurationsdatei gespeichert. Hat der Benutzer sich beim System angemeldet, werden die Attribute "seiner" Dateien entschlüsselt und sind somit für DOS-Befehle wieder erreichbar.

Ein Nachteil ist jedoch aufgefallen: Wird das Betriebssystem des PC von einem Diskettenlaufwerk aus geladen, so dürfte die Umgehung des PC+SOFTLOCK Schutzmechanismus für einen versierten Kenner des DOS-Betriebssystems keine unüberwindlichen Schwierigkeiten bereiten. Der Hersteller hat diese Schwachstelle offensichtlich erkannt und bietet eine technische Schnittstelle zur Installation der ELKEY-CARD (siehe oben Ziff. 4.3.3.2.) an. Mit der Kombination dieser beiden Schutzmechanismen ist eine sichere Abschottung des Gesamtsystems möglich (ab Release 2.0).

9.4.3.3.2

OCULIS

OCULIS (Copyright IBD Informations- und Beratungsdienste GmbH), kontrolliert als Programm den Zugang zur Festplatte eines PC indem es diese mit einem geheimen Paßwort versieht. Das Programm schließt immer die erste im System installierte Platte ab und setzt ein weiteres Diskettenlaufwerk voraus. Es steht z.Zt. für IMB-PC der Typen XT und AT (sowie kompatible Geräte mit dem Betriebssystem PC-DOS bzw. MS-DOS ab Release 2.x) zur Verfügung. Die auf der Festplatte gespeicherten Daten können ohne Kenntnis des Paßwortes weder gelöscht noch in irgend einer Weise manipuliert werden.

Technisch funktioniert OCULIS indem es bestimmte, zum Betrieb des PC unbedingt notwendige Informationen auf der Festplatte wie z.B. Boot-Record oder FAT derart verschlüsselt, daß das Betriebssystem die Festplatte nicht mehr "erkennt". Die Zugriffe auf die Festplatte werden beim Systemstart, der immer von einem Diskettenlaufwerk erfolgen muß, über ein besonderes Programm des Betriebssystems, den sogenannten Device-Driver, geleitet. Dieser steuert alle Systemanforderungen, die die Festplatte betreffen, und verlangt bei OCULIS ein bestimmtes Paßwort. Wird dieses identifiziert, ist die Festplatte für alle Systemanforderungen "transparent", d.h. sie sieht für alle DOS-Aufrufe so aus als wäre sie unverschlüsselt. Dies gilt auch für Befehle wie FORMAT, CHKDISK und bekannte Disk-Utilities. Nach drei Fehlversuchen verriegelt sich das System und verlangt einen erneuten Systemstart. Da das Paßwort weder auf der Startdiskette noch auf der Festplatte in unverschlüsselter Form gespeichert ist, können z.B. vergessene Paßwörter nicht mehr rekonstruiert werden. Die Folge wäre, daß die Festplatte neu formatiert werden müßte (Hard-Format). Dabei gehen sämtliche auf der Platte gespeicherten Daten verloren. Das Programm bietet darüberhinaus eine umfassende Protokollierung aller Systemaktivitäten an. So können in der Log-Datei alle DOS-Befehle, Programmaufrufe, Dateizugriffe sowie alle vom Benutzer betätigten Tasten protokolliert werden. Auf die Protokolldatei kann nur von einem besonders privilegierten Benutzer - z.B. dem behördlichen Datenschutzbeauftragten - zugegriffen werden, da ihre verschlüsselt abgespeicherten Inhalte unter einem besonderen Paßwort stehen. Die Datei kann wahlweise auf dem Bildschirm angezeigt, auf dem Drucker aufgelistet oder als Standard-ASCII-Datei bzw. als Datenbankdatei im Format dBase III ausgegeben werden. Die gesamte Protokollierung ist für den normalen Benutzer unsichtbar und kann von diesem nicht verhindert werden.

Abschließend sei bemerkt, daß es nicht gelungen ist, dieses Sicherungsmodul zu umgehen.

9.4.3.3.4

Ergebnis der Untersuchung

Keines der getesteten Programme ist ohne "Schwachstellen" und erfüllt für sich alleine alle Anforderungen. Allerdings können bestimmte Produkte wie z.B. ELKEY-CARD und PC+SOFTLOCK so kombiniert eingesetzt werden, daß sich ihre Schutzwirkungen ergänzen.

Die zahlreichen Ankündigungen neuer Produkte bzw. neuer Versionen lassen erkennen, daß die Anbieter die Mängel erkannt haben und einen Markt für diese Produkte sehen.

Ich bin der Auffassung, daß es keinen triftigen Grund mehr gibt zu behaupten, die systemimmanenten Schwächen der PC-Betriebssysteme müßten eben hingenommen werden, bestenfalls könne man ihnen durch organisatorische Maßnahmen begegnen.

Wenn die neuen technischen Möglichkeiten konsequent umgesetzt werden, läßt sich bereits jetzt folgendes erreichen:

- Das Gesamtsystem eines PC oder dessen Festplatte lassen sich wirksam gegen unbefugte Benutzung oder Zugriff mittels technischer Maßnahmen schützen.
- Der privilegierte Benutzer kann in seinen Befugnissen beschränkt und kontrolliert werden.
- Schutzbedürftige Dateien können auf der Festplatte eines PC sicher voneinander abgeschottet und verschlüsselt gespeichert werden, wenn das Gerät als Multi-User-System vorgesehen ist. Da sich der technisch realisierbare Sicherheitsstandard in diesem Bereich ständig erhöht, werde ich darauf achten, daß bei DV mit PC diese technischen Möglichkeiten, wo immer erforderlich, in vollem Umfang genutzt werden. Bereits entwickelte Anwenderverfahren, wie z.B. das DV-Verfahren "Schenkungssteuer" in den hessischen Finanzämtern zeigen, daß diese Sicherungskonzepte ohne Einschränkung des Benutzerkomforts realisierbar sind.

9.4.4

Die Anwendung des § 10 HDSG

9.4.4.1

Vorbemerkungen

Die traditionelle Art der Datenverarbeitung, bei der eine Fachabteilung der Behörde bzw. ein externes Rechenzentrum zentrale DV-Leistungen anbot, wird in immer stärkerem Maße ergänzt bzw. teilweise oder ganz verdrängt durch den Einsatz moderner Methoden der Individuellen Datenverarbeitung/Informationsverarbeitung mittels PC, Microcomputern oder auch Textverarbeitungssystemen. Die Behördenleitung - sie ist in erster Linie verantwortlich für die Zulässigkeit der Datenverarbeitung, den Schutz von Datenbeständen und Maschinen sowie die Planung und Durchführung von Maßnahmen nach § 10 HDSG - kann sich nicht mehr allein darauf verlassen, daß das jeweilige Fachrechenzentrum oder die zentrale DV-Fachabteilung aufgrund ihrer Qualifikation die notwendigen und richtigen Datenschutz- und Datensicherungsmaßnahmen ergreifen. Sie muß vielmehr in eigener Verantwortung die erforderlichen Regelungen treffen.

9.4.4.2

Die Rolle des behördlichen Datenschutzbeauftragten bei der Klärung regelungsbedürftiger Sachverhalte

Ob die Verantwortung für den Betrieb eines DV-Systems, dessen Benutzung, die Verfügungsgewalt über Daten, Programme und Verfahren in einer Hand liegen oder aufgeteilt sind, regelt sich in der Praxis meist nach der Größe der Behörde, deren Organisationsstruktur und der personellen Ausstattung. Mit Sicherheit kann aber davon ausgegangen werden, daß es eine durchgehende Funktionstrennung beim Einsatz von PC als Mittel der Individuellen DV nicht mehr gibt. Um so mehr Bedeutung kommt der Ausübung bestimmter Kontrollfunktionen zu.

Nach § 5 Absatz 2 HDSG hat die datenverarbeitende Stelle (Behörde/Dienststelle) einen Beauftragten für den Datenschutz zu bestellen. Ihm obliegt neben einer Reihe anderer Aufgaben die Überwachung der nach § 10 zu treffenden Maßnahmen des Datenschutzes und der Datensicherung. Darüber hinaus sollte er in allen Fällen beteiligt werden, wo Planungen oder Koordinierungsfragen der behördlichen Datenverarbeitung anstehen.

Dazu gehören beispielsweise:

- Festlegung von Verantwortlichkeiten für die Organisation der DV, die Beschaffung von Maschinen und Programmen sowie deren Wartung,
- Maßnahmen zur Objektsicherung/Bausicherung,
- Erstellung einer Dienstanweisung zur Individuellen Datenverarbeitung mit PC,
- Kontrolle der aus der Dienstanweisung resultierenden Maßnahmen (s. Ziff. 4.4.3),
- Regelungen über die Benutzung privater PC für dienstliche Zwecke (s. Ziff. 5.),
- Aus- und Fortbildung von Mitarbeitern in Fragen des Datenschutzes und der Datensicherung.

9.4.4.3

Was sollte in einer Dienstanweisung für die Individuelle Datenverarbeitung geregelt werden?

Klare Verhältnisse und Verantwortlichkeiten schafft eine schriftliche Dienstanweisung durch die Behörden-/Dienststellenleitung. Sie kann z.B. allgemein gültige Maßnahmen wie Verschlusspanweisungen oder Auskunftsverfahren pauschal für alle DV-Anwender im Zuständigkeitsbereich regeln und besonderen Erfordernissen durch ergänzende Einzelfallanweisungen gerecht werden. Wichtig ist jedoch, darauf zu achten, daß die Zuständigkeiten einzelner Stellen oder Personen deutlich herausgestellt werden. Nur dann ist es möglich, Verantwortlichkeiten aus Fehlern oder Versäumnissen zuzuordnen. Ist dies nicht der Fall, leidet die Bereitschaft, solche Vorschriften zu akzeptieren.

Die Erfahrungen zeigen, daß geeignete und ausreichend klar dargelegte Anweisungen in der Regel von den meisten Mitarbeitern beachtet werden. Böswillige Absichten oder fehlende Motivation dürften die Ausnahme sein. Auch beim PC-Einsatz liegt das Risiko mehr in unklaren und unvollständigen Verfahrensbeschreibungen, schlechten oder fehlenden Kontrollen, mangelnden Fachkenntnissen bzw. Überforderung von Mitarbeitern als in der Gefahr evtl. krimineller Handlungen Einzelner. Deswegen sollten Benutzer von PC z.B. so gut ausgebildet sein, daß sie den PC und dessen Peripherie bei normalen Bedingungen beherrschen, d.h. die zur Verfügung gestellten Programme, Verfahren, Wiederanlaufprotokolle und Datensicherungsläufe fehlerfrei anwenden können.

Nach den Erfahrungen aus meinen Prüfungen sollten in einer ADV-Dienstanweisung insbesondere enthalten sein:

1. Die Zuständigkeiten nach Stellen und Funktionen beispielsweise für: Planung und Organisation der ADV einschl. Textverarbeitung und Telexdienst, Anwenderberatung, Beschaffung und Wartung von DV-Geräten, Schulung der Mitarbeiter, Prüfung des DV-Einsatzes, Zusammenarbeit mit anderen Behörden/Dienststellen
2. Vorgehen bei der Einführung von ADV-Verfahren bzw. Beschaffung von ADV-Geräten z.B.: zentrale Zuständigkeit evtl. bei der Zentralabteilung der Dienststelle oder dem Organisationsamt der Kommune, Systembetreuung durch die Fachabteilung bzw. das Fachamt, Beteiligung der Personalvertretung und anderer Stellen, z.B. des behördlichen Datenschutzbeauftragten
3. Regeln für die Benutzung privater PC für dienstliche Zwecke
4. Verfahrensweise beim Einsatz von Programmen: Regeln für die Beschaffung von Standardsoftware bzw. Eigenprogrammierung, Prüfung, Freigabe und Dokumentation der Programme
5. Aufbewahrungs- und Lösungsfristen: für Datenträger auch Erfassungsbelege und Druckausgaben, Dateien, Dokumentationsunterlagen und sonstige ADV-Unterlagen
6. Maßnahmen zum Datenschutz und zur Datensicherung wie: Festlegung der Verantwortlichkeiten nach dem HDSG und Verfahrensweisen für (Benachrichtigung des HDSB bei Auftrags-DV - § 4, Dateibeschriftung und Geräteverzeichnis - § 6, Prüfung der Zulässigkeit der DV - § 7, Unterrichtung der Mitarbeiter - § 9, Datenübermittlungen - §§ 14-17, Auskunftserteilung - § 18, Berichtigung, Sperrung und Löschung - § 19, Registermeldung - § 26) z.B. Fachamt/Fachabteilung unter Beteiligung des behördlichen Datenschutzbeauftragten
Festlegung der Verantwortlichen (Stellen/Funktionen) für Maßnahmen nach § 10 HDSG : insbesondere Zugangskontrolle, Datenträgerkontrolle, Speicherkontrolle, Benutzerkontrolle wenn PC-Netzbetrieb, Zugriffskontrolle bei Mehrplatzsystemen oder zentraler Datenhaltung auf einer gemeinsamen Festplatte, Eingabekontrolle, Transportkontrolle
Anordnung von Einzelmaßnahmen nach § 10 HDSG unter Beachtung der Gegebenheiten in der unmittelbaren Umgebung des PC und deren praxisnaher Umsetzung wie z.B.: Objektsicherung durch Verschlusangaben für Räume, Geräte und Datenträger und sonstige DV-Unterlagen während und außerhalb der Dienststunden. Bei auch nur kurzfristiger Abwesenheit vom Arbeitsplatz Verpflichtung zum Log-Off, Bildschirm löschen und Tastaturschloß betätigen. Regeln für die Abgabe von Datenträgern wie Disketten, Bandkassetten, Listen u.a. Führung von Verzeichnissen (manuell oder maschinell) für Maschinen, Datenträger. Anfertigung von Protokollen für Besucher, Wartungsdienste, Zugriffe auf Verfahren, Programme und Dateien. Regelungen zur Anfertigung von Sicherungskopien (System-Back-Up und Dateisicherung) und deren Aufbewahrung oder soweit notwendig Auslagerung
Einrichtung von Benutzerkennungen und Transaktionscodes, d.h. Beschränkungen durch definierte und geschützte Bildschirmmasken (Menütechnik)
Regelungen für die Datenfernverarbeitung: Soweit PC untereinander vernetzt oder an einen Host-Rechner angeschlossen sind, muß das Verfahren bei Datenfernübertragung vom PC zum Host und umgekehrt, der PC untereinander und des File-Transfers geregelt werden. Besonderer Beachtung bedarf der Zugang zu "offenen" Netzen mittels Akustikkoppler und der Einsatz von Wählverbindungen
Paßwortverfahren für alle Arten der Zugriffsberechtigung: Regelungen für die Vergabe und Änderung von Paßwörtern, deren Mitteilung an die Benutzer, Pflicht zur Geheimhaltung, Verbot trivialer und leicht zu erratender Paßwörter wie Geburtstage, Namen, 4711, 0815 oder 1234 usw.
Notfallplanung gegen Unterbrechungen des Dienstbetriebes: z.B. Aufrechterhaltung des Publikumsverkehrs bei längerem Ausfall von Geräten durch Defekte oder Stromausfall über Reparatur- bzw. Notdienstanweisungen, Anweisungen für die Beschaffung von Ersatzgeräten, Einsatz von Sicherungsdateien, Notstromversorgung
Regelungen für die Anforderung von Auswertungen aus DV-Verfahren: Beteiligte und Vorgehensweise bei regelmäßigen Auswertungen und bei Sonderauswertungen sind festzulegen
7. Behördlicher Datenschutzbeauftragter: Name, Tel., Befugnisse, Unterstellung, Berichtspflicht an ihn und durch ihn, Hinweis, daß sich jeder Mitarbeiter ohne Einhaltung des Dienstweges an ihn wenden kann

9.5

Nutzung privater Personal-Computer für dienstliche Zwecke

Die starke Verbreitung der PC in privaten Haushalten führt u.a. dazu, daß diese Geräte in verstärktem Maße auch zu dienstlichen Zwecken herangezogen werden. Der Landesautomationsausschuß (LAA) hat diese Entwicklung zum Anlaß genommen, über eine Anzeigepflicht dieser besonderen Art der Datenverarbeitung zu eraten (Beschlüßvorschlag LAA Nr. 140-9). Ich habe dem LAA daraufhin vorgeschlagen, eine Genehmigungspflicht anzustreben. Der letztlich gefaßte Beschluß enthielt dann auch die Empfehlung einer Anzeige- oder Genehmigungspflicht gegenüber bzw. durch die Dienststelle (Beschlüß LAA Nr. 141-9).

Auch wenn bisher schon in bestimmten Bereichen der öffentlichen Verwaltung private Büromaschinen wie z.B. Taschenrechner, Tischrechner oder elektronische Speicherschreibmaschinen genutzt wurden, lassen die geschilderten Möglichkeiten der Datenverarbeitung mittels PC und die zu erwartenden Probleme keine analoge Übernahme dieser praktizierten Verfahrensweise zu. Ich empfehle deshalb, die dienstliche Nutzung privater PC restriktiv unter Beachtung folgender Kriterien zu handhaben:

9.5.1

Verarbeitung dienstlicher Daten auf privaten PC in Privaträumen

Die Verarbeitung dienstlicher personenbezogener Daten auf privaten PC in Privaträumen/zu Hause ist grundsätzlich zu untersagen.

Eine denkbare Ausnahme bilden bestimmte Berufsgruppen wie z.B. Lehrer, Richter oder auch Gerichtsvollzieher. Diese leisten aufgrund beamtenrechtlicher oder dienstrechtlicher Vorschriften einen Teil ihrer Arbeitszeit zu Hause ab. Teilweise verfügen sie auch nicht über dienstlich gestellte Arbeitsräume. Der Dienstherr oder die Dienststelle können in solchen Fällen, unter sorgfältiger Abwägung aller Gefährdungskriterien, eine Genehmigung zur Verarbeitung dienstlicher Daten auf einem privaten PC erteilen.

9.5.2

Verarbeitung dienstlicher Daten auf privaten PC in Diensträumen

Grundsätzlich sollte angestrebt werden, daß zur Erfüllung dienstlicher Aufgaben erforderliche Büromaschinen auch mit dienstlichen Mitteln beschafft werden. Ist dies in besonderen Einzelfällen (vorübergehend) nicht möglich, kann nach sorgfältiger Prüfung die Nutzung eines privaten PC genehmigt werden.

9.5.3

Regularien der Genehmigung

Bei der Genehmigung sollte der Dienstherr oder die Dienststelle insbesondere auf folgende Punkte achten:

- Zu prüfen ist, ob die Verarbeitung besonders sensibler Daten wie z.B. aus dem Sicherheitsbereich, Gesundheitsdaten, Daten aus Personalakten u.ä. auf privaten PC u.U. nicht untersagt werden muß.
- Eine Datei, die bisher manuell geführt wurde, darf nicht nur deswegen automatisiert und auf einem privaten PC verarbeitet werden, weil dieser durch einen Mitarbeiter zur Verfügung gestellt wird. Es muß vielmehr ein dienstlicher Bedarf an der automatisierten Verarbeitung bestehen.
- Die Nutzung des privaten PC unterliegt den gleichen gesetzlichen Regelungen und dienstlichen Vorschriften wie der Einsatz dienstlicher DV-Geräte (z.B. HDSG, bereichsspezifische Vorschriften wie SGB X, beamtenrechtliche Vorschriften der Vertraulichkeit bzw. Geheimhaltung dienstlicher Vorgänge u.ä.). Dazu gehört auch die Duldung von Kontrollen z.B. durch die Dienststelle.
- Der Umfang der zu genehmigenden Datenverarbeitung sollte genau festgelegt werden (Daten, Programme, Zweck der Verarbeitung).
- Der Bedienstete hat sicherzustellen, daß nur er allein in den Privaträumen Zugriff auf dienstliche Daten und Programme hat.
- Der Verbleib von Ausdrucken und Datenträgern, dazu gehören auch Fehldrucke, Testlisten, Programmausdrucke und defekte Disketten, sollte geregelt werden.
- Der Bedienstete sollte eine allgemeinverständliche Verfahrens- und soweit erforderlich Programmdokumentation in der Dienststelle hinterlegen.

- Es ist zu prüfen, ob eine aktuelle Sicherungskopie (Back-Up) der dienstlichen Daten und Programme in der Dienststelle aufbewahrt werden muß.
- Das öffentliche Eigentum an Daten und Programmen sowie haftungsrechtliche Fragen bleiben von diesen datenschutzrechtlichen Regelungen unberührt.

10. Recht auf Information/“Freedom of Information“

Im 14. Tätigkeitsbericht (Ziff. 11) ist ausführlich auf verschiedene Versuche zur Regelung eines Rechts auf Information eingegangen worden. Seither haben sich neue Entwicklungen ergeben; auf einige wird im folgenden kurz hingewiesen:

10.1

Europarat

Am 3. Juli 1986 hat die Parlamentarische Versammlung des Europarats in ihrer Empfehlung 1037 (1986) über Datenschutz und Informationsfreiheit festgestellt, daß das gleichzeitige Bestehen von Gesetzen über Informationsfreiheit und über Datenschutz insbesondere dort zu Konflikten führen kann, wo diese Gesetze getrennt von verschiedenen Organen und unter verschiedenen Kriterien angewendet werden. Die Parlamentarische Versammlung hat gleichzeitig dem Ministerrat empfohlen, den Sachverständigenausschuß für Datenschutz zu ersuchen, Kriterien und Grundsätze zu erarbeiten, nach denen Datenschutz und Zugang zu Informationen der öffentlichen Verwaltung miteinander vereinbart werden können sowie entsprechende rechtliche Regelungen vorzubereiten.

10.2

Griechenland

Im vergangenen Jahr sind in Griechenland durch das Gesetz über das Verhältnis des Staates zum Bürger und die Einführung eines neuen Ausweises (Nr. 1599) dem Bürger erstmalig Informationsrechte gegenüber der Verwaltung garantiert worden (Gesetzblatt 1986 Nr. 75 vom 11. Juni 1986).

Art. 16 des Gesetzes regelt, daß mit bestimmten Ausnahmen jeder Bürger das Recht hat, von den Unterlagen der öffentlichen Verwaltung Kenntnis zu erhalten, es sei denn, sie beziehen sich auf das Privat- oder das Familienleben Dritter. Als Verwaltungsunterlagen werden alle Unterlagen angesehen, die von öffentlichen Stellen verfaßt werden, wozu insbesondere Stellungnahmen, Studien, Protokolle, statistische Daten, Verwaltungsvorschriften, Antworten der öffentlichen Verwaltung, Gutachten und Entscheidungen gezählt werden.

Die Unterlagen können entweder eingesehen werden, oder es können Abschriften verlangt werden.

Die öffentlichen Stellen können die Akteneinsicht verweigern, wenn:

- die Geheimhaltung der Kabinettsitzungen und Sitzungen anderer Regierungsorgane, die Geheimhaltung von Maßnahmen der nationalen Verteidigung und der Außenpolitik, von Maßnahmen der Währungspolitik, der Sicherheit des Staates und der öffentlichen Ordnung, das Arzt-, Geschäfts-, Bank- und jedes andere gesetzliche Geheimnis gefährdet sind;
- die Aufklärung von Verbrechen oder Ordnungswidrigkeiten gefährdet ist.

Die öffentlichen Stellen dürfen Einsichtsverlangen nicht den Schutz des Privatlebens und das Arzt- oder Geschäftsgeheimnis entgegenhalten, soweit sich dies ausschließlich auf den Antragsteller bezieht. Informationen medizinischer Art dürfen dem Betroffenen nur über einen von ihm bestimmten Arzt mitgeteilt werden.

10.3

Norwegen

In Norwegen, dessen "Gesetz über die Öffentlichkeit in der Verwaltung" seit 1971 in Kraft und im Jahre 1982 novelliert worden ist, zeichnet sich eine ähnliche Entwicklung ab wie in den USA: die kommerzielle Ausbeutung öffentlicher Akten und Datenverarbeitungssysteme. Die Norwegische Dateninspektion hat sich in ihrem Jahresbericht für 1985 bereits mit dem Thema beschäftigt (Comp. Lex 5/86, Norwegian University Press p. 17-18). Sie hält eine einschränkende Praxis der Behörden für ratsam.

Was das Zusammenwirken zwischen Datenschutz und Informationsfreiheit anbetrifft, so scheinen auch hier - ähnlich wie in Frankreich (s. dort) - Abgrenzungsschwierigkeiten und Unklarheiten zu bestehen: Wie aus einer Mitteilung des "Norwegischen Forschungszentrums für Computer und Recht" an der Universität Oslo auf meine Anfrage hervorgeht, "ergeben sich die Rechte des einzelnen wie die Teile eines Puzzle-Spiels, da die beiden Gesetze in ziemlich komplizierter Weise miteinander verflochten sind" (Brief vom 1.12.1986).

10.4

Kanada

Die Bundesbeauftragte für Informationsrecht (Federal Information Commissioner) für Kanada betont in einem Bericht nach dreijähriger Tätigkeit ihrer Dienststelle, daß wichtige Rechte und Grundsätze des Gesetzes über den Zugang zu Akten der kanadischen Öffentlichkeit nicht bekannt seien (Transnational Data und Communications Report, Sept. 1986, Seite 11). Sie führt dies zum Teil auf die kurze Geltungsdauer des Gesetzes zurück. Außerdem ist sie der Ansicht, das Konzept der transparenten Verwaltung könne nicht erreicht werden, ohne daß die Regierung die Bürger bald und intensiv über ihre Informationsrechte unterrichtet.

35 % der bei der Beauftragten für Informationsrecht eingelegten Bürgerbeschwerden wegen verweigerter Akteneinsicht hielt die Beauftragte für ganz oder teilweise begründet; die Hälfte davon konnte sie mit den betroffenen Behörden einvernehmlich lösen. In 15 % der Fälle war ein Bericht an den zuständigen Ressortminister notwendig; dabei handelte es sich überwiegend um Beschwerden wegen zu später oder verzögerter Gewährung von Akteneinsicht.

10.5

Frankreich

Die Erfahrungen auf dem Gebiet von Information und Bürgerfreiheit ("Informatique et Liberts") sind durch die im Vergleich zu den angelsächsischen und zu den skandinavischen Ländern größere Ähnlichkeit der französischen mit der deutschen Rechtstradition, insbesondere auf dem Gebiet des öffentlichen Rechts, von besonderem Interesse.

Anstelle einer Reihe von Einzelerfahrungen soll hier eine Entscheidung des Conseil d'Etat (in seiner Funktion als oberstes Verfassungs- und Verwaltungsgericht) betrachtet werden, die am 19.05.1983 ergangen ist (vgl. Recueil Dalloz Sirey-1983 Nr. 38 vom 17.11.1983, S. 546 ff.): Aufgrund der Beschwerde eines Bürgers aus Lyon gegen eine vom Verteidigungsminister verweigerte Einsicht in die Akten regionaler Gendarmeriebehörden hatte sich der Conseil d'Etat ausführlich mit der Abgrenzung von Bestimmungen des Datenschutzgesetzes vom 6. Januar 1978 und des Gesetzes über Informationsfreiheit vom 17. Juli 1978 auseinanderzusetzen. Wie aus einer wissenschaftlichen Anmerkung zu der Entscheidung (a.a.O. S. 547 ff.) hervorgeht, hat die in beiden Gesetzen verwendete verschiedene Terminologie zu schwierigen Auslegungsproblemen geführt, die zu Kompetenzkonflikten führten.

Um dieses Problem zu lösen, werden von den Kommentatoren verschiedene Möglichkeiten erwogen, durch Novellierung der beiden Gesetze eine klarere Abgrenzung zu erreichen: Beispielsweise könne man der Kontrolle der Datenschutzkommission alle personenbezogenen Daten, der Kontrolle der Kommission für Informationsfreiheit alle Akten ohne solche unterwerfen. Eine andere Möglichkeit sei es, die automatisierte Datenverarbeitung der Datenschutzkommission, die manuelle (Akten) der Kommission für Informationsfreiheit zuzuweisen. Beide Überlegungen werden als nicht praktikabel verworfen. Die Kommentatoren kommen zu dem Schluß, daß nur eine umfassendere Perspektive eine realistische und vernünftige Lösung der Weiterentwicklung des Informationsrechts bringen kann: "Die Fusion beider Kommissionen in eine einzige Institution" (a.a.O. S. 549).

Professor Maisl, seit mehreren Jahren sowohl Mitglied der Datenschutzkommission als auch der Kommission für Informationsfreiheit, erklärte mir in einem Schreiben vom 9. Oktober 1986 auf meine Anfrage: "Es gibt in der Tat Probleme der Koordination der beiden Gesetze, des Gesetzes über Datenschutz und des Gesetzes über Aktenzugang wie auch auf dem Gebiet der Kompetenz beider Kommissionen.... Hinsichtlich einer einzigen Kommission glaube ich, daß dies tatsächlich eine logische Problemlösung ist unter der Bedingung der Vereinheitlichung der Gesetzgebung."

An den geschilderten Beispielen wird wiederum erkennbar, was bereits im letzten Tätigkeitsbericht festgestellt worden ist: daß einerseits die Regelung des Rechts auf Information notwendig ist, andererseits, um Konflikte zu vermeiden, eine sorgfältige Abstimmung mit den Datenschutzgesetzen erforderlich ist. Datenschutz und Recht auf Information lassen sich nicht voneinander trennen, wie etwa die Datenverarbeitung zu wissenschaftlichen Zwecken deutlich zeigt.

11. Bilanz

11.1

Beschlüsse des Landtags zum 14. Tätigkeitsbericht

Die Arbeitsgruppe "Datenschutz und Datenverarbeitung" des Innenausschusses des Hessischen Landtags hat auf ihrer Sitzung vom 10. Juni 1986 den 14. Tätigkeitsbericht diskutiert und dem Innenausschuß Beschlussempfehlungen vorgeschlagen, die dieser auf seiner Sitzung vom 18. Juni 1986 als Beschlussempfehlungen an das Plenum des Parlaments verabschiedet hat. Der Landtag hat den Beschlussempfehlungen des Innenausschusses (Drucks. 11/6231) in seiner Sitzung vom 19. Juni 1986 zugestimmt (Protokoll der 84. Plenarsitzung vom 19. Juni 1986, S. 4979). In der nachfolgenden Zusammenstellung sind nur die Beschlüsse des Landtags berücksichtigt, die nicht in einzelnen Beiträgen dieses Berichts behandelt werden.

11.1.1

Zu Ziff. 3.2 "Prüfung des Rechenzentrums des AOK-Landesverbands"

Mit seinem Beschluß Nr. 3 zum 14. Tätigkeitsbericht hatte sich der Landtag meiner Kritik an der Praxis der kassenübergreifenden Datenzugriffe im derzeitigen DV-System der Ortskrankenkassen angeschlossen. Außerdem hatte er die Landesregierung und mich gebeten, ihm über den Stand der Beseitigung der beanstandeten Mängel in diesem Verfahren IDVS II (Informations- und Datenverarbeitungssystem der Ortskrankenkassen) zu berichten.

Hintergrund meiner im letzten Tätigkeitsbericht geäußerten Kritik waren meine Feststellungen anlässlich eines Kontrollbesuchs im Rechenzentrum des Landesverbands der Ortskrankenkassen über die weitreichenden Möglichkeiten, Mitglieds- und Leistungsdaten der Versicherten anderer Ortskrankenkassen ohne Prüfung der Erforderlichkeit im Einzelfall abzurufen.

Ein erstes wichtiges Ergebnis wurde 1986 erzielt: Der AOK-Landesverband hat mir mitgeteilt, der kassenübergreifende Zugriff bei Leistungsdaten sei völlig abgestellt worden. Für das Auskunftsverfahren im Bereich der Mitgliederbestandsdaten verweist der Landesverband auf vorliegende Arbeitsergebnisse einer Expertengruppe, die im ersten Halbjahr 1987 in Form von Änderungen der Bildschirmmasken realisiert werden sollen. Spätestens dann werde ich bei einer DV-technischen Nachkontrolle den erreichten Stand der Abschottung und Zugriffssicherung überprüfen.

Am unbefriedigendsten sind die Resultate bei der Umsetzung der Forderung des § 84 SGB X, nicht mehr benötigte Versichertendaten zu löschen, wenn dem nicht schutzwürdige Belange der Betroffenen entgegenstehen. Das IDVS II sieht derzeit keine Sperrung oder Löschung vor. Zu diesem Punkt hat sich der AOK-Landesverband jedoch trotz mehrmaliger Anmahnung damit begnügt, auf die Schwierigkeit des Problems und auf demnächst beginnende Arbeiten im Rahmen des AOK-Bundesverbands zu verweisen. Termine für konkrete Realisierungsschritte wurden nicht genannt. Die Lösung dieser Frage duldet jedoch keinen Aufschub: Sechs Jahre nach Inkrafttreten des SGB X und über ein Jahr nach Formulierung meiner Beanstandung ist es nicht hinnehmbar, daß die Überprüfung der einzelnen gespeicherten Datenkategorien auf die gesetzlich oder aufgabenbedingt notwendige Speicherdauer noch immer nicht weitergekommen ist.

Mit dem Hessischen Sozialminister habe ich in dieser Angelegenheit laufend Kontakt gehalten und ihn über meine Schritte und die Reaktionen des Landesverbands jeweils informiert.

11.1.2

Zu Ziff. 3.3 "Basisdokumentation Psychiatrie (BADO) des Landeswohlfahrtsverbandes Hessen"

Die psychiatrische Basisdokumentation hat zum Ziel, über die Nutzung verschiedener Einrichtungen durch Patienten zu informieren. Die Daten sollen darüber Auskunft geben, welche Patienten in welche stationäre Behandlung gelangen, wie sie dort hinkommen, und wohin sie entlassen werden. In meinem 14. Tätigkeitsbericht habe ich ausführlich über den Stand der Diskussion um die psychiatrische Basisdokumentation berichtet. Als Ergebnis meines zweiten Kontrollbesuchs im Landeswohlfahrtsverband im Oktober 1985 hatte ich insbesondere festgestellt, daß die von den psychiatrischen Krankenhäusern erfaßten und an den Landeswohlfahrtsverband zur Auswertung weitergegebenen BADO-Daten nicht hinreichend anonymisiert sind. Die von mir festgestellten Mängel hatte ich beanstandet. Außerdem hatte ich darauf hingewiesen, daß eine Freigabe der Auswertungsprogramme für die BADO-Daten so lange nicht in Betracht kommt, wie nicht die von mir vorgeschlagenen Maßnahmen durchgeführt worden sind.

In seinem Beschluß Nr. 4 hat der Landtag anlässlich der Beratung meines 14. Tätigkeitsberichtes hierzu festgestellt:

"Der Landtag geht davon aus, daß die im 14. Tätigkeitsbericht des Datenschutzbeauftragten geäußerten Bedenken zur Basisdokumentation Psychiatrie (BADO) des Landeswohlfahrtsverbandes bis spätestens Ende 1986 ausge-

räumt werden. Andernfalls ist die unveränderte Weiterführung von BADO nicht möglich. Dem Landtag ist rechtzeitig ein ergänzender Bericht darüber zu erstatten.“

Seit dem letzten Jahr sind vom Landeswohlfahrtsverband und vom Sozialminister erhebliche Anstrengungen unternommen worden, um den Anforderungen des Datenschutzes bei der Basisdokumentation Psychiatrie Rechnung zu tragen. Ein Teil der von mir aufgezeigten Probleme konnte auch zwischenzeitlich gelöst werden. Positiv ist überdies zu vermerken, daß der Landeswohlfahrtsverband nunmehr einen Datenschutzbeauftragten bestellt hat. Leider ist jedoch ein Teil der Probleme nach wie vor nicht gelöst. Gegen eine Freigabe der Auswertungsprogramme für die BADO-Daten habe ich daher nach wie vor Bedenken.

Im August hat mir der Landeswohlfahrtsverband nunmehr - wie von mir 1985 gefordert - eine aktuelle Verfahrensbeschreibung (Stand: 14.08.1986) für die Basisdokumentation übersandt. Diese Verfahrensbeschreibung hat eine Vielzahl von Fragen aufgeworfen bzw. offengelassen. Im Anschluß an meine schriftliche Stellungnahme sind diese Fragen dann mündlich zwischen dem Landeswohlfahrtsverband, dem Hessischen Sozialminister und mir eingehend erörtert worden. Bei diesem Gespräch hat der Landeswohlfahrtsverband ergänzende Unterlagen vorgelegt. Aufgrund des Gespräches hat der Landeswohlfahrtsverband dann eine neue Verfahrensdokumentation (Stand: 31.10.1986) sowie den Entwurf einer neuen Arbeitsanweisung (ebenfalls Stand: 31.10.1986) vorgelegt. Ausgehend von diesen neuen Unterlagen habe ich dem Landeswohlfahrtsverband und dem Sozialminister Ende November 1986 eine erneute Stellungnahme übersandt, in der ich die Punkte aufgelistet habe, die aus datenschutzrechtlicher Sicht noch geklärt bzw. realisiert werden müssen.

Der neuen Verfahrensbeschreibung zufolge soll die Erfassung der BADO-Daten künftig im ärztlichen Bereich der psychiatrischen Krankenhäuser mit Hilfe von Personal Computern erfolgen. Die psychiatrischen Krankenhäuser sollen jeweils statistische Auswertungen für den Landeswohlfahrtsverband erstellen und diese dann mit Hilfe von Datenträgern an den Landeswohlfahrtsverband übermitteln. Im Landeswohlfahrtsverband sollen die Auswertungen aller psychiatrischen Krankenhäuser zentral erfaßt und ausgewertet werden. Was die Verarbeitung der BADO-Daten in den psychiatrischen Krankenhäusern anbelangt, so habe ich gegen die nunmehr vorgesehene neue Verfahrensweise keine Bedenken, sofern eine Reihe konkreter, insbesondere die Datensicherheit betreffender Maßnahmen realisiert wird und ferner sichergestellt wird, daß die psychiatrischen Krankenhäuser als speichernde Stelle für die BADO-Daten über eine ausreichende Kontrollmöglichkeit bei der Verarbeitung und Übermittlung ihrer Daten an den Landeswohlfahrtsverband verfügen. Sofern die psychiatrischen Krankenhäuser nicht aufgrund einer Ausgabedatenbeschreibung vom Landeswohlfahrtsverband, die die an den Landeswohlfahrtsverband zu übermittelnden Daten beschreibt, selbst programmieren, muß ihnen eine vollständige Kontrolle der eingesetzten Programme und der erzeugten Ausgabedaten möglich sein und sie müssen diese Kontrolle auch tatsächlich und effektiv ausüben.

Zentral ist nach wie vor die Frage, wie eine ausreichende Anonymisierung der von den psychiatrischen Krankenhäusern an den Landeswohlfahrtsverband zu übermittelnden Daten und damit auch die Wahrung der ärztlichen Schweigepflicht sichergestellt werden kann. Es steht außer Frage, daß es sich bei den BADO-Daten um ganz besonders sensible Daten handelt. Das Verfahren muß 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). Im Grundsatz besteht hierüber auch Konsens, die konkrete Ausgestaltung des Verfahrens ist jedoch auch in diesem Jahr mehrfach Gegenstand kontroverser Diskussionen gewesen. Dabei ging es vor allem um das Problem kleiner Feldbesetzungen in den geplanten BADO-Auswertungen, die grundsätzlich die Möglichkeit einer Identifizierung der Patienten eröffnen. Ich halte es in jedem Fall für ganz unerläßlich, sicherzustellen, daß keine Weitergabe von BADO-Auswertungen an Stellen außerhalb der psychiatrischen Krankenhäuser bzw. des Landeswohlfahrtsverbandes erfolgt, in denen kleine Feldbesetzungen vorhanden und Patienten daher prinzipiell bestimmbar sind. Ferner geht es um das Problem einer präzisen Begrenzung der Dauer der Speicherung der BADO-Daten im Landeswohlfahrtsverband sowie um eine Verbesserung der Datensicherheit in seinem Rechenzentrum.

Der Landeswohlfahrtsverband hat mir im Dezember mitgeteilt, daß er den in meiner Stellungnahme aufgelisteten Forderungen Rechnung tragen will. Einzelheiten hierzu sind mir bisher nicht bekannt.

11.1.3

Zu Ziff. 4.1.1 "Demonstrationsanmeldung - Datenübermittlung"

Im Rahmen der Beratung meines 14. Tätigkeitsberichts hat der Landtag die Landesregierung gebeten, "gegenüber dem Landtag und dem Datenschutzbeauftragten anhand von Beispielen zu konkretisieren, in welchen Fällen Erkenntnisfragen im Vorfeld von Demonstrationen und wann die Übermittlung personenbezogener Daten im Rahmen von WE-Mitteilungen der Polizei zulässig sein sollen". Gleichzeitig hat mich der Landtag aufgefordert, im Rahmen meines 15. Tätigkeitsberichts zu den aufgeworfenen Fragen Stellung zu nehmen (vgl. Beschluß Nr. 5).

Im Laufe des vergangenen Jahres habe ich den Hessischen Minister des Innern mehrfach aufgefordert, mir seinen Bericht zur Stellungnahme vorzulegen. Der dem Landtag und mir erst vor kurzem zugesandte Bericht konnte noch nicht gründlich ausgewertet werden, so daß ich meine Stellungnahme zu einem späteren Zeitpunkt vorlegen werde.

11.1.4

Zu Ziff. 4.2 "Zweckwidrige Auswertung von Protokoll Daten"

In meinem 14. Tätigkeitsbericht hatte ich - wie zuvor schon in meinem 12. und 13. Tätigkeitsbericht (Ziff. 3.1.4 bzw. 4.1.5) - dargelegt, daß Protokollierungen von Verarbeitungsvorgängen bei der automatisierten Datenverarbeitung für Kontroll- und Sicherungszwecke erforderlich sind, die Protokoll Daten aber nur zu diesen Zwecken und nicht etwa für die Erfüllung polizeilicher Aufgaben der Gefahrenabwehr oder Strafverfolgung verwendet werden dürfen. Die Landesregierung hat dem in ihrer Stellungnahme zu meinem 14. Tätigkeitsbericht zugestimmt (Drucks. 11/6120, S. 13). Auch der Landtag hat sich in seinem Beschluß Nr. 6 zu meinem 14. Tätigkeitsbericht dieser Auffassung angeschlossen.

Leider mußte ich jedoch auch in diesem Jahr feststellen, daß einzelne Staatsanwaltschaften und Gerichte den Grundsatz der Zweckbindung für Protokoll Daten nicht anerkennen. In mindestens zwei Fällen haben außerhessische Staatsanwaltschaften das Hessische Landeskriminalamt aufgefordert, ihnen für Ermittlungsverfahren auf Protokollbändern gespeicherte Daten zur Verfügung zu stellen. Im ersten Fall hat das Landeskriminalamt auf Anweisung des Hessischen Ministers des Innern eine Herausgabe zunächst verweigert und gegen den daraufhin erfolgten Beschlagnahmebeschluß des Amtsgerichts Wiesbaden Beschwerde eingelegt, die jedoch vom Landgericht Wiesbaden zurückgewiesen wurde. Obwohl in der Beschwerde sowohl auf die in meinem Tätigkeitsbericht dargelegten Gründe wie auch auf die zustimmende Auffassung des Landtags hingewiesen wurde, hat das Landgericht mit keinem Wort die Problematik aufgegriffen. In einem zweiten Fall hat sich das Landeskriminalamt aufgrund der vorangegangenen Erfahrung einem Beschlagnahmebeschluß des Amtsgerichts beugt.

Der Hessische Minister der Justiz, der an der Stellungnahme der Landesregierung zu meinem Tätigkeitsbericht beteiligt war, erklärte mir in der Zwischenzeit, er sähe die Rechtslage ebenso wie die Staatsanwaltschaften bzw. Gerichte. Ohne eine ausdrückliche Änderung der Strafprozeßordnung sei es den Staatsanwaltschaften unbenommen, gem. § 161 StPO auch auf Protokoll Daten zuzugreifen. Damit zeichnen sich für eine Lösung des Problems drei Wege ab:

- Eine vorläufige Teillösung beinhaltet meine Vereinbarung mit dem Hessischen Minister des Innern, wonach der Umfang der Protokoll Daten insbesondere bei Abfragetransaktionen soweit wie möglich eingeschränkt wird. Die Möglichkeit einer umfassenden Protokollierung bleibt zwar erhalten, und auf Wunsch des Datenschutzbeauftragten kann eine solche im Einzelfall und zeitlich begrenzt auch erfolgen; in der Regel wird jedoch die Speicherung von Protokoll Daten auf das systembedingt Notwendige beschränkt. Dies gilt sowohl für die Abfrage des polizeilichen Informationssystems HEPOLIS, als auch für die polizeilichen Zugriffe auf Kraftfahrzeugzulassungs- und Meldedaten.
- Der Grundsatz der Zweckbindung für Protokoll Daten ist nun ausdrücklich in dem ab dem 1. Januar 1987 geltenden Hessischen Datenschutzgesetz (§ 13 Abs. 5) verankert: "Personenbezogene Daten, die ausschließlich zu Zwecken der Datenschutzkontrolle, der Datensicherung oder zur Sicherstellung des ordnungsgemäßen Betriebs einer Datenverarbeitungsanlage gespeichert werden, dürfen nicht für andere Zwecke verwendet werden". Da jedoch das Hessische Datenschutzgesetz als Landesgesetz die Strafprozeßordnung als Bundesgesetz nicht einschränken kann und die erwähnten Zugriffe der Staatsanwaltschaften sich auf dieses Bundesgesetz stützen, ist zu befürchten, daß diese Vorschrift auf die Praxis der Staatsanwaltschaften keine direkte Auswirkung haben wird.
- Langfristig kann damit lediglich der auch im Beschluß des Landtags zu meinem 14. Tätigkeitsbericht unterstützte Weg zum Erfolg führen: Die Landesregierung sollte ihre Bemühungen intensivieren, durch eine Änderung der Strafprozeßordnung eine gerichtliche Beschlagnahme von Protokoll Daten auszuschließen.

11.1.5

Zu Ziff. 13.2.1 "Studentendaten"

Zum wiederholten Mal muß ich in einem Tätigkeitsbericht auf das immer noch bestehende Regelungsdefizit bei der Verarbeitung von Studentendaten hinweisen (vgl. 13. Tätigkeitsbericht, Ziff. 2.4.2 und 14. Tätigkeitsbericht, Ziff. 13.2.1). Allerdings hat die Landesregierung, nachdem auch der Landtag anläßlich der Beratung meines 14. Tätigkeitsberichts einstimmig die Auffassung geäußert hat, "daß im Hochschulbereich Rechtsvorschriften über die konkrete Regelung der Erhebung und Verarbeitung von personenbezogenen Daten zu Verwaltungszwecken geschaffen werden sollen" (Beschluß Nr. 7), nunmehr erstmalig mit einem Vorschlag reagiert. Im November 1986 hat mir der Hessische Minister für Wissenschaft und Kunst den Entwurf einer Verordnung über das Verfahren der Immatrikulation, Rückmeldung, Beurlaubung und Exmatrikulation für Studenten an den Hochschulen des Landes Hessen zugesandt. Gleichzeitig ist der Entwurf den Hochschulen zur Stellungnahme zugegangen.

Die Verordnung aufgrund des § 36 Abs. 8 Hessisches Hochschulgesetz soll die derzeit noch getrennt nach Hochschulformen bestehenden Allgemeinen Vorschriften für die Studierenden ablösen. Eine abschließende Wertung war mir aus zeitlichen Gründen bislang nicht möglich. So viel läßt sich aber bereits feststellen: Der Entwurf kommt in einigen Vorschriften meinen Forderungen entgegen, wenn beispielsweise detailliert die Daten festgelegt werden, die bei der Immatrikulation angegeben werden müssen oder die im Studienbuch eingetragen werden dürfen. Der Zeitplan des Hessischen Ministers für Wissenschaft und Kunst für die Abgabe der Stellungnahmen durch die Hochschulen veranlaßt mich, davon auszugehen, daß es noch in diesem Jahr zu der längst fälligen gesetzlichen Regelung der Verarbeitung von Studentendaten kommen wird.

11.1.6

Zu Ziff. 8.3 "Datensicherheit in Datennetzen"

Im letzten Tätigkeitsbericht habe ich auf die Datensicherungsdefizite beim Einsatz des Synchronknotens SK 12 hingewiesen, der in großem Umfang von den Kommunalen Gebietsrechenzentren zur Datenfernverarbeitung innerhalb des öffentlichen Datennetzes genutzt wird.

Die Stellungnahme der Landesregierung (Drucks. 11/6120, S. 20) macht deutlich, daß zwar Konsens besteht über die technische Funktion des Knotens, nicht jedoch über die Wertung und die Konsequenzen, die zu ziehen sind.

Der Landtag hat daraufhin anläßlich der Beratung meines 14. Tätigkeitsberichts folgenden Beschluß gefaßt (Beschluß Nr. 9): "Die Landesregierung wird beauftragt, die vom Datenschutzbeauftragten aufgeworfenen Bedenken hinsichtlich der Datensicherheit in Datennetzen, soweit dies technisch möglich ist, auszuräumen.

Die Landesregierung wird gebeten, dem Datenschutzbeauftragten die bereits in Angriff genommenen verstärkten Sicherheitsmaßnahmen zu erläutern.

Der Datenschutzbeauftragte wird gebeten, hierzu dem Landtag gegenüber ergänzend Stellung zu nehmen."

Anfang Oktober wurde eine Arbeitsgruppe aus Vertretern des DV-Verbundes und des Hessischen Datenschutzbeauftragten gebildet, mit dem Auftrag:

- Bestandsaufnahme der im DV-Verbund eingesetzten Mehrpunktverbindungen
- differenzierte Darstellung der Gefährdungen und der daraus zu ziehenden Folgerungen
- aufzeigen der technischen Alternativen mit Kostenschätzungen
- Maßnahmenkatalog für begleitende technische und organisatorische Vorkehrungen.

Dieser Auftrag wurde inzwischen erfüllt. Über den Maßnahmenkatalog, der auf die differenzierte Darstellung des Gefährdungspotentials und die konkrete Bestandsaufnahme im DV-Verbund bezogen ist (somit also keine generelle Lösung des Problems darstellen kann und will), bestand in der Arbeitsgruppe Übereinstimmung; damit ist auf der technischen Ebene Konsens erzielbar.

Das Ergebnis dieser Arbeitsgruppe kann aber nur ein erster Schritt sein; ein zweiter muß folgen, in dem der Maßnahmenkatalog für den öffentlichen Bereich in Hessen ab sofort für verbindlich erklärt und seine Umsetzung bis zu einem bestimmten Termin in naher Zukunft zugesagt wird. Nur wenn die Maßnahmen auch umgesetzt werden, können meine Bedenken gegen den Einsatz von Schnittstellenvervielfachern ausgeräumt werden.

11.1.7

Zu Ziff. 7.1 "Telekommunikationsordnung"

Die Telekommunikationsordnung (TKO) - ausführlich: Verordnung über die Bedingungen und Gebühren für die Benutzung der Einrichtungen des Fernmeldewesens - ist nach Zustimmung des Postverwaltungsrats vom 30. Juni 1986 vom Bundespostminister am 5. November 1986 erlassen worden (BGBl. I S. 1749). Die TKO soll am 1. Januar 1988 in Kraft treten. Einen Fortschritt gegenüber der bisherigen Rechtslage ebenso wie gegenüber früheren Verordnungsentwürfen bringt die TKO insoweit, als sie die für die Postdienste geltenden, in zahlreichen Einzelverordnungen geregelten Datenschutzvorschriften übersichtlich in einem Abschnitt zusammenfaßt und damit die Transparenz und Normenklarheit für die Betreiber und Nutzer von Telediensten erheblich verbessert. Auch ist in dem endgültigen Text eine Reihe von Forderungen, die die Datenschutzbeauftragten immer wieder erhoben und in einer gemeinsamen Entschliebung vom 18. April 1986 noch einmal zusammengefaßt haben, in der neuen Verordnung berücksichtigt worden.

Andere, nicht minder wichtige Kritikpunkte, insbesondere die Forderung nach einer verschärften Zweckbindung der beim Betrieb der Postdienste anfallenden Daten, sind dagegen nicht ausgeräumt. Dazu gehören etwa

- die genaue Umschreibung der vom Teilnehmer beantragbaren "anderen Art der Verarbeitung" von Verbindungsdaten,
- die Nutzungsbeschränkung der personenbezogenen Daten auf die Zwecke der jeweils in Anspruch genommenen Dienste statt - wie es jetzt heißt - allgemein zu nicht näher definierten "Telekommunikationszwecken",
- der Ausschluß der Verbindungsdaten von jeglicher Übermittlung.

Abgesehen von diesen Einzelfragen bleiben meine verfassungs- und kompetenzrechtlichen Bedenken, die ich im letzten Tätigkeitsbericht erläutert habe, unverändert aktuell. Zum einen halte ich nach wie vor eine Rechtsverordnung nach § 14 Postverwaltungsgesetz als rechtliche Grundlage für die gesamte Struktur des künftigen Telekommunikationsnetzes nicht für ausreichend. In Anbetracht der Bedeutung, die der mit der TKO zu treffenden Entscheidung über die Ausgestaltung der Telekommunikationsdienste in der Zukunft zukommt, betrifft deren Regelungsinhalt einen solchen wesentlichen Bereich des öffentlichen Lebens, daß nur der Gesetzgeber eine derart einschneidende Entscheidung treffen könnte.

Zum anderen habe ich darüber hinaus - was das Verhältnis von Gesetz und Verordnung angeht - erhebliche Zweifel, ob die Verordnungsermächtigung des § 14 Postverwaltungsgesetz, die sich auf das "Post- und Fernmeldewesen" bezieht, schon vom Wortlaut her die beabsichtigte Entwicklung und Einführung völlig neuer Telekommunikationsdienste sowie die geplante Verbindung von Datenübermittlung, Datenverarbeitung und Massenkommunikation abzudecken vermag. In ihrer Stellungnahme zu meinem letzten Tätigkeitsbericht (Drucks. 11/6120, S. 18) hatte die Landesregierung zugesagt, der Hessische Wirtschaftsminister wolle als Vertreter des Bundesrates im Postverwaltungsrat diese grundsätzliche Frage nach einer ausreichenden gesetzlichen Grundlage für die TKO in diesem Gremium aufwerfen und ihre Prüfung durch den Bundesminister der Justiz anregen. Mir ist nicht bekannt, ob und ggf. mit welchem Ergebnis diese Begutachtung durchgeführt worden ist.

11.2

Sonstige Punkte des 14. Tätigkeitsberichts

11.2.1

Zu Ziff. 6 "Melderecht: Meldedatenübermittlungsverordnung"

Im 14. Tätigkeitsbericht habe ich mich ausführlich mit der Frage der regelmäßigen Übermittlung von Einwohnermeldedaten an verschiedene öffentliche Dienststellen des Landes Hessen beschäftigt. Die damals noch als Entwurf vorliegende Verordnung über regelmäßige Datenübermittlungen der Meldebehörden (Meldedaten-Übermittlungsverordnung - MeldDÜVO) ist am 3. Juli 1986 in Kraft getreten. Nicht alle Vorschläge aus meiner damaligen Stellungnahme sind darin berücksichtigt worden.

Kritisiert hatte ich insbesondere die geplante und nunmehr in die Verordnung aufgenommene Regelung zur Datenübermittlung an Versorgungsämter und an den Landeswohlfahrtsverband Hessen (§ 9). In meiner damaligen Stellungnahme habe ich darauf hingewiesen, daß der Datenabgleich zur Durchführung des Landesblindengesetzes und die Überprüfung jedes Wegzugs oder Todesfalles zur Überwachung der Wohngeldgewährung unverhältnismäßig sind. Im ersten Fall rechtfertigt die geringe Fallzahl - weniger als 100 Leistungsänderungen pro Jahr - die Übermittlung nicht; im zweiten sollten ebenfalls eine unverhältnismäßig große Zahl von Daten auch Nichtbeteiligter an den Empfänger - die öffentlichen Wohngeldstellen - zu Kontrollzwecken weitergegeben werden. Lediglich ein Bruchteil der Wegziehenden oder Verstorbenen bezieht jedoch tatsächlich Wohngeld. In beiden Fällen hat der Minister des Innern meine Überlegungen nicht aufgegriffen.

Bemängelt hatte ich auch die beabsichtigte Vorschrift zur Datenübermittlung an das Statistische Landesamt (§ 10). Mein Hinweis, nach § 4 des Gesetzes über die Statistik der Bevölkerungsbewegung und die Fortschreibung des Bevölkerungsstandes (i. d. F. v. 14. März 1980 - BGBl. I S. 309; geändert durch Gesetz vom 16. August 1980, BGBl. I S. 1429) dürften nur Datensätze ohne Namen, Anschriften und Geburtsdaten von zu- oder wegziehenden Personen an die Statistikbehörde weitergegeben werden, blieb ebenfalls unberücksichtigt. Der Hessische Ministerpräsident als zuständiges Ressort teilte mir zwar in seinem Schreiben vom 26. Februar 1986 mit, er teile meine Ansicht, daß die Übermittlungsverordnung keine selbständige Grundlage für Datenübermittlungen zu statistischen Zwecken sein könne. Andererseits sei die Übermittlung auch personenbezogener Daten zulässig, da diese Daten nur als "Hilfsmerkmale" verwendet würden, die der Kontrolle dienen, ohne tatsächlich gespeichert zu werden.

Demgegenüber bin ich nach wie vor der Ansicht, daß sämtliche zu übermittelnden Daten auch in der entsprechenden Rechtsgrundlage, d. h. im Statistikgesetz, ausdrücklich genannt werden müssen; anderenfalls würde der Grundsatz des Gesetzesvorbehalts und die Normentransparenz nicht ausreichend berücksichtigt werden. Die Verwendung dieser Daten als "Hilfsmerkmale" müßte auch für den Bürger erkennbar sein. Sie ist jedoch lediglich Folge einer eigenständigen Entscheidung der Landesstatistikbehörde.

Zur Regelung des Direktzugriffs der Polizei auf Meldedaten (§ 13) vgl. die Anmerkungen in Ziff. 6.1.3 und 6.1.4 dieses Berichts.

11.2.2**Zu Ziff. 13.1.6 "Hinweis- und Spurendokumentationssysteme"**

In meinen letzten vier Tätigkeitsberichten habe ich das Thema "Hinweis- und Spurendokumentationssysteme" bei der Polizei behandelt (11. Tätigkeitsbericht, Ziff. 3.2.2.4, 12. Tätigkeitsbericht, Ziff. 2.1.3.3, 13. Tätigkeitsbericht, Ziff. 4.2.1.4, 14. Tätigkeitsbericht s.o.).

Der Landtag hatte anlässlich der Beratung meines 13. Tätigkeitsberichts beschlossen: "Die Landesregierung wird gebeten, über den derzeitigen und zurückliegenden Einsatz der Systeme HIDOK und SPUDOK sowie über deren zukünftige Anwendungsbereiche aufgrund der vorgelegten Errichtungsanordnungen zu berichten" (Beschluß Nr. 6 zum 13. Tätigkeitsbericht, Drucks. 11/4696 i.V.m. Protokoll der 63. Plenarsitzung vom 14. November 1985, S. 3615).

Der Bericht des Hessischen Ministers des Innern liegt inzwischen vor. Neben einer überarbeiteten Mustererrichtungsanordnung enthält er eine Aufstellung der früheren und derzeitigen HIDOK- und SPUDOK-Dateien sowohl im Zusammenhang mit einzelnen Ermittlungsverfahren wie für den Anwendungsbereich Meldedienst. Die Mustererrichtungsanordnung weist im Vergleich zu dem früheren Modell HIDOK folgende Veränderungen auf: Bei der Rubrik Hinweisdaten - gemeint sind damit die eigentlichen Ermittlungsdaten - wurden die Unterkategorien "Beschreibung" und "Auffälligkeiten" sowie "Besonderheiten der Beobachtung", die in dieser Abstraktion keinen klaren Maßstab bilden konnten, konkretisiert. Die Unterkategorie heißt nun: "Beschreibung des Sachverhalts (einschließlich Auffälligkeiten der Person, der Institution, des Objekts oder der Sache sowie Besonderheiten der Beobachtungssituation)". Damit wird etwas deutlicher, welche Datenarten erfaßt werden sollen.

Von wesentlich größerer Bedeutung ist die Neufassung der Anweisung zur Speicherdauer. Das System der stufenweisen Bereinigung und Löschung von Daten wurde verbessert. Dies gilt zunächst insoweit, als bei den erfaßten Spuren, "deren Irrelevanz für das Ermittlungsverfahren erkannt worden ist, die Personen, gegen die sich der Tatverdacht gerichtet hatte, als unverdächtig zu kennzeichnen" sind. Darüber hinaus hat der für die Ermittlungen verantwortliche Leiter sich laufend davon zu überzeugen, daß die Hinweise zügig bearbeitet werden. Neu ist auch eine maximale Prüffrist für ihn von drei Monaten. In der früher vorgestellten Fassung war lediglich allgemein vorgesehen worden, daß "die Personalien solcher Personen als Verdächtige zu löschen sind, gegen die sich der Ursprungsverdacht nicht bestätigt hat." Das Verfahren der Überprüfung blieb unregelt.

In Weiterentwicklung des Ursprungsmodells kommt es nicht erst bei der rechtskräftigen Verurteilung aller Angeklagten oder "höchstens zehn Jahre nach dem letztmaligen Abschluß der polizeilichen Ermittlungen" zu einer Löschung, sondern bereits früher.

Der neue Vorschlag lautet:

"Nach Abschluß der polizeilichen Ermittlungen sind zu löschen

- sämtliche in der Datei gespeicherten Daten, wenn (insbesondere wegen eines geringen Datenbestandes) feststeht, daß eine DV-unterstützte Recherche überflüssig ist, andernfalls
- Daten solcher Hinweise, die ausermittelt sind und offenkundig nicht im Zusammenhang mit der aufzuklärenden Straftat stehen,
- die unbrauchbar sind, weil sie keinen Anhaltspunkt für (weitere) Ermittlungen enthalten oder
- die ausschließlich im Zusammenhang mit anderen Straftaten stehen und deshalb an die dafür zuständige Stelle abgegeben wurden."

Dieses Verfahren wurde bereits im Zusammenhang mit der hessischen SPUDOK-Datei "Attentat auf Minister Karry" praktiziert. Hier hat die Polizei ganz im Sinne meiner bereits in den früheren Tätigkeitsberichten gemachten Vorschläge einen vorläufigen Abschluß ihrer Ermittlungen festgestellt und - auch wenn eine Aufklärung des Falles nicht erzielt werden konnte - die sich als irrelevant erwiesenen Daten aus dem System ausgesondert und gelöscht.

Eine noch relativ unbefriedigende Lösung wird für die Fälle vorgeschlagen, in denen es nach Abschluß der polizeilichen Ermittlungen zu keiner rechtskräftigen Verurteilung kommt, das Verfahren jedoch aufgrund staatsanwaltschaftlicher Verfügung oder gerichtlicher Entscheidung vorzeitig oder endgültig beendet wird. Hier ist vorgesehen, daß die Datei "bis zum Ablauf der Verfolgungsverjährungsfrist aufbewahrt werden (kann)", die Daten "höchstens jedoch zehn Jahre nach dem letztmaligen Abschluß der polizeilichen Ermittlungen" zu löschen sind. Diese pauschale Regelung differenziert zu wenig nach dem Grund und dem Zusammenhang dieser Abschlußentscheidungen.

Zu den Meldediensten enthält der Bericht wie gesagt noch keine detaillierten Vorschläge. Insoweit kann ich nur auf die bereits in meinen früheren Tätigkeitsberichten erörterten Kritikpunkte hinweisen. Bereits jetzt sind jedoch einige Einschränkungen für diesen HIDOK/SPUDOK-Typ erkennbar, die als unbedingte Voraussetzung für deren Einsatz anzusehen sind:

- In der Kategorie "betroffener Personenkreis" ist eine Beschränkung auf "Tatverdächtige" und - soweit ein Tatverdächtiger in einem konkreten Ermittlungsverfahren noch nicht feststeht - vorläufig "Geschädigte" vorzunehmen. Daten von Hinweisgebern und Zeugen dürfen hier nicht gespeichert werden.
- Auch im Bereich der "Hinweisdaten" kann es nicht darum gehen, beliebig viele Daten aufzunehmen. Vielmehr muß vorher bei der Errichtung der jeweiligen Datei sowohl der Katalog der zu erfassenden Straftatbestände als auch die Art und Weise der Straftatenbegehung (Modus operandi) festgelegt werden, die als Daten eingespeichert werden. Ebenso müssen inhaltliche und räumliche Aspekte berücksichtigt werden, die sowohl die Einspeicherung von Bagatelldelikten als auch von rein örtlich relevanten Straftaten ausschließen.
- Für Anwendungen im Bereich Meldedienst ist als speichernde Stelle in jedem Fall das LKA vorzusehen. Auf diese Weise steht bei diesem besonders problematischen Dateientypus ein fachlich und rechtlich besonders qualifizierter Verantwortlicher zur Verfügung.
- Hinsichtlich der Lösungsverpflichtungen bzw. der Speicherdauer kann es bei Meldedienstdateien nur Lösungen geben, die an die individuell eingespeicherte Straftat anknüpfen, nicht aber an die Verwendung der Datei insgesamt.

In jedem Fall ist zu fordern, daß die Maßstäbe, die für die abschließend im Bereich des Hessischen Landeskriminalamts bearbeiteten Dateien (HIDOK) entwickelt wurden, auch für die Dateien Anwendung finden müssen, die im hessischen Auftrag beim Bundeskriminalamt als SPUDOK-Datei geführt werden.

11.3

Frühere Tätigkeitsberichte

11.3.1

Bildschirmtext

(13. Tätigkeitsbericht, Ziff. 3.1.1)

Die am 5. November 1986 vom Bundespostminister erlassene Telekommunikationsordnung (TKO), die am 1. Januar 1988 in Kraft treten soll (vgl. Ziff. 11.1.7 dieses Berichts), enthält in § 391 eine eigene Bestimmung über den Datenschutz im Bildschirmtextdienst. Dies ist insoweit positiv zu werten, als meiner wiederholt geäußerten Forderung, die im Staatsvertrag über den Bildschirmtext festgelegten Datenschutzvorkehrungen in das für die Post geltende Bundesrecht zu übernehmen, zumindest im Grundsatz Rechnung getragen worden ist. Allerdings bringt die neue Bestimmung nicht - wie dies auch die Landesregierung in ihrer Stellungnahme zu meinem 13. Tätigkeitsbericht (Drucks. 11/3951, S. 11) verlangt hatte - eine lückenlose Umsetzung des Art. 9 des Staatsvertrags in Bundesrecht. Der Btx-Koordinierungskreis der Bundesländer, dem für Hessen der Innenminister angehört, hatte zum Vorentwurf der TKO eine Liste aufgestellt mit Punkten, in denen der Staatsvertrag und die TKO nicht übereinstimmen (vgl. Stellungnahme der Landesregierung zu meinem 14. Tätigkeitsbericht, Drucks. 11/6120, S. 17f.). Im endgültigen TKO-Text ist nur ein Teil dieser Bestimmungen korrigiert worden.

Die Verordnung bleibt daher in einigen Punkten nach wie vor hinter den Anforderungen des Btx-Staatsvertrages zurück. Dazu nur ein Beispiel: Nach Art. 9 Abs. 3 Satz 1 Btx-Staatsvertrag soll der exakte Zeitpunkt des Abrufs von Angeboten nicht festgehalten werden, damit nicht Rückschlüsse auf das zeitbezogene Benutzerverhalten eines Teilnehmers möglich werden. Hingegen sieht § 391 Abs. 2 der TKO vor, daß bei den Vergütungsdaten auch "der Zeitpunkt der Beendigung der Verbindung zu den Endeinrichtungen des Informationsanbieters" erhoben wird. Ich gehe davon aus, daß die Landesregierung zur bundesrechtlichen Umsetzung des Art. 9 Staatsvertrag Stellung nehmen wird im Zusammenhang mit der Aufforderung des Landtags, "erneut über die Durchsetzung der Datenschutzregelungen bei Bildschirmtext zu berichten" (Beschluß Nr. 11 zum 14. Tätigkeitsbericht, Beschlußempfehlung und Bericht des Innenausschusses, Drucks. 11/6231).

11.3.2

Fernmeß- und Fernwirkdienste

(13. Tätigkeitsbericht, Ziff. 3.1.2)

Die 29. Verordnung zur Änderung der Fernmeldeordnung vom 22. Mai 1986 (BGBl. I S. 777) spricht auch den Datenschutz bei dem für das Fernmessen und Fernwirken von der Deutschen Bundespost vorgesehenen TEMEX-

Dienst an. Der hessische Gesetzgeber hat mit der Verabschiedung des Hessischen Datenschutzgesetzes vom 11. November 1986 implizit verdeutlicht, daß ihm die von der Post vorgesehenen Vorkehrungen nicht genügen. § 36 des neuen HDSG verlangt, daß diese Dienste nur betrieben werden dürfen, wenn die Einwilligung des Betroffenen vorliegt. Mit dieser Regelung auf landesgesetzlicher Ebene hat der Landtag gleichzeitig seinen Willen unterstrichen, die Regelungsbefugnis der Länder für die Nutzung der neuen Medien zumindest für den Einsatz dieser Fernmeß- und Fernwirkssysteme wahrzunehmen. In Hessen werden allerdings TEMEX-Verfahren derzeit nicht eingesetzt. Die Post befindet sich für diesen Teledienst noch im Stadium der Systemversuche.

Meinen Standpunkt habe ich auch in die Arbeit der Kommission "Telekommunikation in Hessen", die vom Hessischen Wirtschaftsminister einberufen worden ist, eingebracht. Der Bericht dieser Kommission liegt noch nicht vor; seine Vorlage ist für das Frühjahr 1987 vorgesehen. Die Arbeitsergebnisse dieser Kommission werden einen zusätzlichen Anlaß für die notwendige Debatte über einen eigenen landesrechtlichen Ordnungsrahmen für Telekommunikationsdienste bieten.

11.3.3

Übermittlung amtsärztlicher Zeugnisse an den Dienstherrn

(11. Tätigkeitsbericht, Ziff. 5.2.3, 5.2.4, 12. Tätigkeitsbericht, Ziff. 2.1.6.1, 13. Tätigkeitsbericht, Ziff. 4.2.2.1)

Die im 13. Tätigkeitsbericht (Ziff. 4.2.2.1.2) als Entwurf erwähnte "Verordnung zur Änderung der Zweiten Durchführungsverordnung zum Gesetz über die Vereinheitlichung des Gesundheitswesens" ist inzwischen ergangen (Verordnung vom 23. Mai 1986, GVBl. I S. 197). Ein in die 2. DVO neu eingefügter § 18a schreibt den Gesundheitsämtern bzw. Amtsärzten vor, bei Untersuchungen in dienst- und arbeitsrechtlichen Angelegenheiten grundsätzlich nur ein Gesundheitszeugnis mit dem Ergebnis der medizinischen Prüfung, nicht aber mit den Befunden im einzelnen - wie früher praktiziert - an die personalführenden bzw. - verwaltenden Stellen zu senden. Nur bei konkreten Zweifeln an der Vollständigkeit oder Aussagefähigkeit dieses Zeugnisses ist die auftraggebende Behörde berechtigt, vom untersuchenden Arzt zusätzliche Informationen zu erfragen, und auch dies nur unter Berücksichtigung des Prinzips der Verhältnismäßigkeit. Damit ist gemeint, daß Rückfragen nur dann erfolgen dürfen, wenn die Aufklärung vorhandener Zweifel an der amtsärztlichen Aussage auch wirklich im Hinblick auf die konkret von dem Untersuchten einzunehmende Stelle erforderlich ist.

Bei Einstellungsuntersuchungen darf das Gesundheitsamt Anamnese- oder Befunddaten nur dann an die Behörde weitergeben, wenn der Betroffene vorher über den Inhalt und den Umfang des ärztlichen Gutachtens aufgeklärt wurde und schriftlich zugestimmt hat. Damit soll u.a. verhindert werden, daß sensitive Gesundheitsdaten eines Bewerbers ohne sein Einverständnis und ohne Kenntnis der weiteren Verwendung der Angaben an Dritte offenbart werden, obwohl er wegen mangelnder Tauglichkeit ohnehin keine Chance hat, eingestellt zu werden.

Der dieser Verordnung korrespondierende Erlaß des Hessischen Ministers des Innern betr. "Inhalt ärztlicher Gutachten und Zeugnisse in dienstrechtlichen Angelegenheiten" (vgl. 13. Tätigkeitsbericht, Ziff. 4.2.2.1.1) wurde inzwischen ebenfalls herausgegeben und veröffentlicht (Erlaß vom 12. November 1986, StAnz. 1986, S. 2270). Er weist die Landesbehörden entsprechend dem in der 2. DVO geregelten Verfahren an, in der Regel nur das Gesundheitszeugnis anzufordern und nur bei konkreten, aufklärungsbedürftigen Zweifeln dem Gesundheitsamt zusätzliche Fragen zu stellen. Vor allem aber fordert er die personalverwaltenden Stellen auf, bei der Formulierung des Untersuchungsauftrags den Untersuchungszweck und die konkret zu stellenden Gesundheitsanforderungen dem Amtsarzt präzise zu benennen, um überflüssige medizinische Tests ebenso wie nicht notwendige Datenübermittlungen zu verhindern.

Mit diesen beiden Regelungen ist - wenn auch mit erheblicher Verspätung - der Auftrag des Hessischen Landtags erledigt, der in seinem Beschluß Nr. 10 zu meinem 12. Tätigkeitsbericht die Landesregierung gebeten hatte, "bis zum 31. Dezember 1984 ihre bereits zugesagten Regelungsvorschläge zur Begrenzung der Übermittlung von Gesundheitsdaten an die personalführenden Stellen vorzulegen" (Drucks. 11/1551 i.V.m. Protokoll der 22. Plenarsitzung vom 5. Juli 1984, S. 1378). Nicht erledigt jedoch ist mit dieser Lösung auf der Verordnungsebene die Anforderung des Bundesverfassungsgerichts aus dem Volkszählungs-Urteil vom 15. Dezember 1983, wonach die Datenverarbeitung und der Datenschutz auch im öffentlichen Gesundheitsdienst bereichsspezifisch gesetzlich zu regeln sind. Wie ich bereits im 13. Tätigkeitsbericht (vgl. Ziff. 4.2.2.1.3) dargelegt habe, ist die Änderung einer Verordnung aus dem Jahr 1935 nur als Übergangslösung akzeptabel.

11.3.4

Kontrollmitteilungen an die Finanzämter - Zur Reform der Abgabenordnung

(11. Tätigkeitsbericht, Ziff. 2.1.6)

Eine Vielzahl von Behörden übersenden den Finanzämtern regelmäßig sog. Kontrollmitteilungen, die Auskunft über die Zahlung von Honoraren, Vergütungen oder die Leistung anderer Zuwendungen an Privatpersonen enthalten. Für

diese Praxis gab es in der Vergangenheit keine gesetzliche Grundlage. Der Gesetzgeber hat sich im Rahmen der Novellierung der Abgabenordnung (AO) mit diesem Problem befaßt und nunmehr in § 93a Abgabenordnung i.d.F. v. 19. Dezember 1985 (BGBl. I S. 2436) die Bundesregierung ermächtigt, eine die allgemeinen Mitteilungspflichten regelnde Rechtsverordnung zu erlassen.

Ich habe in meinem 11. Tätigkeitsbericht (Ziff. 2.1.6) über den Referentenentwurf zur Gesetzesnovellierung berichtet. Die jetzige Vorschrift berücksichtigt im wesentlichen die gegenüber dem Entwurf vorgebrachten Bedenken: So sind die Mitteilungspflichten auf bestimmte Fallgruppen (z.B. Gewährung von Subventionen, Erlaß von Verwaltungsakten, die dem Betroffenen steuerpflichtige Einnahmen ermöglichen) beschränkt worden. Ferner müssen die Betroffenen darüber unterrichtet werden, daß eine Datenübermittlung an die Finanzbehörde erfolgt ist. Eine Regelung, daß auch Private vermehrt Auskünfte an die Finanzbehörde über Zuwendungsempfänger zu erteilen haben, ist nicht in das Gesetz aufgenommen worden.

Eine Rechtsverordnung zu § 93a AO hat die Bundesregierung noch nicht erlassen. Bisher liegt lediglich der Entwurf einer Rechtsverordnung des Bundesministers der Finanzen vor. Die Rechtsverordnung muß jedoch bald in Kraft treten, da erst dann eine ausreichende gesetzliche Grundlage für die Kontrollmitteilungen vorhanden ist.

Von besonderer Bedeutung ist die Frage, inwieweit die aufgrund § 93a AO zu erlassende Rechtsverordnung auch Sozialleistungsträger zur regelmäßigen Übersendung von Kontrollmitteilungen verpflichten könnte. Auch für eine Reihe von Sozialbehörden gilt, daß sie Verwaltungsakte erlassen, die "dem Betroffenen steuerpflichtige Einnahmen ermöglichen" (§ 93a Abs. 1 Satz 1 Nr. 1 AO), etwa für die Rentenversicherungsträger. Diese Frage ist jedoch zu verneinen: Das Sozialgeheimnis kann nur durchbrochen werden, wenn dies im Sozialgesetzbuch selbst ausdrücklich vorgesehen ist (§ 35 Abs. 2 SGB I). Zwar ist in § 71 Abs. 1 Nr. 3 SGB X die Pflicht zur Mitteilung besteuierungserheblicher Sachverhalte an die Finanzämter ausdrücklich geregelt, doch wird nur § 93 explizit genannt, der eine Anfrage der Steuerbehörde und eine vorherige Sachverhaltsklärung beim Betroffenen voraussetzt. Der neue § 93a ist dort nicht eingefügt worden und kann daher keine Unterrichtungspflicht der Sozialbehörden begründen.

11.3.5

Automatisierte Telefondatenerfassung

(9. Tätigkeitsbericht, Ziff. 3.1.4, 11. Tätigkeitsbericht, Ziff. 2.2.2)

Am 1. April 1986 sind die neuen Fernsprechvorschriften für die Verwaltung des Landes Hessen in Kraft getreten (vgl. StAnz. 14/1986, S. 720). Sie enthalten einen ausführlichen Abschnitt über Art und Umfang der Telefondatenerfassung zu Zwecken der Gesprächsnachweise sowie über die einzuhaltenden Datensicherungsmaßnahmen beim Umgang mit Fernsprechdaten. In diesen Abschnitt hat der Hessische Finanzminister mit wenigen Ausnahmen alle Vorschläge aufgenommen und die datenschutzrechtlichen Bedenken berücksichtigt, wie ich sie bereits im 9. Tätigkeitsbericht (Ziff. 3.1.4) angesprochen, später im 11. Tätigkeitsbericht (Ziff. 2.2.2) präzisiert und dann im einzelnen noch einmal im Verfahren der Ausarbeitung des Erlasses vorgetragen hatte.

Wichtigster Punkt ist der völlige Verzicht auf die Speicherung der Zielnummer des angerufenen Teilnehmers, gleich ob es sich um Dienst- oder um Privatgespräche handelt. In den Gesprächsnachweis ist, was den Anrufpartner angeht, nur die Vorwahlnummer des Ortsnetzes aufzunehmen. Mit dieser Regelung wurde meiner Auffassung gefolgt, daß es zur Kontrolle des ordnungsgemäßen Telefonverhaltens der Behördenmitarbeiter ausreicht, Angaben aufzuzeichnen, die dem Bediensteten im Bedarfsfall zur näheren Erläuterung vorgehalten werden können, daß eine komplette Registrierung der Zielnummer zu diesem Zweck jedoch nicht erforderlich und damit auch datenschutzrechtlich nicht zulässig ist.

Mit dieser Lösung werden auch die datenschutzrechtlichen Probleme vermieden, die sich daraus ergeben, daß mit der Speicherung der Zielnummer zur arbeits- bzw. dienstrechtlichen Überprüfungszwecken gleichzeitig nicht nur ein Datum des Beschäftigten, sondern auch eine Angabe über den Gesprächspartner bzw. Anschlußinhaber aufgezeichnet wird, ohne daß dieser davon weiß.

Der Unabhängigkeit der Personalvertretung trägt die Regelung dadurch Rechnung, daß bei Telefongesprächen, die von Nebenstelleninhabern in ihrer Funktion als Mitglieder der Personal- oder Jugendvertretung, des Richterrats usw. geführt worden sind, als Erläuterung gegenüber der Dienststellenleitung der Hinweis auf diese Funktion genügt.

Um eine strenge Zweckbindung der Datenverwendung für die Kontrolle der Telefonpraxis der Beschäftigten sicherzustellen, wird ausdrücklich festgelegt, daß die gespeicherten Angaben ebenso wie die gefertigten Ausdrucke ausschließlich zur Überprüfung der Einhaltung der Fernsprechvorschriften bestimmt sind. Eine Verknüpfung mit

anderen Systemen, mit denen personenbezogene Daten der Beschäftigten verarbeitet werden, wird explizit für unzulässig erklärt, so daß Gesprächsdaten-Aufzeichnungssysteme nicht zum Bestandteil von umfassenderen Personalinformationssystemen gemacht werden dürfen.

Diese Fernsprechvorschriften, die noch eine Reihe weiterer Bestimmungen über die Anfertigung, Verwendung, Weiterleitung und Vernichtung von Gesprächsnachweisen enthalten, bedeuten einen wichtigen Fortschritt in der Debatte um Zweck und Grenzen der Telefondatenerfassung. Sie sind geeignet, Konflikte zwischen Dienststellenleitungen und Personalvertretungen weitgehend zu vermeiden, ohne die berechtigten Wirtschaftlichkeitsinteressen der öffentlichen Verwaltung zu beeinträchtigen.

Die Beschränkung bei der Datenspeicherung und die Zweckbindung bei der Datenverwendung, wie sie im Abschnitt über die Gesprächsnachweise enthalten ist, entspricht auch den Vorgaben, die § 34 des neuen HDSG für die Verarbeitung von Beschäftigtendaten aufstellt. § 34 Abs. 1 des am 1. Januar 1987 in Kraft getretenen HDSG beschränkt die Zulässigkeit der Datenverarbeitung in diesem Bereich auf die Fälle, in denen dies zur Eingehung, Durchführung, Beendigung oder Abwicklung des Dienst- oder Arbeitsverhältnisses oder zur Durchführung innerdienstlicher organisatorischer, sozialer oder personeller Maßnahmen erforderlich ist. Mit diesen Kriterien wird die mit Generalklauseln umschriebene Verarbeitungsbefugnis, wie sie bisher nach § 23 BDSG gegeben war, für Arbeitnehmerdaten restriktiver gefaßt. Dies führt im übrigen auch dazu, daß die in der letzten Zeit zahlreich ergangenen arbeitsgerichtlichen Urteile, die auf der Grundlage des § 23 BDSG über die Zulässigkeit der Telefondatenerfassung in der Privatwirtschaft entscheiden, für die Beurteilung der Rechtssituation bei hessischen Dienststellen nicht mehr herangezogen werden können.

Als Konkretisierung des neuen § 34 HDSG dienen die Regelungen der Fernsprechvorschriften über ihren unmittelbaren Geltungsbereich - die Landesverwaltung - hinaus als Beurteilungs- und Prüfungsmaßstab für die Gesprächsdatenregistrierung auch bei Kommunen und sonstigen öffentlichen Stellen.

Wiesbaden, den 19. Februar 1987

gez. Professor Dr. Simitis

12. Materialien

12.1

Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 27. Januar 1986 zu den "Sicherheits- und Datenschutzgesetzen"

Die Datenschutzbeauftragten erinnern an ihre Entschließungen zu den Auswirkungen des Volkszählungsurteils des Bundesverfassungsgerichts, zur Einführung eines maschinenlesbaren Personalausweises und zur Datenverarbeitung bei Polizei und Verfassungsschutz. Sie stellen fest, daß die angekündigten "Sicherheits- und Datenschutzgesetze" den von ihnen erhobenen Forderungen nur unzureichend Rechnung tragen und den Vorgaben des Bundesverfassungsgerichts nur teilweise entsprechen. Die geplanten Regelungen haben erhebliche Konsequenzen für die Datenverarbeitung in den Ländern und präjudizieren die Landesgesetzgeber in vielerlei Hinsicht.

Die Datenschutzbeauftragten sehen sich zu folgender ersten Bewertung veranlaßt:

1. Zum Bundesdatenschutzgesetz

Das Recht auf informationelle Selbstbestimmung gilt für jeglichen Umgang mit personenbezogenen Daten. Daher ist es nicht gerechtfertigt, die Beschränkung des Bundesdatenschutzgesetzes auf Dateien festzuschreiben und die Datenerhebung auszugrenzen. Die vorgeschlagenen Regelungen im Verwaltungsverfahrensgesetz sind kein ausreichender Ersatz, weil wichtige Verwaltungsbereiche, wie z.B. die Finanzbehörden, ausgenommen sind und die Datenverarbeitung in Akten und anderen Unterlagen der Datenschutzkontrolle weitgehend entzogen wird.

Eine wirksame Kontrolle durch die Datenschutzbeauftragten in Bund und Ländern ist nach wie vor nicht sichergestellt.

Das Auskunftsrecht des Bürgers bleibt stark eingeschränkt.

Unbefriedigend ist auch, daß der Datenschutz im nicht-öffentlichen Bereich insgesamt nicht verbessert wird.

2. Zu Personalausweisgesetz und Paßgesetz

Die Einführung des maschinenlesbaren Ausweises verändert entscheidend die Bedingungen, unter denen Informationen über die Bürger im Sicherheitsbereich erhoben und verarbeitet werden. Mit seiner Hilfe soll die Polizei vorhandene Dateien automatisiert abrufen und abgleichen sowie neue Datensammlungen anlegen können. Der behauptete Sicherheitsgewinn ist bis heute nicht dargetan.

Darüber hinaus fehlt es an bereichsspezifischen Gesetzen, die den Umgang der Sicherheitsbehörden mit dem Ausweis regeln, wie sie auch der Deutsche Bundestag in seiner EntschlieÙung vom 17. Januar 1980 gefordert hat. Die jetzt diskutierten Begleitgesetze einschließlich der Ergänzung der StrafprozeÙordnung genügen den Anforderungen nicht. Dies gilt umso mehr, als auch unverdächtige Bürger betroffen sind.

Die Gefahren wachsen, wenn die gleichzeitig beabsichtigte automatisierte Nutzung des Verkehrszentralregisters in der vorgesehenen Form verwirklicht und der Datenverbund der Sicherheitsbehörden untereinander weiter ausgebaut werden.

3. Zum Bundesverfassungsschutzgesetz

Auch für den Verfassungsschutz gilt, daß seine Aufgaben im Gesetz klar in einer für den Bürger nachvollziehbaren Weise zu beschreiben sind. Gerade weil seine Tätigkeit weitgehend im Geheimen stattfindet, müssen die Bürger die Gewißheit haben, daß der Verfassungsschutz an eindeutige, eng umrissene und abschließend geregelte Aufgaben und Befugnisse gebunden ist. Der vorliegende Entwurf verfehlt dieses Ziel.

Weitere schwerwiegende Mängel kommen hinzu:

- Dem Bürger kann nach wie vor jegliche Auskunft verweigert werden.
- Es fehlen gesetzliche Fristen für die Löschung gespeicherter Daten.
- Dem Verfassungsschutz darf nicht das Recht zugestanden werden, in jedes amtliche Datenregister Einblick zu nehmen und jede Art von Daten anzufordern. Im Gesetzentwurf sind davon nicht einmal Gesundheits- und Steuerdaten ausgenommen.
- Während sich das nachrichtendienstliche Informationssystem (NADIS) bisher nur auf die Speicherung von Aktennachweisen beschränkte, sollen nach dem Gesetzentwurf auch Textzusätze über den Bürger automatisiert den Nachrichtendiensten bundesweit zur Verfügung stehen. Damit werden zu Lasten des Bürgers Akteninhalte verkürzt und aus ihrem Entstehungszusammenhang herausgenommen.

4. Zur Zusammenarbeit von Nachrichtendiensten und Polizei

Die rechtsstaatlichen Grenzen der Zusammenarbeit von Nachrichtendiensten und Polizei werden durch das Trennungsgebot bestimmt. Das Trennungsgebot erschöpft sich nicht in einer bloßen organisatorischen Trennung zwischen Nachrichtendiensten und Polizei. Gerade wegen der automatisierten Datenverarbeitung kommt es mindestens ebenso auf eine strikte Trennung der Informationsbestände an. Das Trennungsgebot darf nicht durch einen umfassenden Informationsaustausch unterlaufen werden.

Im übrigen darf eine Zusammenarbeit zwischen Polizei, MAD, Verfassungsschutz und BND erst erfolgen, wenn für die einzelnen Dienste eindeutige, auch den Datenschutz sichernde Rechtsgrundlagen geschaffen sind.

12.2

EntschlieÙung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 14. März 1986 zur Änderung des Bundesdatenschutzgesetzes

Die Datenschutzbeauftragten beurteilen den Entwurf zur Novellierung des Bundesdatenschutzgesetzes (Drucks. 10/4737) nach den Grundsätzen des Volkszählungsurteils des Bundesverfassungsgerichts, den Notwendigkeiten, die sich aus der technischen Entwicklung der Informationsverarbeitung ergeben und den Forderungen, die sie bereits in früheren EntschlieÙungen formuliert haben. Sie messen ihn auch an der Erklärung der Bundesregierung, den Datenschutz im Interesse der Bürger zu verbessern und die Datenverarbeitung transparenter zu gestalten.

Die Datenschutzbeauftragten stellen fest, daß der Entwurf zwar Verbesserungen enthält (I). Sie bemängeln insbesondere die Beschränkungen des Gesetzes auf Dateien, die Ausklammerung der Datenerhebung, die unzureichenden Kontrollbefugnisse des Datenschutzbeauftragten und die unbefriedigenden Regelungen für den nicht-öffentlichen Bereich.

I.

1.

Die Klarstellung, daß Datenschutz weder Schutz von Daten noch ausschließlich Schutz vor Mißbrauch, sondern Schutz des Bürgers vor Verletzungen seines Persönlichkeitsrechts ist, wird begrüßt.

2.

Einige der vorgesehenen Änderungen entsprechen Forderungen, die die Datenschutzbeauftragten immer wieder erhoben haben. Das gilt - unbeschadet noch notwendiger Verbesserungen in Einzelheiten - für

- die Einführung eines verschuldensunabhängigen Schadenersatzanspruchs, auch für Nichtvermögensschäden,
- die Aufnahme einer Regelung der Datenverarbeitung für wissenschaftliche Zwecke,
- die Abschaffung der Entgeltspflicht für die Auskunft über die eigenen Daten und die Ausdehnung der Auskunft auf Herkunft und Empfänger der Daten,
- die Pflicht zur Löschung von Daten, die für den Speicherungszweck nicht mehr erforderlich sind,
- die gesetzliche Anerkennung der Zweckbindung personenbezogener Daten,
- die Klarstellung, daß Geheimhaltungsvorschriften der Kontrolle durch den Bundesbeauftragten nicht entgegengehalten werden können,
- die Verstärkung der Befugnisse der Aufsichtsbehörden für den nicht-öffentlichen Bereich und der Stellung des betrieblichen Datenschutzbeauftragten.

II.

Einzuwenden ist gegen den Entwurf vor allem:

1.

Ein gravierender Mangel ist bereits die Beschränkung auf die Datenverarbeitung in Dateien, die schon in der neuen Gesetzesbezeichnung zum Ausdruck kommt und den gesamten Entwurf prägt (§ 1 Abs. 1). Das Recht auf informationelle Selbstbestimmung umfaßt jeden Umgang mit personenbezogenen Daten. Die dem Volkszählungsurteil folgende Einbeziehung der Datennutzung bleibt weitgehend wirkungslos, weil nur die Nutzung unmittelbar aus Dateien gewonnener Daten geregelt wird. Die zunehmende Verknüpfung von Akten-, Text- und Datenverarbeitung wurde ebensowenig berücksichtigt wie z.B. neue Formen der Bildverarbeitung, etwa durch Videoaufzeichnungen. Im übrigen ist auch der neue Dateibegriff zu eng.

2.

Neue Vorschriften im Verwaltungsverfahrensgesetz des Bundes über den Schutz personenbezogener Daten bei ihrer Verarbeitung außerhalb von Dateien gleichen die Nachteile des auf Dateien beschränkten Anwendungsbereichs des BDSG nicht aus, zumal nach § 19 Abs. 1 ihre Einhaltung nur begrenzt kontrollierbar ist. Außerdem gilt das Verwaltungsverfahrensgesetz im Gegensatz zum BDSG nicht umfassend, sondern von seinem Anwendungsbereich sind große und wichtige Verwaltungsbereiche und -tätigkeiten, wie Finanzverwaltung, Post, Strafverfolgung, Verfolgung von Ordnungswidrigkeiten und weite Bereiche der Sozialverwaltung ausgenommen, ebenso die privatrechtliche Betätigung der öffentlichen Hand. Auch im nicht-öffentlichen Bereich bleibt die Datenverarbeitung außerhalb von Dateien unregelt.

3.

Der BDSG-Entwurf enthält keine ausdrückliche Regelung der Datenerhebung, obwohl gerade die Erhebung den Bürger unmittelbar belastet. Kein ausreichender Ersatz ist die Erhebungsvorschrift im Verwaltungsverfahrensgesetz. In ihr fehlt zudem die Verpflichtung der erhebenden Stelle, den Erhebungszweck ausdrücklich festzulegen, an den die gesamte weitere Verarbeitung und Nutzung grundsätzlich gebunden ist. Er müßte dem Betroffenen auch mitgeteilt werden, um ihm Kenntnis darüber zu verschaffen, wer was wann und bei welcher Gelegenheit über ihn weiß.

4.

Die weitgehende Ausklammerung "interner Dateien" ist nicht hinnehmbar (§ 1 Abs. 3). Es ist verfassungsrechtlich bedenklich, die interne Datenverarbeitung von jeglicher Kontrolle durch die Betroffenen, die Datenschutzbeauftragten und die Aufsichtsbehörden freizustellen.

5.

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

6.

Die Regelung für die Datenverarbeitung zu Zwecken der wissenschaftlichen Forschung (§ 3a) weist noch eine Reihe von Mängeln auf. Der Vorrang der Berufs- und besonderen Amtsgeheimnisse muß klargestellt werden. Auch muß - nach dem Vorbild des Sozialgesetzbuchs - ein Forschungsgeheimnis aufgenommen werden, das den Betroffenen vor jeder zweckfremden Nutzung der für ein Forschungsvorhaben zur Verfügung gestellten Daten schützt.

7.

Der zunehmende Ausbau von Datenverarbeitungsnetzen und der vermehrte Einsatz von Kleincomputern (PC) erfordern weitere gesetzliche Maßnahmen zur Gewährleistung der Transparenz und der Kontrollierbarkeit dieser Datenverarbeitungsformen. Die unveränderte Übernahme von § 6 und dessen Anlage vernachlässigt den Einfluß neuer Technologien auf die automatisierte Datenverarbeitung.

8.

Die Regelung für automatisierte Abrufverfahren (Online) (§ 6a) weist Mängel auf. Die inhaltlichen Anforderungen an die Zulassung solcher Verfahren sind weiter zu präzisieren. Die Risiken, die in der möglichen Selbstbedienung des Datenempfängers liegen, müssen zumindest durch wirksame Kontrollmechanismen gemindert werden. In der öffentlichen Verwaltung ist die Einführung von Online-Verfahren jedenfalls in besonders sensiblen Bereichen unter den Vorbehalt einer Rechtsvorschrift zu stellen.

9.

Die Datenspeicherung sollte grundsätzlich nur für den bei der Erhebung festgelegten Zweck zugelassen werden, der dem Betroffenen bekanntzugeben ist (§ 9). Der Katalog erlaubter Zweckänderungen ist zu weit; soweit zweckfremde Datenspeicherungen und -nutzungen zugelassen werden, müßten sie den Betroffenen mitgeteilt oder in anderer Weise transparent gemacht werden. Das gilt auch für Datenübermittlungen, sofern damit eine Zweckänderung verbunden ist.

10.

Das Recht des Bürgers auf Auskunft über seine Daten (§ 13) muß Herkunft und Empfänger umfassen, auch wenn diese Informationen nicht in Dateien gespeichert sind. Das Auskunftsrecht darf im übrigen nicht dadurch geschmälert werden, daß Nachrichtendienste ohne Verpflichtung zur Interessenabwägung im Einzelfall und ohne Begründung die Auskunft verweigern dürfen (§ 13).

11.

Die Kontrollbefugnis des Bundesbeauftragten für den Datenschutz (BfD) wird - gemessen auch an der gegenwärtigen Kontrollpraxis - insgesamt dadurch verschlechtert,

- daß eine Kontrolle der Einhaltung "anderer Vorschriften" über den Datenschutz bei einer Datenverarbeitung außerhalb von Dateien nur noch dann möglich ist, wenn durch eine Beschwerde oder auf andere Weise Anhaltspunkte für eine Rechtsverletzung vorliegen,
- daß in solchen Fällen systematische Kontrollen des BfD - z.B. im Sozialleistungsbereich - entgegen der bisherigen Praxis ausgeschlossen sind, weil die Kontrolle auf den Einzelfall beschränkt wird,
- daß die Formulierung in § 19 Abs. 1 Satz 1, wonach die Kontrolle der Behörden "unbeschadet ihrer fachlichen Beurteilung und Verantwortlichkeit" stattfindet, von den kontrollierten Stellen so verstanden werden könnte, als ob eine Datenverarbeitung künftig nicht mehr inhaltlich, z.B. nicht mehr auf ihre Erforderlichkeit, überprüft werden kann,
- daß die Datenerhebung selbst dann nicht mehr kontrollierbar ist, wenn sie zur Dateispeicherung führt, weil sie nicht mehr im BDSG geregelt wird und auch nicht als Datenverarbeitung oder Nutzung im Sinne des § 19 Abs. 1 Nr. 1 und 2 gilt,
- daß nach § 19 Abs. 5 Satz 3 Nr. 1 personenbezogene Daten durch besonderes Gesetz von der Kontrolle ausgenommen werden können, obwohl es nach dem Volkszählungsurteil keine kontrollfreien Räume geben darf,
- daß nach § 19 Abs. 5 Satz 3 Nr. 2 personenbezogene Daten, die bei Beschränkungen des Brief-, Post- und Fernmeldegeheimnisses nach dem G 10 anfallen, der Datenschutzkontrolle grundsätzlich entzogen sind, obwohl das Bundesverfassungsgericht im Beschluß vom 20. Juni 1984 die Kontrolle durch Datenschutzbeauftragte zur Voraussetzung für die Zulässigkeit solcher Maßnahmen erklärt hat.

Schließlich ist festzustellen:

- § 19 Abs. 5 Satz 3 Nr. 3 muß gestrichen werden, da es für die Datenschutzbeauftragten selbstverständlich ist, das informationelle Selbstbestimmungsrecht bei der Kontrolle zu wahren, und die geplante Regelung dazu führen kann, die Datenschutzkontrolle nachhaltig zu erschweren.
- Die Klarstellung, daß (bundesrechtliche) Berufs- oder Amtsgeheimnisse der Datenschutzkontrolle nicht entgegeng gehalten werden können, muß auch die Kontrolle durch die Landesbeauftragten für den Datenschutz einbeziehen.
- Es fehlt eine zum Teil in früheren Gesetzentwürfen vorgesehene Verpflichtung der Behörden, den BfD über Planungen wichtiger Automatisierungsvorhaben zu unterrichten und bei datenschutzrelevanten Gesetzgebungsvorhaben zu beteiligen.

12.

Die Datenschutzvorschriften für den nicht-öffentlichen Bereich orientieren sich nicht am Grundsatz der Zweckbindung und räumen verfassungsrechtlich bedenkliche Verarbeitungsprivilegien ein. So kann die Personen-Gruppe, über die listenmäßig bestimmte Daten übermittelt werden dürfen, beliebig festgelegt werden (§ 24 Abs. 1 Nr. 3). Für Zwecke der Markt- und Meinungsforschung und der Werbung können auch Vertragsdaten, beispielsweise aus einem Arbeitsverhältnis, ohne Einwilligung des Betroffenen und ohne Rücksicht auf seine schutzwürdigen Belange listenmäßig übermittelt werden.

13.

Die Auskunft an den Betroffenen über seine Daten muß auch im nicht-öffentlichen Bereich den Speicherungszweck umfassen (§ 26). Gleiches gilt für die Benachrichtigung über die erstmalige Speicherung von Daten. Über Herkunft und Empfänger ist auch dann Auskunft zu erteilen, wenn diese Angaben nicht in Dateien gespeichert sind.

14.

Der Empfänger übermittelter Daten muß strenger an den Übermittlungszweck gebunden werden. Zweckfremde Nutzungen dürfen nicht schon dann zulässig sein, wenn der Nutzer keinen Grund zur Annahme sieht, daß dadurch schutzwürdige Belange des Betroffenen beeinträchtigt werden (§ 24 Abs. 3).

15.

Die Datenschutzbeauftragten halten eine Ergänzung des BDSG um Sonderregelungen für den Adreßhandel für erforderlich.

16.

Im übrigen erinnern die Datenschutzbeauftragten an ihre früheren Forderungen nach bereichsspezifischen Regelungen nicht nur für den öffentlichen, sondern auch für den nicht-öffentlichen Bereich. Hierzu zählen insbesondere Regelungen für die Verarbeitung von Arbeitnehmerdaten sowie für den Kredit- und Versicherungsbereich.

12.3

Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 18. April 1986 zur Änderung des Bundesverfassungsschutzgesetzes

Die Datenschutzbeauftragten beurteilen den Entwurf zur Novellierung des Bundesverfassungsschutzgesetzes (Drucks. 10/4737) nach den Grundsätzen des Volkszählungsurteils des Bundesverfassungsgerichts, den Notwendigkeiten, die sich aus der technischen Entwicklung der Informationsverarbeitung ergeben, und den Forderungen, die sie bereits in früheren Entschließungen formuliert haben. Sie messen ihn auch an der Erklärung der Bundesregierung, den Datenschutz im Interesse der Bürger zu verbessern und die Datenverarbeitung transparenter zu gestalten.

Der Entwurf wird den sich aus dem Urteil des Bundesverfassungsgerichts zum Volkszählungsgesetz ergebenden Anforderungen nicht gerecht. Seine Vorschriften müssen schon deshalb wesentlich präziser gefaßt werden, weil die Arbeit des Verfassungsschutzes vorwiegend unter Ausschluß der Öffentlichkeit und der Kontrolle der betroffenen Bürger stattfindet.

Hauptkritikpunkte sind:

1.

Da sich der zulässige Umfang der Informationsverarbeitung maßgeblich nach den Aufgaben der datenverarbeitenden Stelle bemißt, bedarf es einer möglichst genauen gesetzlichen Beschreibung dieser Aufgaben. Die in § 3 Abs. 1 verwendeten Begriffe wie etwa "Bestrebungen gegen die freiheitlich-demokratische Grundordnung" oder "Gefährdung auswärtiger Belange" sind unpräzise.

Unklar bleibt weiterhin, unter welchen Voraussetzungen "beeinflusste" Organisationen beobachtet werden dürfen und wie weit hierbei die Beobachtung auf Einzelpersonen ausgedehnt werden darf. Für den einzelnen muß feststellbar sein, wann er die Schwelle von der Ausübung der Grundrechte zur verfassungsfeindlichen Bestrebung überschreitet. Auf jeden Fall ist es notwendig, die Voraussetzungen für die Erhebung, Speicherung und sonstige Verwendung personenbezogener Daten im Rahmen der Erfüllung dieser Aufgaben präziser und für den Bürger transparent zu regeln. Begriffe wie "Aufgaben des Verfassungsschutzes" und "Zwecke des Verfassungsschutzes" sind nicht hinreichend bestimmt.

Die Mitwirkung der Verfassungsschutzbehörden an der Überprüfung von Personen durch andere Stellen muß im Verfassungsschutzgesetz abschließend geregelt werden. Sofern über die Sicherheitsüberprüfung (§ 3 Abs. 2) hinaus eine Mitwirkung in anderen Verfahren wie etwa Einbürgerungen, Asylverfahren, Ordensverleihung oder der Überprüfung von Bewerbern für den öffentlichen Dienst für unabdingbar gehalten wird, sind diese im Gesetz ausdrücklich zu nennen. Auch die damit im Zusammenhang stehende Datenverarbeitung ist im Verfassungsschutzgesetz präzise zu regeln. Unabhängig davon ist für die Sicherheitsüberprüfung und jedes andere Verfahren zur Überprüfung von Personen eine bereichsspezifische Regelung erforderlich.

2.

Der im Entwurf vorgesehene Informationsaustausch der Verfassungsschutzbehörden untereinander (§ 4 Abs. 1) ist zu umfassend und bedarf einer aufgabenbezogenen Einschränkung. Er ist nur zulässig, soweit Informationen für die jeweilige Aufgabenerfüllung der einzelnen Verfassungsschutzbehörden erforderlich sind. So dürfen beispielsweise die aus einer Telefonüberwachung gewonnenen Daten auch zwischen Verfassungsschutzbehörden nur unter den engen Voraussetzungen des § 7 Abs. 3 G 10 ausgetauscht werden.

Besondere datenschutzrechtliche Risiken birgt die Aufnahme von Textzusätzen aus Akten der Verfassungsschutzbehörden in automatisierte Dateien. Damit werden zu Lasten des Bürgers Akteninhalte verkürzt und aus ihrem Entstehungszusammenhang herausgenommen. Sollten trotz dieser Bedenken Textzusätze in eingeschränktem Umfang zugelassen werden, ist es über die bereits im Entwurf getroffenen Beschränkungen und Schutzvorkehrungen hinaus unerlässlich, in der Datei die für die Bewertung und Überprüfung solcher Textzusätze maßgeblichen Unterlagen anzugeben. Entscheidungen dürfen auf diese Textzusätze allein nicht gestützt werden. Die im Gesetz gewollte Begrenzung auf Spionageabwehr und Terrorismusbekämpfung wird nicht erreicht, weil der Gewaltbegriff nicht einschränkend definiert ist.

3.

Die in § 5 und § 6 Abs. 2 vorgesehene Befugnis, nachrichtendienstliche Mittel einzusetzen, entspricht nicht dem Grundsatz der Normenklarheit. Zumindest sind die wichtigsten Mittel im Gesetz aufzuzählen. Auch zum Zwecke der Datenschutzkontrolle sollte daneben die interne Festlegung der zulässigen Mittel und die Dokumentation ihres Einsatzes im einzelnen vorgeschrieben werden. Angesichts der Schwere des mit der Anwendung nachrichtendienstlicher Mittel verbundenen Eingriffs in das Persönlichkeitsrecht darf sich ihr Einsatz grundsätzlich nur gegen konkret verdächtige Personen richten. Entsprechend den Regelungen über die Post- und Telefonüberwachung sind Verwertungsbeschränkungen und eine Verpflichtung zur nachträglichen Unterrichtung des Betroffenen vorzusehen.

4.

Die in § 6 Abs. 1 geregelte Befugnis zur Datenerhebung entspricht wegen der Bezugnahme auf die zu weitreichende Klausel "zur Erfüllung der Aufgaben der Verfassungsschutzbehörden erforderlich" nicht dem Grundsatz der Verhältnismäßigkeit. Die verfassungsrechtlich gebotene Güterabwägung im Einzelfall kann ergeben, daß vorrangige Individualrechte einer personenbezogenen Erhebung entgegenstehen, so beispielsweise bei der Ausübung des Demonstrationsrechts (vgl. Brokdorf-Beschluß des Bundesverfassungsgerichts). Dies gilt gleichermaßen hinsichtlich solcher Personen, die selbst keinerlei verfassungswidriger Bestrebungen verdächtig sind.

5.

Die in § 7 getroffene Regelung über die Speicherung, Veränderung und sonstige Nutzung personenbezogener Daten darf nicht - wie jetzt vorgesehen - auf Dateien beschränkt bleiben, zumal bei Verfassungsschutzbehörden ein Großteil der das Persönlichkeitsrecht der Bürger maßgeblich berührenden Daten in Akten geführt wird und komplexe Aktensammlungen bereits heute gezielt und mit Hilfe automatisierter Verfahren erschlossen werden können.

Im Bereich der Beobachtung verfassungswidriger Bestrebungen ohne Gewaltbezug sollte die personenbezogene Speicherbefugnis davon abhängig gemacht werden, daß der Extremismusbezug in der Person des zu Speichernden vorliegt.

Überdies muß die Vorschrift um die Festlegung von Überprüfungs- und Lösungsfristen, differenziert nach den einzelnen Aufgabenbereichen, erweitert werden.

6.

Der Entwurf will in § 8 die Verpflichtung anderer Behörden, den Verfassungsschutz über eigene Wahrnehmungen von sich aus zu unterrichten, auf Erkenntnisse aus den Bereichen Spionage und Terrorismus beschränken, ohne jedoch - wegen des zu weiten Gewaltbegriffs - dieses Ziel voll zu erreichen. Die darüber hinaus allen Behörden

eingräumte Befugnis, dem Verfassungsschutz auch Informationen über gewaltfreie extremistische Bestrebungen zuzuleiten, birgt in dieser uneingeschränkten Form die Gefahr in sich, daß ein Klima allgemeiner Verdächtigungen entsteht. Auch vermag der Bürger, der in Kontakt mit einer Verwaltungsbehörde tritt, nicht zu erkennen, wann und bei welcher Gelegenheit an die Verfassungsschutzbehörde übermittelt.

Schließlich fehlt in der Vorschrift eine Regelung, unter welchen Voraussetzungen Veränderungen des Sachverhalts der Verfassungsschutzbehörde nachzuberichten sind.

7.

Die in §§ 9 und 16 des Entwurfs festgelegte Verpflichtung für alle übrigen öffentlichen Stellen, den Verfassungsschutzbehörden auf Ersuchen die zur Erfüllung ihrer Aufgaben erforderlichen Auskünfte zu erteilen, geht zu weit, da sie im Einzelfall z.B. der Zweckbindung widersprechen kann. Noch weniger hinnehmbar ist die vorgesehene pauschale Ermächtigung der Verfassungsschutzbehörde, in alle amtlich geführten Register Einsicht zu nehmen. Schließlich fehlt es auch an einer Regelung für die Übermittlung von Informationen durch andere Stellen, die diese aufgrund besonderer Eingriffsbefugnisse erlangt haben. Die in § 9 Abs. 2 vorgesehene Befreiung der Verfassungsschutzbehörde von der Verpflichtung, ihre Auskunftersuchen zu begründen, kann nur für die Fälle hingenommen werden, in denen Sicherheitsinteressen oder schutzwürdige Belange des Betroffenen einer Begründung entgegenstehen.

8.

Angesichts des weitreichenden Auftrages der Verfassungsschutzbehörden zur Sammlung von Informationen bedürfen die dabei angefallenen personenbezogenen Erkenntnisse einer besonders strengen Abschottung nach außen. Dem trägt § 10 Abs. 1 des Entwurfs nicht hinreichend Rechnung, der es für eine Weiterleitung verfassungsschutzbehördlicher Erkenntnisse an andere öffentliche Stellen genügen läßt, daß die Daten dort im Rahmen der Aufgabenerfüllung für Zwecke der öffentlichen Sicherheit benötigt werden.

Die in § 10 Abs. 2 zugelassene Übermittlung von Daten der Verfassungsschutzbehörde an Dienststellen der Stationierungstreitkräfte muß angesichts der unübersehbaren Folgewirkungen und wegen der fehlenden Geltung deutschen Datenschutzrechts an besonders enge Voraussetzungen geknüpft werden. Zumindest ist in jedem Fall eine Abwägung mit den schutzwürdigen Belangen der Betroffenen vorzuschreiben.

Die Weitergabe von Erkenntnissen an private Stellen (§ 10 Abs. 3 muß auf die Fälle der Sicherheitsüberprüfung und der Spionage- bzw. Terrorismusabwehr beschränkt werden.

9.

Die Übermittlung personenbezogener Daten durch das Bundesamt für Verfassungsschutz an die politische Führung (§ 11 Abs. 1) darf nur zugelassen werden, soweit dies für Zwecke der Aufsicht oder im Rahmen der politischen Berichtspflicht erforderlich ist. Darüber hinaus ist eine strenge Zweckbindung für die übermittelten Daten vorzusehen.

Die nach § 11 Abs. 2 zugelassene Unterrichtung der Öffentlichkeit über personenbezogene Daten muß die Ausnahme bleiben.

10.

Die in § 14 auf automatisierte Dateien beschränkte Verpflichtung, Errichtungsanordnungen zu erstellen, muß auf alle Datensammlungen ausgedehnt werden. Die Unterrichtung des Datenschutzbeauftragten vor Aufnahme des Dateibetriebes ist vorzusehen. Schließlich ist gesetzlich sicherzustellen, daß die Frage der Notwendigkeit zur Weiterführung oder Änderung einer Datei in bestimmten Zeitabständen aufgabenbezogen überprüft wird.

12.4

Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 14. März 1986 zum Datenschutz im Krankenhaus

Die Datenschutzbeauftragten haben in ihrer Entschließung vom 27./28. März 1984 über die Auswirkungen des Volkszählungsurteils auf die Notwendigkeit hingewiesen, auch im Bereich des Gesundheitswesens bereichsspezifische gesetzliche Regelungen zu erlassen. Die ärztliche Schweigepflicht und die allgemeinen Datenschutzgesetze reichen nicht aus, alle Fälle, in denen im Bereich des Krankenhauses das Persönlichkeitsrecht des Patienten berührt wird, angemessen zu lösen. Konkrete Regelungen für diesen Bereich sind insbesondere deshalb notwendig, weil automatisierte Datenverarbeitung in immer stärkerem Maße im Krankenhausbereich auch für die Verarbeitung medizinischer Daten eingesetzt wird. Die zunehmende Komplexität der Verarbeitung und Nutzung von Patientendaten führt dazu, daß für den einzelnen Patienten der Umfang und die Zwecke der Verwendung seiner Daten undurchschaubar werden. Der Bürger muß aber auch künftig die Gewähr haben, daß das Vertrauensverhältnis zwischen Arzt und Patient (Arzt-/Patientengeheimnis) und sein Persönlichkeitsrecht gewahrt bleiben.

Bisher wird die Datenverarbeitung in Krankenhäusern vielfach aufgrund sehr weit gefaßter formularmäßiger Einwilligungen gerechtfertigt. Die Einwilligung kann jedoch in vielen Fällen keine ausreichende Grundlage für die Verarbeitung von Patientendaten sein, da für den Patienten die Informationsmöglichkeit und die Entscheidungsfreiheit häufig eingeschränkt sind.

Maßstab für den Umfang der Erhebung, Verarbeitung und Nutzung von Patientendaten muß stets die Behandlung des Patienten sein. Eine zusätzliche, vom Behandlungszweck nicht gedeckte Datenerhebung, -verarbeitung und -nutzung bedarf einer besonderen Legitimation.

Auch die für die Behandlung verwendeten Vordrucke und Aufnahmeverträge müssen diesen Grundsätzen angepaßt werden. Die zuständigen Stellen werden aufgefordert, ihre Vordrucke und Aufnahmeverträge entsprechend zu überarbeiten.

Zur Wahrung des Patientengeheimnisses ist es geboten, im Krankenhaus den ärztlichen Bereich von der Verwaltung informationell abzuschotten. Daraus folgt, daß z.B. die Akten der Krankenhausverwaltung getrennt von denjenigen des ärztlichen Bereichs zu führen sind. Daraus folgt weiter, daß auch im ärztlichen Bereich nur vom jeweils behandelnden Arzt auf die Daten zugegriffen werden kann.

Läßt das Krankenhaus Patientendaten bei anderen Stellen im Auftrag verarbeiten, wird das Arztgeheimnis durchbrochen. Auch besteht die Gefahr einer Grundrechtsbeeinträchtigung durch Verknüpfung von medizinischen Daten und solchen aus anderen Bereichen und durch überregionale Konzentration medizinischer Daten. Die Verarbeitung medizinischer Daten außerhalb des eigenen Krankenhauses sollte daher - in eingeschränktem Umfang - allenfalls bei einem anderen Krankenhaus zugelassen werden.

Das Krankenhaus steht im Zentrum vielfältiger Informationsanforderungen, nicht zuletzt von Sozialleistungsträgern und anderen öffentlichen Stellen. Diese Informationsanforderungen sind häufig nicht normenklar festgelegt. Ihre Notwendigkeit muß überprüft, die gesetzlichen Grundlagen müssen präzisiert werden. Dies gilt insbesondere dann, wenn die Übermittlung zu belastenden Konsequenzen für den Patienten im Verwaltungsvollzug (z.B. Führerscheinenzug) führen kann.

Der Patient darf ohne sein Wissen und sein Einverständnis grundsätzlich nicht zum Objekt der Forschung mit Daten gemacht werden, die zu seiner Behandlung erhoben werden. Die Verarbeitung von Daten zu Forschungszwecken ohne Beteiligung des Patienten sollte nur zugelassen werden, wenn dies im Interesse der wissenschaftlichen Forschung unabdingbar ist und die Rahmenbedingungen der Verarbeitung durch den Gesetzgeber näher festgelegt sind. Dies gilt auch für gemeinsame Dokumentationssysteme mehrerer behandelnder Einrichtungen.

Das informationelle Selbstbestimmungsrecht umfaßt auch das Recht des Patienten, Einsicht in Patientenakten und ärztliche Unterlagen zu nehmen und Auskunft zu erhalten, sofern nicht überwiegende Geheimhaltungsinteressen anderer entgegenstehen.

Eine undifferenzierte, zeitlich unbefristete Aufbewahrung von Patientenunterlagen darf es auch im Krankenhaus nicht geben. Deshalb müssen die Krankenhäuser prüfen, wann welche Patientenunterlagen ohne Beeinträchtigung schutzwürdiger Belange der Patienten vernichtet werden können.