



13. Wahlperiode

Drucksache **13/3887**

HESSISCHER LANDTAG

23. 02. 93

FR Leiten

Einundzwanzigster Tätigkeitsbericht des Hessischen Datenschutzbeauftragten

vorgelegt zum 31. Dezember 1992
nach § 30 des Hessischen Datenschutzgesetzes vom 11. November 1986

Eingegangen am 23. Februar 1993 · Ausgegeben am 25. März 1993

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

13/3887

INHALTSVERZEICHNIS

Seite

1.	Vorwort	9
2.	Verfassungsschutz	9
2.1	Prüfung von Akten über die Sicherheitsüberprüfung von Angehörigen des öffentlichen Dienstes beim Landesamt für Verfassungsschutz	9
2.1.1	Erster Versuch:	10
2.1.2	Zweiter Versuch:	10
2.1.3	Dritter Versuch:	11
2.2	Gesetzentwürfe für die Durchführung der Sicherheitsüberprüfung auf Bundes- und Länderebene	13
2.3	Dateimeldungen zum Register	13
3.	Ausländerrecht	14
3.1	Gesetz zur Neuregelung des Ausländerrechts	14
3.1.1	Verwaltungsvorschriften zu §§ 75 bis 77 Ausländergesetz	14
3.1.2	Weitere Probleme	14
3.2	Erkennungsdienstliche Behandlung von Asylbewerbern	15
3.3	Pläne für ein europaweites automatisiertes Fingerabdrucksystem	15
4.	Polizei	16
4.1	Polizeiliche Datenspeicherung von Schwangerschaftsabbrüchen	16
4.2	Anträge der Polizei an Gesundheitsaufsicht und Gesundheitsamt mit dem Ziel, "lästige Anzeigerstatter" zu überprüfen	17
5.	Justiz	18
5.1	Gesetz zur Bekämpfung des illegalen Rauschgifthandels und anderer Erscheinungsformen der Organisierten Kriminalität (OrgKG)	18
5.1.1	Neue Fahndungs- und Ermittlungsmethoden im strafrechtlichen Ermittlungsverfahren	18
5.1.2	Neue Aufgabenverteilung zwischen Staatsanwaltschaft und Polizei	19
5.1.3	Die weitere Entwicklung – der "Lauschangriff"	19
5.2	Justizmitteilungsgesetz	20
5.2.1	Kritische Punkte	20
5.2.2	Positive Ansätze	20
5.3	Beschlagnahme von Patientendaten	21
5.3.1	Zur Rechtslage	21
5.3.2	Kritik an der bestehenden gesetzlichen Regelung	21
5.3.3	Gesetzesantrag des Landes Hessen zur Änderung der Strafprozeßordnung	22
5.4	Justizprüfungsamt	22
6.	Kommunen	23
6.1	Vorlagen von Akten an Akteneinsichtsausschüsse	23
6.1.1	Das Recht der Gemeindevertreter, Akten einzusehen	23
6.1.2	Kriftel	23
6.1.3	Frankfurt	24
6.2	Fehlbelegungsabgabe	24
6.2.1	Gesetz	24
6.2.2	Stand der Umsetzung	25
6.3	Die ungültigen Schwerbehindertenparkausweise	26
6.4	Kommunale Umfragen	26
7.	Finanzwesen: Zweitwohnungssteuer	27
8.	Rundfunk: Weitergabe von Hörerbriefen durch einen privaten Rundfunksender	28
9.	Gesundheit	28
9.1	Krebsregister: Treuhandmodell als neuer Lösungsweg	28
9.1.1	Verhindert Datenschutz Krebsregister?	28

9.1.2	Datenschutz als Rahmenbedingung für Krebsregister	28
9.1.3	Treuhandmodell	29
9.2	Krankenversichertenkarte in Chipkartenform wird Krankenscheinersatz	29
9.2.1	Die Vorgaben des Gesundheitsreformgesetzes	29
9.2.2	Entscheidung für die Krankenversichertenkarte in Chipkartenform	30
9.2.3	Vorgezogene Einführung der Krankenversichertenkarte in Wiesbaden und im Rheingau-Taunus-Kreis	30
9.2.4	Führt der Einsatz der Chipkartentechnik langfristig zum "gläsernen Patienten"?	31
9.3	Unzulässige Öffnung von Leichenschauheinen in Frankfurt am Main	31
9.3.1	Leichenschauheine dürfen nur vom Amtsarzt geöffnet werden	31
9.3.2	Prüfungsergebnisse	32
9.3.3	Konsequenzen	32
9.3.4	Abschließende Kontrollprüfung	32
9.4	Zentrale Registrierung von Methadon-Empfängern zur Verhinderung von Mehrfachvergaben ...	33
9.5	Unzulässige Ablehnung der Einsicht in amtsärztliches Gutachten	33
9.6	Unzulässige Veröffentlichungen über das Ruhen der Approbation von Zahnärzten	34
10.	Soziales	34
10.1	Pauschale Einwilligungsfomulare in Schuldnerberatungsstellen	34
10.1.1	Schuldnerberatungsstellen benötigen viele persönliche Informationen	35
10.1.2	Transparenz der Datenverarbeitung	35
10.2	Benachrichtigung der Gesundheitsämter über die Notwendigkeit einer Entwöhnungsbehandlung	36
10.3	Inhalt von Rechtswahrungs- und Überleitungsanzeigen der Sozialämter bei Aufenthalt hilfeschender Frauen im Frauenhaus	36
11.	Schulen	37
11.1	Hessisches Schulgesetz	37
11.1.1	Beseitigung eines Regelungsdefizits	37
11.1.2	Schulärzte und Schulpsychologischer Dienst	37
11.1.3	Wissenschaftliche Forschung im Schulbereich	38
11.1.4	Informationsrechte der Schüler und Eltern	38
11.1.5	Ordnungsmaßnahmen	39
11.1.6	Automatisierte Datenverarbeitung	39
11.1.7	Rechtsverordnung zum Datenschutz in der Schule	39
11.2	Weitergabe von Schülerdaten	39
12.	Umwelt	40
12.1	Ad hoc-Arbeitsgruppe Umweltschutz und Datenschutz	40
12.2	Abfallbeseitigung ("Müllanalysen")	41
13.	Landwirtschaft	41
13.1	Datensicherheit: Ministerialerlaß – 10 v.H. der Haushaltsmittel für sächliche Ausgaben zweckgebunden für Datensicherheit	41
13.2	Ölsaatzbeihilfe	42
13.3	Tierschutz	42
14.	Gesetz über das Liegenschaftskataster und die Landesvermessung	42
14.1	Inhalt des Gesetzes	42
14.2	Verordnung über den automatisierten Abruf von Daten aus dem Liegenschaftskataster	43
15.	Kammern	43
15.1	Übermittlung von Adressen an Private zu Werbezwecken durch die Industrie- und Handelskammern und die Handwerkskammern	43
15.1.1	Daten aus dem Handelsregister	44
15.1.2	Das am 1. Januar 1993 in Kraft getretene Gesetz zur vorläufigen Regelung des Rechts der Industrie- und Handelskammern	44
15.2	Datenübermittlung zwischen Rechtsanwaltskammern	44

16.	Datensicherheit	45
16.1	Probleme der Löschung von Daten am Beispiel von WORM-Platten	45
16.1.1	Nutzung von WORM-Platten	45
16.1.2	Begriffsbestimmungen	46
16.1.3	Probleme	47
16.1.4	Zusammenfassung	49
16.2	Prüfung der Datensicherheitsmaßnahmen in einem kommunalen Gebietsrechenzentrum	49
16.2.1	Ausgangssituation	49
16.2.2	Festgestellte Mängel	50
16.2.3	Fazit	56
16.3	Abhörproblematik des Funkverkehrs	56
16.3.1	Ausgangslage	56
16.3.2	Technische Details und Rahmenbedingungen des BOS-Funks	57
16.3.3	Aussichten	58
16.3.4	Organisatorische Maßnahmen zur Risikominderung beim Funkverkehr	60
16.3.5	Fazit	60
16.4	Erste Erfahrungen beim Einsatz von Novell Netware	60
16.4.1	Motivationen für die Integration von PC in Netze	60
16.4.2	Mängel bei der Konzeption	61
16.4.3	Einsatz von Schutzfunktionen und Kontrollmitteln	61
16.4.4	Forderungen	64
17.	Unzureichende Umsetzung des Hessischen Datenschutzgesetzes durch öffentliche Stellen	64
17.1	Mangelnde Kooperationsbereitschaft bei öffentlichen Stellen	64
17.1.1	Mißachtung meiner Rechte nach § 29 HDSG durch verzögerte oder unterlassene Auskunftserteilung	64
17.1.2	Mißachtung meiner Rechte nach § 29 HDSG durch falsche Auskünfte	65
17.2	Fehlende Sorgfalt bei der Organisation der Aktenführung	66
17.2.1	Vorgefundene Situation	66
17.2.2	Grundsätze zur Neuorganisation	66
18.	Bilanz	67
18.1	Aufnahme des Rechts auf informationelle Selbstbestimmung und Informationsfreiheit in das Grundgesetz	67
18.2	EG-Richtlinie zum Datenschutz (19. Tätigkeitsbericht Ziff. 2; 20. Tätigkeitsbericht Ziff. 16.3) ..	68
18.3	Telefax in Krankenhäusern (20. Tätigkeitsbericht, Ziff. 9.1)	69
18.4	Verabschiedung des neunten Gesetzes zur Änderung dienstrechtlicher Vorschriften (18. Tätigkeitsbericht, Ziff. 12.3)	70
18.5	Prüfung der Datenerhebung in Krankenhäusern (20. Tätigkeitsbericht Ziff. 9.2)	71
19.	Materialien	71
19.1	Entschließungen der Konferenz der Datenschutzbeauftragten des Bundes und der Länder	71
19.1.1	Entschließung der 43. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 23./24. März 1992 in Stuttgart zum Arbeitnehmerdatenschutz	71
19.1.2	Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder zum Grundrecht auf Datenschutz vom 28. April 1992	72
19.1.3	Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder zur Neuregelung des Asylverfahrens (BT-Drucks. 12/2062) vom 28. April 1992	73
19.1.4	Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 1./2. Oktober 1992 zum Datenschutz bei internen Telekommunikationsanlagen	74
19.1.5	Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 1./2. Oktober 1992 zum Entwurf eines Gesetzes zur Sicherung und Strukturverbesserung der gesetzlichen Krankenversicherung – Gesundheits-Strukturgesetz 1993 – (BR-Drucks. 560/92) ..	75
19.1.6	Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 1./2. Oktober 1992 zum "Lauschangriff"	75

13|3887

KERNPUNKTE DES 21. TÄTIGKEITSBERICHTS

1. Eine Prüfung von Akten über die Sicherheitsüberprüfung von Angehörigen des öffentlichen Dienstes beim Landesamt für Verfassungsschutz hat eine Reihe von Verfahrensmängeln aufgedeckt (Ziff. 2.1).
2. Auf Bundes- und Länderebene fehlen nach wie vor bereichsspezifische gesetzliche Regelungen zur Durchführung der Sicherheitsüberprüfung. Zwei Gesetzentwürfe, die zur Zeit zur Diskussion stehen, weisen aus datenschutzrechtlicher Sicht wichtige Ansätze auf, sind allerdings in vielerlei Hinsicht noch verbesserungsbedürftig (Ziff. 2.2).
3. Auch fast zwei Jahre nach Inkrafttreten des Ausländergesetzes hat der Bundesminister des Inneren noch keine verbindlichen Ausfüllungs- und Anwendungsbestimmungen in Kraft gesetzt. Das Hessische Ministerium des Inneren und für Europaangelegenheiten hat mir zugesagt, Anfang dieses Jahres Hessische Verwaltungsvorschriften zu erlassen (Ziff. 3.1).
4. Das Gesetz zur Bekämpfung des illegalen Rauschgifthandels und anderer Erscheinungsformen der organisierten Kriminalität (OrgKG) führt neue Fahndungs- und Ermittlungsmethoden im strafrechtlichen Ermittlungsverfahren ein, von denen zwangsläufig nicht nur Verdächtige, sondern im großen Umfang auch Unbeteiligte betroffen sind (Ziff. 5.1).
5. Das Land Hessen hat einen Gesetzesantrag zur Änderung der Strafprozeßordnung in den Bundesrat eingebracht, mit dem der strafprozessuale Schutz des "Patientengeheimnisses" verbessert werden soll (Ziff. 5.3).
6. Soweit für ihre Aufgabenerfüllung erforderlich, können die Akteneinsichtsausschüsse der Gemeindevertretungen bzw. Stadtverordnetenversammlungen auch die Offenlegung personenbezogener Daten verlangen (Ziff. 6.1).
7. Verschiedene hessische Gemeinden haben Satzungen erlassen, nach denen für sog. Zweitwohnungen eine kommunale Steuer zu erheben ist. Bei der Umsetzung dieser Vorschriften wurden die Grundsätze des Datenschutzes häufig nicht ausreichend berücksichtigt (Ziff. 7).
8. Die Einführung der Krankenversichertenkarte in Chipkartenform als Krankenscheinersatz darf nicht zum "Gläsernen Patienten" führen, der seine Daten in umfassender Weise überall offenlegen muß (Ziff. 9.2).
9. Die Gesundheitsämter sind verpflichtet, den Betroffenen in dienst- und arbeitsrechtlichen Angelegenheiten Einsicht in die Aufzeichnungen über die Untersuchungen zu gewähren, auch wenn anläßlich der amtsärztlichen Untersuchung ein Zusatzgutachten von einem externen Gutachter eingeholt wurde (Ziff. 9.5).
10. Die Gesundheitsämter dürfen von der Landesversicherungsanstalt nicht über die Notwendigkeit einer Entwöhnungsbehandlung informiert werden (Ziff. 10.2).
11. Der Landesgesetzgeber hat mit der Verabschiedung des Hessischen Schulgesetzes vom 17. Juni 1992 für einen weiteren wichtigen Bereich der Landesverwaltung bereichsspezifische Datenschutzvorschriften erlassen und damit ein vom Hessischen Datenschutzbeauftragten wiederholt kritisiertes, verfassungswidriges Regelungsdefizit behoben (Ziff. 11.1).
12. Die vom Bundestag verabschiedete Novelle des Industrie- und Handelskammergesetzes verstößt zum Teil gravierend gegen den Datenschutz. Den Industrie- und Handelskammern ist erlaubt, Firma, Anschrift und Wirtschaftszweig der Kammermitglieder auch gegen deren erklärten Willen für kommerzielle Zwecke, zum Beispiel an Versicherungen, weiterzugeben. Der Gesetzgeber sanktioniert damit eine Praxis, über die es in der Vergangenheit zu Recht immer wieder Beschwerden von Firmeninhabern gegeben hat (Ziff. 15.1).
13. Der BOS-Funk der Polizei und anderer Behörden und Organisationen mit Sicherheitsaufgaben, zu denen die Funkleitstellen der Rettungsdienste gehören, kann ohne größere Probleme von nicht berechtigten Personen abgehört werden. Dieser Zustand ist aus Sicht des Datenschutzes auf Dauer nicht hinnehmbar (Ziff. 16.3).
14. Die Vorschriften des Hessischen Datenschutzgesetzes und auch die Befugnisse des Hessischen Datenschutzbeauftragten werden von den Behörden und anderen öffentlichen Stellen nicht immer hinreichend beachtet (Ziff. 17).

13/3887

1. Vorwort

Die Tätigkeitsberichte, welche die Datenschutzbeauftragten des Bundes und der Länder vorlegen, sind seit jeher von einer Sorge geprägt: daß das Recht auf informationelle Selbstbestimmung sich den Bürgerinnen und Bürgern nur schwer als ein Menschenrecht vermitteln läßt, daß die Behörden das Recht auf den Schutz persönlicher Daten bisweilen gar nicht auf der Liste ihrer Entscheidungskriterien haben und daß sie es – durchaus nicht aus bösem Willen – nicht selten verletzen. Diese Rechtsverletzungen sind in der Regel gar nicht spektakulär. Mein Tätigkeitsbericht zeigt, wie schnell man in das Räderwerk der behördlichen Beobachtung gelangen und wie schwierig man wieder aus ihm herausfinden kann (etwa wenn es um mangelnde Kooperationsbereitschaft bei öffentlichen Stellen geht (17.1), oder wie gering die Sorgfalt ist, mit der immer wieder die Aktenführung organisiert wird (17.2). Ich habe deshalb schon in meiner Antrittsrede vor dem Hessischen Landtag am 22. Oktober 1991 anläßlich meiner Wahl zum Hessischen Datenschutzbeauftragten gesagt (vgl. 20. Tätigkeitsbericht, Ziff. 17.5), daß das Recht auf informationelle Selbstbestimmung mit allem Nachdruck als Grundrecht allgemein verständlich gemacht werden solle; Bürgerinnen und Bürger müßten verstehen, daß es beim Datenschutz um ihre eigenen Interessen geht.

Dieser Tätigkeitsbericht zeigt an vielen Stellen, daß das Recht auf Schutz persönlicher Daten sowohl von Behörden als auch von aufmerksamen Bürgern in der richtigen Weise wahrgenommen wird, und er belegt auch an vielen Stellen, daß Öffentlichkeit und öffentliche Verwaltung durchaus bereit sind, den Datenschutz zu fördern, wenn die Überzeugungsarbeit des Datenschutzbeauftragten gelingt. Hier bleibt noch viel zu tun. Ein Mittel unter vielen, von dem ich mir eine gute Wirkung verspreche, ist die öffentliche Behandlung aktueller Probleme, welche mit dem Datenschutz zusammenhängen: das "Forum Datenschutz".

Am 12. Juni 1992 fand im Plenarsaal des Hessischen Landtages das erste öffentliche "Forum Datenschutz" statt. Es stand unter dem Thema "Datenschutz und Stasi-Unterlagen – Verdrängen oder Bewältigen?" und wurde gemeinsam vom Präsidenten des Hessischen Landtages und dem Hessischen Datenschutzbeauftragten veranstaltet. Das Forum, das künftig einmal jährlich stattfinden soll, ist der Versuch, das Recht auf informationelle Selbstbestimmung als Grundrecht darzustellen. Einer breiten Öffentlichkeit soll anhand aktueller Fragestellungen vermittelt werden, welche unterschiedliche Bedeutung das Recht auf Schutz der persönlichen Daten heute haben kann, welche differenzierten Antworten zu geben und welche Konsequenzen zu ziehen sind.

1992 ging es um Notwendigkeit, Zweckmäßigkeit und Grenzen einer Verwertung der Stasi-Unterlagen. Der Bundesbeauftragte für die Unterlagen des Staatssicherheitsdienstes der ehemaligen Deutschen Demokratischen Republik, Joachim Gauck, und Professor Spiros Simitis, von 1975 bis 1991 Hessischer Datenschutzbeauftragter, haben – aus unterschiedlichen Perspektiven, aber doch weithin übereinstimmend in den Schlußfolgerungen – in ein breites Spektrum von Problemen und Lösungen eingeführt.

Als Koreferenten beteiligten sich Professor Bruce Ackerman (Yale Law School, USA), der Thüringer Landtagsabgeordnete Matthias Büchner (Fraktion Neues Forum/Bündnis 90/Die Grünen im Thüringer Landtag), der Bundestagsabgeordnete Dr. Burkhard Hirsch (F.D.P.-Fraktion im Deutschen Bundestag) und der Präsident des ungarischen Verfassungsgerichts, Professor László Sólyom (Budapest).

Aus dem Publikum kamen pointierte und ganz unterschiedliche Einschätzungen: Wissenschaft und Politik, "alte" und "neue" Länder, deutsche und ausländische Erfahrungen. Soll man die Akten verbrennen (soweit man sie hat)? Kann man zwischen "Tätern" und "Opfern" unterscheiden? Was kann man aus fremden Erfahrungen lernen? Setzt Verarbeiten Wissen voraus? Wie verlässlich sind die Unterlagen der "Staatssicherheit"? Können Westdeutsche überhaupt mitreden? Kann man zwischen Bereichen des "Politischen" und des "Persönlichen" unterscheiden?

Die Referate und Diskussionsbeiträge dieses ersten Forums Datenschutz – wie auch die folgenden – sind bzw. werden in einer Schriftenreihe unter dem Titel "Forum Datenschutz" veröffentlicht (NOMOS-Verlag Baden-Baden) und sind im Buchhandel erhältlich.

Das nächste "Forum Datenschutz" wird im Frühsommer 1993 stattfinden.

W.H.

2. Verfassungsschutz

2.1

Prüfung von Akten über die Sicherheitsüberprüfung von Angehörigen des öffentlichen Dienstes beim Landesamt für Verfassungsschutz

Anfang September 1992 konnte ich endlich beim Hessischen Landesamt für Verfassungsschutz (LfV) die seit langem vorgesehene Prüfung von Akten über die von einer Sicherheitsüberprüfung betroffenen Angehörigen des öffentlichen Dienstes durchführen. Dabei handelt es sich um Personen, die Zugang zu geheimhaltungsbedürftigen Unterlagen erhalten sollen und sich deshalb einer besonderen Überprüfung durch den Verfassungsschutz unterziehen müssen.

Diesem Besuch beim LfV gingen zwei erfolglose Prüfungsversuche voraus.

2.1.1**Erster Versuch:**

Eine noch von meinem Amtsvorgänger im Herbst 1990 vorbereitete Prüfung wurde nach längerer Diskussion mit dem Direktor des LfV und seinen Mitarbeitern abgebrochen. Grund dafür war die Weigerung des Verfassungsschutzes, den Hessischen Datenschutzbeauftragten Einblick in die Akten nehmen zu lassen. Es wurde behauptet, daß bei derartig sensiblen Informationen – wie es bei den Sicherheitsüberprüfungsakten der Fall ist – der Betroffene gefragt werden müsse, ob er mit der Einsichtnahme durch den Datenschutzbeauftragten einverstanden sei. Jedenfalls aus dem Kreis der Mitarbeiter des LfV – so wurde uns berichtet – seien Stimmen laut geworden, die sich der Einsichtnahme strikt widersetzen. Auch der Hinweis, diesen ausdrücklichen erklärten Willen der Betroffenen selbstverständlich zu respektieren, führte zu keiner Lösung.

Hintergrund der Argumentation des Verfassungsschutzes war die nunmehr in § 24 Abs. 2 i.V.m. Abs. 6 Bundesdatenschutzgesetz (BDSG) vorgesehene Möglichkeit des Bürgers, der Einsichtnahme des Hessischen Datenschutzbeauftragten unter anderem in seine Akten über die Sicherheitsüberprüfung widersprechen zu können. Zum Zeitpunkt meiner Prüfung befand sich die entsprechende Regelung des BDSG allerdings noch im Entwurfsstadium und wurde erst – ca. acht Monate später – mit Inkrafttreten des Gesetzes am 1. Juni 1991 geltendes Recht. Trotz der klaren Rechtslage kam ich mit den Vertretern des Verfassungsschutzes überein, zunächst das weitere Gesetzgebungsverfahren und die näheren Einzelheiten der Ausführung der entsprechenden Bestimmung des BDSG im Land Hessen abzuwarten.

Zu dem nunmehr geltenden § 24 BDSG und zu der Erstreckung der Regelung auch auf Landesbeauftragte durch Abs. 6 der Vorschrift hat sich mein Amtsvorgänger bereits im 19. Tätigkeitsbericht (Ziff. 1.3.2 und 1.3.3) geäußert. Die verfassungsrechtlichen Bedenken bestehen nach wie vor.

Allerdings hat ein Erlaß des Hessischen Ministeriums des Innern und für Europaangelegenheiten vom 20. August 1991 (StAnz. 35/1991 S. 2006) zu folgenden wichtigen Punkten Feststellungen getroffen:

1. Die Kontrolle des HDSB kann unabhängig davon, ob die Betroffenen auf ihr Widerspruchsrecht hingewiesen wurden, durchgeführt werden. Erst der tatsächlich eingelegte Widerspruch des Betroffenen schließt die Kontrolle der auf ihn bezogenen Daten aus.
2. Der Widerspruch ist beim Hessischen Datenschutzbeauftragten einzulegen.
3. Der HDSB kann sich beim Betroffenen anlässlich einer Kontrolle vergewissern, ob der vorsorglich eingelegte Widerspruch auch im Einzelfall für die gerade anstehende Überprüfung gelten soll.

Der mancherorts prophezeite Ansturm von Widersprüchen gegen meine Einsichtnahme in Akten über die Sicherheitsüberprüfung (die Regelung gilt ebenfalls unter anderem für die Personalakten und Daten, die dem Arztgeheimnis unterliegen etc.) hielt sich in Grenzen. Bisher sind 142 Widersprüche bei mir eingegangen, die sich entweder insgesamt gegen die Einsichtnahme des HDSB oder nur auf bestimmte der o.g. Bereiche beziehen.

2.1.2**Zweiter Versuch:**

Im Juni 1992 verabredete ich mit dem LfV einen neuen Termin für eine Prüfung der Sicherheitsüberprüfungsakten. Ohne Schwierigkeiten kamen wir dieses Mal überein, daß die von mir auszuwählenden Akten mit der von mir mitgeführten Liste der Widersprüche abgeglichen und die Akten der Personen, die Widerspruch eingelegt hatten, von vornherein ausgesondert werden sollten. Probleme tauchten allerdings an anderer Stelle auf: Die Vertreter des LfV weigerten sich, mich in die in vielen Akten enthaltenen Berichte von Referenz- und Auskunftspersonen einsehen zu lassen. Bei den Referenzpersonen handelt es sich um solche, die der Betroffene selbst angegeben hat und die dann von Mitarbeitern des Verfassungsschutzes aufgesucht werden, um sie über die zu überprüfende Person zu befragen. Auskunftspersonen sind weitere Personen, die der Betroffene nicht angegeben hat, die aber ebenfalls Informationen über ihn liefern sollen. Die Mitarbeiter des Verfassungsschutzes fertigen über die Befragungen Berichte an, die dann zu der entsprechenden Akte genommen werden.

Der Verfassungsschutz argumentierte mit der sog. "Quellenschutz"-Vorschrift des § 29 Abs. 2 HDSG. Danach ist die Offenbarung personenbezogener Daten des Verfassungsschutzes gegenüber dem HDSB unter folgenden Voraussetzungen eingeschränkt bzw. ausgeschlossen:

1. Die Einsichtnahme und das Auskunftsrecht dürfen nur durch den HDSB persönlich ausgeübt werden, wenn das Hessische Ministerium des Innern und für Europaangelegenheiten festgestellt hat, daß die Sicherheit des Bundes oder des Landes dies gebietet.
2. Soweit diese Voraussetzungen vorliegen, ist die Offenbarung personenbezogener Daten gänzlich ausgeschlossen, wenn dem Betroffenen besondere Vertraulichkeit zugesichert wurde.

Es handelt sich demnach um eine Vorschrift, die den Ausnahmefall im Auge hat – im Vordergrund steht die Wahrung der Anonymität des V-Mannes – und deren formale Voraussetzung (Feststellung des HMDIuE, daß die Sicherheit des Landes berührt ist) im vorliegenden Fall schon nicht gegeben war.

Um die Durchführung der Prüfung nicht wiederum zu gefährden, versuchte ich, den Überlegungen des Verfassungsschutzes entgegenzukommen. Ich schlug vor, ein Verfahren zu finden, in dem die Namen der Referenz- und Auskunftspersonen – auf die es mir entgegen den Vermutungen des LfV gar nicht ankam – anonymisiert werden, mir aber ansonsten die Berichte vorzulegen sind. Auf diesen Vorschlag ging der Verfassungsschutz zunächst nicht ein, so daß sich meine Mitarbeiter wiederum unverrichteter Dinge zurückziehen mußten.

Erst nach einer weiteren Pause einigte man sich in einem Gespräch auf meinen Vorschlag. Daraufhin wurde alsbald ein dritter Termin verabredet.

2.1.3

Dritter Versuch:

Im September 1992 kamen meine Mitarbeiter dann endlich zum Zuge. Zweck der Prüfung war es, einen Überblick über die Praxis des LfV bei der Erhebung und weiteren Verarbeitung von Daten im Rahmen der Sicherheitsüberprüfung zu gewinnen. Die angesichts des Materials natürlich nur stichprobenartige Auswahl erfolgte zum Teil von mit Hilfe des Nachrichtendienstlichen Informationssystems (NADIS, vgl. 18. Tätigkeitsbericht, Ziff. 5.1.1) ausgedruckten Aktenfundstellen. Daneben zogen wir eine Reihe von Akten unter bestimmten Gesichtspunkten direkt aus dem Archiv beim LfV.

2.1.3.1

Ablauf der Sicherheitsüberprüfung

Betroffen von der Sicherheitsüberprüfung sind Angehörige des öffentlichen Dienstes, die die Ermächtigung zum Zugang zu oder Umgang mit Verschlusssachen erhalten sollen, die "VS-Vertraulich", "Geheim" oder "Streng Geheim" eingestuft werden. Bis Juni 1990 wurden auch Beschäftigte in sog. "sicherheitsempfindlichen Bereichen" überprüft.

Nach der mir vorliegenden Statistik haben in den Jahren 1987 bis 1992 im Schnitt jährlich 400 bis 600 Überprüfungen – einschließlich der Wiederholungsüberprüfungen – stattgefunden. Die Fälle, in denen das LfV Bedenken gegen eine entsprechende Ermächtigung geltend machte, liegen unter zehn v.H.

Das Verfahren beginnt damit, daß der Betroffene vom Geheimschutzbeauftragten der Beschäftigungsbehörde eine sog. "Sicherheitserklärung" erhält, in der er aufgefordert wird, unter anderem Angaben zu seiner Person, seinen Familienangehörigen, den letzten Wohnsitzen, Vorstrafen oder anhängigen Ermittlungs-, Straf- und Disziplinarverfahren, der Beziehung zu verfassungseindlichen Organisationen, zu Reisen in bestimmte Länder und seiner finanziellen Situation zu machen. Außerdem wird verlangt, mindestens drei Referenzpersonen zu nennen. Die Beschäftigungsbehörde bittet daraufhin das LfV um Überprüfung des Betroffenen und übersendet die ausgefüllte "Sicherheitserklärung".

Nunmehr beginnt die im Verfassungsschutzgesetz (VerfSchG) vorgesehene "Mitwirkung" des LfV.

Diese besteht aus:

- einer Abfrage der Personalien des Betroffenen mit NADIS, um festzustellen, ob beim LfV Hessen oder anderen Verfassungsschutzämtern Erkenntnisse vorliegen; dasselbe gilt für die vom Betroffenen genannten Familienangehörigen, also dem Ehegatten oder Lebenspartner, den Eltern, Geschwistern, Kindern oder auch Angehörigen in den ehemals sozialistischen Ländern;
- einer Anfrage bei den Polizeidienststellen der letzten Wohnsitze des Betroffenen und evtl. beim Landeskriminalamt;
- der Anforderung von Akten der Polizei, der Staatsanwaltschaft, des Gerichts, falls Erkenntnisse vorliegen;
- der Anforderung der Ausländerakte, wenn der Betroffene oder dessen Ehegatte bzw. Lebenspartner Ausländer ist;
- Anfragen beim Bundesnachrichtendienst und Militärischen Abschirmdienst, wenn ein Bezug zur Bundeswehr gegeben ist;
- einer Anfrage beim Bundeszentralregister;
- Referenzpersonen und gegebenenfalls Auskunftspersonen wurden bis März 1992 bei Personen, die der Geheimhaltungsstufe "Geheim" und "Streng Geheim" unterliegen, befragt. Seit März 1992 gilt dies nur noch für die zuletzt genannte Gruppe.

Das LfV bewertet die gesammelten Informationen und gibt gegenüber der Beschäftigungsbehörde ein Votum ab. Letztere entscheidet unter Berücksichtigung dieses Votums, ob sie die entsprechende Ermächtigung erteilt.

2.1.3.2

Mängel des Verfahrens

Mein Eindruck, daß im Rahmen der Sicherheitsüberprüfung umfangreiche Datensammlungen entstehen, die ein detailliertes Persönlichkeitsbild des Betroffenen bieten können, hat sich aufgrund der Prüfung verstärkt. Mir ist kaum eine andere staatliche Stelle bekannt, bei der über einen so langen Zeitraum so systematisch aus so breit gefächerten Quellen Daten zusammengetragen und gespeichert werden.

Insgesamt weist das Verfahren der Sicherheitsüberprüfung eine Reihe von Mängeln auf, von denen hier einige genannt werden sollen:

1. In der sog. "Sicherheitserklärung" werden beim Betroffenen zum Teil Informationen erhoben ohne Rücksicht darauf, ob die Daten für die entsprechende Überprüfungsart überhaupt erforderlich sind. So sieht die Sicherheitserklärung die Angabe von Referenzpersonen vor, obwohl eine Befragung dieser Personen bei der Überprüfung "VS-Vertraulich" und neuerdings auch bei "Geheim" nicht durchgeführt wird. Aus meiner Sicht handelt es sich deshalb um eine datenschutzrechtlich unzulässige Datensammlung "auf Vorrat".
2. Gravierende Bedenken habe ich weiterhin gegen die Praxis der Beiziehung von Akten anderer Behörden und öffentlicher Stellen.

Nach meinen Feststellungen wird, soweit der Betroffene oder der Ehegatte bzw. Lebenspartner Ausländer ist, die gesamte Ausländerakte beigezogen und wesentliche Teile als Kopie in die Sicherheitsüberprüfungsakte übernommen. Der Verfassungsschutz erhält damit ein vieles mehr an Informationen zu der betroffenen Person als er für seine Aufgaben benötigt. Aus meiner Sicht ist deshalb zu prüfen, ob es nicht im Regelfall ausreicht, bei der entsprechenden Ausländerbehörde die gewünschten Informationen einzuholen. Weiterhin habe ich festgestellt, daß die Akten der zuständigen Polizeibehörden, der Staatsanwaltschaft oder des Gerichts angefordert werden, soweit irgendein Anhaltspunkt für ein strafrechtlich relevantes Verhalten vorliegt. Auch hier werden die wesentlichen Passagen in Kopie in die Sicherheitsüberprüfungsakte aufgenommen. Teilweise geht es um Jahrzehnte zurückliegende Sachverhalte, deren Eintragung im Bundeszentralregister längst getilgt ist.

Die Beiziehung der Akten erfolgt unabhängig vom Strafvorwurf (beispielsweise Trunkenheitsfahrt, Personalienverweigerung, Diebstahl geringwertiger Sachen), aber auch unabhängig vom Ausgang des Verfahrens (beispielsweise Einstellung durch Polizei, Staatsanwaltschaft oder Gericht, Freispruch). Eine Akte enthielt ein vollständiges ausführliches psychologisches Gutachten aus dem Jahre 1971 zur Glaubwürdigkeit einer dritten Person. Diese dritte Person hatte Strafanzeige gegen den Betroffenen wegen eines Sexualdelikts gestellt. In dem daraufhin erfolgten Strafverfahren wurde der Betroffene freigesprochen. Das LfV hat auf meine Beanstandung hin das psychologische Gutachten vernichtet.

Über diesen Fall hinaus muß überlegt werden, ob eine nach dem jeweiligen Strafvorwurf und dem Ausgang des Verfahrens differenzierende Erhebung und Speicherung von Informationen erfolgen kann.

3. Erstaunt war ich – obwohl darauf vorbereitet – über die Brisanz der Berichte über die Gespräche mit Referenz- und Auskunftspersonen. Nach meinem Eindruck sind diese Berichte sehr unterschiedlich. Teilweise werden mehr oder weniger standardisiert die Antworten auf bestimmte Fragen festgehalten. Einige Berichte sind aber auch sehr ausführlich und enthalten eine Menge von Informationen aus dem engsten Privat- und Familienleben des Betroffenen, über Charaktereigenschaften und Schwächen. Beispielsweise wird dort berichtet, daß eine Person "verwaltungsintern als Alkoholiker" bekannt ist oder "in betrunkenem Zustand Frauen an der Hotelbar belästigt hat". Es existieren ausführliche Schilderungen des Intimlebens, beispielsweise von Liebschaften während verschiedener Dienstreisen. Die (geschiedene!) Ehefrau des Betroffenen wird mit abfälligen Bemerkungen zur finanziellen Lage und zum Berufsleben ("dubiose Baugeschäfte") zitiert.

Angesichts der Qualität der Informationen und der ungesicherten Aussagekraft stellt sich für mich die Frage, ob diese Informationssammlungen im Verhältnis zu dem sich daraus ergebenden Nutzen stehen. Auf jeden Fall ist zu überdenken, ob derartige Informationen über viele Jahre hinweg aufzubewahren sind oder ob nicht hier eine Teilbereinigung vorzunehmen ist.

In diesem Zusammenhang ist allerdings hervorzuheben, daß ein wichtiger Schritt die Entscheidung vom März vergangenen Jahres war, Referenzbefragungen nur noch für die Geheimhaltungsstufe "Streng Geheim" durchzuführen.

4. Kritisch beurteile ich auch die für den Betroffenen unbedingt erforderliche Transparenz des Verfahrens. Aus meiner Sicht muß die überprüfte Person Gelegenheit erhalten, sich zu negativen Erkenntnissen des Verfassungsschutzes zu äußern, bevor ein abschließendes Votum abgegeben wird. Auch dies wird nach meinen Feststellungen nicht in jedem Fall eingehalten.

Derzeit stehe ich mit dem Verfassungsschutz und dem Hessischen Ministerium des Innern und für Europaangelegenheiten in Gesprächen, um für diese Probleme eine datenschutzfreundliche Lösung zu finden.

2.1.3.3

Fehlende gesetzliche Grundlage

Die dargestellten Datenerhebungen und -sammlungen greifen in sehr weitgehender Weise in das Recht auf informationelle Selbstbestimmung des von der Sicherheitsüberprüfung Betroffenen, aber auch von Dritten – die oft gar nichts davon wissen – ein. Ich halte es fast zehn Jahre nach dem Urteil des Bundesverfassungsgerichts zum Volkszählungsgesetz 1983 (BVerfGE 65, 1 ff.) nicht mehr für hinnehmbar, daß für diesen Bereich keine tragfähige Rechtsgrundlage existiert. Die entsprechenden Vorschriften des Landesverfassungsschutzgesetzes beschränken sich darauf, dem LfV die Aufgabe der Mitwirkung bei der Sicherheitsüberprüfung sowie ganz allgemein die Befugnis zur Informationsverarbeitung zuzuweisen. Der Bereich der Sicherheitsüberprüfung wurde im Gesetzgebungsverfahren zum Verfassungsschutzgesetz gerade deshalb ausgespart, weil man sich einig darüber war, diese Fragen in einem speziellen Gesetz zu regeln. Auch in den Beamtengesetzen finden sich keine entsprechenden Rechtsgrundlagen. Die Sicherheitsrichtlinien aus dem Jahr 1962 sind, abgesehen von der mangelnden Gesetzesqualität, aus datenschutzrechtlicher Sicht unzulänglich und, wie auch die Mitarbeiter des LfV bestätigten, längst durch die Praxis überholt.

2.2

Gesetzentwürfe für die Durchführung der Sicherheitsüberprüfung auf Bundes- und Länderebene

Die von mir erhobene Forderung nach der Schaffung gesetzlicher Grundlagen für die Sicherheitsüberprüfung ist nicht neu. Die Datenschutzbeauftragten des Bundes und der Länder haben immer wieder, zuletzt in ihrer Entschließung vom 26./27. September 1991 (20. Tätigkeitsbericht, Ziff. 17.1.3), bereichsspezifische Regelungen für diesen Bereich angemahnt.

Positiv zu bewerten ist deshalb, daß nunmehr zwei verschiedene Entwürfe zur Diskussion stehen:

Vom Bundesminister des Innern stammt ein Referentenentwurf für ein "Sicherheitsüberprüfungsgesetz" (Stand: 15. April 1992). Auf Länderebene wird im Arbeitskreis Verfassungsschutz der Arbeitsgemeinschaft der Innenministerien der Bundesländer ein Entwurf für ein "Geheimhaltungsgesetz" (Stand 24. Januar 1992) als Modellentwurf für die Gesetzgebungsdiskussion in den Ländern erarbeitet.

Beide Entwürfe weisen aus datenschutzrechtlicher Sicht wichtige Ansätze auf, allerdings sind sie in vielerlei Hinsicht noch verbesserungsbedürftig. Mir kommt es insbesondere auf folgende Punkte an:

Eine gesetzliche Regelung muß klarstellen,

- welche Mitarbeiter in welchem Umfang einer Sicherheitsüberprüfung unterzogen werden;
- welche personenbezogenen Daten für die einzelnen Überprüfungsarten erhoben und verarbeitet werden dürfen;
- welche öffentlichen oder aber auch – falls dies für erforderlich angesehen wird – welche privaten Stellen bzw. Privatpersonen in das Verfahren einbezogen werden dürfen und wie diese Einbeziehung im einzelnen zu erfolgen hat;
- welche Voraussetzungen vorliegen müssen, damit beim Betroffenen "Sicherheitsbedenken" erhoben werden können;
- daß die im Rahmen der Sicherheitsüberprüfung erhobenen Daten grundsätzlich nur für diesen Zweck verwandt werden dürfen;
- daß für den Betroffenen größtmögliche Transparenz, unter anderem durch eine möglichst frühzeitige Unterrichtung über bestehende Sicherheitsbedenken, hergestellt wird.

2.3

Dateimeldungen zum Register

Das Hessische Landesamt für Verfassungsschutz (LfV) hat im Berichtszeitraum eine große Anzahl Dateien zu dem von mir geführten Register angemeldet. Dies verschafft mir die Möglichkeit, aufgrund eines formalisierten Verfahrens Kenntnis von dem Umfang der vom LfV genutzten Dateien zu erhalten. Für den einzelnen Bürger ist die in § 26 Hessisches Datenschutzgesetz (HDSG) vorgesehene Registermeldung im Bereich des Verfassungsschutzes allerdings von geringer Bedeutung, da sowohl das Recht zur Einsicht in das Register als auch die Veröffentlichung ausgeschlossen werden können und der Verfassungsschutz von diesem Recht auch Gebrauch macht.

Das LfV nutzt eine Reihe von automatisierten Dateien, an der die anderen Landesämter und das Bundesamt für Verfassungsschutz (BfV) partizipieren. Wichtigstes Beispiel ist das nachrichtendienstliche Informationssystem NADIS (siehe dazu 18. Tätigkeitsbericht, Ziff. 5.1.1). In die im Rahmen von NADIS beim BfV in Köln installierten Dateien können alle Verfassungsschutzämter Daten im Online-Verfahren eingeben, abrufen und unter bestimmten Voraussetzungen ändern und löschen. Dazu kommen verschiedene Dateien, z.B. im Terrorismus- und Spionagebereich, an denen die Verfassungsschutzbehörden des Bundes und der Länder teilnehmen, die aber rechtlich und technisch unterschiedlich ausgestaltet sind.

Im Rahmen der Diskussion um die einzelnen Registermeldungen wurde nun vom Verfassungsschutz die Frage aufgeworfen, ob in diesen Fällen überhaupt meine Zuständigkeit gegeben ist. Dabei stellte man sich jedenfalls für eine Reihe dieser Dateien auf den Standpunkt, daß nicht das LfV Hessen, sondern nur das BfV "speichernde Stelle" im Sinne von § 26 Abs. 1 HDSG sei. Ich habe dieser Auffassung energisch widersprochen. Aus meiner Sicht kann es nicht darauf ankommen, bei welcher Stelle der Schwerpunkt der technischen Installation liegt, sondern allein darauf, welche Befugnisse der teilnehmenden Stelle bei der Nutzung der Datei eingeräumt werden. Meine Zuständigkeit ist deshalb für alle Dateien, über deren Daten das LfV in der dargestellten Weise verfügen kann, gegeben. Das LV hat dann auch in allen diskutierten Fällen die entsprechenden Dateien zu meinem Register gemeldet.

3. Ausländerrecht

3.1

Gesetz zur Neuregelung des Ausländerrechts

3.1.1

Verwaltungsvorschriften zu §§ 75 bis 77 Ausländergesetz

In meinem letzten Tätigkeitsbericht (20. Tätigkeitsbericht, Ziff. 5.1) hatte ich darauf hingewiesen, daß das gesamte Ausländergesetz (AuslG, BGBl. I 1990 S. 1354) der Konkretisierung durch Verwaltungsvorschriften bedarf. Ich hatte berichtet, daß der Bundesminister des Innern für einen Teil der Datenverarbeitungsvorschriften einen Richtlinienentwurf für "vorläufige Anwendungshinweise zu §§ 76 und 77 AuslG" vorgelegt hatte. Unverständlich ist, daß bis jetzt – also fast zwei Jahre nach Inkrafttreten des Ausländergesetzes – immer noch keine verbindlichen Ausführungs- und Anwendungsbestimmungen in Kraft gesetzt sind.

Ich habe deshalb eine vom Amt für Multikulturelle Angelegenheiten in Frankfurt am Main ausgehende Initiative unterstützt, für Hessen einen Entwurf eigener Verwaltungsvorschriften zur Konkretisierung der Datenverarbeitungsvorschriften zu erarbeiten. Das Ergebnis der Arbeitsgruppe, an der Richter, Anwälte, Vertreter von Ausländerberatungseinrichtungen – anfänglich auch ein Vertreter des Hessischen Ministers des Innern und für Europaangelegenheiten – und ich teilnahmen, liegt seit Sommer vergangenen Jahres vor. Das Innenministerium hat zugesagt, diesen Entwurf noch Anfang dieses Jahres in Hessische Verwaltungsvorschriften umzusetzen.

Damit würde eine Konkretisierung der im Ausländergesetz vorgesehenen weitgehenden Informationspflichten verschiedenster Stellen an die Ausländerbehörden erreicht.

Einige allgemeine Grundsätze des Entwurfs sollen hier genannt werden:

- Übermittlungspflichtig sind nur öffentliche Stellen, also nicht die Kirchen, Einrichtungen in kirchlicher Trägerschaft, die freien Wohlfahrtsverbände sowie soziale und sonstige Einrichtungen in freier Trägerschaft.
- Erkenntnisse, die ausschließlich im Rahmen von einer Auskunfts- und Beratungstätigkeit öffentlicher Stellen gewonnen werden, sind nicht zu übermitteln.
- Darüber hinaus besteht immer dann, wenn es Anhaltspunkte dafür gibt, daß die Aufgabenerfüllung der öffentlichen Stelle gefährdet wird, keine Übermittlungspflicht. Zu denken ist hier beispielsweise an Fälle, in denen der Ausländer – wenn er mit der Weitergabe von Informationen durch die Stelle, an die er sich wendet, rechnen muß – dieser nicht mehr das erforderliche Vertrauen entgegenbringen kann.
- Übermittelt werden müssen nur Erkenntnisse, die die öffentliche Stelle im Rahmen ihrer Aufgabenerfüllung und nicht nur bei Gelegenheit, etwa in einem informellen Gespräch mit dem Betroffenen, erfahren hat.

3.1.2

Weitere Probleme

Der geplante Erlass von Verwaltungsvorschriften für die §§ 75 bis 77 AuslG darf allerdings nicht darüber hinwegtäuschen, daß eine Reihe datenschutzrechtlicher Fragen weiter bestehen:

- Noch nicht geklärt ist, in welchem Umfang Ausländerbehörden Informationen an andere öffentliche, private oder auch ausländische Stellen übermitteln dürfen. Das Ausländergesetz beschränkt sich in § 79 auf die Regelung von

Mitteilungen zum Zweck der Bekämpfung der illegalen Beschäftigung von Ausländern. Soweit man sich auf den Standpunkt stellt, daß es sich dabei um keine abschließende Vorschrift handelt und neben anderen speziellen Regelungen für den Empfänger Datenübermittlungen unter den Voraussetzungen der allgemeinen Vorschriften des Hessischen Datenschutzgesetzes (HDSG) erfolgen können, gibt man die an eine moderne Gesetzgebung zu stellende Forderung nach einer bereichsspezifischen, auf die jeweilige Übermittlungssituation zugeschnittenen, Regelung auf.

- Übereinstimmung habe ich auch noch nicht bei der Frage erzielt, ob die in zunehmendem Maße automatisiert erfolgende Datenverarbeitung bei den Ausländerbehörden auf den in § 80 AuslG i.V.m. der Ausländerdateienverordnung (AuslDatV) vom 18. Dezember 1990 festgelegten Datensatz beschränkt ist. Sowohl der Wortlaut des § 80 AuslG als auch die Begründung der AuslDatV sprechen für die Auffassung, daß der Gesetzgeber damit eine abschließende Regelung treffen wollte.

Meine Erfahrungen mit den Ausländerbehörden, die die Verwaltung der Ausländerdaten automatisiert mit Hilfe des "landeseinheitlichen Dialogverfahrens für das Ausländerwesen" (LADIVA) betreiben, zeigen allerdings, daß man sich nicht auf den in den rechtlichen Bestimmungen vorgesehenen Umfang beschränkt. Sofern die Ausländerbehörden die Speicherung von einigen dieser Daten für unverzichtbar halten, ist die AuslDatV insoweit zu ändern.

3.2

Erkennungsdienstliche Behandlung von Asylbewerbern

Am 1. Juli 1992 trat das Gesetz zur Neuregelung des Asylverfahrens in Kraft (AsylVfG, BGBl. I S. 1733). Eine der aus datenschutzrechtlicher Sicht bedenklichsten Vorschriften stellt die in § 16 vorgesehene Verpflichtung dar, daß – von unbedeutenden Ausnahmen abgesehen – bei sämtlichen Ausländern, die in der Bundesrepublik um Asyl nachsuchen, erkennungsdienstliche Maßnahmen durchzuführen sind. Im Rahmen dieser Maßnahmen werden Lichtbilder sowie die Abdrücke aller zehn Finger aufgenommen.

Während nach dem alten Asylverfahrensgesetz vom 16. Juli 1982 (BGBl. I S. 946) erkennungsdienstliche Maßnahmen ausschließlich in Zweifelsfällen zur Feststellung der Identität – etwa bei Verlust oder Vernichtung der Ausweispapiere – erlaubt waren, unterstellt die neue Regelung gleichsam bei allen Asylbewerbern ein Bedürfnis nach Sicherung ihrer Identität. Berücksichtigt man weiter die ganze Breite der in § 16 vorgesehenen Nutzungsmöglichkeiten für die erkennungsdienstlichen Unterlagen, wird deutlich, daß es um eine neue Qualität der Registrierung von Asylbewerbern geht. Die von sämtlichen Asylbewerbern gewonnenen Unterlagen dürfen auch zu ganz anderen Zwecken, nämlich im Rahmen der Strafverfolgung und der polizeilichen Gefahrenabwehr, genutzt werden. Die beim Bundeskriminalamt erfolgende Auswertung der Fingerabdruckblätter wurde zudem durch die Einführung des automatisierten Fingerabdruck-Identifizierungs-Systems (AFIS) speziell auf diese Nutzungsmöglichkeiten zugeschnitten. Während bisher die regelmäßig vom Bundeskriminalamt durchgeführte Verformelung der Fingerabdrücke nur für die Identitätsfeststellung nutzbar war, wird durch den Einsatz von AFIS eine Aufarbeitung erreicht, die eine Spurenuordnung im Rahmen der Strafverfolgung und der polizeilichen Gefahrenabwehr zuläßt.

Im Ergebnis werden damit – zwangsweise erhobene – sensible Daten über jeden Asylsuchenden auf Vorrat gesammelt und für eine breite Nutzung bereitgehalten. Diese Regelung stellt aus meiner Sicht einen dem Verhältnismäßigkeitsgrundsatz widersprechenden Eingriff in das Recht auf informationelle Selbstbestimmung dar.

Ich habe bei verschiedenen Gelegenheiten, unter anderem im Rahmen der öffentlichen Anhörung des Deutschen Bundestages zum Entwurf eines Gesetzes zur Neuregelung des Asylverfahrens am 18. März 1992 Kritik an dieser Regelung geäußert. Auch die Datenschutzbeauftragten des Bundes und der Länder haben auf einer Sonderkonferenz am 28. April 1992 in Stuttgart ihre Forderungen an eine gesetzliche Regelung der erkennungsdienstlichen Behandlung in einer Entschließung zusammengefaßt (Materialien, Ziff. 19.1.3). Leider waren diese Bemühungen nicht erfolgreich. § 16 ist ohne nennenswerte Änderungen in Kraft getreten.

Der für die rechtliche Bewertung des § 16 wichtige Ausbau des automatisierten Fingerabdrucksystems (AFIS) beim Bundeskriminalamt nimmt seinen geplanten Verlauf. Seit 1. Dezember 1992 ist die erste Stufe des Aufbaus, die die elektronische Aufarbeitung der Fingerabdruckblätter von Asylbewerbern umfaßt, einsatzbereit. Auch die für AFIS erforderliche qualifizierte Aufarbeitung des Altbestands an Fingerabdrücken geht weiter. Für die Hälfte des Altbestands, etwa 700.000 Fingerabdrücke, soll dies bereits erfolgt sein.

3.3

Pläne für ein europaweites automatisiertes Fingerabdrucksystem

Es verwundert nicht, daß der Einsatz eines Instruments, von dem man sich in der Bundesrepublik sicherheits- und ordnungspolitischen Nutzen verspricht, auch auf europäischer Ebene diskutiert wird.

So hat beispielsweise das Eidgenössische Justiz- und Polizeidepartement der Schweiz im Juni 1992 eine "Machbarkeitsstudie für ein europäisches Informations-System über Fingerabdrücke von Asylbewerbern" vorgelegt.

Auch die für Einwanderungsfragen zuständigen Minister der EG haben bereits im Dezember 1991 die ad hoc-Gruppe "Einwanderung" beauftragt, eine "Durchführbarkeitsstudie zu einem europäischen System für den Vergleich der daktyloskopischen Identifizierungsmerkmale von Asylbewerbern (EURODAC)" zu erstellen. Der daraufhin erarbeitete Bericht der Arbeitsgruppe (Stand 21. August 1992) sieht vor, daß jedem Asylbewerber bei der örtlichen Stelle, bei der der Erstantrag auf Asyl gestellt wird, Abdrücke aller zehn Finger abgenommen werden. Dieser Satz Fingerabdrücke wird in ein von allen Mitgliedstaaten gemeinsam geführtes automatisiertes Fingerabdrucksystem eingegeben und mit dem bereits vorhandenen Bestand abgeglichen. Die Ergebnisse können dann der nachforschenden Stelle, die die Fingerabdrücke eingespeichert hat, übermittelt werden. Den Schätzungen des Berichts zufolge würden in EURODAC Datensätze zu etwa 6 Mio. Asylbewerbern verarbeitet und jährlich etwa 500 000 Anfragen erledigt.

Nähere Einzelheiten der Ausgestaltung läßt der Bericht noch offen. Er beschränkt sich darauf, verschiedene Modelle mit deren Vor- und Nachteilen vorzustellen. Diese unterscheiden sich insbesondere nach dem Grad der Zusammenführung der Aufgaben bei einer zentralen Stelle sowie dem Ausmaß der Automatisierung bei der Erhebung und weiteren Verarbeitung der Fingerabdrücke.

Der Zusammenhang dieser Pläne für ein europaweites Fingerabdrucksystem mit den im "Schengener Zusatzabkommen" und "Dubliner Abkommen" getroffenen Vereinbarungen liegt auf der Hand. In diesen Abkommen soll durch detaillierte Zuständigkeitsregelungen sichergestellt werden, daß asylsuchenden Flüchtlingen grundsätzlich nur ein Anerkennungsverfahren in einem EG-Land eingeräumt wird. Die europaweite Zusammenführung der Fingerabdrücke soll nun verhindern, daß Asylbewerber mehrfach in verschiedenen EG-Ländern einen Antrag stellen. Ähnlich wie bei AFIS (vgl. Ziff. 3.2) stellt sich auch hier die Frage, ob es dazu einer derart umfangreichen Datensammlung auf Vorrat bedarf. Wichtig erscheint mir weiterhin, daß es in jedem Fall bei der – wie bisher im Bericht zu EURODAC vorgesehenen – Verwendung der gewonnenen Informationen ausschließlich zum Zweck der Verhinderung einer mehrfachen Antragstellung bleibt. Wie die Erfahrung zeigt, wecken umfassende und aussagekräftige Datensammlungen die Wünsche von Interessenten, die dann zu ganz anderen Zwecken davon profitieren wollen. Ich werde deshalb die weitere Entwicklung von EURODAC auch unter diesem Gesichtspunkt kritisch verfolgen.

4. Polizei

4.1

Polizeiliche Datenspeicherung von Schwangerschaftsabbrüchen

In ihrem 11. Tätigkeitsbericht hat meine baden-württembergische Kollegin kritisiert, daß von der dortigen Polizei wahllos Daten von Frauen gespeichert wurden, die in den Verdacht geraten waren, mit dem § 218 Strafgesetzbuch in Konflikt geraten zu sein.

Mein Vorgänger mußte feststellen, daß auch im hessischen Polizeiinformationssystem (HEPOLIS) 21 Frauen wegen eben dieses Verdachts gespeichert waren (Stand Anfang 1991). Elf der Frauen waren ausschließlich wegen des Schwangerschaftsabbruchs gespeichert, in den anderen Fällen hatte die Polizei auch wegen anderer Straftaten Ermittlungen durchgeführt. Sieben der Datenspeicherungen zugrunde liegenden Schwangerschaftsabbrüche fanden in den siebziger Jahren, fünf in den Jahren 1981 bis 1987 und neun in den Jahren 1988 und 1989 statt. Seit Geltung des neuen Hessischen Polizeigesetzes (HSOG), wonach die Speicherung in polizeilichen Dateien nur zulässig ist, wenn die Besorgnis der Begehung einer weiteren Straftat besteht, wurde ein Fall wegen eines im Jahre 1989 vorgenommenen Schwangerschaftsabbruchs gespeichert.

Wegen des aktuellen Ablaufs von Aufbewahrungsfristen, insbesondere aber auf Intervention meines Vorgängers, wurde der überwiegende Teil der Datenspeicherungen noch im Jahr 1991 gelöscht.

Auf meine Initiative hin hat das Hessische Ministerium des Innern und für Europaangelegenheiten inzwischen eine datenschutzfreundliche Lösung gefunden:

Die Fälle, in denen sich die Ermittlungen gegen die Schwangere selbst richten, werden in HEPOLIS nur noch zum Zweck der Aufnahme des Falles in die polizeiliche Kriminalstatistik (PKS) anonymisiert, d.h. ohne daß ein Bezug zu den betroffenen Frauen hergestellt werden kann, erfaßt. Eine Speicherung im Kriminalaktennachweis (KAN) unterbleibt. Der Vorgang selbst wird bei der sachbearbeitenden Polizeidienststelle in einem Sonderordner abgelegt, aus dem keine Auskünfte erteilt werden dürfen. Soweit bereits eine kriminalpolizeiliche personenbezogene Sammlung (KPS) für die betreffende Frau besteht, ist dort keine Eintragung über den Schwangerschaftsabbruch vorzunehmen. Die Aussonderung der Unterlagen aus dem Sonderordner erfolgt nach rechtskräftigem Abschluß des Verfahrens, unabhängig von dessen Ausgang. Zur Sicherstellung der rechtzeitigen Aussonderung ist der Sonderordner einmal jährlich dahingehend zu überprüfen, ob die Verfahren durch die Justiz inzwischen abgeschlossen wurden. Zugang zu dem Sonderordner haben nur die Polizeibediensteten, die mit der Ermittlung der einzelnen Fälle betraut sind.

Diese Regelung wird m.E. den Interessen der betroffenen Frauen gerecht und berücksichtigt, daß die Speicherung der Daten zur Aufgabenerfüllung der Polizei ohnehin nicht erforderlich ist, da sie keine geeignete Maßnahme zur vorbeugenden Bekämpfung von Straftaten darstellt.

4.2

Anträge der Polizei an Gesundheitsaufsicht und Gesundheitsamt mit dem Ziel, "lästige Anzeigerstatter" zu überprüfen

Wer sich auffällig normabweichend (oder vermeintlich normabweichend) verhält, muß damit rechnen, daß sich eines Tages Bedienstete der Stadtverwaltung oder des Landratsamtes nach seinem Geisteszustand erkundigen. Nach § 1 des Hessischen Gesetzes über die Entziehung der Freiheit Geisteskranker, Geistesschwacher, rauschgift- oder alkoholsüchtiger Personen (HFEG) können Menschen auch gegen ihren Willen in einer geschlossenen Krankenabteilung untergebracht werden, wenn aus ihrem Geisteszustand oder ihrer Sucht eine erhebliche Gefahr für ihre Mitmenschen droht oder eine erhebliche Eigengefährdung vorliegt, die nicht anders abgewendet werden kann.

Voraussetzung ist ein Unterbringungsbeschluß des Vormundschaftsgerichts. Es entscheidet auf Antrag der Verwaltungsbehörde, die ein Zeugnis eines Arztes über den Geisteszustand oder die Sucht des Unterzubringenden einreichen muß. Zuständige Verwaltungsbehörde ist in Gemeinden mit bis zu 7.500 Einwohnern der Landrat, im übrigen der Gemeindevorstand. Die Aufgabe wird von der Ordnungsbehörde wahrgenommen, diese wiederum hat in größeren Städten und in den Landkreisen ein Sachgebiet "Gesundheitsaufsicht" eingerichtet. Liegen die Voraussetzungen für eine Unterbringung mit hoher Wahrscheinlichkeit vor und ist Gefahr im Verzug, kann die Ordnungsbehörde die sofortige Unterbringung anordnen und vollziehen. In diesem Falle ist die richterliche Entscheidung unverzüglich herbeizuführen.

Alle Datenübermittlungen und jegliche Form der Datenverwendung im Zusammenhang mit der Durchführung dieses Gesetzes sind sehr sensibel und belasten die Betroffenen mit hoher Intensität. Insbesondere dann, wenn (noch) nicht feststeht, daß die betroffene Person tatsächlich für sich oder ihre Mitmenschen eine Gefahr darstellt, muß die Ordnungsbehörde bei den ihr bekannt gewordenen Informationen sorgfältig prüfen, ob es sich tatsächlich um Hinweise handelt, die für eine konkrete Eigengefährdung oder Gefährdung anderer aufgrund einer Sucht oder psychischen Erkrankung sprechen. Diese Entscheidung kann im Einzelfall sehr schwierig sein.

Durch die Konstellation vieler Faktoren können Lebenssituationen entstehen, die fast jedes normabweichende Verhalten plausibel erscheinen lassen. Legt sich die Ordnungsbehörde ein solches Szenario selbst zurecht, gerät sie in die Gefahr, tatsächliche Bedrohungen zu übersehen und muß sich, falls eine tatsächlich geisteskranke Person sich oder einem anderen einen Schaden zufügt, dem Vorwurf der Untätigkeit stellen. Sie setzt deshalb die Schwelle einer Information, die für eine Eigengefährdung oder Gefährdung anderer aufgrund einer psychischen Erkrankung spricht, überhaupt nachzugehen, sehr niedrig an. Andererseits reagieren gesunde Menschen verständlicherweise oft entrüstet auf das Anliegen der Ordnungsbehörde, ihren Geisteszustand begutachten zu wollen.

In folgenden Fällen baten mich die Betroffenen um eine datenschutzrechtliche Beurteilung:

- Eine Auseinandersetzung zweier Nachbarinnen endete damit, daß eine der beiden Kontrahentinnen der anderen einen Eimer Wasser über dem Kopf ausschüttete. Diese forderte die Ordnungsbehörde auf, ihre Nachbarin auf ihren Geisteszustand untersuchen zu lassen, weil sie sich von ihr bedroht fühle. Die Ordnungsbehörde lud die Betroffene vor und führte mit ihr ein Gespräch. Dabei stellte der Bearbeiter fest, daß es sich lediglich um eine eskalierte Nachbarschaftsstreiterei handelte, und nahm keine Anhaltspunkte wahr, die für eine Eigengefährdung oder Gefährdung anderer aufgrund einer Geisteskrankheit sprachen. Maßnahmen nach dem HFEG waren nicht zu treffen.
- Frau D. aus Frankfurt wunderte sich sehr, als sie erfuhr, daß sich drei Bedienstete der Ordnungsbehörde bei ihrer Nachbarin nach ihrem Geisteszustand erkundigt hatten. Nachdem sie einen Rechtsanwalt eingeschaltet und mit den Bearbeitern im Ordnungsamt ein Telefongespräch geführt hatte, wurde verfügt, daß auf weitere Überprüfungen im Sinne des HFEG verzichtet werden könne und weiter nichts zu veranlassen sei. Der Bericht über die Befragung der Nachbarin lautet auszugsweise wie folgt: "Bei der heutigen Ermittlung gegen 10 Uhr wurde auf Klingeln, Klopfen und Rufen nicht geöffnet. Daraufhin wurde an der Nachbarwohnung geklingelt. Die Nachbarin öffnete die Tür und gab auf Befragen an, daß Frau D. in keiner Weise im Hause auffalle, freundlich sei und jeden Morgen das Haus verlasse und zur Arbeit ginge. Sie mache einen intelligenten Eindruck und sei Akademikerin. Weitere Hausbewohner konnten nicht angetroffen werden."

Die Aktion des Ordnungsamtes erfolgte aufgrund folgenden Sachverhaltes: Frau D. hatte mit der Leitung eines Supermarktes darüber gestritten, ob ihre Tasche durchsucht werden dürfe. Sie hatte sich gegen diese für alle Kunden geltende Kontrolle gewehrt und war von dem Supermarkt mit einem Hausverbot belegt worden, das ein Gericht aber als unbegründet aufhob. Als sie erneut den Supermarkt aufsuchte, kam es zu einer handgreiflichen Auseinandersetzung mit dem Marktleiter, der die Polizei rief, um sie zum Verlassen des Marktes zu zwingen. Als sie daraufhin in zahlreichen Postkarten der Polizei verschiedene Vorwürfe machte, wandte sich das Polizeipräsidium Frankfurt an das Sozialamt – Sozialpsychiatrischer Dienst -, das Gesundheitsamt – Abteilung Psychiatrie – und das Ordnungsamt als zuständige Stellen nach dem HFEG und schilderte darin die Vermutung einer psychischen Störung. Da bei psychisch Gestörten Überraschungen nicht auszuschließen seien, so das Polizeipräsidium, sollte im Falle von Frau D. Ausweitungen vorgebeugt werden.

- Eine Person aus einer anderen hessischen Stadt erstattete mehrfach bei der Polizei Anzeige wegen versuchten Einbruchs, Diebstahls und weiterer Straftaten. Die Ermittlungen ergaben allesamt, daß die Anzeigen jeder

Grundlage entbehrten. Sie entsprangen der Phantasie der Anzeigerstatterin. In einem Brief an das Kreisgesundheitsamt und an die Ordnungsbehörde der Stadtverwaltung schilderte die Polizei ihren Eindruck, daß die Person psychisch krank sei, und regte eine amtsärztliche Untersuchung an. Sie begründete ihre Anregung mit der Angabe, es sei nicht ihre Aufgabe, laufend Anzeigen, die jeder Grundlage entbehrten, entgegenzunehmen und dadurch Personalkapazität zu binden. Das Gesundheitsamt lud die betroffene Person vor und untersuchte sie amtsärztlich. Danach teilte es dem Ordnungsamt der Stadtverwaltung mit, daß Maßnahmen nach dem HFEG nicht erforderlich seien.

Die Rechtslage:

Das Hessische Gesetz über die öffentliche Sicherheit und Ordnung (HSOG) regelt in seinem § 22 die Übermittlung personenbezogener Daten an andere öffentliche Stellen. Zwischen Gefahrenabwehrbehörden (bei der für Maßnahmen nach dem HFEG zuständigen Ordnungsbehörde handelt es sich um eine Gefahrenabwehrbehörde) und den Polizeibehörden dürfen personenbezogene Daten übermittelt werden, soweit die Kenntnis dieser Daten zur Erfüllung der Aufgaben des Empfängers erforderlich "erscheint".

Im Falle der streitenden Nachbarinnen wandte sich die sich bedroht fühlende Person direkt an die Ordnungsbehörde. Diese nahm keine Datenübermittlung an andere Stellen vor. Insoweit ist ihr Verhalten aus datenschutzrechtlicher Sicht nicht zu beanstanden. Allerdings entstand bei der Ordnungsbehörde eine Akte, die nun mindestens zehn Jahre lang aufbewahrt wird. Diesen Zeitraum halte ich, wie auch in den beiden nachfolgenden Fällen, für zu lang.

Im Falle von Frau D. waren die drei Datenübermittlungen der Polizei an das Ordnungsamt, das Sozialamt und das Gesundheitsamt objektiv nicht erforderlich. Da aber § 22 Abs. 1 HSOG lediglich verlangt, daß die Datenübermittlung an die Ordnungsbehörde erforderlich "erscheinen" muß, und die Postkarten, die Frau D. an die Polizei richtete, Passagen enthielten, die eine Gefährdung nicht ausschließen ließen, habe ich die Datenübermittlung an das Ordnungsamt nicht beanstandet. Ich teile aber die Ansicht des Polizeipräsidenten in Frankfurt, der Frau D. auf ihre Dienstaufsichtsbeschwerde mitteilte, daß die Datenübermittlung an die Ordnungsbehörde nicht der angemessene und der Sache dienliche Weg gewesen sei. Dagegen entbehren die Datenübermittlungen an das Sozialamt – Sozialpsychiatrischer Dienst – und das Gesundheitsamt – Abteilung Psychiatrie – einer Rechtsgrundlage. Sie waren unzulässig. Den Polizeipräsidenten in Frankfurt habe ich auf diese Beurteilung hingewiesen, und ich habe diese beiden Datenübermittlungen nach § 27 Abs. 1 Hessisches Datenschutzgesetz (HDSG) gegenüber dem Hessischen Ministerium des Innern und für Europaangelegenheiten beanstandet. Das Innenministerium hat meine Rechtsauffassung im Ergebnis bestätigt und, um Fälle dieser Art künftig zu vermeiden, die Regierungspräsidien über die Angelegenheit unterrichtet.

In dem dritten Fall habe ich der Polizeidienststelle mitgeteilt, daß es keinen Grund gab, die Stadtverwaltung und das Kreisgesundheitsamt über ihre Annahme zu informieren, daß die Anzeigerstatterin psychisch krank sei. Hinter der Datenübermittlung stand nicht eine konkrete Gefahrensituation, sondern das Bestreben der Polizei zu vermeiden, weiterhin Strafanzeigen aufnehmen zu müssen, die jeder Grundlage entbehrten. Natürlich handelt es sich bei der Abwehr einer unnützen Inanspruchnahme um ein legitimes Interesse der Polizei. Dieses bietet aber keine ausreichende Rechtsgrundlage für die Information der Ordnungsbehörde oder psychiatrischer Beratungsstellen. Es ist nicht Aufgabe der Polizei, ohne konkrete Gefahrensituation vermeintlich oder tatsächlich psychisch kranke Menschen in der Weise einer ärztlichen Behandlung zuzuführen, indem sie andere Stellen über ihre Annahme einer psychischen Erkrankung informiert. Unbenommen bleibt es ihr selbstverständlich, Personen in geeigneter Form auf sozialpsychiatrische Beratungsangebote hinzuweisen.

5. Justiz

5.1

Gesetz zur Bekämpfung des illegalen Rauschgifthandels und anderer Erscheinungsformen der Organisierten Kriminalität (OrgKG)

Der Gesetzgeber will mit dem Gesetz zur Bekämpfung des illegalen Rauschgifthandels und anderer Erscheinungsformen der organisierten Kriminalität (OrgKG) eine wirksamere Bekämpfung der organisierten Kriminalität ermöglichen. Mit dem Ziel besteht Einvernehmen, nicht jedoch mit den Mitteln, mit denen das Ziel erreicht werden soll. Denn dies soll nach dem Willen des Gesetzgebers geschehen durch neue Kriminalisierungen, Ausdehnung von Strafbarkeiten und Erhöhungen von Strafdrohungen im materiellen Strafrecht, begleitet von einer Verschärfung der Eingriffsinstrumente mit weiterer Ausdehnung in den Bereich unverdächtiger Dritter im formellen Strafrecht. Denn mit den modernen Ermittlungsmaßnahmen werden zwangsläufig nicht nur Daten über Verdächtige, sondern im großen Umfang auch über Unbeteiligte erhoben, ohne daß die so auflaufenden Daten einer strengen Zweckbindung unterworfen sind. Das Gesetz stellt damit ein Musterbeispiel modernen Strafrechts, geprägt durch den Glauben an Effektivität strafrechtlicher Instrumente zur Lösung gesellschaftlicher Probleme, dar.

5.1.1

Neue Fahndungs- und Ermittlungsmethoden im strafrechtlichen Ermittlungsverfahren

Die nunmehr bundesweit geregelten modernen Fahndungs- und Ermittlungsmethoden, die Rasterfahndung, Einsatz Verdeckter Ermittler, Ausschreibung zur polizeilichen Beobachtung und Einsatz technischer Mittel zur Bild- und

Tonaufzeichnung gehören schon längst zum Polizeialtag und haben, weitgehend unbemerkt von der Öffentlichkeit, Einzug in die meisten Polizeigesetze der Länder gehalten. Das OrgKG greift diese Methoden für das strafrechtliche Ermittlungsverfahren auf und gibt gleichzeitig die Unterscheidung von polizeilicher Gefahrenabwehr einerseits und Strafverfolgung andererseits, die allgemein anerkannt zu unseren wichtigsten rechtsstaatlichen Traditionen gehört, weitgehend preis. So dürfen z.B. zur Gefahrenabwehr gespeicherte Daten für Zwecke der Strafverfolgung maschinell abgeglichen werden.

5.1.2

Neue Aufgabenverteilung zwischen Staatsanwaltschaft und Polizei

Damit nicht genug, leistet das Gesetz der gefährlichen Entwicklung Vorschub, Leitung und Verantwortlichkeit für das Ermittlungsverfahren von der Staatsanwaltschaft auf die Polizei zu verlagern. Der Einsatz moderner Technologien im Bereich strafrechtlicher Ermittlungen, verbunden mit dem Umstand, daß das Know-how der Datensammlung und die Informationstechnologie bei der Polizei liegen, führt mehr und mehr dazu, daß Auswahl, Umfang und Methodik der Beweiserhebung von der Polizei bestimmt werden.

Ich möchte am Beispiel des Verdeckten Ermittlers aufzeigen, wie die Polizei bei der Erhebung sensibler personenbezogener Daten ohne nennenswerte Beeinträchtigung durch eine justizielle Kontrolle ihr Interesse an Datensammlung verwirklichen kann: Der Einsatz eines Verdeckten Ermittlers im strafrechtlichen Ermittlungsverfahren bedarf der Zustimmung der Staatsanwaltschaft, in bestimmten Fällen des Richters. In Eilfällen kann die Polizei den Einsatz anordnen, muß dann aber unverzüglich die Entscheidung der Staatsanwaltschaft herbeiführen. Versagen der Staatsanwalt oder der Richter die Zustimmung, kann der Verdeckte Ermittler mit dem Hinweis der Polizei, Aufgaben der Gefahrenabwehr seien zu erfüllen, im Einsatz bleiben. Die im OrgKG festgeschriebenen Entscheidungsvorbehalte können ohne weiteres zur Makulatur werden.

Hinzu kommt, daß die Zulässigkeit des Einsatzes des Verdeckten Ermittlers nicht an einen klar definierten Straftatenkatalog gebunden ist, sondern an den konturenlosen Rechtsbegriff der "Straftat von erheblicher Bedeutung", über dessen Vorliegen im Eilfall dann ein Polizeibeamter zu entscheiden hat.

5.1.3

Die weitere Entwicklung – der "Lauschangriff"

Doch noch immer ist ein Wunsch der Ermittler, insbesondere der Polizei, offen.

So fordert nicht nur der Präsident des Bundeskriminalamtes mit Nachdruck die Einführung von Abhörmöglichkeiten in Wohnungen, die er allerdings nicht als "Lauschangriff", sondern als "elektronische Aufklärung" bzw. "elektronische Überwachung" bezeichnet haben will. Er verweist in diesem Zusammenhang ganz allgemein auf Erfahrungen in den USA und Italien. Die dort erzielten Ermittlungserfolge führt er darauf zurück, daß die Tatverdächtigen "häufig nicht mit derartigen Abhörmaßnahmen in der Wohnung, sondern nur mit der herkömmlichen Telefonüberwachung in der Wohnung" rechnen. Andererseits ist er der Auffassung, daß sich organisierte Straftäter erfahrungsgemäß schnell auf die rechtlichen und tatsächlichen Möglichkeiten der Strafverfolgungsbehörden einstellen, so daß eine enge Auslegung des verfassungsrechtlichen Wohnungsbegriffs, in den Arbeits-, Geschäfts- und Betriebsräume nicht einbezogen sind, die Ermittler nicht weiterbrächte, da die einschlägigen Gespräche in weiter durch Art. 13 GG geschützte Räume verlegt würden (DRiZ 1992, S. 355 ff.). Die Vision der Bedrohung unseres Rechtsstaates durch eine handlungsunfähige Strafrechtspflege hat ihre Wirkung nicht verfehlt.

In einer EntschlieÙung des Deutschen Bundestages vom 4. Juni 1992 heißt es dann auch, daß der Bundestag nach der Sommerpause "Möglichkeit und Notwendigkeit einer verfassungsrechtlich einwandfreien und praxisgerechten Regelung des Einsatzes technischer Mittel" in Wohnungen prüfen wird. Dieses Vorhaben wird im Bundestag parteiübergreifend unterstützt.

Ob nun der "GroÙe Lauschangriff", der Angriff auf das in einer Wohnung nicht öffentlich gesprochene Wort in Abwesenheit eines nicht offen ermittelnden Beamten, oder der "Kleine Lauschangriff", der die Anwesenheit eines Verdeckten Ermittlers voraussetzt, geführt wird, kann dahingestellt bleiben. Da auch der Unverdächtige Ziel eines Lauschangriffs sein kann, bedeutet dies die weitgehende Entgrenzung des privaten Bereichs. Der "Lauschangriff" auf die Wohnung verletzt den unantastbaren Bereich privater Lebensgestaltung, der der Einwirkung der öffentlichen Gewalt entzogen sein muß. Das Bundesverfassungsgericht (BVerfGE 27, 1 ff.) hat entschieden, daß dem einzelnen zur freien und selbstverantwortlichen Entfaltung seiner Persönlichkeit ein Innenraum verbleiben muß, in dem er "sich selbst besitzt" und "in den er sich zurückziehen kann, zu dem die Umwelt keinen Zutritt hat, in dem man in Ruhe gelassen wird und ein Recht auf Einsamkeit genieÙt". Auch strafprozessuale Maßnahmen dürfen nicht den Kernbereich eines Grundrechts verletzen.

Die Datenschutzbeauftragten des Bundes und der Länder haben daher auf ihrer Konferenz vom 1./2. Oktober 1992 (bei Gegenstimme des Bayerischen Landesbeauftragten für den Datenschutz) eine EntschlieÙung gefaÙt, in der sie fordern, daß eine angemessene Abwägung zwischen der Verfolgung der Organisierten Kriminalität und dem Schutz der Persönlichkeitsrechte der Bürger vorgenommen wird und eine Wahrheitserforschung um jeden Preis unterbleibt. Sie lehnen den "Lauschangriff" auf Privatwohnungen zum Zwecke der Strafverfolgung auch in Zukunft ab. Sie sind

der Meinung, daß andere Maßstäbe lediglich für Räume, die allgemein zugänglich sind, oder beruflichen oder geschäftlichen Tätigkeiten dienen (z.B. Hinterzimmer von Gaststätten, Spielcasinos, Saunacclubs, Bordelle), gelten können.

5.2

Justizmitteilungsgesetz

In Straf- und Zivilsachen einschließlich der Angelegenheiten der freiwilligen Gerichtsbarkeit machen die Gerichte und Staatsanwaltschaften während eines Verfahrens zahlreiche Mitteilungen von Amts wegen an andere öffentliche Stellen. Die Mitteilungen beruhen in der Straf- und Jugendgerichtsbarkeit auf der "Anordnung über Mitteilungen in Strafsachen (MiStra)" in der Fassung vom 15. März 1985 (BAnz. Nr. 60/1985) und für die Zivil- und freiwillige Gerichtsbarkeit auf der "Anordnung über Mitteilungen in Zivilsachen (MiZi)" vom 1. Oktober 1967 (BAnz. Nr. 218/1967), für den Bund zuletzt geändert durch Erlass vom 11. November 1985 (BAnz. Nr. 219/1985); außerdem gibt es weitere Verordnungen der Länder.

Als Rechtsgrundlage für die Mitteilungsanordnungen wurde bei deren Erlass der Amtshilfegrundsatz des Art. 35 Abs. 1 Grundgesetz, nach dem sich alle Behörden des Bundes und der Länder gegenseitig Rechts- und Amtshilfe zu leisten haben, angesehen. Diese Auffassung mußte spätestens mit der Entscheidung des Bundesverfassungsgerichts zum Volkszählungsgesetz 1983 (BVerfGE 65,1) aufgegeben werden.

Im Dezember 1986 hatte daher der Bundesminister der Justiz den Entwurf eines "Gesetzes über Mitteilungen der Justiz von Amts wegen in Zivil- und Strafsachen (Justizmitteilungsgesetz)" vorgelegt. Der Entwurf wurde zwischenzeitlich mehrfach überarbeitet und geändert. Während die neuen Vorschriften ursprünglich in das Gerichtsverfassungsgesetz (GVG) aufgenommen werden sollten, sieht der jetzige Regierungsentwurf (BR-Drucks. 206/1992) eine Änderung des Einführungsgesetzes zum Gerichtsverfassungsgesetz (EGGVG) vor.

5.2.1

Kritische Punkte

Der Entwurf sieht ungeachtet der mehrfach geäußerten Kritik der Datenschutzbeauftragten des Bundes und der Länder weiterhin nur Mitteilungsermächtigungen statt einer abschließenden Regelung der Mitteilungspflichten vor. Die Vorschriften des Entwurfs haben generalklauselartigen Charakter und sollen nicht durch Rechtsnormen, sondern durch bloße Verwaltungsvorschriften der Länder ausgefüllt werden. Maßstäbe dafür, unter welchen Voraussetzungen Übermittlungspflichten begründet werden dürfen, setzt der Entwurf auch in seiner jetzigen Fassung nicht. Er entspricht damit nicht den im Urteil des Bundesverfassungsgerichts zum Volkszählungsgesetz 1983 genannten Anforderungen, wonach Beschränkungen des Rechts auf informationelle Selbstbestimmung "einer (verfassungsmäßigen) gesetzlichen Grundlage bedürfen, aus der sich die Voraussetzungen und der Umfang der Beschränkungen klar und für den Bürger erkennbar ergeben und die damit dem rechtsstaatlichen Gebot der Normenklarheit entspricht".

Für besonders bedenklich halte ich die Regelung des § 13 Abs. 1 Nr. 1 EGGVG, wonach Gerichte und Staatsanwaltschaften personenbezogene Daten zur Erfüllung der in der Zuständigkeit des Empfängers liegenden Aufgaben übermitteln dürfen, wenn eine besondere Rechtsvorschrift dies zwingend voraussetzt. Nicht nur, daß die Erforderlichkeit zur Aufgabenerfüllung, die nach § 15 Abs. 1 Nr. 1 Bundesdatenschutzgesetz (BDSG) immer Zulässigkeitsvoraussetzung für die Übermittlung ist, nicht in die Regelung aufgenommen wurde – die Vorschrift kann ohne weiteres so ausgelegt werden, daß jede Rechtsnorm, die einer öffentlichen Stelle eine Aufgabe zuweist, für die sie personenbezogene Daten benötigt, gleichzeitig Datenübermittlungen an diese Stelle zuläßt. In einer bereichsspezifischen Vorschrift sollte auf eine derartige Generalklausel verzichtet und eine Zweckänderung nur zugelassen werden, wenn ein Gesetz diese ausdrücklich vorsieht.

Das Gesetz sieht nur für einige wenige Übermittlungsfälle einen Entscheidungsvorbehalt für den Richter, Staatsanwalt, Amtsanwalt oder den Beamten des gehobenen Justizdienstes vor. Der Entscheidungsvorbehalt sollte darüber hinaus auch für die übrigen Fälle gelten, soweit sich die Entscheidung über die Mitteilung nicht bereits unmittelbar aus dem Gesetz ergibt.

Die Gelegenheit, den Umfang der Mitteilungen zu verringern, indem beispielsweise – wie schon im 15. Tätigkeitsbericht (vgl. Ziff. 5.1.1) vorgeschlagen – bei Straftaten mit geringem Schuldgehalt und bei Fahrlässigkeitstaten in der Regel von einer Übermittlung abgesehen wird, hat die Bundesregierung nicht ergriffen.

5.2.2

Positive Ansätze

Der Gesetzesentwurf greift aber auch Punkte auf, die von den Datenschutzbeauftragten bereits seit längerer Zeit gefordert werden.

Eine Mitteilung vor rechtskräftigem Abschluß oder nicht nur vorläufiger Einstellung des Verfahrens ist die Ausnahme. Sie ist ausschließlich dann zulässig, wenn die zu benachrichtigende Behörde bereits zu diesem Zeitpunkt unaufschiebbare Maßnahmen treffen muß.

Der Betroffene ist über die Mitteilung zu unterrichten. Dieser Grundsatz ist jedoch durch zahlreiche Ausnahmen erheblich eingeschränkt. Negativ zu vermerken ist außerdem, daß die Mitteilung grundsätzlich gleichzeitig mit der Benachrichtigung erfolgt. Aus der Sicht des Rechtsschutzes des Betroffenen wäre eine vorherige Unterrichtung vorzuziehen.

Eine Nachberichts- und Unterrichtungspflicht der übermittelnden Stelle stellt sicher, daß der Empfänger keine überholten oder unrichtigen Daten nutzt.

Vorläufig, bis zum Inkrafttreten des derzeit in Vorbereitung befindlichen Gesetzes zur Änderung und Ergänzung des Strafverfahrensrechts (StVÄG) wurden die Meldungen der Staatsanwaltschaften und Gerichte über den Ausgang eines Strafverfahrens an die Polizei geregelt. Damit wurde eine Forderung aufgegriffen, die die Datenschutzbeauftragten des Bundes und der Länder in ihrer Konferenz am 4. Mai 1987 bereits in einem Beschluß verlangt hatten.

5.3

Beschlagnahme von Patientendaten

5.3.1

Zur Rechtslage

Nach § 53 Abs. 1 Nr. 3 Strafprozeßordnung (StPO) sind Ärzte, Zahnärzte, Apotheker und Hebammen berechtigt, das Zeugnis über das, was ihnen in ihrer beruflichen Eigenschaft anvertraut worden ist, zu verweigern. Zweck der Vorschrift ist der Schutz des Vertrauensverhältnisses zwischen diesen Berufsangehörigen und denen, die ihre Hilfe und Sachkunde in Anspruch nehmen. Entsprechend dazu normiert § 97 Abs. 1 und 2 StPO ein Beschlagnahmeverbot für schriftliche Mitteilungen, Aufzeichnungen und andere Gegenstände, auf die sich das Zeugnisverweigerungsrecht erstreckt.

Der strafprozessuale Schutz des "Patientengeheimnisses" ist somit begrenzt auf die Vertrauensperson als Zeugen. Im Strafverfahren gegen den Arzt oder in Fällen des Verdachts gemeinschaftlichen Handelns zwischen Arzt und Patient beispielsweise haben die Strafverfolgungsbehörden unbegrenzten Zugriff auf die Patientendaten.

Ein Beispiel dafür ist das "Memminger Strafverfahren". Angefangen hatte es im September 1986, als die Steuerfahndung die Wohnung und Praxis eines Frauenarztes wegen des Verdachts der Steuerhinterziehung durchsuchte und die Patientinnenkartei beschlagnahmte. Im Oktober 1986 wandte sich das Finanzamt an die Staatsanwaltschaft mit der Bitte, das Verfahren wegen des Verdachts illegaler Schwangerschaftsabbrüche zu übernehmen. Das tat die Staatsanwaltschaft und erwirkte vom Amtsgericht die Beschlagnahme der Karteikarten. In der Folgezeit wurde von der Staatsanwaltschaft nicht nur gegen den Frauenarzt, sondern auch gegen seine Patientinnen wegen des Verdachts des unerlaubten Schwangerschaftsabbruchs ermittelt.

Die Strafverfahren gegen die Patientinnen wurden, soweit sie nicht schon verjährt waren, in den meisten Fällen durch den Erlaß eines Strafbefehls abgeschlossen. Der Frauenarzt wurde wegen Steuerhinterziehung, unerlaubten Schwangerschaftsabbruchs, Abbruchs der Schwangerschaft ohne Beratung der Schwangeren und Abbruchs der Schwangerschaft ohne ärztliche Feststellung verurteilt. Gegen das Urteil legte der Arzt unter anderem mit der Begründung Revision ein, daß die erfolgte Beschlagnahme und Verwertung seiner Patientinnenkartei gegen das in § 97 StPO enthaltene Beschlagnahmeverbot und gegen Verfassungsrecht verstoße.

Der BGH bestätigte jedoch in seinem Urteil vom Dezember 1991 (BGH NJW 1992, 763) die Rechtmäßigkeit der Beschlagnahme.

5.3.2

Kritik an der bestehenden gesetzlichen Regelung

Unter dem Eindruck des "Memminger Strafverfahrens" hatte die Abgeordnete Frau Dr. Strelitz (SPD) im Dezember 1991 die mündliche Frage an den Landtag (Nr. 0189) gestellt, ob nach dem Urteil des Bundesgerichtshofs in Zukunft "in jedem Verdachtsfall gegen einen Arzt oder eine Ärztin Patientenkarteien bei allen Fachärzten und -ärztinnen beschlagnahmt werden können, ohne Berücksichtigung von Datenschutz und des besonderen Vertrauensverhältnisses zwischen Arzt bzw. Ärztin und Patient bzw. Patientin".

Patientenkarteien enthalten äußerst sensible personenbezogene Daten.

Das Bundesverfassungsgericht hat dazu ausgeführt (BVerfGE 32, 373, 380):

"Wer sich in ärztliche Behandlung begibt, muß und darf erwarten, daß alles, was der Arzt im Rahmen seiner Berufsausübung über seine gesundheitliche Verfassung erfährt, geheim bleibt und nicht zur Kenntnis Unberufener gelangt. Nur so kann zwischen Patient und Arzt jenes Vertrauen entstehen, das zu den Grundvoraussetzungen ärztlichen Wirkens zählt, weil es die Chancen der Heilung vergrößert und damit – im ganzen gesehen – der Aufrechterhaltung einer leistungsfähigen Gesundheitsfürsorge dient.

Bezieht sich der verfassungsrechtliche Schutz der Privatsphäre des einzelnen demnach auch auf die Karteikarte des Arztes, der sie dazu benutzt, die kraft seiner Sachkunde gemachten Wahrnehmungen über den Gesundheitszustand des Patienten festzuhalten und als Gedächtnisstütze für dessen weitere Behandlung zu verwenden, dann bedeutet dies, daß eine solche Karteikarte dem Zugriff der öffentlichen Gewalt grundsätzlich entzogen ist. Das ändert freilich nichts daran, daß selbst insoweit schutzwürdige Geheimhaltungsinteressen des Einzelnen zurücktreten müssen, wo überwiegende Belange des Gemeinwohls dies zwingend gebieten.“

Nimmt man diese Ausführungen als Maßstab, so wird das Recht des Patienten auf informationelle Selbstbestimmung in den derzeitigen Regelungen der Strafprozeßordnung zur Beschlagnahme nur unzulänglich berücksichtigt. Die Differenzierung, daß einerseits im Strafverfahren gegen den Patienten als Beschuldigten seine Karteikarte nicht beschlagnahmt werden darf (§ 97 Abs. 1 StPO), und daß andererseits im Strafverfahren gegen den Arzt als Beschuldigten die allgemeinen Beschlagnahmenvorschriften gelten (§§ 94 ff. StPO) und damit Patientenkarteeien generell beschlagnahmt werden dürfen, überzeugt nicht. Der Patient hat nicht nur ein schutzwürdiges Interesse daran, daß sein Arzt in einem Verfahren gegen ihn keine Beweismittel zur Verfügung stellt, sondern er hat darüber hinausgehend ein Interesse daran, daß seine persönlichen Daten, die er dem Arzt anvertraut hat, nur für Zwecke der Behandlung verwendet werden und Dritten nicht zur Kenntnis gelangen. Muß der Patient damit rechnen, daß Dritte Kenntnis von seiner Privatsphäre erhalten und diese Kenntnis u.U. – wie im “Memminger Strafverfahren“ – gegen ihn verwenden, beeinträchtigt dies den Aufbau eines Vertrauensverhältnisses zum Arzt.

5.3.3

Gesetzesantrag des Landes Hessen zur Änderung der Strafprozeßordnung

Die Hessische Landesregierung hatte deshalb am 4. August 1992 beschlossen, dem Bundesrat den Entwurf eines Gesetzes zur Änderung der Strafprozeßordnung mit dem Antrag zuzuleiten, seine Einbringung beim Deutschen Bundestag zu beschließen.

Der Entwurf sieht ein generelles, allein durch richterliche Anordnung einzuschränkendes Auskunftsverweigerungsrecht hinsichtlich der Angaben zu ärztlichen und zahnärztlichen Heilbehandlungen, der Beratung oder Versorgung in einer Apotheke oder den Beistand durch eine Hebamme vor und überträgt diesen allgemeinen Schutz des Patientengeheimnisses in gleicher Weise auf die Beschlagnahme von Arztunterlagen. Der Patient steht damit grundsätzlich als Zeuge zur Verfügung, kann aber auf alle Fragen, die das “Patientengeheimnis“ betreffen, die Auskunft verweigern und im selben Umfang über die Verwertung von entsprechenden Unterlagen entscheiden. Die Durchsetzbarkeit des staatlichen Strafverfolgungsanspruchs wird im Rahmen der Erforderlichkeit und Verhältnismäßigkeit durch einen richterlichen Anordnungsvorbehalt begrenzt: Gegenstand des Verfahrens muß ein Verbrechen oder eine Straftat von erheblicher Bedeutung sein; weitere Voraussetzung ist die Aussichtslosigkeit oder wesentliche Erschwernis der Ermittlungen ohne die Auskunft oder Beschlagnahme.

Obwohl der Entwurf ausgewogen einerseits das Recht auf informationelle Selbstbestimmung und andererseits auch legitime Ermittlungsinteressen berücksichtigt, haben der federführende Rechtsausschuß und der Ausschuß für Innere Angelegenheiten dem Bundesrat empfohlen, den Gesetzesentwurf beim Deutschen Bundestag nicht einzubringen. Ihrer Meinung nach sind das im Gesetzesantrag vorgesehene Auskunftsverweigerungsrecht und das korrespondierende Beschlagnahmeverbot kriminalpolitisch unvertretbar, verfassungspolitisch bedenklich und zum Schutz des Persönlichkeitsrechts von Zeugen nicht erforderlich. Der Bundesrat hat die Vorlage daraufhin am 6. November 1992 erneut in die Ausschüsse zurückverwiesen.

Sollten die Bedenken gegen den Gesetzesentwurf in den Ausschüssen, insbesondere was die Einschränkung der Strafverfolgung des Abrechnungsbetruges betrifft, nicht ausgeräumt werden können, wäre es wünschenswert, zumindest eine Regelung zu finden, die den Zugriff auf die Patientendaten zur Strafverfolgung gegen die Vertrauensperson zuläßt, eine Verwertung der daraus gewonnenen Erkenntnisse zur Strafverfolgung gegen den Patienten in der Regel jedoch nicht erlaubt.

5.4

Justizprüfungsamt

Nach dem Juristenausbildungsgesetz (JAG) haben die Rechtsreferendare in Hessen für die zweite juristische Staatsprüfung unter anderem eine Hausarbeit anzufertigen sowie einen Aktenvortrag zu halten.

Der Hausarbeit sind in der Rechtswirklichkeit entstandene Aktenstücke und Vorgänge, dem Aktenvortrag sind Rechtsfälle nach Vorgängen der Rechtswirklichkeit zugrunde zu legen (§§ 45 Abs. 3, 46 Abs. 3 JAG).

Nach Auffassung des Justizprüfungsamts setzen diese Vorschriften voraus, daß den Prüfungskandidaten Originalakten ausgehändigt werden. Obwohl in den Akten natürlich oft sehr sensible Daten enthalten sind, sieht das Justizprüfungsamt darin keine Beeinträchtigung der Persönlichkeitsrechte der Verfahrensbeteiligten, da die Kandidaten nach der juristischen Ausbildungsordnung (JAO) die Versicherung abzugeben hätten, daß sie von den als Prüfungsaufgabe überlassenen Akten keine Abschriften, Ablichtungen oder sonstige Kopien herstellen und Dritten keine Einsicht in die Akten gewähren. Lediglich in den Fällen, die der Sozial- oder Finanzgerichtsbarkeit unterliegen, sei es erforderlich, wegen der besonderen Schutzwürdigkeit der in diesen Akten verarbeiteten Daten, das Einverständnis der Betroffenen vor Ausgabe der Akten einzuholen.

M.E. ist in allen Fällen eine Ausgabe der Akten ohne Einverständnis oder ohne eine Anonymisierung, die keine Rückschlüsse auf die Beteiligten mehr zuläßt, unzulässig. Sicherlich besteht ein öffentliches Interesse an einer realitätsbezogenen Ausbildung und damit auch Prüfung des juristischen Nachwuchses. § 13 Abs. 4 Hessisches Datenschutzgesetz (HDSG) bestimmt daher, daß personenbezogene Daten, die für andere Zwecke erhoben worden sind, auch zu Ausbildungs- und Prüfungszwecken in dem dafür erforderlichen Umfang verwendet werden dürfen. Danach gilt auch hier der Erforderlichkeitsgrundsatz, der die Verwendung personenbezogener Daten nur dann zuläßt, wenn ohne sie eine Aufgabe nicht oder nicht vollständig erfüllt werden kann.

Nun ist die Ausgabe von Originalakten aber gerade nicht erforderlich, um die nach dem JAG praxisnahe Examensaufgabe zu stellen. Denn schließlich geht die Authentizität eines Falles nicht dadurch verloren, daß die Namen der Betroffenen geschwärzt oder, falls dies wegen der Vielzahl der Beteiligten nicht möglich ist, durch andere ersetzt werden. Sicher zieht diese Verfahrensweise einen gewissen Aufwand an Zeit und Personal nach sich. Diesen halte ich jedoch für unvermeidbar, wenn das Justizprüfungsamt die Akten trotz des entgegenstehenden Willens der Verfahrensbeteiligten an die Prüfungskandidaten ausgibt.

6. Kommunen

6.1

Vorlagen von Akten an Akteneinsichtsausschüsse

6.1.1

Das Recht der Gemeindevertreter, Akten einzusehen

Die Hessische Gemeindeordnung (HGO) räumt der Gemeindevertretung bzw. der Stadtverordnetenversammlung das Recht ein, zum Zwecke der Überwachung des Gemeindevorstands/Magistrats dessen Akten durch einen von ihr gebildeten Ausschuß einzusehen (§ 50 Abs. 2 S. 2 HGO). In aller Regel enthalten derartige Akten auch personenbezogene Daten, so daß sich die Frage stellt, ob und inwieweit diese Daten gegenüber den Mitgliedern des Akteneinsichtsausschusses offenbart werden dürfen. Für eine wirksame Ausübung des Kontrollrechtes kann auch eine Offenlegung personenbezogener Daten zulässig sein. Dabei kommt es zum einen auf die Sensibilität der jeweiligen Daten, zum anderen auf den Kontrollzweck an. Jedenfalls muß die Offenbarung personenbezogener Daten auf das erforderliche Maß beschränkt werden. Voraussetzung dafür ist, daß der Untersuchungsauftrag den Untersuchungsgegenstand deutlich benennt, d.h. der Kontrollzweck muß klar umrissen und eingegrenzt sein. Im Rahmen dieses Untersuchungsauftrages müssen und dürfen auch personenbezogene Daten offenbart werden. Die Kontrollbefugnisse der Gemeindevertretungen können jedenfalls nicht pauschal mit dem Hinweis auf datenschutzrechtliche Belange beschnitten werden.

Im zurückliegenden Berichtszeitraum gab es zwei herausragende Fälle, in denen die Kontrollrechte der Gemeindevertretung in einem besonderen Spannungsverhältnis zur Frage des Schutzes von personenbezogenen Daten standen:

6.1.2

Kriftel

In der Gemeinde war ein Fall der Veruntreuung gemeindlicher Gelder in Millionenhöhe aufzuklären. Das Rechnungsprüfungsamt des Main-Taunus-Kreises, eine im Auftrag des Gemeindevorstandes tätige Wirtschaftsprüfungsgesellschaft sowie der Prüfungsverband Südwestdeutscher Wohnungsunternehmen e.V. untersuchten diesen Fall und legten umfangreiche Prüfberichte vor. Die Gemeindevertretung hatte einen Akteneinsichtsausschuß gebildet, der Einsicht in diese Berichte nehmen wollte. Es galt aus Sicht der Gemeindevertretung insbesondere zu klären, welche Rolle der Gemeindevorstand im Gesamtverfahrensablauf spielte. Da die Berichte eine Vielzahl personenbezogener Daten enthielten, sei es über Mitarbeiter im Rathaus, sei es über Bankangestellte oder Angehörige von Baufirmen, stellte sich für den Gemeindevorstand die Frage, ob er dem Akteneinsichtsausschuß uneingeschränkte Einsicht nehmen lassen könnte.

Die Klärung der Frage, wie es zu der Veruntreuung gemeindlicher Gelder durch einen Gemeindebediensteten kommen konnte, gehört zu den Aufgaben der Gemeindevertretung. § 50 Abs. 2 S. 1 HGO bestimmt, daß die Gemeindevertretung die gesamte Verwaltung der Gemeinde und die Geschäftsführung des Gemeindevorstandes, insbesondere die Verwendung der Gemeindecinnahmen, überwacht. Um die Einzelheiten nachvollziehen zu können, kann deshalb ein von der Gemeindevertretung gebildeter Akteneinsichtsausschuß Einsicht in die zur Überprüfung erforderlichen Unterlagen verlangen. Es lag auf der Hand, daß dies in diesem Fall nur die erstellten Prüfberichte sein konnten; denn in ihnen war eine Aufarbeitung der Vorkommnisse vorgenommen worden.

Ich habe deshalb dem Gemeindevorstand mitgeteilt, daß den Mitgliedern des Akteneinsichtsausschusses die vollständigen Prüfberichte vorzulegen sind, da die Gemeindevertreter nur so ihre ihnen durch die HGO zugewiesene Kontrollfunktion ausüben können.

6.1.3

Frankfurt

In Frankfurt hatte die Stadtverordnetenversammlung einen Akteneinsichtsausschuß gebildet, um die Einzelheiten der Vergütung von Überstunden verschiedener Referenten zu klären. Festzustellen war, welche Referenten wieviel Überstunden zu welcher Bezahlung geleistet hatten. Eine Stadtverordnetenfraktion hatte deshalb beantragt, daß der Akteneinsichtsausschuß uneingeschränkt Einsicht in die Personalakten erhält.

Nun dürfen öffentliche Stellen die Daten ihrer Beschäftigten nach § 34 Abs. 1 Hessisches Datenschutzgesetz (HDSG) nur verarbeiten, wenn dies zur Eingehung, Durchführung, Beendigung oder Abwicklung des Dienst- oder Arbeitsverhältnisses oder zur Durchführung innerdienstlicher, organisatorischer, sozialer und personeller Maßnahmen erforderlich ist oder eine Rechtsvorschrift, ein Tarifvertrag oder eine Dienstvereinbarung es vorsieht. "Verarbeiten" im Sinne dieser Vorschrift ist auch die Offenbarung von Mitarbeiterdaten gegenüber der Stadtverordnetenversammlung oder einem Akteneinsichtsausschuß.

§ 50 Abs. 2 HGO, der die Einsichtsrechte eines Akteneinsichtsausschusses festschreibt, kann zwar Rechtsnorm im Sinne des § 34 Abs. 1 HDSG sein; aber auch, wenn es eine konkrete Rechtsnorm für die Offenbarung der durch § 34 HDSG besonders geschützten Personaldaten gibt, darf die Offenbarung nur in dem jeweils erforderlichen Umfang gestattet werden.

Die Forderung nach Vorlage der gesamten Personalakte ohne Präzisierung des Untersuchungsauftrages ist nicht mit § 34 Abs. 1 HDSG vereinbar; denn Berücksichtigung finden muß auch, was rechtlich gemeint ist, wenn man von der "Personalakte" spricht. Nach dem in der Rechtsprechung verwendeten sog. materiellen Personalaktenbegriff gehört alles, was den Bediensteten betrifft und in einem inneren Zusammenhang zum Beschäftigungsverhältnis steht, zur Personalakte. In der Regel sind deshalb in der Personalakte folgende Unterlagen enthalten:

- Einstellungsunterlagen (Bewerbungen, Lebenslauf, Lichtbild, Personenstandsurkunden, Schul- und Prüfungszeugnisse sowie Befähigungsnachweise),
- (soweit es Beamte betrifft) Abschriften der Urkunden über die Ernennungen, die Entlassung oder die Zuruhesetzung; (bei Angestellten) Arbeitsverträge mit evtl. Zusatzvereinbarungen,
- Abschriften von Versetzungs-, Abordnungs- und Umsetzungsverfügungen,
- dienstliche Beurteilungen und Ablichtungen von Dienstzeugnissen,
- Auszüge aus Versetzungsberichten zu Stellenausschreibungen, soweit sich die Berichte auf die Persönlichkeit oder die fachliche Leistung des Bediensteten beziehen,
- Besoldung und Versorgung, Beihilfen, Unterstützungen und Zuschüsse betreffende Unterlagen sowie Abschriften der einschlägigen Bescheide und Mitteilungen,
- ärztliche Äußerungen und Gutachten,
- Mitteilungen über strafrechtliche Ermittlungsverfahren oder Strafverfahren gegen den Beschäftigten, soweit sie Bezug zu seiner Rechtsstellung bzw. seinem Aufgabenfeld haben,
- Vorermittlungen und behördliche Disziplinarvorgänge einschließlich des Berichts des Untersuchungsführers (allerdings erst, sobald das Verfahren abgeschlossen ist), sowie
- Disziplinarverfügungen, -urteile und -beschlüsse; zudem sind (Gegen-)Äußerungen des Bediensteten aufzunehmen.

Würde dem Akteneinsichtsausschuß Einsicht in "die" Personalakte gewährt, würde ihm ein fast vollständiger Überblick über Lebensgeschichte und konkrete Verhältnisse der von der Überprüfung betroffenen Referenten gegeben, der in keinem Verhältnis zum Prüfungsauftrag "Überprüfung der Modalitäten der Abrechnung von Überstunden" gestanden hätte. Ein solcher Gesamteindruck wäre unter keinem Aspekt als erforderlich anzusehen.

Ich habe daher in diesem Fall lediglich die Vorlage der Arbeitsverträge mit möglichen Nebenabsprachen, der Arbeitszeitkarten und der Urlaubslisten für zulässig gehalten.

6.2

Fehlbelegungsabgabe

6.2.1

Gesetz

Am 4. März 1992 ist das Gesetz zum Abbau der Fehlsubventionen im Wohnungswesen (HessAFWoG, GVBl. I S. 87) in Kraft getreten. Mit diesem Gesetz wurden die rechtlichen Grundlagen dafür geschaffen, daß von Mietern, die in

einer Sozialwohnung leben, aber aufgrund gestiegenen Einkommens nicht mehr als Sozialmieter anzusehen sind, eine Ausgleichszahlung verlangt werden kann.

Die Ausgleichspflicht entsteht, wenn das Einkommen des Mieters die Einkommensgrenze nach § 25 Abs. 1 und 2 des Zweiten Wohnungsbaugesetzes (II. WoBauG, BGBl. I (1990) S. 1730) um mehr als 40 v.H. übersteigt. Insgesamt sieht das HessAFWoG eine Staffelung nach neun Gruppen bis zu einer Überschreitung der Einkommensgrenze um 150 v.H. vor.

Da sich die Höhe der möglichen Ausgleichszahlung nach dem Einkommen des Mieters richtet, mußten Regelungen über die Erhebung der Einkommensdaten gefunden werden. Ursprünglich wurde daran gedacht, die Regelung des Bundes in § 5 Abs. 1 des Gesetzes über den Abbau der Fehlsubventionierung im Wohnungswesen (AFWoG, BGBl. I (1981) S. 1542) zu übernehmen. Danach ist jeder Mitbewohner einer Sozialwohnung gegenüber dem Wohnungsinhaber verpflichtet, Auskünfte über sein Einkommen zu erteilen und ihm entsprechende Unterlagen auszuhändigen. Ich hielt diese Regelung für bedenklich, da nach Sinn und Zweck des Gesetzes die Kenntnis über das Einkommen lediglich für die Stelle, die die Höhe evtl. Ausgleichszahlungen festlegt und nicht für alle weiteren Wohnungsinhaber erforderlich ist. Der Landesgesetzgeber hat daraufhin die Bestimmung über die Erteilung von Auskünften über das Einkommen so gefaßt, daß jeder Wohnungsinhaber die weiteren in der Wohnung lebenden Personen benennen muß. Diese Personen sind dann selbst verpflichtet, der zuständigen Stelle auf Aufforderung die notwendigen Auskünfte über die Höhe ihres Einkommens zu erteilen (§ 7 Abs. 1 HessAFWoG).

Der Landesgesetzgeber hat ausdrücklich die Anwendung des § 5 Abs. 3 AFWoG ausgeschlossen, nachdem andere Behörden, insbesondere Finanzbehörden, sowie Arbeitgeber, der für die Festsetzung von Ausgleichszahlungen zuständigen Stelle Auskünfte über die Einkommensverhältnisse der Wohnungsinhaber zur Durchführung der Aufgaben nach dem Gesetz zu erteilen haben (§ 7 Abs. 6 HessAFWoG). Die Einkommensdaten werden also ausschließlich bei den Betroffenen erhoben.

6.2.2

Stand der Umsetzung

Zur Erhebung der notwendigen Daten zur Berechnung der Ausgleichszahlungen hat das Hessische Ministerium für Landesentwicklung, Wohnen, Landwirtschaft, Forsten und Naturschutz einen Fragebogen entwickelt, der mit mir abgestimmt wurde. Er wurde inzwischen in den meisten hessischen Kommunen den Mietern der aus öffentlichen Mitteln geförderten Wohnungen übersandt.

Nach dem Gesetz sind Empfänger von Sozialhilfe und Wohngeld von der Verpflichtung zur Leistung von Ausgleichszahlungen grundsätzlich befreit. In dem Fragebogen wird daher darauf verwiesen, daß für diesen Personenkreis kein Einkommensnachweis erbracht werden muß, wenn ein Bescheid über den Bezug der genannten Leistungen vorgelegt wird. Zunächst war beabsichtigt, die Einkommensdaten der Mieter von Sozialwohnungen unmittelbar bei den Sozialämtern zu erheben, diese Daten mit den Mieterlisten der sozialen Wohnungsgesellschaften abzugleichen und sodann die in beiden Datensätzen erscheinenden Personen, also Mieter, die auch Sozialhilfe- bzw. Wohngeldempfänger sind, aus der Fehlbelegungsliste zu streichen. Diesem Verfahren konnte ich nicht zustimmen. Zum einen dürfen Sozialdaten lediglich unter den engen Voraussetzungen der §§ 67 ff. Sozialgesetzbuch – Zehntes Buch – (SGB X), die hier nicht vorlagen, offenbart werden. Zum anderen sind personenbezogene Daten grundsätzlich bei dem Betroffenen mit seiner Kenntnis zu erheben (§ 12 Abs. 1 HDSG).

Jedoch war zu befürchten, daß viele der angeschriebenen Mieter nicht oder nicht innerhalb der gesetzten Frist auf die Aufforderung zur Abgabe einer Erklärung über ihr Einkommen reagieren würden. Ein solches Verhalten hätte zur Folge gehabt, daß die Festsetzungsstelle diese Mieter nach den höchsten Abgabesätzen zur Ausgleichszahlung herangezogen hätte. Da dies – insbesondere unter sozialen Gesichtspunkten – zu unbefriedigenden Ergebnissen geführt hätte, habe ich mich mit folgender Verfahrensweise einverstanden erklärt: Gibt der Mieter keine fristgerechte Erklärung ab und beantragt auch keine Fristverlängerung, gilt dies als Erklärung seines Einverständnisses, daß Auskünfte beim Sozialamt und der Wohngeldstelle darüber eingeholt werden, ob er Sozialhilfe oder Wohngeld erhält.

Aber grundsätzlich füllen auch Sozialhilfe- und Wohngeldempfänger den ersten Teil des Formblattes aus (siehe Anlage).

Dieses Verfahren schützt – mit Einschränkungen – das Recht auf informationelle Selbstbestimmung, indem es eine Zustimmung des Betroffenen zur Datenerhebung beim Sozialamt vermutet. Es weicht aber dem Zwang aus, bei einem – wie auch immer motivierten – Schweigen des Befragten den Höchstsatz der Fehlbelegungsabgabe festsetzen zu müssen. Ich muß betonen, daß ich diesem Verfahren nur unter Bedenken zustimmen konnte. Das Abweichen von der Regel, daß die ausdrückliche, nicht nur die implizite Zustimmung des Betroffenen zur Datenerhebung erforderlich ist, wurde nur mit Rücksicht auf die hier vorliegenden besonderen Umstände akzeptiert. Keinesfalls läßt sich dieses Verfahren für andere Zwecke generalisieren. Allgemein gilt vielmehr nach wie vor der Grundsatz der ausdrücklichen Zustimmung.

6.3

Die ungültigen Schwerbehindertenparkausweise

Bei der Lektüre des Amtsblattes der Stadt Frankfurt am Main ist ein Mitglied der Frankfurter Behindertenarbeitsgemeinschaft auf eine Rubrik gestoßen, in der vom Ordnungsamt der Stadt die Ungültigkeitserklärung von Schwerbehindertenparkausweisen mitgeteilt wurde. Genannt waren hier die Nummer des Schwerbehindertenparkausweises, der Name des Inhabers bzw. ehemaligen Inhabers sowie die Wohnanschrift. Insgesamt waren in dieser Ausgabe des Amtsblattes acht Namen aufgeführt.

Das Mitglied der Frankfurter Behindertenarbeitsgemeinschaft sah in dieser Mitteilung eine generelle Diskriminierung Schwerbehinderter und wertete die Auflistung der Betroffenen mit Name und Anschrift zudem als Verletzung ihres informationellen Selbstbestimmungsrechtes. Es wandte sich deshalb mit der Bitte um rechtliche Überprüfung an mich.

Eine Nachfrage beim Ordnungsamt der Stadt Frankfurt ergab, daß es sich bei dieser Art der Veröffentlichung um eine langjährige Übung handelt. Zu Beschwerden hierüber sei es noch nicht gekommen.

Ich wies den Leiter des Ordnungsamtes darauf hin, daß es für eine solche Mitteilung keine Rechtsgrundlage gibt und daß der von der Veröffentlichung betroffene Personenkreis erheblich in seinen Persönlichkeitsrechten beeinträchtigt ist; denn die Mitteilung des Ordnungsamtes gibt einem unbegrenztem Personenkreis Kenntnis über die mögliche Schwerbehinderteneigenschaft einzelner Personen und informiert über die Ungültigkeit ausgestellter Parkausweise, obwohl diese Information keineswegs für jeden Leser des Amtsblattes erforderlich ist. Auch im Ordnungsamt hielt man diese Veröffentlichungen nicht für erforderlich. Allenfalls die Stellen, die zulässigerweise den korrekten Einsatz des Schwerbehindertenparkausweises kontrollieren können, dürfen diese Information erhalten.

Der Leiter des Ordnungsamtes hat mir zugesichert, daß künftig auf die Veröffentlichung der Ungültigkeitserklärungen von Schwerbehindertenparkausweisen verzichtet werde.

6.4

Kommunale Umfragen

Immer häufiger versuchen Kommunen, durch Umfragen festzustellen, wie geplante Maßnahmen von ihren Einwohnern aufgenommen werden:

Die Verwaltung einer kleinen Gemeinde im Rheingau-Taunus-Kreis beabsichtigte, flächendeckend im gesamten Gemeindegebiet Tempo 30 einzuführen. Um zu sehen, wie die örtlichen Verkehrsteilnehmer dieses Vorhaben beurteilen, führte die Gemeindeverwaltung eine Fragebogenaktion durch. In den Bogen waren unter anderem Name und Anschrift des Befragten anzugeben; der Bogen war außerdem im Rathaus abzugeben. Ein Hinweis auf die Freiwilligkeit der Teilnahme an der Aktion erfolgte nicht. Die – vom Grundsatz her sicher sinnvolle – Umfrage hätte so nicht durchgeführt werden dürfen.

Seit mehr als fünf Jahren ist nun schon die Durchführung kommunaler statistischer Umfragen durch das Hessische Landesstatistikgesetz (HLStatG) geregelt. Dennoch wird immer wieder gegen die gesetzlichen Vorgaben verstoßen. In der Mehrzahl der Fälle ist Unkenntnis die Ursache. Je kleiner die Gemeinde, desto größer ist oft das Informationsdefizit. Das überrascht nicht, wenn man bedenkt, daß größere Kommunen über Statistikämter und damit zwangsläufig über größeres Fachwissen auf dem Gebiet der Statistik verfügen.

Statistische Umfragen dürfen jeweils bis zu 3.000 Befragte umfassen (§ 10 Abs. 4, 2 HLStatG). Voraussetzung ist, daß der Gemeindevorstand die Notwendigkeit für eine kommunale statistische Umfrage festgestellt hat und die statistische Geheimhaltung gewährleistet ist. Das heißt, die mit der Umfrage zusammenhängenden Aufgaben müssen einer Stelle innerhalb der Gemeindeverwaltung übertragen werden, die organisatorisch von den anderen Verwaltungsstellen getrennt und räumlich sowie personell abgeschottet ist. Sie darf außerdem keine auf den einzelnen Betroffenen gerichtete Verwaltungsaufgabe wahrnehmen. Darüber hinaus sind die Befragten – gegebenenfalls in einem Begleitschreiben – darauf hinzuweisen, daß keine Auskunftspflicht besteht, und daß durch die Versagung der Auskunft keine Rechtsnachteile entstehen. Aufzuklären ist auch über Sinn und Zweck der Umfrage sowie über den Zeitpunkt der Vernichtung der Fragebögen. Personenbezogene Daten dürfen nur erhoben werden, wenn das Befragungsziel ansonsten nicht zu erreichen ist. Aspekte der einfacheren Durchführung der Erhebung oder auch der Kontrolle über den Umfang der Beteiligung dürfen in diesem Zusammenhang nicht ausschlaggebend sein.

Die Durchführung einer kommunalen statistischen Umfrage kann ganz oder teilweise einer privaten Stelle (Befragungsinstitut, Ingenieurbüro) übertragen werden, sofern sichergestellt ist, daß die Vorschriften zum Schutz personenbezogener Daten und der statistischen Geheimhaltung eingehalten werden (§ 6 HLStatG). Der behördliche Datenschutzbeauftragte ist davon zu unterrichten. Die Verantwortung für die Rechtmäßigkeit der Datenverarbeitung bleibt bei der Kommune. Sie hat den Auftragnehmer unter besonderer Berücksichtigung der Eignung der von ihm getroffenen technischen und organisatorischen Maßnahmen sorgfältig auszuwählen und darauf zu achten, daß er die für den nicht-öffentlichen Bereich geltenden Vorschriften des Bundesdatenschutzgesetzes (BDSG) beachtet.

Im Einzelfall kann, abhängig von Art und Umfang des Auftrages, der an eine private Stelle vergeben wird, die Frage der Abgrenzung, ob das HLStatG oder das BDSG anzuwenden ist, erhebliche Probleme bereiten. Ich bin daher gerne bereit, die Kommunen bei der Vorbereitung von Umfragen zu unterstützen und zu beraten. In diesem Zusammenhang möchte ich nochmals darauf hinweisen, daß ich eine datenschutzrechtliche Bewertung nur dann vornehmen kann, wenn mir die notwendigen Unterlagen zur Verfügung stehen (vgl. 17. Tätigkeitsbericht, Ziff. 7.2.2.2).

7. Finanzwesen: Zweitwohnungssteuer

Verschiedene hessische Gemeinden haben die durch die Änderung des Kommunalabgabengesetzes vom 30. Oktober 1991 (GVBl. I S. 333) geschaffene Möglichkeit genutzt, für sog. Zweitwohnungen eine kommunale Steuer zu erheben. Entsprechende Satzungen sind erlassen worden bzw. in Vorbereitung.

Die Umsetzung der Vorschriften dieser Zweitwohnungssteuersatzungen in die Praxis hat zu einer Reihe datenschutzrechtlicher Probleme geführt. So haben einige Gemeinden einen von der Stadtverwaltung Winterberg in Nordrhein-Westfalen entworfenen Fragebogen übernommen, ohne dessen Zulässigkeit nach den Grundsätzen des Hessischen Datenschutzgesetzes (HDSG) geprüft zu haben. Der mehrseitige Fragebogen sollte von allen Bürgerinnen und Bürgern ausgefüllt werden ohne Rücksicht darauf, ob diese als Eigentümer oder Mieter von Zweitwohnungen überhaupt in Frage kamen; außerdem enthielt der Fragebogen einen völlig überzogenen Fragenkatalog, mit dem sämtliche nur denkbaren Eventualitäten gleichzeitig abgedeckt werden sollten.

Nach dem rechtsstaatlichen Gebot der Verhältnismäßigkeit des Mittels (BVerfGE 24,404; 25,292; 37,185), unter dem alles Handeln der Verwaltungsbehörden steht, muß eine behördliche Maßnahme zur Erreichung des vom Gesetzgeber erstrebten Ziels geeignet, aber auch erforderlich sein, d.h. daß das Ziel nicht auf eine andere, den einzelnen weniger belastende Weise ebenso gut erreicht werden kann. Dieser Grundsatz wird durch die genannte Praxis der Datenerhebung verletzt: Einmal dadurch, daß der Fragebogen allen Bürgerinnen und Bürgern zur Beantwortung übersandt wurde – also auch denen, die für die Steuer überhaupt nicht in Frage kamen –, zum andern durch die große Anzahl der – zum Teil entbehrlichen – Fragen.

Grundsätzlich dürfen ausschließlich die Daten erhoben und weiterverarbeitet werden, die aufgrund einer Satzung über die Zweitwohnungssteuer zur Aufgabenerfüllung, also beispielsweise zur Ermittlung der Steuerpflichtigen, Berechnung der Steuer etc., erforderlich sind (§ 11 HDSG).

Konkret bedeutet dies, daß die Datenerhebung auf die Einwohnerinnen und Einwohner beschränkt werden muß, die in dem betreffenden Ort mit Nebenwohnsitz (§ 16 Abs. 3 Hessisches Meldegesetz (HMG) vom 14. Juni 1982 – GVBl. I S. 126) gemeldet sind. Für die Übersendung des Fragebogens an alle Einwohner enthält die Satzung keine Rechtsgrundlage. Auch das Argument, dadurch erreiche man die in der Gemeinde Wohnenden, aber nicht Angemeldeten – z.B. die Bewohner von Wochenendhäusern – überzeugt nicht. Da nach §§ 15 und 16 Abs. 3 HMG Wochenendhäuser Nebenwohnungen sind, müssen in diesen Fällen die Betroffenen zunächst von der Gemeinde aufgefordert werden, ihrer Meldepflicht nach § 13 Abs. 1 HMG nachzukommen.

Auch der Fragebogen selbst, der für die Datenerhebung verwendet werden soll, darf nicht zur Datenerhebung auf Vorrat oder zur Ausforschung der Betroffenen führen. Diese Möglichkeit bietet der erwähnte Entwurf in hohem Maße; er kommt in bedenkliche Nähe einer jenseits der Vorschriften der §§ 12, 13, 18, 19 des Hessischen Landesstatistikgesetzes (HessLStatG) vom 19. Mai 1987 (GVBl. I S. 67) erhobenen Kommunalstatistik.

Daten, über die die Gemeinde bereits verfügt, dürfen nicht nochmals erhoben werden. Beispielsweise kann die Gemeinde durch Abgleich der Grundstücksdatei mit den Meldedaten – die Übermittlung von Meldedaten an das Gemeindesteueramtsamt ist gemäß § 38 Abs. 1 und 7 HMG zulässig – unschwer ermitteln, ob es sich bei Inhabern von Nebenwohnungen um deren Eigentümer oder aber um Mieter handelt. Dementsprechend kann entweder ein Fragebogen für Eigentümer oder ein solcher für Mieter versandt werden, aber nicht beide zugleich.

Zu Fragen, die nicht auf die Satzung gestützt werden können, muß ein Hinweis enthalten sein, daß deren Beantwortung freiwillig ist, und daß dem Betroffenen aus einer Nichtbeantwortung keine Nachteile entstehen.

Der Fragebogen darf mit seinen Fragen nicht alle Eventualitäten abdecken, wie dies bei dem genannten Muster der Fall ist. Sollte sich im Einzelfall zusätzlicher Informationsbedarf ergeben, muß die Behörde bei dem Betroffenen rückfragen. Hier ist also im Einzelfall ein stufenweises Vorgehen erforderlich; nur so kann verhindert werden, daß von einer Vielzahl von Betroffenen überflüssigerweise Daten erhoben werden, die nur für wenige gebraucht werden.

Ich habe die im Zusammenhang mit der Zweitwohnungssteuer entstandenen datenschutzrechtlichen Fragen mit dem Hessischen Städte- und Gemeindebund – der die hier betroffenen Gemeinden und Kleinstädte vertritt – beraten. Dabei hat sich erwiesen, daß diese Institution meine Auffassung in der Sache teilt. Der Hessische Städte- und Gemeindebund hat inzwischen im Kreise seiner Mitglieder Einzelheiten des Fragebogens besprochen und eine entsprechend geänderte, den Forderungen des Datenschutzes angepaßte Fassung erarbeitet.

8. Rundfunk: Weitergabe von Hörerbriefen durch einen privaten Rundfunksender

Nachdem der private Rundfunksender Radio FFH einen Werbespot der deutschen Pelzindustrie ausgestrahlt hatte, erhielt er zahlreiche Protestbriefe, mit denen sich Hörer gegen Art und Inhalt der Sendung wandten und die Redaktion aufforderten, sich zu den erhobenen Vorwürfen zu äußern.

Doch statt eines Briefes von Radio FFH erreichte die Tierschützer ein Schreiben des Deutschen Pelzinstituts, in dem die von den Tierschützern gegenüber Radio FFH gemachten Vorwürfe – insbesondere über die Art der Tötung der Tiere – in harscher Form zurückgewiesen wurden. Die unterzeichnende Geschäftsführerin forderte "Beweise" und verwies unter anderem auf die Möglichkeit einer Verleumdungsklage.

Die Betroffenen baten mich daraufhin um Prüfung, ob der Sender ihre persönlichen Daten an Dritte weitergegeben habe.

Nach § 54 des Hessischen Privatrundfunkgesetzes vom 30. November 1988 (HPRG, GVBl. I S. 385) überwacht der Hessische Datenschutzbeauftragte die Einhaltung der Datenschutzbestimmungen im Anwendungsbereich dieses Gesetzes, zu dem auch der private Rundfunk gehört. Der zweite Teil des Hessischen Datenschutzgesetzes (HDSG), in dem unter anderem meine Prüfungsbefugnisse geregelt sind, findet entsprechende Anwendung; im übrigen sind die Vorschriften des Bundesdatenschutzgesetzes (BDSG) anzuwenden.

Ich bat die Redaktion von Radio FFH, sich zu den erhobenen Vorwürfen zu äußern. In seiner ersten Stellungnahme versicherte mir der Programmdirektor und Geschäftsführer, daß die Briefe nicht weitergeleitet worden seien. Diese Aussage stand jedoch im Widerspruch zu dem Schreiben des Deutschen Pelzinstituts, in dem den Protestschreibern eindeutig und unmißverständlich mitgeteilt wurde, daß es die Briefe von Radio FFH erhalten habe. Erst die Vorlage einer anonymisierten Kopie des Briefes an die Tierschützer veranlaßte den Sender zu erneuten Recherchen und dem Eingeständnis, in zehn Fällen die Adressen weitergegeben zu haben. Gleichzeitig räumte man ein, die Übermittlung ohne die Einwilligung der Absender vorgenommen zu haben und sicherte zu, dies künftig zu unterlassen.

Nun ist nach § 28 Abs. 2 Ziff. 1b BDSG eine Datenübermittlung nicht-öffentlicher Stellen nicht zulässig, wenn Grund zu der Annahme besteht, daß der Betroffene ein schutzwürdiges Interesse an dem Ausschluß der Übermittlung hat. Dies ist hier der Fall. M.E. müssen die Hörer darauf vertrauen können, daß der Sender Briefe, mit denen Kritik an Sendungen geübt wird, selbst beantwortet und nicht an den für den Inhalt der Werbesendung Verantwortlichen weiterleitet, von dem sie dann unverlangt Briefe oder Anrufe erhalten.

Von einer formellen Beanstandung gegenüber der Hessischen Landesanstalt für privaten Rundfunk habe ich dennoch abgesehen, da mir von der Leitung des Senders ausdrücklich zugesichert wurde, daß künftig keine Anschriften mehr an Dritte weitergegeben werden.

9. Gesundheit

9.1

Krebsregister: Treuhandmodell als neuer Lösungsweg

9.1.1

Verhindert Datenschutz Krebsregister?

Im vergangenen Jahr gab es vielfach Diskussionen über die Frage, ob in Hessen ein epidemiologisches Krebsregister aufgebaut werden sollte. Anlässe hierfür waren unter anderem öffentlich erhobene Forderungen des leitenden Betriebsarztes der Firma Hoechst nach umfassenderen Möglichkeiten epidemiologischer Erforschung von Krebserkrankungen sowie das Bekanntwerden einer möglicherweise erhöhten Krebsrate im Kreis Bergstraße. Im Rahmen dieser Diskussionen wurde in einigen Presseveröffentlichungen die pauschale Behauptung aufgestellt, daß "der Datenschutz Krebsregister verhindert".

Diese Darstellung ist unzutreffend. Obwohl ich ihr in zahlreichen Vorträgen, Stellungnahmen und Gesprächen entschieden entgegengetreten bin, werden derartige schlagwortartige Behauptungen jedoch nach wie vor immer wieder erhoben. Da mir daran liegt, daß der Datenschutz nicht in dieser unangemessenen Weise als Verhinderer gesundheitspolitischer Maßnahmen dargestellt – vielleicht auch vorgeschoben – wird, habe ich die aktuelle datenschutzrechtliche Position zu Krebsregistern noch einmal im persönlichen Gespräch mit der Ministerin für Jugend, Familie und Gesundheit, im Unterausschuß für Informationsverarbeitung und Datenschutz des Hessischen Landtags sowie in meiner Rede zur Beratung des 20. Tätigkeitsberichts in der Plenarsitzung des Hessischen Landtags am 24. September 1992 dargelegt.

9.1.2

Datenschutz als Rahmenbedingung für Krebsregister

Die Datenschutzbeauftragten sind weder für noch gegen epidemiologische Krebsregister; sie haben vielmehr immer die Auffassung vertreten, daß der Aufbau eines Krebsregisters eine gesundheitspolitische Frage ist, die von den

jeweils zuständigen politischen Gremien entschieden werden muß. Sie fordern jedoch, daß bestimmte datenschutzrechtliche Rahmenbedingungen gewährleistet sein müssen, wenn ein solches Register aufgebaut wird. Die in ein Krebsregister aufzunehmenden Daten über Krebserkrankungen werden im Rahmen eines konkreten Arzt-Patienten-Verhältnisses zum Zwecke der Behandlung erhoben und unterliegen der ärztlichen Schweigepflicht i.S.d. § 203 Strafgesetzbuch. Die Belange der Patienten dürfen nicht völlig unberücksichtigt bleiben, sondern es ist ein angemessener Ausgleich zwischen den Interessen an epidemiologischer Forschung einerseits und dem Recht auf informationelle Selbstbestimmung der Patienten andererseits herzustellen. Ein solcher Ausgleich ist durchaus möglich. Es sind verschiedene Modelle hierfür denkbar.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat im Jahre 1990 in einem Beschluß zur Erarbeitung von Krebsregistergesetzen in Bund oder Ländern ein Einwilligungsmodell und ein dezentrales Verschlüsselungsmodell als aus datenschutzrechtlicher Sicht gangbare Wege bezeichnet und zugleich darauf hingewiesen, daß eine Entwicklung weiterer Modelle denkbar ist (19. Tätigkeitsbericht, Ziff. 17.3.7). Das Einwilligungsmodell sieht vor, daß eine Meldung der Krebserkrankung an ein zentrales Register grundsätzlich nur mit Einwilligung der Patienten möglich ist. Bestimmte Ausnahmeregelungen sind vorgesehen, z.B. für die Fälle, in denen die Patienten über ihre Krebserkrankung vom Arzt nicht aufgeklärt wurden. In Hamburg und Münster wird derzeit das Einwilligungsmodell auf gesetzlicher Grundlage praktiziert. Das dezentrale Verschlüsselungsmodell sieht vor, daß die Ärzte die personenidentifizierenden Angaben nur verschlüsselt an das Register weitergeben: Die personenidentifizierenden Angaben werden von den Ärzten in einen Verschlüsselungsrechner eingegeben. Der von allen Ärzten in der gleichen Weise verwendete Verschlüsselungsalgorithmus bildet die Daten auf einen nichtsprechenden Code ab, der zusammen mit den übrigen Angaben an das Register weitergeleitet wird. Dieses Modell wurde in Baden-Württemberg von 1985 bis 1989 im Rahmen einer Pilotstudie getestet (s. hierzu Ministerium für Arbeit, Gesundheit, Familie und Sozialordnung Baden-Württemberg (Hrsg.), Epidemiologisches Krebsregister Baden-Württemberg, Kurzfassung des Abschlußberichts, 1989).

9.1.3

Treuhandmodell

In der Zwischenzeit ist ein neues Modell entwickelt worden, das sog. Treuhandmodell. Dieses von Professor Michaelis im Universitätsklinikum Mainz vorgeschlagene Modell sieht eine neue Form des Ausgleichs zwischen Forschungsinteressen und dem Recht auf informationelle Selbstbestimmung der betroffenen Patienten vor und zwar in der Weise, daß das Krebsregister aus zwei getrennten Stellen besteht: Es gibt die Vertrauensstelle, die die Identifikationsdaten der Patienten (insbesondere Name, Geburtsdatum, Adresse) ohne Einwilligung der Patienten erhält, sie verschlüsselt und anschließend an die eigentliche Registerstelle weitergibt. Die Registerstelle speichert den gesamten Registerdatenbestand, also insbesondere die detaillierten medizinischen Daten, auf anonymisierter Basis. In Einzelfällen, z.B. für bestimmte Forschungsvorhaben, können die Patientendaten von der Vertrauensstelle wieder entschlüsselt werden. Kern des Modells ist es also, daß zwar einerseits personenbezogene Daten ohne Einwilligung der Patienten gemeldet werden und damit eine weitgehende Vollständigkeit des Registers sowie die Möglichkeit der Durchführung von Forschungsprojekten mit personenbezogenen Daten aus dem Register sichergestellt sind, andererseits aber die Verarbeitung personenbezogener Daten insgesamt auf ein Minimum reduziert ist, weil das Register im wesentlichen auf anonymisierter Basis arbeitet. Verschiedene Ausgestaltungen im einzelnen sind denkbar.

Im Frühjahr 1992 hat sich ein Arbeitskreis der Konferenz der Datenschutzbeauftragten des Bundes und der Länder in meiner Dienststelle unter teilweiser Beteiligung von Professor Michaelis eingehend mit dem Treuhandmodell befaßt. Ich sehe dieses Modell als einen interessanten neuen Lösungsweg an und habe hierüber auch das Ministerium für Jugend, Familie und Gesundheit informiert. Was immer in Hessen künftig gesundheitspolitisch in dieser Frage entschieden wird – der Datenschutz steht jedenfalls einem Krebsregister nicht entgegen.

9.2

Krankenversichertenkarte in Chipkartenform wird Krankenscheinersatz

9.2.1

Die Vorgaben des Gesundheitsreformgesetzes

Mit dem Gesundheitsreformgesetz vom 20. Dezember 1988 (BGBl. I S. 2477; siehe hierzu auch 19. Tätigkeitsbericht, Ziff. 5.2) hat der Gesetzgeber festgelegt, daß der bisher in der gesetzlichen Krankenversicherung verwendete Krankenschein durch eine Krankenversichertenkarte ersetzt wird, die künftig bei jeder ärztlichen Behandlung von den Versicherten vorgelegt werden soll (§ 291 Abs. 1 Fünftes Buch Sozialgesetzbuch (SGB V)). Mit der Einführung der Krankenversichertenkarte als Krankenscheinersatz werden rationellere Arbeitsabläufe und besserer Service für die Versicherten angestrebt, vor allem aber ist die Karte ein Teil der im Gesundheitsreformgesetz und im Gesundheitsstrukturgesetz vorgesehenen Maßnahmen, mit denen der Gesetzgeber "Transparenz des Leistungsgeschehens" und Kostenbegrenzung im Gesundheitswesen erreichen will.

Der Umfang der auf der Krankenversichertenkarte enthaltenen personenbezogenen Daten sowie ihr Verwendungszweck sind in § 291 Abs. 2 SGB V abschließend geregelt. Danach enthält die Karte neben der Bezeichnung der ausstellenden Krankenkasse Familien- und Vornamen des Versicherten, Geburtsdatum, Anschrift, Krankenversichertennummer, Versichertenstatus, Beginn und – bei befristeter Gültigkeit – Ablauf des Versicherungsschutzes. Sie

darf nur für den Nachweis der Berechtigung zur Inanspruchnahme von Leistungen im Rahmen der kassen- oder vertragsärztlichen Versorgung sowie für die Abrechnung mit den Leistungserbringern verwendet werden. Die Karte ist also ausschließlich eine Identifikationskarte.

Die technische Form der Krankenversichertenkarte ist im Gesetz nicht festgelegt. Das Gesetz schreibt lediglich vor, daß die Angaben auf der Karte in einer für die maschinelle Übertragung auf die für die kassenärztliche Versorgung vorgesehenen Abrechnungsunterlagen und -vordrucke geeignet sein muß (§ 291 Abs. 2 SGB V). Denkbar wäre beispielsweise eine Prägekarte, die eine Übertragung der Daten im Adremaverfahren auf die Abrechnungsunterlagen und -vordrucke zuließe, oder eine maschinenlesbare Chip- oder Magnetstreifenkarte, die es ermöglicht, gespeicherte Daten unmittelbar auf andere Speichermedien zu übernehmen und weiter zu verarbeiten. Nach der gesetzlichen Regelung vereinbaren die Spitzenverbände der Krankenkassen und die Kassenärztlichen Bundesvereinigungen vertraglich die Einzelheiten über die bundesweite Einführung und Gestaltung der Krankenversichertenkarte (§ 291 Abs. 1 i.V.m. § 1 SGB V).

9.2.2

Entscheidung für die Krankenversichertenkarte in Chipkartenform

Die für die Ausgestaltung der Krankenversichertenkarte zuständigen Vertragsparteien haben nach langwierigen Verhandlungen beschlossen, daß die Krankenversichertenkarte in der Form einer Chipkarte eingeführt werden soll. Hintergrund dieser Entscheidung war auch, daß seit einigen Jahren in Europa verschiedene medizinische Anwendungen der Chipkartentechnik erprobt werden. Als Gründe wurden unter anderem die folgenden Aspekte angeführt:

- Die Datensicherheit der Chipkartentechnik kann gegenüber der Magnetkartentechnik wesentlich höher sein.
- Die Chipkarte bietet eine wesentlich höhere Speicherkapazität sowie vielfältige Verwendungsmöglichkeiten und eröffnet eine neue Dimension medizinischer Information und Kommunikation.

Aus datenschutzrechtlicher Sicht trifft es sicherlich zu, daß die Chipkartentechnik grundsätzlich umfassendere Möglichkeiten zur Datensicherung bietet als z.B. eine Magnetstreifenkarte. So ist es möglich, die auf der Chipkarte enthaltenen Informationen mit Paßwörtern bzw. mit einer Zugriffsberechtigungskarte des Arztes zu sichern, und auch verschiedene Zugriffsebenen zu definieren und ein abgestuftes Zugriffsverfahren vorzuschreiben. Demgegenüber sind die auf der Magnetstreifenkarte gespeicherten Daten grundsätzlich lesbar und können nicht durch einen in das Medium integrierten Zugriffsschutz gesichert werden. Die Frage der Datensicherung würde allerdings in erster Linie dann relevant werden, wenn der Datenumfang auf der Krankenversichertenkarte wesentlich erweitert würde.

9.2.3

Vorgezogene Einführung der Krankenversichertenkarte in Wiesbaden und im Rheingau-Taunus-Kreis

Der im Gesundheitsreformgesetz für die Einführung der Krankenversichertenkarte vorgesehene Termin (1. Januar 1992) konnte nicht eingehalten werden. Dem jetzt geschlossenen Vertrag zufolge wird die bundesweite Einführung der Krankenversichertenkarte in zwei Stufen erfolgen. In einer ersten Stufe mit wissenschaftlicher Begleituntersuchung werden ca. 800.000 Versicherte mit der Karte und etwa 1.700 Arzt- und Zahnarztpraxen mit den zur Verarbeitung erforderlichen Geräten in ausgewählten Regionen, zu denen die Stadt Wiesbaden und der Rheingau-Taunus-Kreis gehören, ausgestattet. Für Wiesbaden und den Rheingau-Taunus-Kreis geht man derzeit davon aus, daß die Krankenversichertenkarte bis zum 1. April 1993 eingeführt werden kann. Beteiligte Krankenkassen sind die AOK Wiesbaden-Rheingau-Taunus, die Betriebskrankenkassen, die Innungskrankenkasse Wiesbaden, Bundesknappschaft und neun Ersatzkassen. Die Einführung betrifft ca. 410.000 Patienten, 600 Ärzte und 300 Zahnärzte. Im November 1992 erfolgte die Auftragsvergabe für die Herstellung der Chipkarte einschließlich der Erstspeicherung der Patientenangaben.

Wegen der Einzelheiten der Einführung der Karte in der Region Wiesbaden und Rheingau-Taunus-Kreis habe ich bereits erste Gespräche mit Krankenkassen und der Kassenärztlichen Vereinigung geführt. Aus datenschutzrechtlicher Sicht müssen bei der Umsetzung der gesetzlichen und vertraglichen Bestimmungen vor allem die folgenden Punkte beachtet werden:

- Eine Begrenzung der Speicherkapazität der Chipkarte muß sichergestellt werden. Die Karte sollte nur lesbar, nicht jedoch beschreibbar sein. Die Arzt- und Zahnarztpraxen dürfen nur Chipkarten-Terminals erhalten, die ausschließlich den Lesezugriff auf die Karte ermöglichen. Es muß sichergestellt werden, daß kein Unbefugter den Inhalt der Daten verändern kann. Geräte und Software müssen diesen Anforderungen entsprechen. Es wird überlegt, die Komponenten durch das BSI bzw. ein vom BSI autorisiertes Institut zertifizieren zu lassen. Als Konsequenz muß auch erreicht werden, daß die Komponenten nur in der zertifizierten Version zum Einsatz kommen. Zumindest für die Zeit nach der Einführungsphase sind daher Vorkehrungen zu treffen, daß Manipulationen an den Geräten und der Software nicht möglich sind oder erkannt werden. Hier können insbesondere kryptographische Methoden in Betracht gezogen werden.
- Die betroffenen Patienten müssen sich jederzeit über den Inhalt der auf der Krankenversichertenkarte enthaltenen Angaben informieren können, d.h. ein Leserecht bei der Krankenkasse oder beim Arzt haben.

9.2.4**Führt der Einsatz der Chipkartentechnik langfristig zum "gläsernen Patienten"?**

Wenngleich derzeit Einigkeit darüber besteht, daß die Krankenversichertenkarte als Chipkarte ausschließlich mit den gesetzlich vorgesehenen Angaben eingeführt werden soll, so bleibt doch die Tatsache bestehen, daß die Verwendung der Chipkartentechnik grundsätzlich die Möglichkeit eröffnet, erheblich mehr Daten auf der Krankenversichertenkarte zu speichern und diese Karte – oder auch vergleichbare weitere Karten – und die bei den Ärzten vorhandenen Lesegeräte zu vielfältigen Zwecken einzusetzen. Die erhöhte Speicherkapazität der Chipkarte stellt grundsätzlich einen Anreiz dar, den Informationsgehalt der Karte zu erweitern und beispielsweise Daten über Medikamentenunverträglichkeiten, Allergien, Röntgenaufnahmen, Unfalldaten, Anamnesedaten, Einwilligungen in Organtransplantationen im Todesfall oder die gesamte Krankengeschichte der Patienten aufzunehmen.

Kritiker haben deshalb die Befürchtung geäußert, daß die Entwicklung zum "gläsernen Patienten" führt, der seine Daten in umfassender Weise überall offenlegen muß.

Da das Gesundheitsreformgesetz eine abschließende Regelung zu Inhalt und Zweck der Krankenversichertenkarte getroffen hat, könnten eine generelle Erweiterung der Angaben auf der Karte oder eine Änderung ihrer Nutzung nur aufgrund einer Gesetzesänderung eingeführt werden.

Sicher gibt es, angefangen von der Versorgung von Unfallopfern bis hin zur Vermeidung unnötiger Untersuchungen, gute Argumente für die Aufnahme medizinischer Daten auf die Krankenversichertenkarte. Sollte eine entsprechende Verfahrensweise vom Gesetzgeber überlegt werden, so wäre jedoch zunächst zu klären, welche Ärzte bzw. Stellen auf welche Daten in welcher Weise Zugriff haben sollen. Die Entscheidungsfreiheit des Patienten über die Verwendung seiner Daten dürfte nicht beschränkt werden. Es darf nicht dazu kommen, daß vom Patienten routinemäßig erwartet wird, daß er auf der Chipkarte vorhandene zusätzliche Daten offenbart, ohne daß deren Kenntnis für die konkrete Behandlung erforderlich ist.

Eine andere Frage ist es, ob die Krankenversichertenkarte als Chipkarte auf freiwilliger Basis in einem weiteren Umfang als im Gesundheitsreformgesetz vorgesehen genutzt werden könnte, d.h. in der Weise, daß der Patient in die Aufnahme zusätzlicher Daten auf die Karte einwilligen kann. Auch bei einer solchen Lösung gibt es datenschutzrechtliche Aspekte, die zu berücksichtigen sind. Zunächst müßten auf der Chipkarte verschiedene Zugriffsebenen und -berechtigungen unterschieden werden, damit der Patient auch bei dieser Konstellation steuern kann, wer Daten von ihm erhält. Unabhängig davon bestünde aber das Problem, daß die Versicherten verpflichtet wären, eine Krankenversichertenkarte zu benutzen, auf der sich außer solchen Daten, für die eine gesetzliche Offenbarungspflicht besteht, auch Daten befinden, für die eine solche Eingriffsgrundlage nicht vorhanden ist (Kombination der Pflichtkarte mit freiwilligen Zusatzinformationen), und daß sich ein faktischer Zwang zur Offenbarung aller auf der Karte enthaltenen Daten ergeben könnte. Die Erfahrung zeigt, daß Patienten sich wegen ihrer in gewisser Weise vorhandenen Abhängigkeit vom Arzt unter den Druck gesetzt fühlen können, Einwilligungen in die Offenbarung ihrer Daten zu erteilen. Unter diesem Gesichtspunkt wäre die Einführung einer zweiten Chipkarte, z.B. einem Notfallausweis oder einer Karte für die Langzeitbetreuung von Diabetikern, auf freiwilliger Basis die bessere Lösung, weil sie der notwendigen Freiwilligkeit der Entscheidung der Patienten in umfassenderer Weise Rechnung tragen würde.

Diese Karte könnte dann auch an Patienten, die privat versichert sind oder deren Behandlungskosten die Sozialhilfeträger übernehmen, ausgegeben werden.

9.3**Unzulässige Öffnung von Leichenschauschein in Frankfurt am Main**

Aufgrund verschiedener Hinweise auf unzulässige Öffnungen der Leichenschauschein habe ich im Frühjahr 1992 Prüfungen beim Standesamt, Garten- und Friedhofsamt sowie beim Gesundheitsamt in Frankfurt am Main durchgeführt. In diese Prüfungen war das Referat Datenschutz des Frankfurter Magistrats einbezogen. Ergebnis meiner Prüfungen war, daß der Umgang mit den Leichenschauschein nicht den Rechtsvorschriften entsprach und die Vertraulichkeit der in den Leichenschauschein enthaltenen medizinischen Daten nicht gewährleistet war.

9.3.1**Leichenschauschein dürfen nur vom Amtsarzt geöffnet werden**

Nach dem § 11 des Gesetzes über das Friedhofs- und Bestattungswesen vom 17. Dezember 1964 (GVBl. I S. 225) müssen vor jeder Bestattung Tod, Todesart und -ursache im Wege der Leichenschau festgestellt werden. Einzelheiten sind in der hierzu erlassenen Verordnung über das Leichenwesen vom 12. März 1965 (GVBl. I S. 63) geregelt. Der Verordnung zufolge hat der zur Leichenschau zugezogene Arzt die Leiche sorgfältig zu untersuchen und den Leichenschauschein auszustellen (§ 3 Abs. 1). Der Leichenschauschein besteht aus einem offenen Teil, der insbesondere die Personalien des Verstorbenen, Ort und Zeitpunkt des Todes, Todesart (natürlicher Tod, Unglücksfall, Selbstmord, Tötung, Verdacht einer strafbaren Handlung) und den Namen des Leichenschauers enthält, und einem vertraulichen Teil mit medizinischen Angaben über die genaue Todesursache und Krankheiten etc. des Verstorbenen, der durch den ärztlichen Leichenschauer zu verschließen ist. Der vertrauliche Teil darf – sofern nicht Anhaltspunkte dazu vorhanden sind, daß jemand eines nicht natürlichen Todes gestorben ist (§ 159

Strafprozeßordnung (StPO)) – nur vom Amtsarzt im Gesundheitsamt geöffnet werden (§ 3 Abs. 1). Der Hinweis: "Öffnen nur durch den Amtsarzt" ist auch auf dem durch die Verordnung vorgeschriebenen Formular für den Leichenschauschein zu lesen. Die medizinischen Angaben im Leichenschauschein unterstehen der ärztlichen Schweigepflicht im Sinne von § 203 Strafgesetzbuch (StGB). Ob der Verstorbene einen Herzinfarkt hatte, an Krebs oder Aids erkrankt war etc., geht Dritte – dazu zählen auch die Angehörigen – nichts an, es sei denn, eine Offenbarung der Daten entspricht dem Willen des Verstorbenen.

Im Sterbefall müssen verschiedene Ämter tätig werden, insbesondere das Standesamt (Beurkundung des Sterbefalls), das Ordnungsamt (z.B. Entscheidung über Anträge auf Bestattungsfristverlängerung), das Gesundheitsamt (Prüfung, ob medizinische Gründe gegen eine Bestattungsfristverlängerung sprechen), die Polizeibehörde (Bescheinigung für Feuerbestattungen, daß keine Anhaltspunkte für eine Straftat vorliegen) und das Garten- und Friedhofsamt (Durchführung der Bestattung). Zentrale Sammelstelle für die Leichenschauscheine ist schließlich das Gesundheitsamt. Der Amtsarzt des Gesundheitsamts ist berechtigt, den vertraulichen Teil des Leichenschauscheins zu öffnen und auf Vollständigkeit und Plausibilität zu prüfen.

9.3.2

Prüfungsergebnisse

Meine Prüfungen haben ergeben, daß die o.g. Vorschriften beim Umgang mit den Leichenschauscheinen in Frankfurt am Main bereits seit längerer Zeit nicht eingehalten wurden. Der vertrauliche Teil der Scheine wurde teilweise vom Leichenschauarzt nicht verschlossen oder von Angehörigen, Mitarbeitern der Bestattungsunternehmen oder vom Standesamt, Garten- und Friedhofsamt sowie Ordnungsamt geöffnet bzw. konnte von den genannten Ämtern zur Kenntnis genommen werden.

So waren beispielsweise im Standesamt Frankfurt am Main von 23 vorliegenden Leichenschauscheinen 15 geöffnet. Mitarbeiter des Standesamtes konnten damit die vertraulichen, nur für den Amtsarzt bestimmten medizinischen Angaben über den Verstorbenen zur Kenntnis nehmen, obwohl diese Angaben für die Erfüllung ihrer Aufgaben nicht erforderlich waren. Den von mir geführten Gesprächen zufolge war dies in den vergangenen Jahren generelle Praxis. In einer Anordnung des Ordnungsamtes Frankfurt am Main – Gesundheitsaufsicht -, die das Garten- und Friedhofsamt umgesetzt hat, wurde das Garten- und Friedhofsamt – im Widerspruch zu den gesetzlichen Regelungen – als berechtigt bezeichnet, Leichenschauscheine zum Zwecke der Feuerbestattung und zur Beantragung der Bestattungsfristverlängerung zu öffnen. In Fällen einer Beantragung einer Fristverlängerung schrieb die Anordnung vor, daß der gesamte Leichenschauschein zu kopieren und an das Ordnungsamt weiterzuleiten ist. Die Leiterin des Gesundheitsamtes teilte mir mit, sie dränge bereits seit Jahren darauf, daß die Leichenschauscheine ordnungsgemäß verschlossen im Gesundheitsamt ankommen.

9.3.3

Konsequenzen

Das Personal- und Organisationsamt der Stadt Frankfurt am Main hat nach Kenntnisnahme meiner Prüfungsergebnisse umgehend reagiert. Die von ihm selbst durchgeführte organisatorische Prüfung kam im wesentlichen zu denselben Resultaten. In einem gemeinsamen Gespräch wurde festgestellt, daß das Standesamt, das Garten- und Friedhofsamt und das Ordnungsamt ihre im Zusammenhang mit einem Todesfall zu erledigenden Aufgaben durchaus ohne die Angaben des vertraulichen Teils des Leichenschauscheins erfüllen können und in erster Linie Mängel im organisatorischen Ablauf der Zusammenarbeit der betroffenen Ämter ursächlich für die unzulässigen Öffnungen waren. Vom Personal- und Organisationsamt wurden daraufhin neue Verfahrensregelungen und Anweisungen im Umgang mit den Leichenschauscheinen erarbeitet, die der Vertraulichkeit der medizinischen Angaben umfassend Rechnung tragen. Darüber hinaus wurden das Standesamt und das Gesundheitsamt beauftragt, ein Informationsblatt an die Pietäten, die Ärzte und die Frankfurter Krankenhäuser zu übersenden, in dem auf die gesetzliche Vorschrift über die Vertraulichkeit der medizinischen Angaben im Leichenschauschein hingewiesen wird.

9.3.4

Abschließende Kontrollprüfung

Bei meiner Kontrollprüfung im Oktober 1992 ergab sich zunächst das Problem, wann ein Leichenschauschein hinreichend verschlossen ist. Ich habe darauf hingewiesen, daß ein Zusammenheften des vertraulichen Teils des Leichenschauscheins in der Weise, daß der Inhalt dieses Teils noch teilweise einsehbar ist, kein hinreichender Verschluß ist.

Im übrigen habe ich bei der Prüfung festgestellt, daß die Informationsblätter wie vorgesehen verschickt und die vom Personal- und Organisationsamt festgelegten Verfahrensabläufe eingehalten wurden:

- Die Leichenschauscheine wurden von den Leichenschauärzten durchgehend verschlossen.
- Bei den 90 im Standesamt zu dieser Zeit vorhandenen Leichenschauscheinen war – mit Ausnahme von drei Fällen, in denen offensichtlich Angehörige den Leichenschauschein unberechtigterweise geöffnet hatten – der vertrauliche Teil entsprechend der gesetzlichen Regelung verschlossen.

- Standesamt, Garten- und Friedhofsamt sowie Ordnungsamt haben den Leichenschauschein nicht geöffnet bzw. den vertraulichen Teil nicht zur Kenntnis nehmen können.

Da nicht auszuschließen ist, daß entsprechende Probleme im Umgang mit den Leichenschauscheinen auch in anderen Kommunen bestehen, habe ich alle hessischen Gesundheitsämter auf die Rechtslage hingewiesen.

9.4

Zentrale Registrierung von Methadon-Empfängern zur Verhinderung von Mehrfachvergaben

Im August 1992 wurde in den Medien von einem internen Papier des Frankfurter Magistrats – einem Entwurf zum „Ausbau der Drogenhilfe“ – berichtet, das eine „zentrale Registrierung“ derjenigen Drogenabhängigen vorsah, die unter ärztlicher Aufsicht die Ersatzdroge Methadon erhalten. Konkret ging es um Pläne des Magistrats, für Heroinsüchtige, die sich überwiegend im Bereich der offenen Drogenszene aufhalten, die Methadon-Vergabe zu erweitern. In diesem Zusammenhang sollten in den drei Krisenzentren im Bahnhofsgelände je eine Methadon-Vergabestelle eingerichtet werden. Aus medizinischen und rechtlichen (Betäubungsmittelgesetz) Gründen sah der Magistrat die Notwendigkeit, Maßnahmen zu treffen, welche die Möglichkeit von unberechtigten Mehrfachvergaben von Methadon an einen Drogensüchtigen verhindern. Als einziger Weg wurde eine zentrale Registrierung der Methadon-Empfänger im Drogenreferat gesehen.

Da die vom Magistrat geplante „zentrale Registrierung“ der Methadon-Empfänger in dem internen Papier nicht näher geschildert war, entstand zunächst in der Öffentlichkeit der Eindruck, daß eine zentrale Datei mit den vollständigen Personalien aller Methadon-Empfänger aufgebaut werden sollte. Ein Gespräch mit dem Frankfurter Drogenreferat ergab jedoch, daß nur eine codierte Speicherung der Betroffenen geplant war.

Zentraler Gesichtspunkt für mich bei dem Gespräch mit dem Frankfurter Magistrat war, daß der Umfang der in dem zentralen Register gespeicherten Angaben über die Betroffenen auf das unerläßliche Minimum beschränkt wird, das zur Verhinderung von Mehrfachvergaben notwendig ist, und daß die Registrierung auf eine Art und Weise durchgeführt wird, die eine Identifizierung der Betroffenen in dem das Register führenden Drogenreferat unmöglich macht. Es wurde folgender Konsens über die rechtliche Bewertung und die weitere Verfahrensweise gefunden, der datenschutzrechtlichen Aspekten hinreichend Rechnung trägt:

- Die Verhinderung einer Mehrfachvergabe von Methadon ist rechtliche Voraussetzung der Durchführung der erweiterten Methadon-Vergabe. Die Drogenabhängigen werden im Rahmen des Behandlungsvertrages schriftlich über die Rechtslage und das konkrete Verfahren informiert.
- An das Drogenreferat dürfen von den Methadon-Vergabestellen nur die Angaben weitergegeben werden, die zur Verhinderung einer Mehrfachvergabe unerläßlich sind. Dies sind lediglich der erste Buchstabe des Vornamens, der letzte Buchstabe des Nachnamens, Monat und Jahr des Geburtsdatums sowie der Anfangsbuchstabe der jeweiligen Vergabestellen.
- Das Drogenreferat speichert diese Daten und prüft, ob sich ein Drogenabhängiger bei mehreren Vergabestellen Methadon geholt hat. Stellt das Drogenreferat eine evtl. Doppelversorgung fest, so werden hiervon die betroffenen Vergabestellen informiert, die den konkreten Fall dann abklären. Das Drogenreferat erhält zu keinem Zeitpunkt weitergehende Angaben über die betroffenen Drogensüchtigen.
- Die für die zentrale codierte Registrierung geführte Datei im Drogenreferat wird nur für diesen Zweck verwandt, und es werden die notwendigen technischen, organisatorischen und räumlichen Maßnahmen zur Gewährleistung der Datensicherheit getroffen, damit die Angaben nicht Dritten unberechtigt zur Kenntnis gelangen.

In dem Gespräch habe ich mich mit dem Drogenreferat darüber verständigt, daß ich über jede Abänderung des Verfahrens informiert werde.

9.5

Unzulässige Ablehnung der Einsicht in amtsärztliches Gutachten

Ein Bürger, der – mit der Begründung, daß mit der Wiederherstellung seiner vollen Dienstfähigkeit in absehbarer Zeit nicht zu rechnen sei (§ 51 Hessisches Beamtengesetz (HBG)) – auf Lebenszeit in den Ruhestand versetzt worden war, wandte sich an mich, weil ihm das Gesundheitsamt keine Einsicht in das der Versetzung zugrunde liegende amtsärztliche Gutachten gewährte. Das Gesundheitsamt hatte im Rahmen der amtsärztlichen Begutachtung ein Zusatzgutachten von einem externen Arzt erstellen lassen und die von dem Betroffenen erbetene Akteneinsicht mit der Begründung verweigert, daß dieser externe Gutachter damit nicht einverstanden sei.

Ich habe dem Gesundheitsamt mitgeteilt, daß die Verfahrensweise im konkreten Fall nicht der gesetzlichen Regelung entspricht. Die amts-, gerichts- und vertrauensärztliche Tätigkeit der Gesundheitsämter ist in der 2. Durchführungsverordnung zum Gesetz über die Vereinheitlichung des Gesundheitswesens vom 22. Februar 1935 (RGBl. I S. 215) geregelt. In § 18 a Abs. 3 (eingefügt aufgrund ÄndVO vom 23. Mai 1986, GVBl. I S. 147) ist festgelegt, daß in dienst- und arbeitsrechtlichen Angelegenheiten die untersuchte Person berechtigt ist, Einsicht in die anläßlich der Untersuchung gemachten Aufzeichnungen zu nehmen. Diese Bestimmung gilt selbstverständlich auch dann, wenn im

Rahmen der amtsärztlichen Untersuchung ein Zusatzgutachten an einen externen Gutachter in Auftrag gegeben wird. Das Zusatzgutachten ist Bestandteil der amtsärztlichen Untersuchung im Sinne dieser Vorschrift. Ein anderes Ergebnis würde auch dem Zweck der Regelung völlig zuwider laufen: Die Regelung in § 18 a Abs. 1 S. 3 der 2. Durchführungsverordnung zielt darauf ab, uneingeschränkte Transparenz des Verfahrens für die Betroffenen herzustellen – nicht zuletzt auch im Hinblick darauf, daß die Untersuchungen schwerwiegende Konsequenzen für die Betroffenen haben können. Eine Einsichtnahme des Betroffenen in die amtsärztlichen Unterlagen – einschließlich evtl. externer Gutachten – darf daher auf keinen Fall von der "Erlaubnis" der ärztlichen Gutachter abhängig gemacht werden.

Unabhängig von der in § 18 a der 2. Durchführungsverordnung getroffenen Regelung, die Einsichtsrechte nach anderen Vorschriften unberührt läßt (§ 18 a Abs. 1 S. 4), findet auch das in § 18 Hessisches Datenschutzgesetz (HDSG) geregelte Recht auf Einsicht des Betroffenen in Akten öffentlich-rechtlicher Stellen Anwendung. Nach § 18 Abs. 4 HDSG hat der Betroffene grundsätzlich ein Recht auf Akteneinsicht. Im Einzelfall kann ihm statt Einsicht Auskunft gewährt werden. Nach § 18 Abs. 5 HDSG gilt dies nicht, soweit eine Abwägung ergibt, daß das Recht des Betroffenen hinter dem öffentlichen Interesse an der Geheimhaltung oder einem überwiegenden Geheimhaltungsinteresse Dritter zurücktreten muß. Die Entscheidung trifft der Leiter der speichernden Stelle oder dessen Stellvertreter. Wenn Auskunft oder Einsicht nicht gewährt werden, ist der Betroffene unter Mitteilung der wesentlichen Gründe darauf hinzuweisen, daß er sich an den Hessischen Datenschutzbeauftragten wenden kann. Mit dieser Regelung stand die Verfahrensweise des Gesundheitsamts im vorliegenden konkreten Fall ebenfalls nicht im Einklang. Selbst wenn man davon ausgeht, daß unter Umständen Interessen des ärztlichen Gutachters i.S.v. § 18 Abs. 5 HDSG einer Akteneinsicht durch den Betroffenen entgegenstehen könnten, so kann jedenfalls die fehlende "Erlaubnis" des Gutachters nicht der entscheidende Gesichtspunkt sein. Vielmehr muß das Gesundheitsamt auch hier eine Einzelfallentscheidung unter Abwägung der verschiedenen Interessen treffen.

Aufgrund meiner Stellungnahme hat das Gesundheitsamt mir mitgeteilt, daß dem Betroffenen nunmehr die erbetene Akteneinsicht gewährt wird.

9.6

Unzulässige Veröffentlichungen über das Ruhen der Approbation von Zahnärzten

Der Regierungspräsident Düsseldorf, der in Nordrhein-Westfalen zuständig ist für die Approbation der Zahnärzte nach dem Gesetz über die Ausübung der Zahnheilkunde vom 31. März 1952 (ZahnHKG, BGBl. I S. 221, in der Fassung der Bekanntmachung vom 16. April 1987, BGBl. I S. 1225, geändert durch Einigungsvertrag vom 31. August 1990, BGBl. II S. 885), ordnete gegen zwei in seinem Bezirk niedergelassene Zahnärzte das Ruhen der Approbation an. Das Ruhen der Approbation kann angeordnet werden, wenn gegen den Zahnarzt wegen einer Straftat, aus der sich seine Unwürdigkeit oder Unzuverlässigkeit zur Ausübung seines Berufs ergeben kann, ein Strafverfahren eingeleitet ist oder auch wenn nachträglich eine der Voraussetzungen für die Erteilung der Approbation weggefallen ist (§ 5 Abs. 1 ZahnHKG). Da die Anordnungen des Regierungspräsidenten bundesweit gelten, wurden die obersten Gesundheitsbehörden der Länder davon unterrichtet. Das Hessische Ministerium für Jugend, Familie und Gesundheit leitete diese Anordnungen nicht nur an die nachgeordneten Gesundheitsbehörden weiter, sondern machte sie außerdem als "Amtliche Mitteilungen" in dem frei beziehbaren Fachblatt "Der Hessische Zahnarzt" bekannt.

Diese Verfahrensweise verstößt gegen das Hessische Datenschutzgesetz (HDSG).

Da die Zeitschrift jedem zugänglich ist, ist die Veröffentlichung der Angaben über die betroffenen Zahnärzte eine Übermittlung personenbezogener Daten an Personen oder Stellen außerhalb des öffentlichen Bereichs (§ 16 Abs. 1 HDSG). Solche Übermittlungen sind nur zulässig, wenn der Empfänger ein berechtigtes Interesse an der Kenntnis der zu übermittelnden Daten glaubhaft macht und keine Anhaltspunkte dafür bestehen, daß schutzwürdige Belange des Betroffenen beeinträchtigt werden können. Die Abwägung zwischen berechtigtem Interesse und schutzwürdigen Belangen muß grundsätzlich im Einzelfall erfolgen. Eine Veröffentlichung, die diese Einzelfallprüfung unmöglich macht, ist unzulässig.

Auf meine Anfrage hat mir das Hessische Ministerium für Jugend, Familie und Gesundheit mitgeteilt, daß es meine Rechtsauffassung teilt und in Zukunft eine Veröffentlichung der entsprechenden Anordnungen unterbleiben soll.

10. Soziales

10.1

Pauschale Einwilligungsfomulare in Schuldnerberatungsstellen

Wer bei einer Schuldnerberatungsstelle Rat und Unterstützung sucht, muß sein Einverständnis damit erklären, daß bei den unterschiedlichsten Personen und Institutionen Auskünfte über ihn eingeholt werden. Die hessischen Schuldnerberatungsstellen verwenden dafür Formulare mit einem mehr oder weniger ausführlichen Fragenkatalog.

Im letzten Jahr wandten sich erstmals Bürgerinnen und Bürger an mich, weil ihnen die Einwilligungserklärung, die sie abgeben sollten, zu weitgehend erschien. Meine Überprüfung ergab, daß die Formulare vielfach zu pauschale Formulierungen enthielten und daß außerdem mehr Transparenz für die Hilfesuchenden hinsichtlich der Verarbeitung ihrer Daten sichergestellt werden muß.

10.1.1

Schuldnerberatungsstellen benötigen viele persönliche Informationen

In der Bundesrepublik gibt es derzeit etwa 400 Schuldnerberatungsstellen. Sie werden vor allem von Städten und Gemeinden, freien Wohlfahrtsverbänden und Verbraucherorganisationen getragen. Schuldnerberatungsstellen nehmen die zunehmend wichtigere Aufgabe wahr, Haushalten, die – aus den verschiedensten Gründen – ihre finanziellen Verpflichtungen nicht mehr bewältigen können und durch Überschuldung in Not geraten, bei der Ordnung und Regulierung ihrer Schulden zu helfen. Bei der Erfüllung ihrer Aufgabe haben sie mit einer Vielzahl persönlicher Informationen über die Hilfesuchenden zu tun: Sie erfahren die Gründe, die zur Überschuldung geführt haben, und Einzelheiten über die familiäre und berufliche Situation sowie über die Einnahmen und Ausgaben des Haushalts, insbesondere über den aktuellen Stand der Schulden (z.B. Ratenkredite bei Banken und Sparkassen, Ratenkäufe bei Waren- und Versandhäusern, Pfandleihe, Versicherungsschulden, Mietschulden, Schulden aus Unterhaltsverpflichtungen, Wett- und Spielschulden, Schulden bei Ärzten, Rechtsanwälten, beim örtlichen Handel, bei der Post, bei Freunden, beim Finanzamt oder beim Sozial-, Jugend- und Arbeitsamt). Ferner benötigen die Schuldnerberatungsstellen konkrete Angaben von den Betroffenen, um überprüfen zu können, ob gesetzliche Sozialleistungen (z.B. Kindergeld, Erziehungsgeld, Wohngeld, Unterhaltsvorschuß für den Kindesunterhalt oder Sozialhilfe) in Betracht kommen. Die Schuldnerberatungsstellen versuchen dann, durch Gespräche mit den Gläubigern Regelungen zu treffen, die es den Hilfesuchenden ermöglichen, ihre Schulden abzutragen.

10.1.2

Transparenz der Datenverarbeitung

Auch wenn die Schuldnerberatungsstellen zur Erfüllung ihrer Aufgaben vielfältige persönliche Informationen über die Hilfesuchenden benötigen und häufig zur Schuldenregulierung mit einer Reihe von Stellen Kontakt aufnehmen müssen, muß auch und gerade in diesem Bereich Transparenz für die Betroffenen hinsichtlich der Verarbeitung ihrer personenbezogenen Daten sichergestellt werden. Pauschale Einwilligungserklärungen zur Einholung von Auskünften bei anderen Stellen bzw. Personen dürfen nicht verwandt werden. Das Formular einer Schuldnerberatungsstelle enthielt beispielsweise den folgenden Text:

“Hiermit bevollmächtige ich ... vor allem zur Regulierung meiner finanziellen Verbindlichkeiten und im Interesse meiner sozialen und wirtschaftlichen Situation, bei allen nachfolgend aufgeführten Personen, Dienststellen und Institutionen die erforderlichen Informationen einzuholen, Unterlagen einzusehen und daraus Kopien anzufertigen und Verhandlungen zu führen:

Privatpersonen, die als Gläubiger mir gegenüber auftreten; meine jetzigen bzw. früheren Arbeitgeber; Rechtsanwälte, soweit sie mich vertreten oder vertreten haben bzw. als Gläubiger mir gegenüber auftreten oder aufgetreten sind; Bedienstete bei Verbraucherberatungsstellen, Schuldnerberatungsstellen und Gerichten; Bedienstete bei Banken, Inkassobüros, Auskunftsteilen, Versicherungsgesellschaften o.ä.; Bedienstete bei Behörden und öffentlichen Dienststellen, bei den freien Wohlfahrtsverbänden und Kirchen, soweit sie Aufgaben nach § 18 f. Sozialgesetzbuch Band I wahrnehmen; Bedienstete bei psychologischen Beratungsstellen (Familien-, Drogen-, Sucht-, Schwangerschaftsberatung, Sozialpsychiatrischer Dienst).“

Formulierungen in anderen Einwilligungserklärungen waren kürzer, jedoch auch zu pauschal, so z.B. der folgende Text:

“Hiermit entbinde ich Banken, Sparkassen und andere Kreditinstitute vom Bankgeheimnis bzw. von der Einschränkung durch das Datenschutzgesetz. Entsprechendes gilt auch für den oder die Arbeitgeber, öffentliche Stellen und für Auskunftsbüros, einschließlich der SCHUFA.“

Aus datenschutzrechtlicher Sicht sind Einwilligungserklärungen nur rechtswirksam, wenn die Betroffenen vorher über Umfang und Zweck der vorgesehenen Verarbeitung ihrer personenbezogenen Daten informiert wurden. Das heißt, daß nicht routinemäßig für jede nur denkbare Fallkonstellation (“öffentliche Stellen”) eine Einwilligung in die Erteilung von Auskünften eingeholt werden darf, ohne daß feststeht, daß die Auskünfte im Einzelfall tatsächlich benötigt werden.

Da die Schuldnerberatungsstellen unterschiedlich arbeiten, kann ich hier nur einige allgemeine Verfahrensvorschläge darlegen, die von jeder Stelle entsprechend ihrer Arbeitsweise konkretisiert bzw. modifiziert werden müssen. Die Schuldnerberatungsstellen benötigen im Regelfall zunächst einmal die Einwilligung in die Erteilung von Auskünften durch alle Gläubiger. Eine Einwilligungserklärung könnte etwa wie folgt aussehen:

“Hiermit bevollmächtige ich meinen Schuldnerberater, zum Zwecke der Unterstützung bei der Regulierung meiner Schulden bei meinen Gläubigern die für die Beratung erforderlichen Auskünfte einzuholen, Unterlagen einzusehen und daraus Kopien zu fertigen.“

Im übrigen stellt sich die Frage, auf welche Weise je nach Einzelfall differenziert verfahren werden kann. Die Betroffenen müssen auch die Möglichkeit haben, in die Erteilung von Auskünften bestimmter Stellen nicht einzuwilligen. Vor allem auch eine Einwilligung in die Erteilung von Auskünften bei Familien-, Drogen-, Sucht-, Schwangerschaftsberatungsstellen sowie Sozialpsychiatrischen Diensten sollte allenfalls im Einzelfall, wenn der konkrete Anlaß feststeht und besprochen werden kann (z.B. ein Antrag auf Vollstreckungsschutz, weil die Vollstreckung aus gesundheitlichen Gründen eine besondere Härte für den Schuldner darstellen würde), eingeholt werden.

Bei der Formulierung der Einwilligungserklärung ist zwischen den verschiedenen Zwecken, nämlich Regulierung der Schulden mit den Gläubigern einerseits und Überprüfung und gegebenenfalls Geltendmachung von Ansprüchen auf gesetzliche Sozialleistungen andererseits, zu unterscheiden. Gegenüber den Betroffenen ist klarzustellen, daß die zu ihrer Person erhobenen Daten nur für Zwecke der Schuldnerberatung verwendet werden. Hier ist positiv anzumerken, daß die Formulare überwiegend bereits entsprechende Formulierungen zur Zweckbindung enthielten. Wegen des Umfangs und der Sensibilität der Daten sollten auch die Fristen für die Löschung bzw. Vernichtung der Daten intern konkret festgelegt und den Betroffenen auch mitgeteilt werden. Es könnte z.B. wie folgt formuliert werden:

“Die eingeholten Informationen werden nur für die Schuldnerberatung verwendet und dürfen ohne meine ausdrückliche schriftliche Einwilligung nicht für andere Zwecke verwendet werden.

Die zu meiner Person bei der Schuldnerberatungsstelle gespeicherten Daten werden fünf Jahre nach Abschluß der Beratung vernichtet bzw. gelöscht.“

Soweit die Daten über die Hilfesuchenden in einer automatisierten Datei gespeichert werden, müssen die Betroffenen davon, z.B. durch Aushändigung eines Ausdrucks des Drucksatzes, benachrichtigt werden (§ 18 Abs. 2 HDSG).

10.2

Benachrichtigung der Gesundheitsämter über die Notwendigkeit einer Entwöhnungsbehandlung

Beantragt ein Versicherter eine Rente vor Erreichung der Altersgrenze, wertet die Landesversicherungsanstalt (LVA) vorgelegte ärztliche Unterlagen bei entsprechenden Anhaltspunkten auch zu der Frage aus, ob Anlaß für eine (Alkohol-)Entwöhnungsbehandlung besteht. Eine solche Feststellung wird dem Versicherten schriftlich mitgeteilt. Gleichzeitig ergeht die Aufforderung, eine Suchtkrankenberatungsstelle aufzusuchen. Dort wird geprüft, ob beim Versicherten die Motivation für eine Entwöhnungsbehandlung gegeben ist, da diese Therapie ohne eine aktive Mitarbeit naturgemäß nicht zum Erfolg führen kann. Die Beratungsstelle erstellt dann einen Sozialbericht, der der LVA vorgelegt wird. Das Aufsuchen einer solchen Beratungsstelle ist freiwillig, die Auswahl der konkreten Beratungsstelle bleibt dem Versicherten überlassen. Die LVA macht ihm jedoch einen Vorschlag. Entwöhnungsbehandlungen gehören zu den Heilbehandlungen, die gegebenenfalls im Rahmen der Mitwirkungspflicht nach § 63 Sozialgesetzbuch I (SGB I) verlangt werden können.

Suchtkrankenberatung wird auch von Gesundheitsämtern durchgeführt. Praxis der LVA war es bislang, den Betroffenen in der Regel diese Beratungsstellen vorzuschlagen. Eine Durchschrift des Aufforderungsschreibens wurde deswegen auch an das jeweils örtlich zuständige Gesundheitsamt verschickt. Die Gesundheitsämter sollten dafür sorgen, daß der Versicherte rasch einer Entwöhnungsbehandlung zugeführt wird.

Dieses Verfahren ist unzulässig. Mit der Mitteilung an das Gesundheitsamt werden Sozialdaten, nämlich daß der Betroffene eine Leistung der LVA beantragt hat, offenbart. Eine Offenbarungsbefugnis besteht jedoch nicht, da es dem Versicherten freigestellt ist, an welche Beratungsstelle er sich wendet. Auf meine Intervention hin hat die LVA dieses Verfahren eingestellt und gleichzeitig die Beratungsstellen aufgefordert, noch vorhandene Durchschriften zu vernichten.

10.3

Inhalt von Rechtswahrungs- und Überleitungsanzeigen der Sozialämter bei Aufenthalt hilfesuchender Frauen im Frauenhaus

Eine Frau, die sich in ein Frauenhaus begibt, erwartet hier Hilfe und gegebenenfalls auch Schutz vor evtl. Nachstellungen des (mitunter) gewalttätigen Partners bzw. Ehemannes. Diesen Schutz kann ein Frauenhaus nur bieten, wenn der Aufenthalt nicht bekannt wird. In vielen Fällen können die Frauen ihren Aufenthalt im Frauenhaus nicht selbst finanzieren. Sie sind gezwungen, Sozialhilfe zur Deckung der entstehenden Kosten zu beantragen.

Die Sozialhilfeträger prüfen sodann, ob den Frauen Unterhaltsansprüche gegen den Ehemann oder andere Unterhaltspflichtige zustehen. Ist dies der Fall, zeigt das Sozialamt dem Unterhaltspflichtigen mit einer Rechtswahrungsanzeige an, daß Sozialhilfe gewährt wird, und leitet mit einer Überleitungsanzeige die Unterhaltsansprüche der Frauen auf sich über.

Ich bin der Frage nachgegangen, ob und in welchem Umfang die Sozialhilfeträger bei der Prüfung von Unterhaltsansprüchen gegenüber den Unterhaltspflichtigen den Aufenthalt im Frauenhaus offenbaren.

Hierfür habe ich Anfang September 1992 sämtliche örtliche Träger der Sozialhilfe in Hessen gebeten, mir mitzuteilen, welchen Inhalt die Rechtswahrungs- und Überleitungsanzeigen haben.

Meine Umfrage hat ergeben, daß einige Sozialämter es den Frauen selbst überlassen, mit anwaltlicher Hilfe ihre Unterhaltsansprüche geltend zu machen. Die Mehrzahl der Sozialämter offenbart in den Benachrichtigungen an Unterhaltspflichtige nicht den Aufenthalt der Frauen.

Lediglich drei Sozialämter unterrichten die Unterhaltspflichtigen über den Aufenthalt im Frauenhaus. Diese Stellen wurden von mir aufgefordert, ihre Praxis zu ändern.

11. Schulen

11.1

Hessisches Schulgesetz

11.1.1

Beseitigung eines Regelungsdefizits

Mit der Verabschiedung des Hessischen Schulgesetzes vom 17. Juni 1992 (SchulG, GVBl. I S. 233) hat der Landtag für einen weiteren bedeutsamen Bereich der Landesverwaltung spezifische Datenschutzvorschriften erlassen und damit ein vom Hessischen Datenschutzbeauftragten wiederholt kritisierendes verfassungswidriges Regelungsdefizit behoben (19. Tätigkeitsbericht, Ziff. 6.3.1; 20. Tätigkeitsbericht, Ziff. 16.5). Bis auf einige Bestimmungen, die allerdings nicht den Datenschutz berühren, tritt das Gesetz am 1. August 1993 in Kraft.

Zu dem Entwurf der Fraktionen der SPD und der GRÜNEN vom 4. November 1991 (Drucks. 13/858), der dem Gesetz zugrunde liegt, habe ich im Rahmen der vom kulturpolitischen Ausschuß des Landtags durchgeführten Anhörung am 18. März 1992 ausführlich Stellung genommen (vgl. Ausschußvorlage KPA 13/10, stenografische Niederschrift der 15. – öffentlichen – Sitzung des Kulturpolitischen Ausschusses vom 18. März 1992, Teil II). Der Gesetzgeber hat die meisten der von mir vorgeschlagenen Änderungen und Ergänzungen berücksichtigt (vgl. Änderungsantrag der SPD und der GRÜNEN, Drucks. 13/1995).

Das SchulG beseitigt die Zersplitterung des hessischen Schulrechts, indem es insbesondere die Regelungsbereiche des bisherigen Schulverwaltungsgesetzes (Schulverwaltungsg), des Schulpflichtgesetzes (SchulpflichtG), des Gesetzes über Unterrichtsgeld- und Lernmittelfreiheit, des Gesetzes über die Mitbestimmung der Erziehungsberechtigten und den Landeselternbeirat, des Gesetzes über Schulen in freier Trägerschaft und des Gesetzes über die Gymnasiale Oberstufe zusammenfaßt. Deshalb war es nur konsequent, auch die notwendigen Datenschutzregelungen in das Gesetz aufzunehmen.

Ein daraus resultierender positiver Effekt sei hier nur am Rande erwähnt: Künftig werden sich die Schulen bei Verstößen gegen das Datenschutzrecht weniger überzeugend damit entschuldigen können, sie hätten die einschlägigen Vorschriften wegen der Unübersichtlichkeit der für den Schulbereich geltenden gesetzlichen Bestimmungen nicht gekannt – ein bislang relativ häufig zu hörendes Argument. Auf einige besonders wichtige Vorschriften wird im folgenden näher eingegangen.

11.1.2

Schulärzte und Schulpsychologischer Dienst

Für die Datenverarbeitung der Schulärzte, Schulzahnärzte und des schulpsychologischen Dienstes sieht das SchulG erstmals eine ausreichende Rechtsgrundlage vor. Das Schulverwaltungsg und das SchulpflichtG enthalten lediglich eine allgemeine Duldungs- und Auskunftspflicht der Schüler und Erziehungsberechtigten. Daß dies angesichts der Sensibilität der Daten, die diese Stellen verarbeiten, nicht der vom Bundesverfassungsgericht geforderten gesetzlichen Verarbeitungsbefugnis entspricht, war denn auch unstrittig.

Schulärztliche Untersuchungen erfolgen beispielsweise bei der Einschulung und mindestens zwei weitere Male im Laufe der Schulzeit, außerdem in besonderen Fällen, etwa bei auftretenden Hör- und Sprachstörungen eines Schülers oder vor der Überweisung in eine Sonderschule. Schulzahnärztliche Untersuchungen werden jährlich durchgeführt. Von dem bei den staatlichen Schulämtern, den unteren Schulaufsichtsbehörden, eingerichteten schulpsychologischen Dienst, müssen sich Schüler z.B. vor einer Entscheidung über die Zurückstellung von der Teilnahme am Unterricht der Grundschule oder die Überweisung in eine Sonderschule untersuchen lassen.

Das SchulG enthält strikte Vorgaben für derartige Untersuchungen. So dürfen Kinder, Jugendliche und auch volljährige Schüler bei schulärztlichen und schulpsychologischen Pflichtuntersuchungen in der Regel über Angelegenheiten, die ihre oder die Persönlichkeitssphäre der Eltern und Angehörigen betreffen, nicht befragt werden. Der Gesetzentwurf wollte solche Fragen sogar ausnahmslos verbieten, was manche notwendige Untersuchung verhindert oder zumindest unangemessen erschwert hätte. Denn es gibt durchaus Fälle, in denen es sinnvoller ist, die Schüler statt die Erziehungsberechtigten zu befragen. Das gilt z.B. bei Kindesmißhandlungen oder sexuellem

Mißbrauch in der Familie. Nach Rücksprache mit verschiedenen Schulärzten und Schulpsychologen hatte ich deshalb in der Anhörung erfolgreich für das Regel-Ausnahme-Verhältnis plädiert.

Es wird außerdem sichergestellt, daß die Schulen und Aufsichtsbehörden nur die Untersuchungsdaten erhalten, die sie für ihre schulverwaltungsfachlichen und pädagogischen Entscheidungen benötigen. Im Gesetzgebungsverfahren bestand Einvernehmen, daß die Mitteilung des Untersuchungsergebnisses genügt. Deshalb schreibt das Gesetz vor, daß der schulärztliche und schulpsychologische Dienst der Schule nur das Ergebnis der Pflichtuntersuchungen übermitteln dürfen.

Schulpsychologen werden aber nicht nur im Rahmen von Pflichtuntersuchungen tätig, sondern auch auf Wunsch von Erziehungsberechtigten und Schülern oder auf Anraten von Lehrern. Diese freiwilligen Untersuchungen sind zu behandeln wie Konsultationen frei praktizierender Psychologen. Das Gesetz schreibt hier die vom Hessischen Kultusministerium erlassenen Richtlinien für die Tätigkeit der Schulpsychologen in der Abteilung Schulpsychologischer Dienst des Staatlichen Schulamtes vom 10. Januar 1983 (Abl. S. 92) fest, daß Informationen über diese Untersuchungen und Beratungen nur mit schriftlicher Einwilligung der Betroffenen weitergegeben werden dürfen.

11.1.3

Wissenschaftliche Forschung im Schulbereich

Daß wohlverstandener Datenschutz sich nicht darin erschöpft, die Erhebung und Übermittlung personenbezogener Daten möglichst zu verhindern, dürfte bereits an den Bemerkungen zum schulpsychologischen Dienst deutlich geworden sein. Zu den Aufgaben des Datenschutzbeauftragten zählt genauso die Berücksichtigung berechtigter Informationsinteressen. Aus diesem Grunde hatte ich mich für eine Änderung der zu restriktiven Wissenschaftsklausel des Entwurfs eingesetzt. Sie erlaubte die Datenverarbeitung für Forschungszwecke nur, wenn die Eltern und Schüler eingewilligt hatten. Dabei blieb zum einen unbeachtet, daß auch personenbezogene Lehrerdaten mitunter für Forschungszwecke benötigt werden. Für die Verarbeitung der Lehrerdaten wären bei der im Entwurf vorgesehenen Regelung allein die Bestimmungen des Hessischen Datenschutzgesetzes und dort insbesondere die Übermittlungsvorschrift des § 33 maßgeblich gewesen. Diese waren allerdings großzügiger als der Schulgesetzentwurf. Nach dem HDSG können nämlich die datenverarbeitenden Stellen (Schulen und Schulaufsichtsbehörden) auch ohne Einwilligung der Betroffenen deren personenbezogene Daten für Forschungszwecke übermitteln, wenn entweder durch die Weitergabe keine schutzwürdigen Interessen der Betroffenen beeinträchtigt werden oder das öffentliche Interesse an der Durchführung des Forschungsvorhabens die schutzwürdigen Belange des Betroffenen erheblich überwiegt und der Zweck der Forschung nicht auf andere Weise erreicht werden kann.

Es gab und gibt keinen plausiblen Grund, Schüler- und Elterndaten anders zu behandeln. Die Einwilligung der Schüler und Erziehungsberechtigten in die Verarbeitung ihrer Daten aus Schülerakten ist insbesondere dann rein technisch kaum oder nur schwer einzuholen, wenn die betroffenen Schüler die Schule bereits verlassen haben.

Konkretisiert wurden die bereits aufgrund des Hessischen Datenschutzgesetzes (HDSG) bestehenden Informationspflichten der Forscher. Die Schüler, Erziehungsberechtigten oder Lehrer sind darauf hinzuweisen, daß sie die Einwilligung ohne Rechtsnachteile verweigern können, und sie sind über das Ziel und den wesentlichen Inhalt des Forschungsprojekts, die Art der Beteiligung an der Untersuchung sowie über die Verarbeitung der erhobenen Daten aufzuklären. Gerade in diesem Punkt gab es in der Vergangenheit immer wieder Anlaß zu Beanstandungen mit zum Teil erheblichen negativen Auswirkungen auf das Forschungsvorhaben. Werden die Informationspflichten verletzt, sind die Datenerhebung und -speicherung rechtswidrig. Das hat zur Folge, daß die Daten gelöscht werden müssen. Zwar lassen sich die Konsequenzen insofern etwas mildern, als unter Löschen auch das Anonymisieren der Datensätze zu verstehen ist; ein Informationsverlust, der unter ungünstigen Umständen sogar das Forschungsziel gefährden kann, ist jedoch unvermeidlich. Nach der gesetzlichen Klarstellung sollten solche Fehler in Zukunft jedoch leichter vermeidbar sein.

11.1.4

Informationsrechte der Schüler und Eltern

Die Bürger müssen wissen können, "wer was, wann und bei welcher Gelegenheit über sie weiß", postuliert das Bundesverfassungsgericht im Volkszählungsurteil von 1983 (BVerfGE 65,1,43). Das ist fraglos nur möglich, wenn sie von der Behörde Auskunft hinsichtlich der über sie gespeicherten Daten oder – noch besser – Einsichtnahme in die einschlägigen Akten verlangen können. Geht es um eine konkrete Verwaltungsentscheidung, also beispielsweise um eine Versetzungsentscheidung, gewährt § 29 Hessisches Verwaltungsverfahrensgesetz (HVwVfG) ein Akteneinsichtsrecht der Betroffenen. Es ist jedoch keinesfalls selten, daß Schüler und Eltern auch außerhalb eines Verwaltungsverfahrens Unterlagen, die Daten über sie enthalten, einsehen wollen.

Dem HDSG ließe sich zwar für diese Fälle ebenfalls ein Akteneinsichtsrecht entnehmen (§ 18 Abs. 4), die Vorschrift ist allerdings nicht eindeutig formuliert, so daß streitig ist, ob die Behörde nicht eine Wahlmöglichkeit zwischen der Gewährung der Akteneinsicht und der Erteilung einer Auskunft hat. Das SchulG trifft hier eine klare Regelung: Eltern und Schüler haben das Recht, Akten der Schule, Schulaufsichtsbehörden und des schulärztlichen Dienstes, in denen Daten über sie gespeichert sind, einzusehen. Dieses Recht können auch jugendliche Schüler ausüben.

Das Gesetz bedeutet für die Schulen nichts Neues, denn der Erlass des Hessischen Kultusministeriums über Einsichtnahme in Schüler- und Prüfungsakten der Schulen vom 26. Februar 1979 (ABl. S. 131), erneut in Kraft gesetzt am 25. August 1979 (ABl. S. 815), gewährt den Erziehungsberechtigten und Schülern der Jahrgangsstufen zehn bis dreizehn schon seit Jahren die Möglichkeit zur Akteneinsicht. Neu ist freilich die Ausdehnung des Einsichtsrechts auf die Unterlagen der Schulaufsichtsbehörden und des schulärztlichen Dienstes. Neu ist außerdem, und das ist das Bedeutsame an der Vorschrift, die fast vorbehaltlose gesetzliche Anerkennung eines Akteneinsichtsrechts. Lediglich wenn die Daten der Betroffenen mit Angaben Dritter derart verbunden sind, daß die Trennung nicht oder nur mit unverhältnismäßig großem Aufwand möglich ist, ist die Einsichtnahme unzulässig. In diesem Fall ist die Behörde zur Auskunft verpflichtet.

11.1.5

Ordnungsmaßnahmen

Das SchulG sieht eine ganze Reihe von Ordnungsmaßnahmen vor (§ 82). Die mildeste Maßnahme ist der Ausschluß vom Unterricht für den Rest des Schultages, die härteste die Verweisung von der besuchten Schule. Dazwischen gibt es mehrere abgestufte Sanktionsmöglichkeiten, wie beispielsweise die Androhung der Zuweisung in eine Parallelklasse oder die Androhung der Überweisung in eine andere Schule. Die notwendige Dokumentation dieser Maßnahmen in der Schülerakte ist ein schwerwiegender Eingriff in das Recht auf informationelle Selbstbestimmung, der nach der Rechtsprechung des Bundesverfassungsgerichts besondere grundrechtssichernde verfahrenstechnische Vorkehrungen erfordert. Deshalb hat der Gesetzgeber auf meine Anregung hin eine Tilgungsvorschrift in das Gesetz aufgenommen. Eintragungen und Vorgänge über Ordnungsmaßnahmen müssen spätestens am Ende des zweiten Schuljahres nach der Eintragung gelöscht werden, wenn nicht während dieser Zeit eine erneute Maßnahme getroffen wurde. Es bleibt nur zu hoffen, daß diese Vorschrift von den Schulen genauer eingehalten wird als eine in der Verordnung über das Verfahren bei Ordnungsmaßnahmen vom 20. Januar 1983 (ABl. S. 89) bereits existierende ähnliche Regelung.

11.1.6

Automatisierte Datenverarbeitung

Besonders detaillierte Vorgaben enthält das SchulG für die automatisierte Verarbeitung personenbezogener Schüler-, Eltern- und Lehrerdaten. Medizinische und psychologische Befunde, die im Rahmen der Schulgesundheitspflege und des schulpsychologischen Dienstes erstellt werden, dürfen nicht automatisiert verarbeitet werden. Um möglichen Mißverständnissen vorzubeugen: Damit ist natürlich nicht verboten, mit einem Personalcomputer die Befunde zu schreiben. Sie dürfen nur nicht dauerhaft auf maschinenlesbaren Datenträgern gespeichert bleiben und ausgewertet werden.

Der Gesetzgeber hat hier eine Regelung aufgegriffen, wie sie in § 34 Abs. 6 HDSG für die Personaldatenverarbeitung bereits existiert. Hier wie dort sind die Beweggründe gleich: Die Daten bedürfen in jedem Einzelfall vor ihrer Verwendung einer kritischen Wertung, die ohne genaue Kenntnis sämtlicher Begleitumstände ihrer Entstehung und des sonstigen Kontextes nicht möglich ist. Die automatisierte Speicherung und Auswertung der Daten könnte nur nach pauschalen Merkmalen erfolgen und müßte die Besonderheiten des Einzelfalles außer acht lassen.

Aus Datensicherheitsgründen dürfen nach dem Willen des Gesetzgebers im schulpsychologischen Dienst eingesetzte Datenverarbeitungsgeräte nicht mit Datenverarbeitungsgeräten vernetzt werden, die für andere Aufgaben benutzt werden. Datensicherheitserwägungen haben außerdem zu der Regelung geführt, daß personenbezogene Daten von Schülern, Eltern und Lehrern in der Regel nur in der Schule verarbeitet werden dürfen. Diese Vorschrift gilt übrigens auch für die Datenverarbeitung in Akten. Die automatisierte Verarbeitung darf außerdem nur auf schuleigenen DV-Geräten erfolgen. Nur in begründeten Ausnahmefällen kann der Schulleiter Lehrern gestatten, Schülerdaten außerhalb der Schule zu verarbeiten. Diese Bestimmungen sind auch eine Reaktion auf meinen 18. Tätigkeitsbericht (Ziff. 9.1.2), in dem geschildert wird, welche Probleme entstehen können, wenn ein Schulleiter Personalnebenakten der Lehrer mit nach Hause nimmt.

11.1.7

Rechtsverordnung zum Datenschutz in der Schule

Das SchulG schafft die Grundlagen für eine verfassungskonforme Verarbeitung personenbezogener Daten im Schulbereich. Es bedarf allerdings noch der Konkretisierung durch eine Rechtsverordnung, die zeitgleich mit dem Parlamentsgesetz in Kraft treten muß. Das Hessische Kultusministerium hat mir bereits einen Entwurf für eine Rechtsverordnung zur Stellungnahme vorgelegt.

11.2

Weitergabe von Schülerdaten

Kurz nach der Einschulung ihres Sohnes erhielten die Eltern durch die Post einen Brief der örtlichen Sparkasse. Darin enthalten war, verbunden mit den besten Wünschen für den schulischen Werdegang, ein Gutschein über 5,- DM, der auf ein bei der Sparkasse für das Kind einzurichtendes Konto eingelöst werden konnte. Eine Rückfrage der Eltern bei der Schulleitung ergab, daß die Schule dem Kreditinstitut die Anschriften sämtlicher Schulanfänger mitgeteilt hatte. Begründet wurde dies damit, die Sparkasse habe in der Vergangenheit des öfteren die Schule mit Spenden unterstützt.

Das Kind hatte bereits am Tag der Einschulung von der Klassenlehrerin einen gleichen Brief eines anderen Kreditinstituts erhalten.

Während im ersten Fall gegen das Datenschutzrecht verstoßen wurde, bietet der zweite ein gutes Beispiel für zulässige Alternativen. Die Schule darf Schülerdaten nur dann an private Dritte weitergeben, wenn die Empfänger ein berechtigtes Interesse an der Kenntnis der Daten glaubhaft gemacht haben und außerdem keine Anhaltspunkte dafür bestehen, daß schutzwürdige Belange der Betroffenen beeinträchtigt werden können. Selbst wenn man den Wunsch des Kreditinstituts, für Werbezwecke die Anschriften der Schulanfänger zu erhalten, als berechtigtes Interesse anerkennt, scheitert die Übermittlung an der fehlenden zweiten gesetzlichen Zulässigkeitsvoraussetzung. Anschriften werden zwar mitunter von den datenverarbeitenden Stellen als wenig oder gar nicht schützenswert angesehen; daß dies ein Irrtum ist, zeigt sich jedoch gerade im Schulbereich. Besonders sozial schwächere Eltern und Schüler, z.B. Bewohner von Obdachlosenunterkünften, Asylanten- oder Übersiedlerheimen, wollen häufig nicht, daß ihre Anschrift privaten Dritten mitgeteilt wird.

Das Kultusministerium hat daraus schon vor Jahren die Konsequenz gezogen und die Übermittlung von Schülerdaten an Private grundsätzlich untersagt (Erlaß über Angaben über Schüler gegenüber Außenstehenden vom 10. Oktober 1977, ABl. S. 565). Der Erlaß ist zwar mittlerweile, wie jeder Erlaß, der nach zehn Jahren nicht erneut bekannt gemacht wird, im Wege der automatischen Erlaßbereinigung außer Kraft getreten, kann aber weiterhin als korrekte Auslegung der Übermittlungsvorschrift des § 16 Hessisches Datenschutzgesetz (HDSG) angesehen werden. Er wurde im übrigen nur deshalb nicht erneuert, weil eine entsprechende Regelung in die in Vorbereitung befindliche Rechtsverordnung zum Datenschutz in der Schule aufgenommen werden soll.

Daß die Schule den Kreditinstituten auch ohne Übermittlung der Anschriften entgegenkommen kann, zeigt der zweite Fall. Die Bank erreichte ihr Ziel, auch ohne daß die Schule gegen das Recht auf informationelle Selbstbestimmung verstieß, denn gegen das Verteilen der Briefe an die Schüler ist datenschutzrechtlich nichts einzuwenden.

Die Begründung der Schulleiterin für ihr Verhalten bestätigt meinen Eindruck, daß trotz der Fortbildungsveranstaltungen des Hessischen Instituts für Lehrerfortbildung und des Hessischen Instituts für Bildungsplanung und Schulentwicklung an manchen Schulen nur äußerst unzureichende datenschutzrechtliche Kenntnisse vorhanden sind. Hier kann letztlich nur eine Intensivierung der Fortbildung weiterhelfen.

12. Umwelt

12.1

Ad hoc-Arbeitsgruppe Umweltschutz und Datenschutz

Mit der wachsenden gesellschaftlichen Bedeutung des Umweltschutzes in den letzten Jahren ist auch das Spannungsverhältnis zwischen Umweltschutz und Datenschutz in das Blickfeld der Öffentlichkeit geraten: Während es im Umweltschutz darum geht, Daten offenzulegen, um Ursachen und Verursacher von Umweltgefahren und -schäden erkennen zu können, verlangt das Recht auf informationelle Selbstbestimmung – also der Datenschutz –, daß personenbezogene Daten nur dann gegen den Willen des Betroffenen übermittelt bzw. veröffentlicht werden dürfen, wenn dies eine Rechtsvorschrift so bestimmt. Diesem Konflikt trägt die gegenwärtige Rechtslage bisher nur unvollkommen Rechnung. Beispiele dafür habe ich in meinen Tätigkeitsberichten der letzten vier Jahre beschrieben (vgl. 17. Tätigkeitsbericht, Ziff. 1.1.2.3; 18. Tätigkeitsbericht, Ziff. 15; 19. Tätigkeitsbericht, Ziff. 12 und 20. Tätigkeitsbericht, Ziff. 11).

Das Land Hessen hat allerdings bereits in mehreren Bereichen gesetzliche Regelungen geschaffen, die einen Ausgleich zwischen den berechtigten Interessen des Umweltschutzes und denen des Datenschutzes ermöglichen und insoweit ein Vorbild für andere Gesetzgeber sein können: Die Regelung in § 105 des Hessischen Wassergesetzes vom 22. Januar 1990 (HWG, GVBl. I S. 114), die Vorschriften in den §§ 26 und 17 des Hessischen Abfallwirtschafts- und Altlastengesetzes vom 26. Februar 1991 (HAbfAG, GVBl. I S. 106) und die Vorschriften der Verdachtsflächendatei-Verordnung vom 1. Oktober 1991 (GVBl. I S. 314). Das Hessische Datenschutzgesetz (HDSG) vom 11. November 1986 hatte bereits in seinem § 12 Abs. 2 Ziff. 3 und Abs. 3 als eines der ersten Datenschutzgesetze auch Regelungen für die Datenerhebung "zur Abwehr erheblicher Nachteile für das Allgemeinwohl oder von Gefahren für Leben, Gesundheit und persönliche Freiheit" sowie zur "Abwehr einer erheblichen Gefährdung der natürlichen Lebensgrundlagen" aufgenommen. Diese Regelungen des HDSG gelten allerdings nur im Einzelfall.

Um einen Beitrag zur Verbesserung der Rechtssituation auf dem Gebiet des Umweltschutzes – insbesondere in den neuen Bundesländern – zu leisten, und zur Förderung des Erfahrungsaustausches auf dem Gebiet Umweltschutz und Datenschutz hatte ich in der Konferenz der Datenschutzbeauftragten des Bundes und der Länder angeregt, eine ad hoc-Arbeitsgruppe zu bilden, die sich diesem Thema ausschließlich widmet.

Dieser Vorschlag wurde inzwischen verwirklicht: Unter der Leitung des Brandenburgischen Datenschutzbeauftragten hat diese Arbeitsgruppe bereits in zwei Tagungen ein umfangreiches Programm von Problemlösungen auf dem Gebiet

Umweltschutz und Datenschutz bewältigt. Dabei hat sich gezeigt, daß dieser Erfahrungsaustausch auch in Zukunft notwendig ist, um auf möglichst einheitliche gesetzliche Regelungen in allen Ländern hinwirken zu können.

12.2

Abfallbeseitigung ("Müllanalysen")

Auch die Müllbeseitigung – eines der dringendsten Umweltprobleme der Gegenwart – kann ein Problem des Schutzes der Privatsphäre der Bürgerinnen und Bürger werden, beispielsweise wenn es um neue Verfahren zur Verringerung und Beseitigung von Hausmüll geht.

Im Rahmen sog. "Pilotverfahren", die derzeit in knapp einem Dutzend Städten in mehreren Bundesländern laufen, werden Müllanalysen vorgenommen, die Menge, Gewicht oder Art des Mülls eines Haushalts betreffen. Beabsichtigt ist einerseits, die Reduzierung der Müllmenge eines Haushalts durch geringere Gebühren zu belohnen, andererseits, durch Kontrolle der Müllarten in den Müllgefäßen zu gewährleisten, daß das Gebot der getrennten Sammlung des Abfalls nach Papier, Glas (Plastik, Metall) und "Restmüll" auch eingehalten wird. Ohne jeden Zweifel begrüßens- und förderungswürdige Ziele!

Nur darf man bei deren Verwirklichung nicht außer acht lassen, daß solche Müllanalysen durchaus detaillierte Rückschlüsse auf die Benutzer der Müllgefäße ermöglichen.

Wenn es auch verfrüht wäre, jetzt schon im einzelnen festlegen zu wollen, was aus der Sicht des Datenschutzes zulässig ist und was nicht – die Verfahren befinden sich überwiegend noch in der Erprobungsphase -, so muß doch hier schon auf ein Grundprinzip des Rechts auf informationelle Selbstbestimmung hingewiesen werden: Es darf keine Erhebung solcher personenbeziehbarer (also personenbezogener) Daten geben ohne die Zustimmung der Betroffenen. Aus der Sicht des Datenschutzes ist es nicht zulässig, daß – wenn auch bisher nur stichprobenweise geschehen – die Mülltonne eines bestimmten privaten Haushalts ohne Wissen der Betroffenen auf dem Hof der Müllabfuhr ausgeleert und deren Inhalt im einzelnen "analysiert" und die Ergebnisse gespeichert werden.

Auch die – zunehmend zu beobachtende – Praxis, durch Verwendung durchsichtiger Plastiksäcke die Benutzer zu zwingen, die Art ihres Mülls jedermann offenzulegen, ist aus der Sicht des Datenschutzes bedenklich.

Da es im Hinblick auf die in der Praxis der Abfallverwertung bestehenden großen Verschiedenheiten von Ort zu Ort kaum möglich erscheint, für alle Verfahren gleichermaßen geeignete Datenschutzrichtlinien zu schaffen, rege ich an, daß diejenigen Kommunen, die solche und ähnliche "Pilotprojekte" auf dem Gebiete der Hausmüllbeseitigung vorbereiten oder anstreben, sich zunächst von ihrem städtischen Datenschutzbeauftragten oder auch von mir beraten lassen. Ich werde inzwischen gemeinsam mit den kommunalen Spitzenverbänden und dem Umweltministerium überlegen, welche datenschutzrechtlichen Einschränkungen solcher Verfahren geeignet, aber auch ausreichend sind.

13. Landwirtschaft

13.1

Datensicherheit: Ministerialerlaß – 10 v.H. der Haushaltsmittel für sächliche Ausgaben zweckgebunden für Datensicherheit

Ein erfreuliches Beispiel von Kooperation im Datenschutz zwischen Verwaltung und Hessischem Datenschutzbeauftragten ist aus dem Ministerium für Landesentwicklung, Wohnen, Landwirtschaft, Forsten und Naturschutz – Bereich Landwirtschaft – zu berichten:

Um eine möglichst rasche und effektive Verbesserung der Datensicherheit in allen Landwirtschaftsämtern zu erreichen – in der Vergangenheit hatte ich mehrfach Fälle ungenügender Datensicherheit, insbesondere bei der Aktenaufbewahrung und Aktenvernichtung, kritisiert – hat mir der Landwirtschaftsminister mit Schreiben vom 5. Februar 1992 folgendes mitgeteilt:

"Das Landesamt hat Ihren Vorschlag aufgegriffen und wird im Haushaltsjahr 1992 bei Kapitel 09 12-515 01 – Geräte, Ausstattungs- und Ausrüstungsgegenstände sowie sonstige Gebrauchsgegenstände – mindestens 10 v.H. für den Datenschutz zur Verfügung stellen, es sei denn, der Datenschutzbeauftragte eines ALLs (Amt für Landwirtschaft und Landentwicklung) würde bestätigen, daß der Datenschutz bereits gewährleistet ist."

Diese Maßnahme des Landwirtschaftsministers, 10 v.H. der Haushaltsmittel für sächliche Ausgaben zweckgebunden für die Datensicherung festzulegen, ist vorbildlich und sollte auch in anderen Ressorts sowie in der Kommunalverwaltung übernommen werden: Meine Prüfungserfahrungen über Jahre hinweg haben gezeigt (vgl. 15. Tätigkeitsbericht, Ziff. 9.4; 16. Tätigkeitsbericht, Ziff. 12.3.2; 17. Tätigkeitsbericht, Ziff. 12.2; 18. Tätigkeitsbericht, Ziff. 17; 19. Tätigkeitsbericht, Ziff. 15; 20. Tätigkeitsbericht, Ziff. 15), daß in den meisten Verwaltungen der sicheren Aufbewahrung von Akten mit personenbezogenen Daten und darüber hinaus generell der Datensicherung zu wenig Aufmerksamkeit gewidmet wird.

13.2

Ölsaatzbeihilfe

Wie schon in früheren Tätigkeitsberichten erwähnt (vgl. insbesondere den 16. Tätigkeitsbericht, Ziff. 12: "Milch-Garantiemengen-Verordnung"), verursachen EG-Vorschriften auf dem Gebiet der Landwirtschaft immer wieder schwierige datenschutzrechtliche Probleme, da eine möglichst gerechte Verteilung von Zuschüssen notwendigerweise eine umfangreiche Erhebung und Übermittlung personenbezogener Daten voraussetzt. Dieses Dilemma ist wegen der großen Verschiedenheit der einzelnen EG-Programme und -Maßnahmen kaum grundsätzlich zu lösen; vielmehr ist in jedem Einzelfall eine Absprache mit dem Ministerium für Landesentwicklung, Wohnen, Landwirtschaft, Forsten und Naturschutz erforderlich.

Nicht selten werden die nationalen Behörden sehr kurzfristig über die Durchführung solcher Beihilfemaßnahmen informiert. Bisher ist es jedoch gelungen, die Abstimmung mit dem Landwirtschaftsministerium so rechtzeitig zu ermöglichen, daß eine Verzögerung der Auszahlung von EG-Beihilfen vermieden werden konnte.

Als Beispiel hierfür sei die EG-Neuregelung für Ölsaaten vom Frühjahr 1992 genannt: Der Entwurf des Antragsformulars auf "Direktzahlungen für Erzeuger von Ölsaaten der Ernte 1992" wurde mir am 28. März 1992 mit der Bitte um datenschutzrechtliche Prüfung übersandt, "da die Antragsformulare für ca. 15.000 hessische Ölsaatenerzeuger im Hinblick auf die auf den 30. Mai 1992 festgesetzte Einreichungsfrist baldmöglichst gedruckt und zum Versand gebracht werden müssen".

In einer Besprechung mit Vertretern des Landwirtschaftsministeriums, die bereits am 2. April 1992 stattfand, konnten – unter Beteiligung des Datenschutzbeauftragten des Ministeriums – die Formulierungen des Antragsbogens einvernehmlich so abgeändert werden, daß sie den Grundsätzen des Datenschutzrechts entsprachen. Insbesondere ging es darum, die personenbezogenen Daten vor einer Weiterübermittlung an Bundes- oder EG-Behörden zu anonymisieren, da diese Behörden für ihre Aufgaben keine personenbezogenen Daten benötigen.

13.3

Tierschutz

Aus dem Hessischen Ministerium für Jugend, Familie und Gesundheit kam eine Anfrage zur Novellierung des (Bundes-) Tierschutzgesetzes (TierschutzG). In § 13 des mir übersandten Entwurfs war vorgesehen, das Grundrecht der Unverletzlichkeit der Wohnung und das Postgeheimnis für die Zwecke des Tierschutzes einzuschränken: "Zur Verhütung dringender Gefahren für Tiere" sollte sowohl Wohnraum betreten werden "sowie Postsendungen, soweit sie Tiere enthalten oder enthalten können", geöffnet werden können.

Bei allem Verständnis für die Notwendigkeit einer Verbesserung des Tierschutzes halte ich die geplanten Einschränkungen des Postgeheimnisses und des Grundrechts auf Unverletzlichkeit der Wohnung für unverhältnismäßig. Ich habe dem Ministerium meine Bedenken mitgeteilt und darauf hingewiesen, daß bei nüchterner Rechtsgüterabwägung die Notwendigkeit der Einschränkung von Grundrechten in diesem Falle nicht hinreichend nachgewiesen ist.

14. Gesetz über das Liegenschaftskataster und die Landesvermessung

14.1

Inhalt des Gesetzes

Am 1. Januar 1993 ist das Hessische Gesetz über das Liegenschaftskataster und die Landesvermessung (HVG, GVBl. I S. 453) in Kraft getreten.

Der Gesetzentwurf vom 18. Dezember 1991 lag mir zur Stellungnahme vor. Ein wesentliches Ziel des Entwurfes war, die seit dem Jahr 1956 geltenden Bestimmungen über die Einrichtung und Führung des Liegenschaftskatasters sowie über die Abmarkung von Grundstücksgrenzen den fortgeschrittenen technischen Entwicklungen und den Anforderungen des Datenschutzes anzupassen. Zur Verwirklichung dieses Zieles enthielt der Gesetzentwurf eine Regelung über die Bestandteile und Grundlagen des Liegenschaftskatasters (§ 2 HVG-E), Bestimmungen zum Auskunfts- und Einsichtsrecht (§ 16 Abs. 1 und 2 HVG-E) sowie eine Verordnungsermächtigung zur Regelung des automatisierten Abrufs von Daten aus dem Liegenschaftskataster (§ 16 Abs. 3 HVG-E).

Einige dieser Vorschriften waren aus datenschutzrechtlicher Sicht verbesserungsbedürftig. So war keine Regelung getroffen, welche personenbezogenen Daten im einzelnen in das Liegenschaftskataster aufzunehmen sind. Letzteres war aus meiner Sicht deshalb besonders wichtig, weil der Entwurf sehr weitgehende Einsichts- und Auskunftsrechte vorsah. Ein weiterer Kritikpunkt war die Unbestimmtheit der rechtlichen Grundlage dieser Einsichts- und Auskunftsrechte. So sah § 16 Abs. 1 HVG-E vor, daß jeder, der ein berechtigtes Interesse darlegt, das Liegenschaftskataster einsehen und Auskunft daraus erhalten kann. Aus dem Gesetz sollte sich zumindest ergeben, unter welchen Voraussetzungen vom Vorliegen eines solchen Interesses auszugehen ist. Die Regelung für Gemeinden und Landkreise ging noch weiter: hier verzichtete der Entwurf sogar auf die Darlegung des berechtigten Interesses.

Ich habe deshalb darauf aufmerksam gemacht, daß auch Gemeinden und Landkreisen Einsichts- bzw. Auskunftsrechte nur insoweit zustehen, als dies zu ihrer Aufgabenerfüllung im Einzelfall erforderlich ist.

Mit § 17 des Entwurfes sollte über das Einsichts- und Auskunftsrecht hinaus eine rechtliche Grundlage für die Möglichkeit der Übermittlung von Auszügen aus dem Liegenschaftskataster geschaffen werden. Auch hier habe ich darauf hingewiesen, daß im Gesetz klargestellt werden sollte, daß bei der Herausgabe von Auszügen aus dem Kataster jeweils nur die personenbezogenen Daten übermittelt werden dürfen, die der Empfänger für die Erfüllung seiner Aufgaben benötigt.

Meine Kritik wurde weitgehend berücksichtigt. Positiv zu vermerken ist, daß § 2 Abs. 6 HVG nunmehr genau festlegt, welche personenbezogenen Daten in das Liegenschaftskataster aufzunehmen sind. Auch mit der jetzigen Fassung des § 16 HVG wurden meine Anregungen im wesentlichen aufgegriffen und umgesetzt, insbesondere wird jetzt im Falle des Einsichts- und Auskunftersuchens von jedem die Glaubhaftmachung des berechtigten Interesses gefordert. Den Gemeinden und anderen öffentlichen Stellen wird Einsicht und Auskunft nur "zur rechtmäßigen Erfüllung ihrer Aufgaben" gewährt.

14.2

Verordnung über den automatisierten Abruf von Daten aus dem Liegenschaftskataster

Die Landesregierung hat nach § 16 Abs. 7 HVG einen Verordnungsentwurf zum automatisierten Abruf von Daten aus dem Liegenschaftskataster (LiKaAVOE) vorgelegt.

Bereits in der Vergangenheit wurden mit dem Hessischen Ministerium für Wirtschaft, Verkehr und Technologie Rahmenbedingungen für eine derartige Abrufverordnung diskutiert. Die aus datenschutzrechtlicher Sicht wichtige Forderung, daß eine detaillierte Protokollierung der Datenabrufe sicherzustellen ist, wurde in dem Entwurf berücksichtigt. § 1 Abs. 1 LiKaAVOE regelt, daß jeder Datenabruf bei der HZD zu protokollieren ist, und zwar gleichgültig, durch welche Stelle der Datenabruf erfolgt. Auch enthält die vorgelegte Fassung des Entwurfs eine abschließende Aufzählung der Stellen, denen die Möglichkeit des automatisierten Zugriffs auf das Liegenschaftskataster gegeben werden soll. Dies sind in erster Linie die Gemeinden und Landkreise für ihr Gemeinde- bzw. Kreisgebiet sowie die Finanzbehörden für ihren Amtsbezirk. In Einzelfällen wird auch den Flurbereinigungsbehörden, der HLT Gesellschaft für Forschung, Planung und Entwicklung mbH sowie den öffentlich bestellten Vermessungsingenieuren der automatisierte Abruf eingeräumt. Zum Abruf bereitgehalten werden Eigentümerdaten und Flurstückdaten. In diesem Zusammenhang hatte ich kritisiert, daß (aus "technischen Gründen") nur eine Trennung nach Flurstückdaten einerseits und Eigentümerdaten andererseits möglich sei; gegenüber dem Hessischen Ministerium für Wirtschaft, Verkehr und Technologie habe ich zum Ausdruck gebracht, daß auch innerhalb der Datengruppe Eigentümerdaten eine Trennung der Daten angestrebt werden sollte, so daß ein Abruf im Rahmen des jeweils Erforderlichen erfolgen kann.

15. Kammern

15.1

Übermittlung von Adressen an Private zu Werbezwecken durch die Industrie- und Handelskammern und die Handwerkskammern

In der Vergangenheit haben sich immer wieder Gewerbetreibende an meine Dienststelle gewandt, weil sie nach Eintragung in die Handwerksrolle bzw. das Register der Industrie- und Handelskammer zahlreiche Anrufe und Besuche von Vertretern sowie Werbesendungen erhielten, ohne ein Interesse daran geäußert zu haben. Die kontaktaufnehmenden Firmen hatten die Adressen der neu angemeldeten Gewerbetreibenden in aller Regel von den Handwerks- oder Industrie- und Handelskammern erhalten.

Die Kammern waren meist der Auffassung, daß es zu ihren Aufgaben als Interessenvertretung ihrer Mitglieder gehöre, durch Versendung von Adreßdaten zu Werbezwecken für Geschäftsanbahnungen zu sorgen. So ist es beispielsweise ständige Übung der Kammern, die Daten neuer Mitglieder an Versicherungsunternehmen weiterzugeben.

Ich habe gegenüber den Vertretern der Kammern immer den Standpunkt vertreten, daß die Regelungen über die allgemeine Aufgabenumschreibung der Kammern im Gesetz zur vorläufigen Regelung des Rechts der Industrie- und Handelskammern vom 18. Dezember 1956 (IHKG, BGBl. I S. 290) und der Handwerksordnung (HwO) den durch das Bundesverfassungsgericht formulierten Anforderungen an die Verarbeitung personenbezogener Daten nicht genügen, so daß Maßstab für den Umgang mit personenbezogenen Daten mangels einer rechtlichen Grundlage im IHKG und der HwO das Hessische Datenschutzgesetz (HDSG) ist. Danach ist eine Weitergabe der Adreßdaten nur dann zulässig, wenn die Betroffenen eingewilligt haben oder wenn – bei Vorliegen eines berechtigten Interesses des Datenempfängers – kein schützenswertes Interesse des von der Datenübermittlung Betroffenen entgegensteht (§ 16 Abs. 1 HDSG).

Der erste Fall ist völlig unproblematisch; willigt jemand in die Übermittlung seiner Daten ein, dürfen die Kammern die Daten selbstverständlich auch weitergeben. Im zweiten Fall ist eine Interessenabwägung vorzunehmen. Auch hier mag im Einzelfall eine Datenübermittlung zulässig sein. Die Übung der Kammern, pauschal und regelmäßig eine Vielzahl von Daten neuer Mitglieder weiterzugeben, ist jedoch nicht zulässig; denn bei regelmäßiger Datenübermittlung wird es grundsätzlich nicht zu einer Abwägung zwischen dem berechtigten Interesse des Datenempfängers einerseits und den schutzwürdigen Belangen des von der Datenübermittlung Betroffenen andererseits kommen.

Überwiegend waren die Vertreter der Kammern, mit denen ich diese Problematik erörtert hatte, bereit, zukünftig unter Berücksichtigung der geschilderten Rechtslage keine Adreßdaten zu Werbezwecken weiterzugeben.

15.1.1

Daten aus dem Handelsregister

Eine Differenz entstand in der Diskussion, wie Daten, die dem Handelsregister entnommen werden, zu behandeln sind. Ich habe darauf verwiesen, daß die Grundsätze, wie ich sie oben dargelegt habe, auch für Daten gelten, die entweder dem Handelsregister entnommen oder jedenfalls in diesem enthalten sind. Zwar bestimmen die meisten Datenschutzgesetze, daß für Daten, die in allgemein zugänglichen Quellen enthalten sind (wie etwa Zeitungen, Telefonbücher oder auch das Handelsregister), kein Schutzbedürfnis bestehe. Jedoch ist allgemein anerkannt, daß dies nur solange gilt, wie die Daten in den allgemein zugänglichen Quellen, wie etwa dem Handelsregister, enthalten sind. Sobald sie in nicht allgemein zugängliche Datensammlungen übernommen werden, finden die Vorschriften der Datenschutzgesetze Anwendung (so ausdrücklich die amtliche Begründung zu § 3 Abs. 7 HambDSG und § 3 Abs. 5 HDSG).

15.1.2

Das am 1. Januar 1993 in Kraft getretene Gesetz zur vorläufigen Regelung des Rechts der Industrie- und Handelskammern

Während es für die Handwerkskammern bei der oben dargelegten Rechtslage bleibt, hat sich für Datenübermittlungen der Industrie- und Handelskammern die gesetzliche Grundlage mit Wirkung vom Januar 1993 durch die Novellierung des IHKG geändert.

Im Rahmen dieser Novelle hatte das Land Hessen im Bundesrat den Antrag eingebracht, eine Regelung für die Datenverarbeitung der Mitgliederdaten in das IHK-Gesetz aufzunehmen. Aus datenschutzrechtlicher Sicht waren mehrere Passagen dieses Gesetzantrages besonders positiv zu bewerten:

Die Daten, die im Register der Industrie- und Handelskammern über die Mitglieder gespeichert werden, sollten grundsätzlich nur beim Inhaber oder Leiter des Unternehmens erhoben werden. Dies entspricht dem datenschutzrechtlichen Grundsatz, daß Daten – soweit möglich – beim Betroffenen zu erheben sind.

Hinsichtlich des oben angesprochenen Adreßhandels sah der hessische Gesetzesantrag vor, daß die Kammern die erhobenen Daten zur Förderung von Geschäftsabschlüssen und zu anderen dem Wirtschaftsverkehr dienenden Zwecken an nicht-öffentliche Stellen übermitteln dürfen, sofern der Kammerzugehörige nicht widersprochen hat. Auf diese Widerspruchsmöglichkeit sollten die Kammerzugehörigen vor der ersten Datenübermittlung hingewiesen werden. Eine Unterscheidung zwischen Firmen, die auch im Handelsregister eingetragen sind, und anderen Unternehmen sah der Antrag nicht vor; vielmehr sollte der Wille des Gewerbetreibenden in jedem Fall Berücksichtigung finden. Der Wirtschaftsausschuß des Bundesrates hatte diesen Antrag angenommen. Gleichwohl legte das Land Baden-Württemberg vor der Plenarsitzung des Bundesrates am 16. Oktober 1992 einen Änderungsantrag vor, der – obwohl er aus datenschutzrechtlicher Sicht wesentliche Verschlechterungen brachte – die Zustimmung im Bundesratsplenium erhielt. Die Regelung, wonach eine Datenerhebung nur beim Betroffenen erfolgen sollte, wurde damit völlig verwässert: Nunmehr sollten die Daten beim Betroffenen erhoben werden dürfen. Hierbei handelt es sich um eine Selbstverständlichkeit, die der gesetzlichen Normierung in keiner Weise bedarf. Wo die Daten aber sonst noch erhoben werden dürfen, ließ der Wortlaut des Gesetzantrages offen. Zudem nahm der Gesetzesantrag Baden-Württembergs denjenigen, die im Handelsregister eingetragen sind, die Möglichkeit, der Weitergabe ihrer Daten zu widersprechen.

Noch weiter geht das am 1. Januar 1993 in Kraft getretene IHKG, nach dessen § 9 Abs. 4 jetzt unabhängig vom Willen der Betroffenen die Übermittlung von Firma, Anschrift und Wirtschaftszweig der Unternehmen zur Förderung von Geschäftsabschlüssen zulässig ist.

Die Folge dieser vom hessischen Antrag abweichenden Regelungen ist, daß das einzelne IHK-Mitglied sein verfassungsrechtlich garantiertes Recht, selbst über die Preisgabe und Verwendung seiner Daten zu bestimmen, nicht ausüben kann.

15.2

Datenübermittlung zwischen Rechtsanwaltskammern

Aus der Anwaltschaft kam die Frage, ob es aus datenschutzrechtlicher Sicht zulässig sei, daß eine Rechtsanwaltskammer, der ein möglicherweise standeswidriges Verhalten eines Rechtsanwaltes aus einem anderen Kammerbezirk bekannt wird, die zuständige Rechtsanwaltskammer informiert.

Die Frage kann nicht in dieser Allgemeinheit, sondern nur bezogen auf den Einzelfall beantwortet werden.

Zwar normiert § 76 Bundesrechtsanwaltsordnung (BRAO) eine weitgehende Verschwiegenheitspflicht für Vorstand und Mitarbeiter der Kammern. Andererseits hat der Gesetzgeber mit Gesetz vom 13. Dezember 1989 (BGBl. I S. 2135) den § 36a in die BRAO eingefügt, nach dem Behörden (darunter fallen auch die Rechtsanwaltskammern) personenbezogene Informationen, die für die Rücknahme oder für den Widerruf einer Erlaubnis, Befreiung oder Zulassung eines Rechtsanwaltes oder zur Einleitung eines Rüge- oder ehrengerichtlichen Verfahrens von Bedeutung sein können, der für die Entscheidung zuständigen Stelle übermitteln dürfen, soweit hierdurch schutzwürdige Belange des Betroffenen nicht beeinträchtigt werden oder das öffentliche Interesse das Geheimhaltungsinteresse des Betroffenen überwiegt. Die Kammer hat demnach eine auf den Einzelfall bezogene Abwägung vorzunehmen, in die insbesondere die Schwere des vermeintlichen Pflichtenverstößes des Rechtsanwaltes einzubeziehen ist, bevor sie andere davon unterrichtet.

16. Datensicherheit

16.1

Probleme der Löschung von Daten am Beispiel von WORM-Platten

16.1.1

Nutzung von WORM-Platten

16.1.1.1

Ausgangslage

In der Datenverarbeitung gibt es eine Reihe von Problemen, an deren Lösung seit vielen Jahren gearbeitet wird. Dazu gehört die Registratur mit dem elektronischen Archiv. Für das elektronische Archiv müssen insbesondere folgende Ziele erreicht werden:

- Es müssen sehr große Datenbestände gespeichert werden können.
- Ein jederzeitiger Zugriff berechtigter Personen auf die Daten muß gewährleistet sein, wobei geringfügige Abstriche bei den Antwortzeiten akzeptiert werden.
- Die gespeicherten Daten müssen authentisch sein, d.h. sie dürfen nicht geändert werden können.
- Die Daten müssen über lange Zeiträume (zehn und mehr Jahre) lesbar bleiben.
- Es sollte möglich sein, Belege zu archivieren, d.h. die Vorlagen müssen originalgetreu wiedergegeben werden (Faksimile).

Für diese Zielsetzung hat sich in den letzten Jahren eine technische Alternative ergeben, die erstaunliche Möglichkeiten bietet: die sog. WORM-Platten (Write-Once-Read-Many). Bei diesen Speichermedien handelt es sich um Scheiben, die CDs ähneln, deren Durchmesser aber größer sein kann. Sie können einmal beschrieben werden und sind dann nicht mehr (beliebig) änderbar. Der Schreibvorgang erfolgt durch einen Laserstrahl mit hoher Kapazität, der "Löcher" in eine Schicht der Platte brennt bzw. chemische Änderungen herbeiführt. Wenn der Laserstrahl mit geringer Kapazität die Platte abtastet, werden die Änderungen erkannt. Die Speicherkapazität einer 30 cm durchmessenden Scheibe beträgt derzeit ca. 6,5 Giga-Byte (das entspricht etwa 3 Millionen Seiten Schreibmaschinentext oder ca. 100.000 als Faksimile gespeicherten Dokumenten). Darüber hinaus sind die Platten sogar robuster als die üblichen Magnetplatten. Bei immer mehr DV-Verfahren wird daher die Nutzung dieser Technik vorgesehen.

16.1.1.2

Eine Anwendung

Mitte des Jahres konnte ich mir ein DV-Verfahren ansehen, das ganz wesentlich auf Möglichkeiten von WORM-Platten zurückgreift. Das Verfahren wird von einer Agentur zur Vermittlung von Führungskräften entwickelt, könnte hinsichtlich der eingesetzten Technik aber ebensogut in einer hessischen Behörde anzutreffen sein. Kernstück ist eine Archivierungskomponente, bei der Schriftstücke als Grafik gespeichert werden. Die Schriftstücke können am Bildschirm angezeigt, ausgedruckt oder per Telefax versandt werden. Zusätzlich werden zu den einzelnen Vorgängen noch Stammdaten gespeichert.

In den Abläufen ist vorgesehen, alle eingehenden und ausgehenden Schriftstücke zu speichern, auch die von Erstbewerbern. Zumindest diesen Personen wäre nicht bekannt, daß alle Unterlagen bei Posteingang eingesehen (gescannt) werden. Sollte eine Bewerbung nicht erfolgreich sein oder zurückgezogen werden, so ist beabsichtigt, die Daten zu löschen.

16.1.1.3

Das Problem: Der Löschvorgang

Bei genauerer Betrachtung können sich im Zusammenhang mit der Löschung von Daten, die auf einmal beschreibbaren Datenträgern wie WORM-Platten gespeichert sind, datenschutzrechtliche Probleme ergeben. Im dargestellten Fall läuft eine Löschung wie folgt ab:

Auf dem Datenträger gibt es einen Datenteil, auf dem Nutzdaten gespeichert werden, sowie einen Verzeichnisteil. Im Verzeichnisteil wird hinterlegt, an welcher Stelle welche Daten gespeichert sind. Sollen nun Daten gelöscht werden, so wird im Verzeichnisteil ein Eintrag erzeugt, der besagt, daß bestimmte Daten als gelöscht zu interpretieren sind und daher überlesen werden müssen. Der Datenteil bleibt unverändert.

Um die Zugriffe auf den Datenträger durchführen zu können, wird ein aktuelles Verzeichnis geführt. Dieses Verzeichnis wird erzeugt, indem der Verzeichnisteil des Datenträgers gelesen und das aktuelle Abbild der Daten erstellt wird. Im vorliegenden Fall tauchen die "gelöschten" Daten daher nicht mehr auf, obwohl sie noch vorhanden sind. Wenn der Datenträger unter Umgehung des Verzeichnisses gelesen werden kann, stehen die Daten wieder im Zugriff.

In der geplanten Anwendung bleiben die Daten auf den Datenträgern faktisch gespeichert. Wenn man die Frage stellt, ob das Verfahren in der geplanten Technik zulässig sein kann, ist es angebracht, sich Begriffe und Probleme, die beim Löschen von Daten auftreten, in Erinnerung zu rufen.

16.1.2

Begriffsbestimmungen

16.1.2.1

Löschen

Im Hessischen Datenschutzgesetz (HDSG) und in ähnlicher Form auch in den anderen Datenschutzgesetzen werden Begriffe erläutert, die bei der Verarbeitung personenbezogener Daten wichtig sind. § 2 Abs. 2 Nr. 5 HDSG definiert das Löschen von Daten als "Unkenntlichmachen gespeicherter Daten". Der Begriff "Unkenntlichmachen" besitzt kein technisches Äquivalent. Es wurde daher versucht, Umschreibungen zu finden. In einer Kommentierung heißt es, daß "... die Kenntnis der Daten für jedermann zu jeder Zeit tatsächlich unmöglich sein muß" (Auernhammer BDSG 2. Aufl. 1981 S. 2 Rdnr. 13).

In den DIN 44300 Teil 8 (Informationsverarbeitung; für Begriffe Verarbeitungsfunktion) wird Löschen als "Daten auf einem Datenträger oder Daten in einem Speicher vernichten" definiert. In einer Anmerkung werden Beispiele wie Überschreiben, Versetzen in einen physikalischen Grundzustand oder Entfernen der Daten aus ihrer Umgebung und Schließen der Lücke genannt.

Nach diesen Definitionen ist vor dem Hintergrund der technischen Gegebenheiten die Löschung im Ausgangsfall nicht gegeben, denn es ist lediglich durch Software, die geändert werden kann, der Zugriff unterbunden. Es ist denkbar, daß der Anbieter der WORM-Platte und des Laufwerks über das Wissen und die Möglichkeiten verfügt, auf gelöschte Daten zuzugreifen, wenn die Platte zur Verfügung steht. Man kann sogar noch weitergehen und feststellen, daß die derzeit praktizierten Umsetzungen einer Löschung bei DV-Verfahren meist nicht in diesem Sinne durchgeführt werden. Logische Löschungen genügen den Definitionen eigentlich nie, und selbst eine physische Löschung erfüllt diesen Anspruch bei strenger Auslegung oft nicht (vgl. 16.1.3.2).

Angesichts immer besserer Analysetechniken und der je nach Schutzbedürftigkeit der Daten unterschiedlichen Schutzziele wird im Entwurf der DIN 33858 ("Löschen von schutzbedürftigen Daten auf magnetischen Datenträgern") für magnetische Datenträger nicht mehr der Anspruch erhoben, daß eine Reproduktion der Daten unmöglich sein muß. Vielleicht wird als Ziel einer Löschung definiert, daß "... der Zustand der physikalischen Darstellung durch äußere Feldeinflüsse (Magnetfeld) so verändert wird, daß eine Reproduktion der Daten unmöglich oder weitgehend erschwert wird".

16.1.2.2

Logisches Löschen

Je nach dem Speichermedium kann das sog. logische Löschen unterschiedlich realisiert werden:

– Wiederbeschreibbare Datenträger

Die zu löschenden Daten (ganze Datensätze oder Dateien) werden dadurch unkenntlich gemacht, daß sie als gelöscht gekennzeichnet werden. Dies kann geschehen, indem Verzeichniseinträge unkenntlich gemacht werden, Pointer (interne Zeiger) zurückgesetzt werden oder ein Löschkennzeichen gesetzt wird. Die Bereiche, in denen die Daten gespeichert sind, werden in der Regel zum Überschreiben freigegeben. (Dieser Kompromiß zum physischen Löschen durch Überschreiben wurde gewählt, da der Zeitaufwand für das Überschreiben großer Datenmengen bei einem Rechner, an dem viele Benutzer arbeiten, nicht akzeptiert werden konnte.) Ein bekanntes Beispiel ist das Löschen von Dateien unter MS-DOS, bei dem lediglich das erste Zeichen des Verzeichniseintrags

mit einem Sonderzeichen ("??") überschrieben wird. Durch das Betriebssystem MS-DOS wird dann die Datei als nicht mehr vorhanden interpretiert.

Sollen einzelne Datenfelder gelöscht werden, so geschieht dies meistens durch Überschreiben mit neuem Inhalt (physisches Löschen).

– Einmal beschreibbare Datenträger

Wie schon oben beschrieben, wird aus den Einträgen im Verzeichnisteil des Datenträgers auf dem Rechner ein aktuelles Verzeichnis der Daten erstellt. Soll eine Löschung erfolgen, so wird als neuer Eintrag ein Löschvermerk vorgenommen, der bei der Generierung des aktuellen Verzeichnisses den Verweis auf die Daten überschreibt. Die Datenbereiche bleiben erhalten.

16.1.2.3

Physisches Löschen

Beim physischen Löschen von Daten gibt es unterschiedliche Möglichkeiten. Sollen nicht alle auf einem Medium gespeicherten Daten gelöscht werden, so geschieht dies üblicherweise durch Überschreiben, was nur bei wiederbeschreibbaren Datenträgern möglich ist (Übrigens: auch einmal beschreibbare Datenträger können in einzelnen Fällen so behandelt werden, vgl. 17.1.3.2). Statt einzelne Daten auf einem Datenträger unkenntlich zu machen, kann es auch angebracht sein, die gesamten gespeicherten Daten unkenntlich zu machen. Dies kann durch Überschreiben, Entmagnetisieren oder Zerstören erfolgen.

16.1.3

Probleme

Bei der Frage, ob eine bestimmte Art, Daten zu löschen, datenschutzgerecht ist, muß das Ausmaß der Gefährdung geklärt und in Relation zur Sensibilität der Daten gesetzt werden. Dabei muß unter anderem geklärt werden, wer mit welchem Aufwand die Daten rekonstruieren kann.

16.1.3.1

Logische Löschung

Es liegt in der Definition einer logischen Löschung (die Daten sind noch gespeichert; sie sind lediglich als gelöscht gekennzeichnet), daß die prinzipielle Möglichkeit der Rekonstruktion immer besteht. Handelt es sich um einen wiederbeschreibbaren Datenträger, so bedeutet eine logische Löschung, daß die als gelöscht gekennzeichneten Bereiche zum Überschreiben freigegeben sind. In Abhängigkeit von der Art der Speicherbereiche und dem zur Verfügung stehenden Speicherplatz kann ein Überschreiben kurzfristig erfolgen, nach längerer Zeit stattfinden oder muß erst im Rahmen eines Reorganisationslaufes angestoßen werden. Beispiele hierfür sind:

– Temporäre Speicher

Die freigegebenen Speicher werden meist kurzfristig überschrieben (physische Löschung). Der Benutzer muß nicht eingreifen.

– Dateien

Je nach dem verfügbaren Speicherplatz erfolgt ein Überschreiben kurzfristig oder erst nach längerer Zeit. Ein Eingriff ist normalen Benutzern oft nicht möglich. Es gibt in vielen Fällen aber die Möglichkeit, ein physisches Löschen durch Überschreiben zu veranlassen.

– Datenfelder oder einzelne Datensätze

Diese bleiben in der Regel erhalten und sind lediglich mit einem Löschkennzeichen versehen. Ein Überschreiben erfolgt erst nach einem Reorganisationslauf. Bei Datenfeldern hängt es von der Anwendung ab, ob sie bei Änderungen sofort überschrieben werden.

Viele Betriebssysteme enthalten Hilfsprogramme, oder es gibt Zusatzprogramme zu den Betriebssystemen (UTILITIES, TOOLS), die eine Rekonstruktion noch nicht überschriebener Dateien ermöglichen; dies gilt analog auch für Datenbanken. Dabei wird einem hoffentlich kleinen Personenkreis (Systemverwalter, Datenbankadministratoren etc.) diese Möglichkeit eingeräumt. Es gibt allerdings Fälle, beispielsweise bei MS-DOS PCs, in denen derartige Programme weitverbreitet sind. Handelt es sich um einmal beschreibbare Speicher, so sind die Daten in jedem Fall weiter vorhanden. Solange der Datenträger noch existiert, ist es mit einem gewissen Aufwand auch möglich, auf die Daten zuzugreifen.

Eine logische Löschung kann, unabhängig von der Sensibilität der Daten, im Grundsatz dann nicht datenschutzgerecht sein, wenn es mit geringem Aufwand möglich ist, gelöschte Daten zu rekonstruieren. Sie ist auch nicht ausreichend, wenn ein Datenträger entsorgt oder im Rahmen eines Datenträgeraustausches genutzt wird.

Wird im täglichen Betrieb eines DV-Systems mit dem logischen Löschen von Daten gearbeitet, ist es eine Mindestanforderung, daß der "normale" Benutzer die durch ein Betriebssystem vorgetäuschte Löschung nicht

umgehen kann. Wird der Speicherplatz ferner mit einer nicht zu großen zeitlichen Verzögerung überschrieben, so kann das Ergebnis einer logischen Löschung in den meisten Fällen akzeptiert werden.

In der eingangs beschriebenen technischen Konstellation muß im Einzelfall geprüft werden, ob die Löschung ausreichend ist. Neben den Fragen nach der Sensibilität der Daten und den tatsächlichen Zugriffsmöglichkeiten, spielt es auch eine Rolle, wie die Entsorgung der Platten erfolgt und in welchen Zeiträumen Reorganisationsabläufe stattfinden (vgl. Ziff. 16.1.3.2 letzter Absatz).

16.1.3.2

Physisches Löschen

Das physische Löschen von Datenträgern ist im Ergebnis wirksamer als ein logisches Löschen. Es ist daher anzustreben, daß in möglichst vielen Fällen so verfahren wird. Zu den Verfahren selbst ist anzumerken:

– Entmagnetisieren

Bei magnetisierbaren Datenträgern gibt es die Möglichkeit, eine Löschung durch Entmagnetisieren durchzuführen. Dabei muß die Stärke des Magnetfeldes, mit dem die Löschung erfolgt, in Abhängigkeit vom Material des Datenträgers gewählt werden, damit es keine Möglichkeit gibt, die gelöschten Daten zu rekonstruieren. Im Entwurf der DIN 33858 ("Löschen von schutzbedürftigen Daten auf magnetischen Datenträgern") wurden die Abhängigkeiten dadurch berücksichtigt, daß als Mittel, um die Wirkung eines Löscherätes festzustellen, Prüfbänder mit entsprechenden physikalischen Eigenschaften vorgesehen sind.

Wenn die Entmagnetisierung korrekt erfolgt, d.h. bei einer ausreichenden Dämpfung (also eine dem jeweiligen Material und den Analysemethoden angepaßten Magnetfeldstärke), kann eine Rekonstruktion ausgeschlossen werden. Es ist dabei durch regelmäßige Kontrollen sicherzustellen, daß das Gerät noch richtig funktioniert, da anders als beim Zerstören eine Prüfung durch Augenschein nicht möglich ist. Im Prinzip ist diese Form der Löschung datenschutzgerecht.

– Überschreiben

Beim Überschreiben bleiben Restinformationen über die vorher gespeicherten Daten erhalten, die aber nur mit einem erheblichen technischen (und damit finanziellen) Aufwand ausgewertet werden können. Durch mehrmaliges Überschreiben kann die Restinformation so weit minimiert werden, daß eine Rekonstruktion ausgeschlossen werden kann.

In den meisten Fällen führt eine Formatierung des Datenträgers (der Datenträger wird zur Nutzung in seinen Grundzustand versetzt) zum gleichen Ergebnis. Es kann aber zu Schwierigkeiten führen, wenn eine Formatierung das Ergebnis nicht herbeiführt. Bei MS-DOS in der Version 5.0 führt der FORMAT-Befehl nur bei Angabe des Parameters/U die Formatierung einer Diskette so aus, daß eine Rekonstruktion der Daten nicht mehr möglich ist. Ohne Eingabe des Parameters ist eine Formatierung im Ergebnis nur eine logische Löschung!

Zu WORM-Platten muß angemerkt werden, daß sie in gewissen Konstellationen "mehrfach beschreibbar" sein können. In Fachzeitschriften wurde ein Verfahren beschrieben, mit dem auch eine Manipulation von Daten möglich sein soll. Bevor eine Schreiboperation auf einer WORM-Platte beginnt, wird bei einigen Herstellern ein "Blank-Check" vorgenommen, d.h. es wird geprüft, ob an der vorgesehenen Stelle, einem Sektor, bereits Daten gespeichert sind. Wenn der "Blank-Check" ausgeschaltet wird, könnte der Sektor ein zweites Mal beschrieben werden. Es würden neue "Löcher" erzeugt, die alten "Löcher" jedoch bestehen bleiben. In diesem Fall würden die Prüfbits i.d.R. nicht mehr stimmen und den Sektor als fehlerhaft ausweisen.

Wenn jetzt mit geänderten Daten versucht wird, den Sektor zu beschreiben, würde zuerst festgestellt, daß er fehlerhaft ist und zu einem Reservesektor verzweigt. Dort würden dann die geänderten Daten gespeichert und bei folgenden Lesezugriffen als echte Daten angezeigt.

In der Betrachtung der Löschproblematik ist wesentlich, daß in diesem Fall gespeicherte Daten durch Überschreiben unkenntlich gemacht werden könnten. Derzeit ist ein Löschen nicht möglich, weil die Software, die die WORM-Platte steuert, die überschriebenen Daten als fehlerhaft interpretieren würde. Die wenigen Reservesektoren der Platte würden dann für Fehlerkorrekturmaßnahmen in Anspruch genommen. Innerhalb kurzer Zeit wäre die Platte unbrauchbar.

Die Software der WORM-Platten ist derzeit nicht in der Lage, die prinzipielle Möglichkeit des Löschens umzusetzen. Hier könnten die Anbieter eine Möglichkeit zum physischen Löschen von Daten erarbeiten.

– Zerstören

Ein Datenträger kann in jedem Fall dadurch "gelöscht" werden, daß man ihn zerstört. Ob diese Form der Löschung im jeweiligen Fall datenschutzgerecht ist, hängt unter anderem von dem Aufwand ab, mit dem aus den Resten eine Rekonstruktion von Daten möglich ist. Für Papier und Mikrofilm kann hier auf die DIN 32757 ("Vernichtung von Informationsträgern") verwiesen werden, in der Regelungen getroffen sind.

Wenn geplant ist, Magnetdatenträger oder optische Speichermedien zu zerkleinern, muß beachtet werden, daß die Speicherkapazitäten sehr groß sind. So können Magnetbandkassetten derzeit ca. zwei Seiten Schreibmaschinentext auf einen Zentimeter Band speichern oder optische Speichermedien bis zu 1.000 Seiten je Quadratzentimeter. Auch wenn bezweifelt werden muß, daß es viele Fälle gibt, in denen technische Geräte zur Verfügung stehen, mit denen aus derartigen Resten eine Rekonstruktion erfolgen kann, muß die Möglichkeit ins Kalkül gezogen werden. Bei neuen Analysetechniken und für sensible Daten können sich ungeahnte Konsequenzen ergeben.

Die Grundsätze der DIN 32757, die für Papier und Mikrofilme gelten, können nicht ohne weiteres übernommen werden.

Während es bei wiederbeschreibbaren Datenträgern mehrere Möglichkeiten gibt, eine physische Löschung durchzuführen, bleibt bei nicht wiederbeschreibbaren Datenträgern in der Regel nur der Weg, den Datenträger zu zerstören, nachdem aktuelle Daten auf einen anderen Datenträger kopiert wurden.

16.1.3.3

Weitere Probleme

Ein weiteres Problem besteht darin, bei der Löschung bestimmter Daten diese tatsächlich an allen Stellen zu löschen, an denen sie gespeichert sind.

Einerseits betrifft dies Sicherungen von Dateien, die in vielen Kopien vorhanden sein können, andererseits kommen die Daten evtl. in Dateien oder Datenbeständen vor, an die man nicht denkt. Werden beispielsweise Daten mit einem Datenbankmanagementsystem verwaltet, so werden Logdateien (Protokolle von Änderungen in Datenbanken) geführt, die es erlauben, Datenbanken zu rekonstruieren. In diesen Logdateien befinden sich Kopien von Änderungen in einer Datenbank. So werden Abbilder von Datensätzen vor und nach einer Löschung gespeichert. Es ist nicht möglich, aus diesen Logdateien Teile zu löschen oder Sperrvermerke vorzunehmen, weil es dann nicht mehr möglich wäre, mit den Logdateien die Datenbank zu rekonstruieren. Ähnlich sieht es mit Systemprotokollen aus, die in Rechenzentren zu Abrechnungszwecken benutzt werden. Die Daten werden noch so lange benötigt, wie es erforderlich sein kann, zur Fehlerklärung auf die Abrechnungsdaten zuzugreifen. Oft beinhalten die Protokolle auch personenbezogene Daten über Benutzer, wie Zeitpunkt der An- und Abmeldung am System. Diese Daten werden dann ebenso lange wie die Abrechnungsdaten gespeichert.

16.1.4

Zusammenfassung

In die Bewertung, ob eine vorgesehene Löschung datenschutzgerecht ist, muß die Angemessenheit einfließen. Als Ziel einer Löschung ist anzusehen:

Es darf nicht oder nur mit einem von der Sensibilität der Daten abhängigen, hohen technischen, zeitlichen und finanziellen Aufwand möglich sein, gelöschte Daten zu rekonstruieren.

Als Regelfall der Löschung ist die physische Löschung anzustreben. In diesem Zusammenhang muß beachtet werden, daß beispielsweise der Formatbefehl des Betriebssystems MS-DOS 5.0 mit dem Parameter /U ausgeführt werden muß, damit eine physische Löschung erfolgt. Es sind Fälle denkbar, in denen auch eine logische Löschung akzeptiert werden kann. Dabei ist aber eine Prüfung im Einzelfall vorzunehmen. Es sollte das Ziel sein, im Rahmen eines Entsorgungskonzepts zu klären, wie durch eine Kombination von logischer Löschung, Überschreiben, Entmagnetisierung, Zerstörung oder einer nachgeschalteten Entsorgung zu erreichen ist, daß gelöschte Daten nicht rekonstruiert werden können.

Um die datenschutzrechtlichen Probleme bei der Löschung von auf WORM-Platten gespeicherten Daten minimieren zu können, sind die Anbieter gefordert, Möglichkeiten zu erarbeiten, mit denen doch eine physische Löschung durchgeführt werden kann.

16.2

Prüfung der Datensicherheitsmaßnahmen in einem kommunalen Gebietsrechenzentrum

16.2.1

Ausgangssituation

In meinem 20. Tätigkeitsbericht (Ziff. 15.2) hatte ich von meiner Prüfung des Kommunalen Gebietsrechenzentrums (KGRZ) Frankfurt berichtet. Die festgestellten Mängel haben mich bewogen, das KGRZ Gießen in ähnlicher Art und Weise zu prüfen. Prüfungsschwerpunkte waren wiederum die Sicherheitsmaßnahmen auf Betriebssystemebene und im systemnahen Bereich; ferner die räumlichen Sicherheitsmaßnahmen und – in Stichproben – die Datenträgerkontrolle, die Anwendungsentwicklung und die Organisationskontrolle. Das Verfahren, an dem das Zusammenspiel der Komponenten geprüft wurde, war das Vertriebswesen.

Das KGRZ Gießen gehört ebenso wie das KGRZ Frankfurt dem Hessischen DV-Verbund an. Dessen Mitglieder arbeiten im Bereich der Entwicklung von DV-Verfahren zusammen. Daher besteht eine weitgehende Übereinstimmung der eingesetzten Software im systemnahen Bereich und ähnlich der technische Verhältnisse in beiden Rechenzentren. Die Zusammenarbeit bedingt Abhängigkeiten, aufgrund derer Änderungen im Umfeld oft nur nach einer (u.U. langwierigen) gegenseitigen Abstimmung erfolgen können. Ein Beispiel dafür ist das Verfahren Vorstellungsdatei (vgl. 20. Tätigkeitsbericht, Ziff. 15.2.2.3).

16.2.1.1 Begriffe

In der Datenverarbeitung gibt es eine Reihe von Begriffen und Abkürzungen, die nicht allgemein verständlich sind. Die folgenden Umschreibungen sollen weniger eine Definition sein als Verständnisschwierigkeiten beheben:

– Betriebssystem

Das Betriebssystem eines Rechners steuert den Rechner und überwacht die angeschlossenen Geräte. Weitere Funktionen dienen der Erstellung von Anwendungsprogrammen oder unterstützen die ständig notwendigen Arbeiten mit dem Rechner. Beispiele für Betriebssysteme sind MS-DOS, UNIX oder – wie im Fall des geprüften KGRZ – MVS (zu MVS vgl. 20. Tätigkeitsbericht, Ziff. 15.2.1).

– Datenbankmanagementsystem

Ein Datenbankmanagementsystem (DBMS) ist eine Gruppe von Programmen, die es erlaubt, Datenbanken einzurichten, zu verwalten und zu nutzen.

– TP-Monitor

Ein TP-Monitor (Tele-Processing-Monitor) steuert Anwendungsprogramme, die von Benutzern im Dialog aufgerufen und genutzt werden.

– JOB

Ein JOB ist ein Auftrag an das Betriebssystem, Arbeitsprogramme in einer vorgegebenen Reihenfolge bestimmte Dateien verarbeiten zu lassen. Wenn Anwendungsprogramme als JOB Daten verarbeiten, spricht man von Batch-Verarbeitung.

In den Rechenzentren des Hessischen DV-Verbundes werden das Betriebssystem MVS, die TP-Monitore Com-Plète und CICS und das Datenbankmanagement ADABAS genutzt. Zur Steuerung des Zugriffs auf Verfahren und teilweise zur verfahrensinternen Kontrolle wird die Vorstellungsdatei benutzt, eine Anwendung, die vom KGRZ Kassel federführend betreut wird. Soweit es bei der Datensicherheit Probleme gibt, die aus dem Einsatz dieser Produkte resultieren, stehen die Rechenzentren des DV-Verbundes vor ähnlichen Aufgaben.

16.2.2 Festgestellte Mängel

Da es mir bei der Prüfung des KGRZ Gießen nicht zuletzt darum ging, den Stand der Datensicherheitsmaßnahmen mit dem des KGRZ Frankfurt zu vergleichen, werde ich an einigen Stellen auch auf den in den Stellungnahmen des KGRZ Frankfurt dargelegten Stand vom Herbst dieses Jahres eingehen.

Zwar war die Ausgangslage beider Rechenzentren nicht identisch, da dem KGRZ Gießen sowohl die Schwerpunkte als auch die Ergebnisse meiner Prüfung in Frankfurt bekannt waren. Dennoch dürfte die Gegenüberstellung bei allen Unterschieden in der Ausgangslage von Interesse sein.

Bei der Prüfung habe ich einige Mängel festgestellt, was aber in Anbetracht der Komplexität des Rechenzentrumsbetriebs nicht weiter verwundert.

Im konzeptionellen Bereich bestanden relativ klare Vorstellungen über Vorgehensweisen und deren Umsetzung. Einige dieser Ansätze, so bei der Revision, waren aber noch nicht zu Ende gebracht. Die Nutzung der Schutzkomponenten war – isoliert betrachtet – meist korrekt. Durch die fehlende Integration der Komponenten ergaben sich aber unnötige Schwachstellen. Die folgenden kurzen Abrisse sollen typische Mängel beleuchten bzw. auf Besonderheiten hinweisen.

An dieser Stelle möchte ich darauf hinweisen, daß in vielen der geprüften Bereiche gute Lösungen gefunden wurden. Als Beispiele können die Anwendungsdokumentation und die Datenträgerverwaltung, die beide durch entsprechende Softwareprodukte unterstützt werden, oder die räumlichen Sicherheitsmaßnahmen genannt werden.

Ein großer Teil der Mängel wurde bereits während der Prüfung behoben. Innerhalb von zwei Monaten ging mir darüber hinaus eine Stellungnahme des KGRZ Gießen zu, in der die Beseitigung der meisten Mängel mitgeteilt wurde. Zu den offenen Punkten, die im wesentlichen konzeptioneller Art sind, wurden mir die ergriffenen Maßnahmen genannt. Vorbehaltlich einer Nachprüfung, ob die getroffenen Maßnahmen ausreichend sind, waren die Reaktionen schnell und präzise.

16.2.2.1

Datenschutzgesamtkonzept

Es lag kein Datenschutzgesamtkonzept vor. Nicht zuletzt deshalb gab es Unklarheiten über Prioritäten bei der Realisierung von Datensicherungsmaßnahmen, wie im Fall von Schnittstellen zwischen ACF2 und TP-Monitoren. Das Konzept wurde allerdings, soweit ACF2 selbst betroffen ist, teilweise durch das ACF2-Handbuch abgedeckt. Dieses Handbuch wurde in den Jahren 1988 bis 1990 von einer Arbeitsgruppe begonnen, die ihre Tätigkeit nach einer Unterbrechung mittlerweile wieder aufgenommen hat. Das KGRZ Frankfurt hat zwischenzeitlich ebenfalls eine Arbeitsgruppe gebildet, die ein Gesamtkonzept erstellen soll; sie ist zur Zeit mit den Vorgaben für die Bereiche Benutzer- und Zugriffskontrolle befaßt.

16.2.2.2

Revisionskonzept

Ich konnte feststellen, daß die Revision von und mit ACF2 in gewissem Umfang stattfand. Die ACF2-Reports wurden mindestens einmal am Tag erstellt und ausgedruckt. Der ACF2-Administrator kontrollierte dann die Reports. Die Vorgehensweise bei der Kontrolle dieser Auswertung war, soweit die ACF2-Administration betroffen ist, in Ordnung. Es fehlte aber die Schriftform, und der durch die Revision abgedeckte Bereich muß noch erweitert werden. Hier ist ein Umfang anzustreben, wie ich ihn in meinem 20. Tätigkeitsbericht, Ziff. 15.2.2.2 beschrieben habe.

Es ergaben sich einige Punkte, die zu einer vermeidbaren Schwächung des Instruments der Revision führen:

- Der ACF2-Administrator prüft die Reports als einzige Person. Zumindest in Stichproben und aufgrund besonderer Anlässe ist eine Kontrolle durch eine weitere Person erforderlich.
- Der ACF2-Administrator kontrolliert seine eigene Tätigkeit.
- ACF2 ist Teil eines Sicherheitssystems, so daß auch die anderen Teile (MVS, TP-Monitore, Datenbanken, Anwendungen etc.) in die Revision einbezogen werden müssen. Punkte, die dabei kontrolliert werden müssen, sind die korrekte Implementierung der diversen Schnittstellen und die Prüfung von Einträgen in den diversen Schutzkomponenten auf ihre Aktualität hin.

Die Prüfungsergebnisse unterstreichen, daß eine externe Prüfung/Revision nicht ausreicht. Abgesehen davon, daß diese nur selten stattfindet, fehlt der Kontakt im täglichen Betrieb und bei den täglichen Schwierigkeiten. Sie ist nur eine notwendige Ergänzung zur internen Revision. Die Überlegungen beim KGRZ Gießen gehen dahin, die Funktion "Innenrevision" zu schaffen, die mit entsprechenden Aufgaben betraut wird.

Die Aufarbeitung dieses Punktes will das KGRZ Frankfurt erst nach Erstellung des Gesamtkonzepts beginnen oder, wenn es sich ergeben sollte, als Teil des Gesamtkonzepts darstellen.

16.2.2.3

Anmeldung am System; Integration der Schutzkomponenten

Bei der Anmeldung am System wird die Benutzerkontrolle durchgeführt, die aus der Identifikation (Eingabe der Kennung) und Authentifikation (zur Zeit in der Regel Eingabe eines Paßwortes) der Benutzer besteht und von zentraler Bedeutung für die systemseitigen Sicherheitsmaßnahmen ist.

Eine datenschutzgerechte Anmeldung mit Kennung (User-ID) und Paßwort bedingt in der Regel Anforderungen an die Paßwortverwaltung, wie ich sie in meinem 19. Tätigkeitsbericht (Ziff. 15.5) genannt habe. Sicherzustellen ist, daß sich nur die Person, der eine Kennung zugewiesen ist, damit anmelden kann, da nur ihr das zugehörige Paßwort bekannt ist.

Beim KGRZ Gießen war die "Philosophie" für die Anmeldung am System, daß ein Benutzer mit möglichst wenig Aufwand die ihm zugewiesenen Aufgaben ausführen kann. Hierzu muß sich der Benutzer an einem sog. Session-Manager mit Kennung und Paßwort anmelden. Der Session-Manager zeigt in Form eines Menues die TP-Monitore oder TSO (Time-Sharing-Option, ein Programm mit dem betriebssystemnah der Benutzer den Rechner nutzen kann) an, mit denen der Benutzer (richtiger: die Kennung) arbeiten darf. Wird ein TP-Monitor bzw. TSO angewählt, so wird die Verbindung hergestellt und ein automatischer Anmeldevorgang (LOGON) durchgeführt. Am TP-Monitor ist die Eingabe einer Benutzerkennung und eines Paßwortes nicht mehr erforderlich, während Anmeldevorgänge auf Anwendungsebene mit spezifischen Abfragen von Berechtigungs-codes weiterhin vorgenommen werden. Dadurch, daß ein Benutzer nicht an jedem TP-Monitor eine Anmeldung versuchen kann, wird eine höhere Sicherheit erreicht. Voraussetzung ist aber, daß die Schnittstellen zwischen den verschiedenen Schutzkomponenten korrekt implementiert sind und daß die erste Anmeldung am Session-Manager ein besonders hohes Maß an Sicherheit erreicht.

In der vorgefundenen Implementierung ergaben sich einige Mängel hinsichtlich der Speicherung bzw. der Pflege von Paßwörtern. Der Produktions-Session-Manager besaß keine Schnittstelle zu ACF2, so daß die nicht so guten

Mechanismen des Session-Managers für die Identifikation/Authentifikation genutzt wurden. Für den Test-Session-Manager wurde zwar die Identifikation/Authentifikation durch ACF2 vorgenommen, jedoch war für das Paßwort die absolut unzureichende Mindestlänge von zwei Stellen vorgegeben. Ferner war für die meisten TP-Monitore ebenfalls keine ACF2-Schnittstelle aktiv, so daß in den Session-Managern definiert wurde, mit welchem Paßwort eine bestimmte Benutzerkennung einen automatischen LOGON am jeweiligen TP-Monitor durchführt. Kennung und Paßwort müssen darüber hinaus auch in den entsprechenden TP-Monitoren definiert sein. Im CICS erfolgt dies beispielsweise in Tabellen im Klartext.

Das hat zur Folge, daß den Mitarbeitern des KGRZ, die die Einträge vornehmen, in diesen Fällen die Kennung und das Paßwort bekannt sind und sie sich mit jeder beliebigen Kennung anmelden könnten. Da unter ACF2 eine ganze Abteilung Schreib- und Leserechte für die CICS-Tabellen hatte, war diese Möglichkeit zumindest für CICS einem noch größeren Personenkreis gegeben. Noch während der Prüfung wurden die Einträge vorgenommen, um die Zugriffsmöglichkeiten auf den derzeitig benötigten Personenkreis zu beschränken.

Ein weiterer Mangel ergab sich aus dem Problem, für mehrere hundert Personen und jeweils mehrere Monitore unterschiedliche Paßwörter zu finden und in den Monitoren zu pflegen. Die Paßwörter wurden oft nach festen Regeln gebildet und waren dementsprechend leicht abzuleiten.

Diese Schwachstellen waren bekannt und ihre Beseitigung war vorgesehen. Durch dringende Neuanforderungen hatte man sie dann zurückgestellt. Ich habe gefordert, schnellstmöglich die Schnittstellen zu aktivieren und damit die Schutzsysteme zu integrieren.

16.2.2.4

Vorstellungsdatei

Die Anwendung "Vertriebswesen" benutzt zur verfahrensinternen Benutzer- und Zugriffskontrolle die Vorstellungsdatei. Im Unterschied zu den Verhältnissen, wie ich sie noch in meinem 16. Tätigkeitsbericht (Ziff. 4.2.2) beschrieben habe, gehören mittlerweile Auswertungen zum Funktionsumfang der Vorstellungsdatei. Die anderen Schwächen des Verfahrens wie z.B. keine Trennung von Identifikation/Authentifikation, keine Möglichkeit zur Änderung des Codes für den Benutzer (einige Codes waren mehr als zwei Jahre alt) oder keine Schnittstellen zu ACF2 lagen aber weiterhin vor.

Beim Verfahren Vorstellungsdatei können weder das KGRZ Gießen noch das KGRZ Frankfurt sinnvollerweise Änderungen vornehmen, da sie nicht federführend sind. Nicht zuletzt wegen der Ergebnisse der Prüfung des KGRZ Frankfurt und des in meinem 19. Tätigkeitsbericht (Ziff. 15.5) beschriebenen Vorfalles, sind für das Jahr 1993 durch das federführende KGRZ Kassel Anpassungen geplant, die die Schwächen der Vorstellungsdatei beseitigen sollen.

16.2.2.5

Einsatz von ACF2

Für die Zugriffskontrolle auf Systemebene ist im DV-Verbund ACF2 vorgesehen. Wegen der Bedeutung für das Gesamtsystem habe ich ACF2 näher untersucht.

Durch den Einsatz von ACF2 mußten ca. 300 Benutzer kontrolliert werden, die mittels TSO arbeiten konnten. Um die Zugriffe auf Dateien zu beschränken, wurden ca. 3.000 Regeln geschrieben.

Die Zahl der Benutzer, die nach Implementierung aller Schnittstellen der Kontrolle von ACF2 unterliegen müssen, beträgt fast 2.000. Wie viele ACF2-Regeln vorhanden sein werden, um alle Ressourcen zu schützen, läßt sich derzeit noch nicht abschätzen. Diese Zahlen lassen erahnen, daß bei einer Prüfung mit ziemlich hoher Wahrscheinlichkeit Stellen gefunden werden, an denen Einträge hätten anders sein sollen oder müssen.

Ich konnte feststellen, daß ACF2 in der vorgefundenen Implementierung den Zugriff auf alle Dateien prinzipiell kontrollierte. Auch erfolgte eine Kontrolle der Anmeldung am TSO und an dem Test-Session-Manager durch ACF2. Insofern waren die Voraussetzungen anders als bei der Prüfung des KGRZ Frankfurt. Dort war ACF2 zwar als Software vorhanden, jedoch waren die Schutzmechanismen beim Dateizugriff in weiten Bereichen nicht aktiviert. Infolgedessen habe ich bei der Prüfung des KGRZ Gießen verstärkt auf die Ausprägung von Zugriffsrechten geachtet, was sich in der Konstellation beim KGRZ Frankfurt erübrigt hatte.

Die wesentlichen Schwachstellen lagen in folgenden Bereichen:

- Zu den meisten TP-Monitoren und zum DBMS fehlten Schnittstellen.
- Batch-Jobs liefen unter "Gruppen-IDs".
- In einigen Fällen waren die eingeräumten Zugriffsrechte zu weitgehend.

16.2.2.5.1 Batch-Jobs

Wenn Mitarbeiter der Systemprogrammierung oder der Arbeitsvorbereitung durch das Operating Jobs starten lassen wollten, stellten sie ihren Job in eine Datei. Das Operating löste die Abläufe durch Aufruf eines Programms aus, das die Jobs in der gespeicherten Reihenfolge startete. Dabei wurde für alle Jobs der Arbeitsvorbereitung und der Systemprogrammierung je eine feste ACF2-Kennung eingesteuert. Jeder Job hat in dieser Konstellation also die Zugriffsmöglichkeiten der jeweiligen Kennung, d.h. die Summe der Zugriffsrechte der jeweiligen Mitarbeitergruppe. Diese Abläufe hatten sich im Laufe der Zeit aus Lösungen entwickelt, die zur einfacheren Steuerung von Jobs dienten.

Neben der Problematik, daß mit einem einzelnen Job evtl. zu weitgehende Zugriffsmöglichkeiten verbunden waren, waren auch die ACF2-Protokolle nicht mehr aussagekräftig. Es konnte den Protokollen nicht entnommen werden, welcher Benutzer im Rahmen eines Jobs welche ACF2-Protokolleinträge verursacht hatte.

In seiner Stellungnahme teilte mir das KGRZ Gießen mit, daß die Abläufe sicherer gestaltet wurden, indem eine weitergehende Differenzierung bei den Kennungen stattfindet. Inwieweit die gefundene Lösung den datenschutzrechtlichen Anforderungen gerecht wird, muß noch geprüft werden.

16.2.2.5.2 Zugriffsregeln

Die Implementierung von ACF2 verlangte, bis auf eine Ausnahme (Zugriff auf Banddateien), daß zu jeder Datei eine Zugriffsregel existieren muß. Bei der stichprobenhaften Kontrolle wurden nur Regeln gefunden, die den Modus ABORT hatten, d.h. bei einem Regelverstoß wurde der Zugriff abgewiesen und der unzulässige Versuch protokolliert.

Bei der Vielzahl der Regeln gibt es verständlicherweise Fälle, in denen zu weit gehende Zugriffsmöglichkeiten eingeräumt wurden, sei es durch Unachtsamkeit oder weil eine andere Auffassung über den zulässigen Zugriff vorlag. Es ergaben sich daher Regeln, die unbedingt anzupassen waren. Beispielhaft sollen hier genannt werden:

- In zu vielen Fällen wurde für alle Benutzer ein Leserecht auf Dateien eingeräumt (dabei muß beachtet werden, daß die "normalen" Benutzer nur innerhalb von Dialoganwendungen auf Daten zugreifen können und dadurch unzulässige Zugriffe auf Dateien ausgeschlossen wurden. Die Schwachstelle trifft im wesentlichen für KGRZ-Mitarbeiter zu. Es gibt freilich eine wichtige Ausnahme davon; vgl. 16.2.2.6).

Der Zugriff auf Systemdateien war in weiten Bereichen nur lesend möglich. Lediglich die Systemprogrammierung besaß Schreibrechte. Obwohl damit ein Schutz gegen unbefugte Änderungen am Betriebssystem und an der systemnahen Software erreicht war, ist doch eine Verschärfung in einigen Bereichen erforderlich. Hier sind die SYS1.PARMLIB, APF-autorisierte Dateien u.ä. zu nennen.

- Die Dateien des Betriebssystems, in denen die Daten der Produktionsdatenbanken gespeichert waren, waren nicht lesegeschützt und für Mitarbeiter des KGRZ auch änderbar. Da gleichzeitig die ADABAS-Programmibliotheken nicht lesegeschützt waren, konnten alle Benutzer mit Zusatzwissen, die Zugang zur Betriebssystemebene besaßen, Datenbanken lesen und mit – allerdings starken – Einschränkungen ändern. Hier wurden umgehend Maßnahmen ergriffen.

Für die Behandlung von Magnetbändern, die im Datenträgeraustausch eingehen und keinen oder einen dem ACF2 nicht bekannten Dateinamen haben, ist die Regel "NORULES" definiert. Diese besagt, daß jeder Mitarbeiter der Systemprogrammierung bzw. Arbeitsvorbereitung die Daten lesen bzw. ändern kann. Dies war erforderlich, da eingehende Magnetbänder zumindest gelesen werden müssen.

In diesem Fall muß ein Verstoß gegen die Grundphilosophie von ACF2, nach der ein Zugriff abgewiesen wird, wenn ACF2 keine Erlaubnis gibt, hingenommen werden, da nicht für alle fremden Banddateien Regeln existieren können. Um dies zu erreichen, kennt ACF2 die Möglichkeit, die Ergebnisse von Regelprüfungen zu modifizieren. Dazu war ein EXIT (ein kleines Programm, das es erlaubt, zu bestimmten Zeitpunkten in die Abläufe von systemnahen Programmen einzugreifen) bestimmt, der nach der Regelprüfung beim Dateizugriff ausgeführt wurde. Es handelte sich um den sog. VIOEXIT. Im vorliegenden Fall wurde in dem Programm festgestellt, ob es sich um eine Banddatei handelt, zu der keine Regel existiert. In diesem Fall wurde dem o.g. Personenkreis der Zugriff eröffnet. Der EXIT hätte aber genausogut einer bestimmten Kennung jeden Dateizugriff erlauben können. Um sicherzustellen, daß ACF2 tatsächlich Zugriffe so kontrolliert, wie es die Regeln vorgeben, muß im Rahmen der Revision dieser oder andere EXITS dahingehend kontrolliert werden, ob sie die geforderten Funktionen tatsächlich ausführen.

16.2.2.5.3 GSO-Record, generelle Parameter

Die Parameter entsprachen im wesentlichen den Erfordernissen. Es waren zwar einige veraltete Einträge vorhanden, die jedoch sofort gelöscht wurden.

Einen Mangel stellte die vorgeschriebene Mindestlänge der Paßwörter dar, die mit einem Wert von zwei erheblich zu gering war (vgl. 19. Tätigkeitsbericht, Ziff. 15.5.4).

16.2.2.5.4 Benutzerdefinitionen

Die Definitionen waren bis auf ganz wenige Ausnahmen korrekt. Auch wurden Benutzerprivilegien im Regelfall nicht zu weit gestreut.

Probleme ergaben sich durch die Häufung von Privilegien bei bestimmten Personen. So waren die Systemprogrammierer MVS gleichzeitig Vertreter des ACF2-Administrators. Diese Zuordnung wurde mittlerweile aufgehoben.

16.2.2.5.5 Reaktionen

Die ACF2-spezifischen Mängel wurden, da meist nur eine Korrektur vorhandener Regeln erforderlich war, oft schon während der Prüfung beseitigt. Ein wesentlicher Punkt, der noch geregelt werden muß, betrifft die Aktualität von Einträgen. Hier und bei der Frage, welche Zugriffe eingeräumt werden dürfen oder müssen, gilt es, tätig zu werden.

Das KGRZ Frankfurt hat in einer Stellungnahme zum Stand bei ACF2 dargelegt, daß die Regelschreibung fortschreitet. So werden die Regeln derzeit vom LOG-Modus (ein nach der Regel unerlaubter Zugriff wird akzeptiert, jedoch erfolgt ein Protokolleintrag) in den ABORT-Modus (ein unerlaubter Zugriff wird abgewiesen und protokolliert) umgestellt. Die Änderung der Grundeinstellung, die zum Zeitpunkt der Prüfung einen Zugriff erlaubte, wenn keine Regel vorlag, wurde mir noch nicht mitgeteilt.

Ein Stand wie beim KGRZ Gießen ist noch nicht erreicht.

16.2.2.6 Zugriffsmöglichkeiten für Mitarbeiter der Verwaltung

Die Online-Anwendungen des DV-Verbundes sind in der Regel mandantenfähig, d.h. es können die Daten mehrerer Anwender verarbeitet werden, und die Abschottung der Datenbestände ist möglich. Je nach Anwendung ist auch noch eine weitere Differenzierung von Zugriffen vorgesehen. Beim Vertriebswesen habe ich keine programmseitigen Mängel der Datensicherheitsmaßnahmen festgestellt.

Das Konzept für die Zugriffskontrolle im Rahmen von Online-Anwendungen bot bei korrekter Umsetzung die Gewähr, daß kein Zugriff auf die Daten anderer Anwender möglich war. Dabei war es wesentlich, daß die Mitarbeiter keinen Zugang zur Systemebene hatten.

Eine Schwachstelle hatte sich aber in Gestalt von "DV-Altlasten" eingeschlichen. Es waren sechs Benutzerkennungen für KGRZ-externe Benutzer vorhanden, die mit TSO arbeiten konnten. Wegen der unter ACF2 vorhandenen Schwächen bei bestimmten Zugriffsregeln konnten auch mit diesen Kennungen die unter 16.2.2.5.2 beschriebenen Zugriffe vorgenommen werden. Bei der Diskussion verschiedener Zugriffsregeln stellte sich heraus, daß die Tatsache bei der Regelschreibung nicht berücksichtigt worden war. Diese Abweichung von dem Konzept, daß externe Benutzer keinen Zugriff auf die Systemebene haben, war nicht ausreichend gegenwärtig.

Das KGRZ Frankfurt hat aufgrund meiner Prüfung die Schnittstelle zwischen dem Com-Plete und ACF2 aktiviert. Dadurch unterliegen die Zugriffe der Kontrolle von ACF2. Wegen der noch vorhandenen Schwächen bei ACF2 ist der Mangel aber noch nicht behoben. Die Situation stellt sich eher ungünstiger dar als beim KGRZ Gießen.

16.2.2.7 Zugriffsmöglichkeiten von KGRZ-Mitarbeitern

Soweit KGRZ-Mitarbeiter unter TSO arbeiten konnten, und das war die Regel, sind die unter 16.2.2.5.2 gemachten Feststellungen relevant.

Die beiden folgenden Fälle sollen deshalb Zugriffsmöglichkeiten illustrieren, die nicht mit ACF2 in Zusammenhang stehen. Sie sind auch deshalb interessant, weil sie typische Abläufe wiedergeben, wie es zu einer Ausweitung von Zugriffsrechten kommen kann.

a) Anwendungsentwicklung Vertriebswesen

Einige Entwickler des Verfahrens Vertriebswesen hatten im Rahmen der Anwendung jederzeit umfassenden Zugriff auf Produktionsdaten. Begründet wurde dies mit dem Erfordernis, im Einzelfall zur Fehlerbehebung oder Unterstützung kurzfristig auf die Daten zugreifen zu müssen. Aus Sicht der Kundenfreundlichkeit mag der Ansatz seine Berechtigung haben, ansonsten ist er in der vorgefundenen Form nicht zu akzeptieren.

Es wurde daher nach einer Lösung gesucht, die der Problematik gerecht wird. Der derzeit verfolgte Ansatz sieht folgende wesentliche Punkte vor:

- Die Anwender werden über den möglichen Service und evtl. Konsequenzen unterrichtet.
- Der Anwender kann den Service annehmen, wobei die Möglichkeit besteht, hinsichtlich der Datenbestände und der Zugriffsrechte von Mitarbeitern Einschränkungen vorzusehen.
- Auch wenn der Service gewählt wurde, muß er im Einzelfall angefordert werden. Die Anforderung wird protokolliert.
- Die Zugriffe werden protokolliert.

b) Zugriffsmöglichkeiten auf Job-Output

Es gibt immer wieder Fälle, in denen Mitarbeiter im Laufe eines Projekts für eine kurze Zeit weitgehende Zugriffsmöglichkeiten auf die Ergebnisse von Job-Läufen haben müssen. Auch beim KGRZ Gießen trat ein solcher Fall auf. Allerdings wurden nach Beendigung der Projektphase die Rechte nicht zurückgenommen, so daß zwei Mitarbeiter der Anwendungsentwicklung auf die Ergebnisse aller Job-Outputs zugreifen konnten. Ferner gab es für einen großen Teil der Mitarbeiter der Arbeitsvorbereitung und der Systemprogrammierung keine Einschränkung der Zugriffsmöglichkeiten auf alle Jobs. Diese zu weit gehenden Zugriffsrechte wurden umgehend zurückgenommen.

16.2.2.8

Sonstige Anmerkungen zu einzelnen Produkten

16.2.2.8.1

Com-Plete

In meinem 20. Tätigkeitsbericht (Ziff. 15.2.2.5) hatte ich Mängel aufgezeigt, die sich aus den fehlenden Schnittstellen zwischen Com-Plete und AFC2 ergeben, wenn Benutzer unter Com-Plete editieren, Jobs starten und deren Ergebnisse ansehen können. Diese Probleme hatte man in Gießen dadurch beseitigt, daß es nicht mehr möglich war, unter Com-Plete Jobs zu starten, und Benutzern die Editiermöglichkeit nicht eingeräumt wurde.

Bei der Umsetzung war der Tatsache keine Bedeutung zugemessen worden, daß der Com-Plete-Administrator weiterhin editieren konnte. Für ihn galt also, daß er mit den Rechten von Com-Plete arbeiten konnte, ohne daß es mit AFC2 möglich war, zwischen seinen Tätigkeiten und denen anderer Benutzer zu unterscheiden. Da die Editiermöglichkeit für die Tätigkeit des Administrators nicht erforderlich war, wurden die entsprechenden Com-Plete-Programme entfernt. Die Schwachstelle war damit beseitigt. In diesem Fall wurde damit ein Standardprodukt um die nicht erforderliche Funktion reduziert.

16.2.2.8.2

Performance-Monitore

Im täglichen Betrieb von Rechnern gibt es immer wieder Probleme mit schlechten Antwortzeiten, Fehlern, die nicht zu lokalisieren sind, oder andere Ereignisse, die tiefgehende Untersuchungen verlangen. Zur Unterstützung in diesen Fällen wird Spezialsoftware angeboten, die auf einer tiefen Ebene in die Software des Rechners eingreift; ein Beispiel sind sog. Performance-Monitore, die Engpässe bei Rechnerressourcen feststellen.

Derartige Monitore bieten zum Teil sensible Funktionen wie Trace (Verfolgung eines Ablaufs mit Anzeige von übertragenen Daten) oder Anzeigen bzw. Ändern von Hauptspeichereinhalten. Im Fehlerfall ist es ohne derartige Hilfsmittel oft nicht mehr möglich, schnell und sicher zu helfen. Diese Abhängigkeit darf aber nicht dazu führen, daß der Einsatz derartiger Produkte unkontrolliert erfolgt.

Bei der Prüfung stellte sich heraus, daß der Personenkreis, der einen Trace aufsetzen konnte oder die Möglichkeit hatte, sich Speichereinhalte anzusehen bzw. sie abzuändern, zu weit gesteckt war. Der Einsatz derartiger Spezialsoftware kann nur unter bestimmten Rahmenbedingungen erfolgen:

- Die Funktionen müssen hinsichtlich ihrer sicherheitsspezifischen Relevanz bewertet werden.
- Es muß festgelegt sein, wer wann welche relevanten Funktionen ausführen darf. Nur berechtigte Personen dürfen die Funktionen ausführen können.
- Es muß nachvollziehbar sein, wer wann mit den Funktionen gearbeitet hat.

Zwischenzeitlich wurde mit den in den Produkten vorhandenen Schutzmechanismen eine stärkere Differenzierung vorgenommen.

16.2.3

Fazit

Ein Großteil der Mängel, die ich bei der Prüfung des KGRZ Frankfurt vorgefunden hatte, waren auch beim KGRZ Gießen anzutreffen. Die Ausprägung war aber generell nicht so gravierend. Hier sind zu nennen:

- Ein Datenschutzkonzept war nur zum Teil vorhanden.
- Es fehlte ein schriftliches Revisionskonzept.
- Die Integration der Schutzkomponenten war noch nicht ausreichend.
- Zugriffsregeln von ACF2 waren nicht in allen Fällen korrekt.
- Einträge in Schutzkomponenten waren nicht immer aktuell. Insbesondere waren nicht alle ungültigen Einträge gelöscht.

Durch die geleistete Vorarbeit war es möglich, die meisten Mängel schnell zu beheben. Es bleibt aber noch einiges zu tun, um den Stand der Umsetzung voranzutreiben. Auch wenn dies erreicht ist, sind die Maßnahmen ständig zu kontrollieren und fortzuschreiben.

Ich werde die Fortschritte bei der Umsetzung von Datensicherungsmaßnahmen verfolgen und die Erfahrungen bei der Prüfung anderer Rechenzentren einfließen lassen.

16.3.

Abhörproblematik des Funkverkehrs

16.3.1

Ausgangslage

16.3.1.1

Schwachstellen beim Funkverkehr

In der letzten Zeit wurde in der Presse des öfteren von spektakulären Fällen berichtet, in denen Funkgespräche unberechtigt mitgehört wurden und das Gehörte mit teilweise gravierenden Folgen ausgenutzt wurde:

- Angeblich hatte ein Funkamateurliebespaar ein Telefonat zwischen Lady Diana und einem guten Freund mitgehört und aufgezeichnet. Er hatte es dann an die Presse weitergeleitet, die es reiflich ausgeschlachtet hatte.
- Bei den von Rechtsextremisten verursachten Krawallen in Rostock hatten diese den Polizeifunk abgehört, um nach dem Hase-und-Igel-Prinzip immer dort zu sein, wo es die Polizei nicht erwartete.
- Ein sehr "erfolgreiches" Bankräubertrio hatte bei seinen Überfällen neben Waffen immer einen Rundfunkempfänger dabei, mit dem der Polizeifunk abgehört wurde. Damit gelang es dem Trio lange Zeit, sich dem Polizeizugriff zu entziehen.

Die Problematik des Mithörens bleibt nicht auf solche Fälle beschränkt.

Auch das Telefonat mit einem Autotelefon, einem schnurlosen Telefon oder einem Funktelefon wird per Funk übertragen und kann im Prinzip mitgehört werden. Bei den neuen Funktelefonen (D1- und D2-Netz) wird dem dadurch begegnet, daß die Gespräche digitalisiert und verschlüsselt übertragen werden; bei schnurlosen Telefonen und Funktelefonen des B-Netzes besteht diese Möglichkeit jedoch weiterhin, während im C-Netz durch die Verschleierung des Gesprächs ein minimaler Schutz erreicht wird.

Neben den Funktelefonen gibt es noch weitere Einrichtungen, bei denen Gespräche per Funk übertragen werden. Hier ist unter anderem der BOS-Funk zu nennen. BOS steht dabei für "Behörden und Organisationen mit Sicherheitsaufgaben" und umfaßt auch die Polizei oder Funkleitstellen des Rettungsdienstes (16.3.2).

Über den BOS-Funk werden beispielsweise folgende personenbezogene Daten übertragen:

- Ein Arzt fordert ein Krankenfahrzeug an, um einen Patienten zum Krankenhaus transportieren zu lassen und teilt seine Diagnose der Funkleitstelle des Rettungsdienstes mit, damit dort das richtige Fahrzeug, also mit Notarzt, zum liegenden Transport etc. angewiesen werden kann. Die Funkleitstelle funkt nun die Rettungsstation oder das Fahrzeug direkt an. Damit sich das Rettungspersonal auf den Fall einstellen kann, wird neben dem Namen und der Adresse des Patienten gegebenenfalls auch die Diagnose weitergeleitet. Aber auch wenn keine Diagnose mitgeteilt wird, ergeben sich aus der Angabe des Krankenhauses bzw. der Abteilung Anhaltspunkte über Erkrankung oder andere persönliche Umstände.

- Nach einem Unfall taucht sofort ein Abschleppwagen auf, dessen Fahrer das Unfallfahrzeug gegen ein entsprechendes Entgelt "fürsorglich" abschleppt. Es hat aber nicht etwa die Polizei oder die Straßenmeisterei diesen Wagen bestellt, sondern der Fahrer hat den Polizeifunk abgehört.
- Bei Verkehrs- oder Personenkontrollen fragt die Polizei oft per Funk nach, ob zu den überprüften Personen Informationen vorliegen. Das Ergebnis der Abfrage wird per Polizeifunk übertragen. Dies kann vom lapidaren "Auskunft negativ" über die verfänglichere Aussage "es liegt zur Zeit nichts vor" bis zu detaillierten Ausführungen über gespeicherte Daten gehen. Die Daten selbst sind unter HEPOLIS gespeichert und betreffen im wesentlichen Fahndungsergebnisse der Polizei, die evtl. bis zu zehn Jahren vorgehalten werden.

Neben vielen anderen Personen würde auch der Fahrer des Abschleppwagens erfahren, ob und gegebenenfalls was zu den Personen vorliegt.

Nicht zuletzt wegen der teilweise sehr sensiblen Daten, die bei der Anforderung von Rettungsfahrzeugen per Funk übertragen werden, habe ich Ende 1991 versucht, generell zu klären, wer den BOS-Funk mithören kann und welche Möglichkeiten es gibt, um zu verhindern, daß unbefugte Personen von der Übertragung personenbezogener Daten Kenntnis nehmen können.

Aufgrund der Vielzahl von Behörden und Organisationen, die mit BOS-Funk arbeiten, nimmt ein großer Personenkreis berechtigt am BOS-Funk-Verkehr teil.

Ferner gibt es zahlreiche Personen, die Funkempfänger besitzen, mit denen sie den BOS-Funk abhören können, obwohl der Betrieb dieser Empfänger bis Mitte 1992 verboten war. Angesichts der Möglichkeiten, derartige Geräte zu niedrigen Preisen zu kaufen, muß davon ausgegangen werden, daß viele Personen solche Empfänger benutzen.

16.3.1.2

Reaktionen

Im Gespräch mit Vertretern mehrerer Ministerien habe ich meine Bedenken zur Sicherheit des BOS-Funks geäußert. Man sah sich jedoch aus verschiedenen Gründen außerstande, durchgreifende Lösungen zu entwickeln. Durch den Hinweis auf die Rechtslage, nach der sowohl der Betrieb von Geräten, die zum Hören des BOS-Funks geeignet waren, als auch das Abhören strafbar waren, glaubte man, einen Mißbrauch im größeren Umfang ausschließen zu können. Diese Ansicht war in Anbetracht der tatsächlich vorhandenen Möglichkeiten zur Kontrolle, ob jemand den BOS-Funk mithört, kaum haltbar. Seit Mitte 1992 ist sie noch kritischer zu bewerten, da im Zuge der Liberalisierung des Rundfunkgerätemarktes der Betrieb derartiger Empfänger nicht mehr verboten ist (ob der Empfang von Sendungen, die nicht für die Allgemeinheit vorgesehen sind, untersagt bleibt, wird derzeit kontrovers diskutiert). Die letzte Sicherung ist damit noch schwächer geworden.

Im ersten Beispielsfall ist es für unberechtigte Personen leicht möglich, Informationen über Erkrankungen zur Kenntnis zu nehmen. Während bei DV-Anlagen, mit denen der ärztlichen Schweigepflicht unterliegende Daten verarbeitet werden, die Sicherheitsanforderungen immer höher geschraubt werden, ergeben sich hier Lücken, deren Beseitigung bislang nicht konsequent genug betrieben wurde.

Die Polizei erhält immer weitergehende Möglichkeiten zur Bekämpfung von Straftaten. Angesichts der Schwachstellen beim Polizeifunk, durch die sich Straftäter oft zum Nulltarif über Polizeiaktivitäten aktuell informieren können, sind Maßnahmen zur Minimierung des Abhörrisikos ebenso dringend geboten, wie auf Gesetzes- oder Verordnungsebene. Zwar versucht die Polizei mit verschiedenen Mitteln, die an dieser Stelle nicht näher erläutert werden sollen, die Probleme in gravierenden Fällen im Griff zu behalten, jedoch sind diese im Regelfall nicht einsetzbar.

16.3.2

Technische Details und Rahmenbedingungen des BOS-Funks

16.3.2.1

Einsatzbereich und Rechtsgrundlage

Derzeit werden von den folgenden Organisationen Funkgeräte nach der Meterwellenrichtlinie BOS (Richtlinie für den nicht-öffentlichen beweglichen Landfunkdienst der Behörden und Organisationen mit Sicherheitsaufgaben, ABl. 1983 S. 443) eingesetzt:

- Polizei der Länder,
- Polizei- und Katastrophenschutzbehörden, die dem Bundesminister des Innern unmittelbar unterstehen (BGS),
- Katastrophenschutzbehörden der Länder, Gemeinden und Gemeindeverbände sowie private Organisationen des Katastrophenschutzes,

- Bundeszollverwaltung,
- Feuerwehren,
- Technisches Hilfswerk,
- Hilfsorganisationen: Arbeiter-Samariter-Bund, Deutsches Rotes Kreuz, Johanniter-Unfall-Hilfe, Malteser-Hilfsdienst.

In dieser Richtlinie, die als Abschnitt 2.2 in die Vorschriften zum Errichten oder Betreiben von Funknetzen oder Funkanlagen des nicht-öffentlichen Landfunks (VORNÖML) integriert wurde, werden alle näheren Einzelheiten, wie z.B. die Sendeleistung der eingesetzten Geräte oder das Anmelde- bzw. Antragsverfahren, vom Bundesminister für Post und Telekommunikation festgelegt.

Die Frequenzzuweisung für diesen Funkdienst ergibt sich aus der sog. "Vollzugsordnung Funk". Die Festlegungen hierin sind international bindende und daher kurzfristig nicht änderbare Zuweisungen für alle Funkdienste.

16.3.2.2

Stand der eingesetzten Gerätetechnik

Die derzeit eingesetzten Geräte entsprechen dem Stand der Kommunikationstechnik, der in technischen Richtlinien 1976 erstmals festgelegt wurde. Im überwiegend eingesetzten sog. 4 m-Bereich wird eine analoge Funktechnik in einem 20 kHz Kanalraaster mit Relaisstellen zur Reichweitenvergrößerung verwendet. Ein Funkkanal entspricht dann einem Frequenzpaar (Unterband und Oberband) oder einer Einzelfrequenz (Unterband oder Oberband). Diese Kanäle werden z.B. für den Brand- und Katastrophenschutz sowie für den Krankentransport und Rettungsdienst so auf die einzelnen Funkverkehrskreise verteilt, daß jeder mindestens einen Betriebs- und einen Reservekanal erhält. So einfach die vorhandene Funktechnik ist, so wirkungsvoll konnte sie bisher auch eingesetzt werden, um den betrieblichen Erfordernissen der BOS gerecht zu werden. Dazu stellte man allerdings hohe Ansprüche an Ausstattung und Qualität der Geräte. Lediglich die Probleme der Frequenzknappheit und der fehlenden Möglichkeit zur Verschlüsselung auf dem Funkweg haben sich mit der vorhandenen Technik nicht lösen lassen.

16.3.2.3

Vermeidung des Abhörens durch Verschlüsselung

Um der geschilderten Abhörproblematik sinnvoll begegnen zu können, muß man den Einsatz eines völlig neu konzipierten digitalen Funknetzes mit der Fähigkeit zur verschlüsselten Übertragung fordern. Durch den Einsatz eines solchen Netzes würde sich auch, z.B. bei einer Konzeption als zelluläres Bündelfunknetz, das Problem der Frequenzknappheit entschärfen, und es könnten zusätzliche, neue Leistungsmerkmale eingeführt werden.

In den vergangenen Jahren wurde durch die Innenministerien des Bundes und der Länder ständig geprüft, inwieweit der Stand der Funktechnik geeignet ist, allen Erfordernissen der BOS an ein neu konzipiertes Funknetz Rechnung zu tragen. Dabei ergab sich in der Vergangenheit das Problem, daß die zur Digitalisierung der Sprache notwendigen Voice-Codex (Vocoder), bei einem Erhalt der betrieblich unumgänglichen Sprechererkennbarkeit, digitale Nutzbitraten erzeugten, die in den vorhandenen 20 kHz-Kanälen selbst mit modernsten Modulationstechniken nicht übertragbar waren.

Die französische Polizei hat aber schon in den achtziger Jahren ein neues digitales Funknetz mit der Option zur Verschlüsselung spezifiziert und ausgeschrieben, bei dem ein digitales Sprachsignal in einem 25 kHz-Kanal zu übertragen war. Die Planungen gingen sogar so weit, daß die Kanalbandbreite künftig noch halbiert werden soll und dann bei verdoppelter Kanalzahl in einem 12,5 kHz-Raster Sprache zu übertragen ist. Wenn die seinerzeit angestrebten Zeitpläne auch nicht eingehalten wurden, so ist doch abzusehen, daß dieses Funknetz in den nächsten Jahren flächendeckend zur Verfügung stehen wird.

Auch bei der Sprachübertragung durch internationale Satellitendienste werden heute schon Standards spezifiziert, bei denen der normale Sprachkanal (0,3 bis 3 kHz) inklusive aller Fehlerkorrekturverfahren in eine Bitrate umgesetzt wird, die in einem 20 kHz-Kanal zu übertragen ist.

16.3.3

Aussichten

16.3.3.1

Rahmenbedingungen beim BOS-Funk

Obwohl es heute angesichts der technischen Entwicklung durchaus denkbar wäre, ein neues digitales System für den BOS-Funk zu spezifizieren, gibt es dazu nur erste Ansätze. Zwar hat man im Bereich der zuständigen Innenminister die Notwendigkeit an sich erkannt, aber da in den letzten Jahren in den fünf neuen Bundesländern die BOS-Funknetze in der vorhandenen Technik neu aufgebaut wurden, ist, nicht zuletzt wegen der organisatorischen und finanziellen Schwierigkeiten eines neuen Systems, mit großen Verzögerungen zu rechnen. Mit der Spezifikation

eines digitalen Funknetzes, das evtl. EG-weit einheitlich sein muß, ist voraussichtlich frühestens Mitte bis Ende der neunziger Jahre zu rechnen.

Erschwerend kommt für Bereiche wie den Rettungsdienst oder (freiwillige) Feuerwehren hinzu, daß es übliche Praxis ist, von der Polizei ausgemusterte Geräte dort einzusetzen. Wenn die Praxis fortgeführt wird, ändert sich die Situation des Rettungsdienstes noch erheblich später.

Dieser Zeitrahmen ist zu weit gesteckt, um die aktuellen Probleme zu lösen. Adäquate technische Maßnahmen müssen vorher ergriffen werden. Die sich daraus selbstverständlich ergebenden finanziellen Belastungen sind nicht zu unterschätzen, jedoch sollte es bei einem ausreichend großen Absatzmarkt möglich sein, die Preise der Geräte auf ein vertretbares Maß zu senken.

Angesichts der Lücken, die der Betrieb des BOS-Funks aus datenschutzrechtlicher Sicht aufweist, stellt sich die Frage nach Alternativen zum vorhandenen Stand, seien sie technischer oder organisatorischer Art. Dabei ist ein Verzicht auf den BOS-Funk nicht möglich, und es müssen auch aus den verschiedensten Gründen personenbezogene Daten übertragen werden.

16.3.3.2

Technische Alternative beim BOS-Funk

Um in den folgenden Jahren bis zur Einführung eines neuen BOS-Funknetzes das Abhören schützenswerter Daten zu verhindern, ist zumindest eine technische Alternative denkbar. Ein namhafter Hersteller von Funkgeräten bietet zu seinen BOS-Handfunkgeräten Erweiterungsmodule an, die jetzt schon im vorhandenen Kanalraster eine Digitalisierung und eine Sprachverschlüsselung ermöglichen. Die verschlüsselte Übertragung ist zwischen Geräten mit einem vergleichbaren technischen Stand möglich. Zu vorhandenen Altgeräten besteht weiterhin die analoge, unverschlüsselte Funkverbindung. Derartige Geräte werden schon heute von verschiedenen Anwendern eingesetzt, die ein besonders hohes Interesse an der Wahrung der Vertraulichkeit ihrer Funkgespräche haben.

Andere Anbieter von BOS-Funkgeräten und sonstigen technischen Komponenten des BOS-Funknetzes arbeiten ebenfalls an Erweiterungsmodellen für ihre Geräte, die eine wahlweise Verschlüsselung unterstützen.

Wenn keine unvorhergesehenen Schwierigkeiten auftreten, steht in der zweiten Jahreshälfte 1993 die Technik zur Verfügung, um nur noch Geräte mit wahlweiser Verschlüsselung anzuschaffen. Es dürfte dann auch möglich sein, Altgeräte, die einen technischen Mindeststandard erfüllen, mit derartigen Modulen auszustatten. Wenn die Geräte einsatzbereit sind, müssen sie im BOS-Funk, nicht nur beim Polizeifunk, genutzt werden.

16.3.3.3

Datenübertragung per Funk

Ein weiteres Problemfeld entsteht durch den Trend, vermehrt Funkverbindungen für die Datenübertragung in DV-Netzen zu nutzen.

Bei dem Aufbau von DV-Netzen ergibt es sich häufig, daß keine oder nur unzureichende Möglichkeiten für eine Verkabelung existieren. Beispiele sind Großraumbüros mit häufig wechselnden Standorten der Rechner, lokale Netze (LAN's), die sich über größere räumliche Entfernungen erstrecken sollen, oder die Anforderung, von mobilen Rechnern jederzeit Daten übertragen zu können. Um die sich daraus ergebenden Forderungen erfüllen zu können, sind Produkte entwickelt worden, die in Teilen eines DV-Netzes per Funk statt durch Kabel Daten übertragen.

In LAN's kann beispielsweise zwischen Gebäuden, die sich in Sichtweite befinden, die Verbindung als Richtfunkstrecke betrieben werden, während in den Gebäuden die Teilnetze weiterhin mit Kabeln erstellt sind. Für die Übertragung von Daten zwischen mobilen und zentralen Rechnern baut die Telekom mit "Modacom" eine Dienstleistung aus, die in den nächsten Jahren bundesweit angeboten werden soll.

All diesen Produkten ist gemeinsam, daß es für Außenstehende die Möglichkeit gibt, sich in das Netz "einzuhängen", ohne vom Betreiber bemerkt werden zu können. Es bereitet im Einzelfall einen nicht unerheblichen Aufwand, um den Funk abzuhören und die empfangenen Signale korrekt zu interpretieren, da aufwendigere Geräte als beim Abhören des Sprechfunks erforderlich sind; die Möglichkeit ist aber gegeben.

Bei der Planung derartiger Netze muß der Anwender Maßnahmen ergreifen, die eine Kenntnisnahme — ein Lesen — der Daten durch Unberechtigte ausschließen, d.h. für personenbezogene Daten muß die Transportkontrolle (§ 10 Abs. 3 Ziff. 9 HDSG) gewährleistet sein. Die beim jetzigen Stand der Technik wohl sinnvollste Maßnahme, um dies zu erreichen, besteht in der Übertragung verschlüsselter Daten. Dabei ist anzumerken, daß eine Datenverschlüsselung in DV-Netzen für die meisten technischen Konstellationen möglich ist und als eine Datensicherheitsmaßnahme immer in Betracht gezogen werden muß.

16.3.4

Organisatorische Maßnahmen zur Risikominderung beim Funkverkehr

Um kurzfristig eine Verbesserung zu erreichen, sind vorrangig organisatorische Maßnahmen möglich, deren Ziel es nur sein kann, die Übertragung personenbezogener und sonstiger sensibler Informationen auf das unumgängliche Maß zu beschränken. Zur Vorbereitung von konkreten Maßnahmen bietet es sich an, folgende Schritte einzuleiten:

- Vornahme einer Bestandsaufnahme
Wo befinden sich Geräte, mit denen per Funk Informationen übertragen werden? (Funkgeräte, Funktelefone, . . .)

Wer benutzt sie?
Welcher Art sind die übertragenen Informationen (personenbezogene Daten, andere sensible Daten, . . .)?
- Prüfung der Erforderlichkeit
Müssen die Informationen per Funk übertragen werden, oder gibt es andere Übertragungswege?
Kann der Umfang der übertragenen personenbezogenen/sensiblen Daten reduziert werden?
- Risikoabschätzung technisch möglicher Varianten
Wie ist das Abhörisiko zu bewerten?
Gibt es technische Varianten mit einer höheren Sicherheit? (Verschlüsselung statt Verschleierung; D-Netz statt C-Netz, . . .)
- Bewertung
Kann das Risiko des Mithörens vor dem Hintergrund der Schutzbedürftigkeit der übertragenen Daten akzeptiert werden?
- Erstellen eines Maßnahmenkatalogs
Als Ergebnis sollte ein Maßnahmenkatalog entstehen, in dem aufgeführt wird, wie die Datensicherung verbessert wird. Eine denkbare Maßnahme könnte beispielsweise die Erstellung einer Dienstanweisung sein, in der organisatorische Regelungen getroffen werden, wie:
 - Wann dürfen personenbezogene sensible Daten übertragen werden.
 - Codetabellen.
 - Wann und wie werden die Codetabellen eingesetzt.
 - Technische Alternativen mit einem Zeitplan für deren Einführung.
 - Schulung der Mitarbeiter hinsichtlich der Risiken und Gegenmaßnahmen.

16.3.5

Fazit

Um Informationen zu übertragen, sei es als Sprache oder als Datenstrom, wird zunehmend der Funk genutzt. Wegen der physikalischen Gegebenheiten kann jede Person im Sendegebiet den Funkverkehr empfangen. Ohne Sicherungsmaßnahmen ist es bei der Übertragung von personenbezogenen Daten auch unberechtigten Personen möglich, die Daten zur Kenntnis zu nehmen. Es ist unumgänglich, Maßnahmen zu ergreifen, die dies, insbesondere für den BOS-Funk, ausschließen.

Der Sicherheitsstandard bei der Übertragung von Informationen per Funk darf nicht eklatant niedriger sein als bei der Verarbeitung durch Computer.

16.4

Erste Erfahrungen beim Einsatz von Novell Netware

Bereits in meinem 18. Tätigkeitsbericht (vgl. Ziff. 16.3) habe ich anlässlich des zunehmenden Einsatzes von PC-Netzen über die Möglichkeiten zum Schutz sensibler Daten und deren Gefährdungen in derartigen Netzen berichtet.

In den vergangenen drei Jahren ist die Zahl der Netze in der Landesverwaltung und im kommunalen Bereich ständig gestiegen, und der Trend, einzelne PC in Netze zu integrieren, wird sich, was an den bereits bekannten Planungsunterlagen einzelner Verwaltungen erkennbar ist, auch in den nächsten Jahren fortsetzen.

16.4.1

Motivationen für die Integration von PC in Netze

Die Gründe der Verwaltungen für eine Netzintegration von PC sind zwar unterschiedlich, lassen sich aber auf die folgenden Grundmotive zurückführen:

- Gemeinsame Datenhaltung (Datenverbund); zwei oder mehr Anwender müssen von verschiedenen Arbeitsplätzen auf denselben Datenbestand zugreifen.
- Funktionsverbund; z.B. die Ergebnisse einer Anwendung müssen für eine nächste Anwendung als Eingangsdaten vorliegen.
- Lastverbund; eine Anwendung wird aus Lastgründen auf einen oder mehrere PC oder den Server verteilt.
- Resource-Sharing; die im Netz möglicherweise nur einmal vorhandenen Spezialgeräte, z.B. ein FAX-PC (vgl. 20. Tätigkeitsbericht, Ziff. 9.1.3) oder ein Plotter können, sofern dies im Rahmen der jeweils eingesetzten Anwendung nötig und zulässig ist, von allen Anwendern benutzt werden.
- Mailing; das Netz wird als zusätzliches, die Hauspost und das Telefon ergänzendes Kommunikationsmittel benutzt.
- Verfügbarkeit; durch die zentrale Datenhaltung oder auch nur zentrale Datensicherung erhöht sich in Verbindung mit den mehrfach vorhandenen Arbeitsplatzausstattungen die Verfügbarkeit erheblich gegenüber einzelnen PC, wenn man das Problem eines Serverausfalls bei der Netzwerkkonzeption mitbedacht hat.
- Zentrale DV-Verwaltung; viele Verwaltungen haben in den vergangenen Jahren erkennen müssen, daß der eigenverantwortliche Einsatz von PC in den einzelnen Abteilungen aus den unterschiedlichsten Gründen den Erfordernissen einer "ordnungsgemäßen Datenverarbeitung" häufig zuwiderläuft. Die zentrale Administration durch die Netzwerkverantwortlichen, die in der Regel einer Zentralabteilung angehören, wird daher als eine Möglichkeit gesehen, Fehlentwicklungen entgegenzuwirken. So baut, in einem mir bekannten Fall, ein Netzwerkadministrator sogar alle Laufwerke aus vorhandenen PC aus, wenn sie in das Netz integriert werden, um sicherzustellen, daß keine Fremdprogramme und -disketten auf den Geräten eingesetzt werden können.

16.4.2

Mängel bei der Konzeption

Die Erfahrung hat gezeigt, daß für die Einführung von DV-Systemen und somit auch von APC-Netzen eine umfassende Konzeption, die die Aspekte der Datensicherung, der allgemeinen Datensicherheit und des Datenschutzes einschließt, unerläßliche Voraussetzung ist. Dabei kann eine derartige Konzeption nicht alle in der Planungsphase ohnehin nicht im Detail bekannten Einzelfragen umfassen, aber sie muß alle grundsätzlichen Probleme und die zur Lösung notwendigen Vorgehensweisen beschreiben.

Ein Beispiel für das Fehlen eines grundsätzlichen Aspekts bei einer an sich vorhandenen Konzeption ist der folgende Fall:

Bei Prüfung einer hessischen Kreisverwaltung mußte ich feststellen, daß vor der Einführung eines Netzwerkes versäumt wurde, das Vorgehen bei der Beantragung und Zuweisung von Zugriffsrechten festzulegen. Später wurden vom Systemverwalter in Absprache mit den zuständigen Fachabteilungen die im Rahmen der Anwendung notwendigen Zugriffsberechtigungen eingetragen. Dabei wurde versäumt, sowohl die aus der Fachabteilung kommenden Bedarfsvorgaben als auch die dabei zustande gekommenen Festlegungen zu dokumentieren. Zwar hatte der Systemverwalter bei der Eintragung der Zugriffsberechtigungen einen anscheinend strengen Maßstab angelegt, aber aufgrund der fehlenden, den vereinbarten Sollzustand dokumentierenden Unterlagen war nicht nachzuvollziehen, ob die vorhandenen Eintragungen dem für die Aufgabenstellung Notwendigen entsprachen. Eine Kontrolle war somit für mich und natürlich auch für den behördlichen Datenschutzbeauftragten unmöglich.

16.4.3

Einsatz von Schutzfunktionen und Kontrollmitteln

Angesichts der eingangs geschilderten Entwicklung erscheint es mir notwendig, auf einige Details des Netzwerkbetriebssystems Novell Netware, das überwiegend zum Einsatz kommt, hinzuweisen.

Mit den neueren Versionen (3.x) von Novell Netware wurden entscheidende Schutzfunktionen realisiert. Ein Teil der schon in früheren Versionen vorhandenen Instrumente zur Regelung von Zugriffsrechten wurde nochmals verfeinert.

Im Bereich der Paßwort-Übertragung von den angeschlossenen PC zum Server wird eine Verschlüsselung eingesetzt, um das Abhören der Paßwörter auf dem Netz auszuschließen. Ferner lassen sich durch den Einsatz verschiedener Systemfunktionen die folgenden Zugriffsrechte (Trustee Rights) auf Verzeichnisse, Unterverzeichnisse und Dateien anwenden:

- Read Leserecht; erlaubt bei Programmen deren Ausführung
- Write Schreibrecht

- Create zum Einrichten von Subdirectories und zum Wiederherstellen mit DELETE gelöschter Dateien
- Erase zum Löschen von Dateien und Directories
- Access Control erlaubt das Ändern der Zugriffsrechte, ausgenommen Supervisory-Recht
- File Scan zum Sichten der Verzeichnisse
- Modify erlaubt das Ändern von Namen und Attributen der Dateien und Directories
- Supervisory überträgt alle vorgenannten Rechte, bestimmte Programme lassen sich nur mit dem Supervisory-Recht ausführen oder bieten erst dann alle Optionen an.

Bei der Zuweisung dieser Zugriffsrechte muß, insbesondere beim Einrichten von Anwendungspaketen, sehr sorgfältig auf der Dateiebene geprüft werden, ob das jeweilige Recht auch wirklich benötigt wird. So mußte ich bei einer Prüfung feststellen, daß den Anwendern für alle Dateien eines Programmpakets das Modify-Recht übertragen worden war. In einer solchen Konstellation ist es z.B. möglich, daß ein Anwender – auch ohne Absicht – Dateien umbenennt oder durch Ändern der Datei-Attribute Störungen oder Schäden verursacht.

Dieselbe Problematik gilt auch für einige Systemprogramme, die einem unprivilegierten Anwender gar nicht oder nur eingeschränkt zur Verfügung stehen dürfen.

Als weiteren Schutzmechanismus können Netzwerkverwalter noch die Funktion "Intruder Detection/Lockout" aktivieren, um Einbruchversuche in das System zu registrieren und zu verhindern. Darüber hinaus gibt es zur Kontrolle von Login-Störungen die Möglichkeit, auf das Protokoll der Netware-Utility "PAUDIT" zurückzugreifen. Über die Art und Weise der Auswertung dieser Protokolle bietet es sich an, eine Ergänzung in die Betriebsvereinbarungen mit dem Personalrat aufzunehmen.

Zu all diesen hier angesprochenen Schutzfunktionen bietet das Betriebssystem sowohl dem Netzwerkadministrator als auch dem behördlichen Datenschutzbeauftragten konkrete Hilfsmittel, die die Kontrolle der vorgenommenen Systemeintragen erleichtern.

16.4.3.1

Einsatz des Befehls "Security"

Der Befehl Security kann nur von der Ebene SYS:SYSTEM aufgerufen werden und listet in eine als Parameter angegebene Datei all jene Sicherheitslücken auf, die folgenden Kriterien entsprechen:

- Kennungen (User-ID), die kein Paßwort oder unsichere Paßwörter führen;
- Kennungen, die dem Supervisor gleichgesetzt sind (Supervisor equivalence);
- Kennungen, die auf das "Root"-Verzeichnis Zugriffsrechte haben;
- Kennungen, für die kein Login Script existiert;
- Kennungen, die Zugriffsrechte auf Systemverzeichnisse haben, die über die folgenden Rechte hinausgehen:

SYS:SYSTEM	(keine)
SYS:PUBLIC	(read, file scan)
SYS:LOGIN	(read, file scan)
SYS:MAIL	(write, create).

Gerade dieser Befehl ist geeignet, dem behördlichen Datenschutzbeauftragten schnell einen Überblick über den Zustand der Systemsicherheit zu verschaffen, da er diese Auswertung auch kurzfristig immer wieder stichprobenartig von den Systemverantwortlichen anfordern kann.

16.4.3.2

Kontrolle der sonstigen Zugriffsberechtigungen

Ob die von den Systemverwaltern oder von den Lieferfirmen, die in der Regel die Erstinstallation durchführen, eingetragenen anwendungsbezogenen Zugriffsberechtigungen dem notwendigen dokumentierten Zugriffsbedarf entsprechen, läßt sich im weiteren am besten mit Funktionen in den Programmen "SYSCON" und "FILER" überprüfen, die fester Bestandteil des Netzwerkbetriebssystems sind.

Mit dem Programm SYSCON können sowohl die User-ID-bezogenen Zugriffsrechte als auch die Gruppenzugehörigkeit und deren Rechte eingetragen und überprüft werden. Darüber hinaus werden mit dem Programm alle

wesentlichen weiteren Eintragungen vorgenommen, die das Umfeld eines Users beschreiben. Dazu gehören unter anderen:

- die “Account Restrictions“ (vgl. Ziff. 16.4.3.3);
- das sog. “Login Script“, mit dem für einen Anwender bestimmte, seine Anwendung vorbereitende Schritte festgelegt werden;
- die “Station Restrictions“, mit denen für eine Kennung nur einzelne Arbeitsplätze (deren Netzwerkkennung) zur Benutzung freigegeben werden;
- die “Time Restrictions“, die die zeitlichen Zugangsvoraussetzungen einer Kennung zum System festlegen.

Da ein Anwender darüber hinaus noch an anderer Stelle bestimmte Zugriffsrechte erhalten kann, ist es nötig, im einzelnen mit der Option “Who Has Rights Here“ aus dem Programm FILER die Übersicht der Zugriffsberechtigungen auf Verzeichnisse und Dateien zu vervollständigen.

Zur eigenen Sicherheit wird eine Verwaltung eine derartige Überprüfung des Systemzustandes gemäß den eigenen Konzeptvorgaben in regelmäßigen Abständen durchführen und die Ergebnisse dem behördlichen Datenschutzbeauftragten zur Kenntnis geben.

Für eine direkte Auswertung des Systemzustandes sind jedoch einige grundlegende Systemkenntnisse erforderlich. Es ist daher – wie mir in einem Fall bekannt wurde – sinnvoll, neben den künftigen Systemverwaltern auch den behördlichen Datenschutzbeauftragten zu entsprechenden Schulungen zu entsenden.

16.4.3.3

Eintragungen zu den “Account Restrictions“ im Programm SYSCON

Im Submenü “User Information“ des Programms SYSCON können im Menüunterpunkt Account Restrictions die wesentlichen Einstellungen vorgenommen werden, um den Einsatz der User-ID bezogenen Paßwörter wirkungsvoll zu regeln. Die einzelnen Felder sollten bei einem Standard-User in etwa folgende Eintragungen aufweisen:

Menüpunkt	Einstellung	Anmerkung
Account Disabled:	Yes	(1)
Account Has Expiration Date:	No	(2)
Data Account Expires:	*	
Limit Concurrent Connections:	Yes	
Maximum Connections:	1	
Allow User To Change Password:	Yes	(3)
Require Password:	Yes	(4)
Minimum Password Length:	8	(5)
Force Periodic Password Changes:	Yes	(6)
Days Between Forced Changes:	30	
Date Password Expires:	*	
Limit Grace Logins:	Yes	(7)
Grace Logins Allowed:	3	
Remaining Grace Logins:	*	
Require Unique Passwords:	Yes	(8)

* Diese Werte ergeben sich aus den vorgenommenen Einstellungen und einigen vom System gespeicherten Daten. Das Betriebssystem trägt automatisch die resultierenden Werte ein.

(1) Eine sonst vollständig beschriebene Kennung kann mit einem “No“ an dieser Stelle deaktiviert werden. Diese Option läßt sich z.B. bei längerfristig beurlaubten Usern oder bei den Servicetechnikern der Vertragspartner sinnvoll einsetzen, um den Mißbrauch dieser Kennungen, solange sie nicht benötigt werden, auszuschließen.

(2) Eine Eintragung eines “Expiration Date“ kann z.B. bei Usern zweckmäßig sein, deren Mitarbeit zeitlich begrenzt ist.

(3) Der User kann sein Paßwort unabhängig vom Supervisor selbst bestimmen. Der Supervisor kann es zwar überschreiben, aber nicht lesen.

(4) Zur Benutzung dieser Kennung ist die Eingabe eines Paßwortes unumgänglich.

(5) Ein wirkungsvolles Paßwort muß mindestens sechs alphanumerische Zeichen umfassen, besser sind jedoch acht Stellen.

(6) Durch diese Eintragung wird dem User automatisch ein regelmäßiger, systemgeführter Paßwortwechsel abverlangt. Der 30-Tage-Zeitraum hat sich dabei als in jeder Hinsicht praxisgerechte Größe erwiesen.

(7) Ein User kann den geschilderten Paßwortwechsel umgehen. Durch die Eintragungen wird festgelegt, daß das alte Paßwort nach Ablauf seiner Gültigkeit lediglich noch dreimal zum Login verwendet werden kann.

(8) Die letzten acht Paßwörter, die zu einer Kennung verwendet wurden, werden vom System gespeichert und sind bei einem Paßwortwechsel nicht wieder zu benutzen.

16.4.4

Forderungen

Die beschriebenen Programme und Funktionen zeigen, daß das Netzwerkbetriebssystem Novell Netware ein umfangreiches Instrumentarium bietet, das die Netzwerkverwalter in die Lage versetzt, einige grundsätzliche Anforderungen des Datenschutzes zu realisieren. Ziel einer Verwaltung muß es sein, dieses Instrumentarium im Spannungsfeld zwischen Zugriffserfordernissen und Systemsicherheit optimal einzusetzen.

Leider verbleibt auch dann beim Einsatz von PC-Netzwerken das Problem der PC, die über eigene Festplatten- oder Diskettenlaufwerke verfügen, aber nicht mit einer Schutzsoftware ausgestattet sind (18. Tätigkeitsbericht, Ziff. 16.3.2).

Ich werde diesen Aspekt und die weitere Entwicklung von Netzwerken in den folgenden Jahren beobachten und zu einem geeigneten Zeitpunkt erneut zu diesem Thema berichten.

17. Unzureichende Umsetzung des Hessischen Datenschutzgesetzes durch öffentliche Stellen

17.1

Mangelnde Kooperationsbereitschaft bei öffentlichen Stellen

§ 28 Abs. 1 des Hessischen Datenschutzgesetzes (HDSG) räumt allen Bürgerinnen und Bürgern das Recht ein, sich an mich zu wenden, wenn sie annehmen, bei der Verarbeitung ihrer personenbezogenen Daten in ihren Rechten verletzt worden zu sein. Als unabhängige Kontrollinstanz gehe ich allen Eingaben nach und unterrichte die Betroffenen von dem Ergebnis meiner Feststellungen. Als Instrument steht mir dazu § 29 HDSG zur Verfügung, wonach mir von allen datenverarbeitenden Stellen nicht nur Zutritt zu den Diensträumen, sondern auch Auskunft zu meinen Fragen und Einsicht in alle Unterlagen, die in Zusammenhang mit der Verarbeitung personenbezogener Daten stehen, zu gewähren ist. Dabei reicht es oft aus, die in den betroffenen Behörden nach § 5 Abs. 2 HDSG mit der Sicherstellung der Einhaltung von Vorschriften über den Datenschutz bestellten Datenschutzbeauftragten einzuschalten und im konkreten Einzelfall die Überprüfung der Einhaltung datenschutzrechtlicher Bestimmungen zu veranlassen.

Ein Beispiel:

Ein Bürger geriet 1982 in den Verdacht, eine Straftat nach dem Betäubungsmittelgesetz (BTMG) begangen zu haben. Es wurden Ermittlungen angestellt, und er wurde erkennungsdienstlich behandelt. Nachdem die Staatsanwaltschaft das Verfahren eingestellt hatte, bemühte sich der Betroffene um die Vernichtung der erkennungsdienstlichen Unterlagen. Die Polizei lehnte dies ab, weil die Ermittlungen nicht zweifelsfrei ergeben hätten, daß er die Straftat nicht begangen habe. Nachdem der Betroffene im Jahre 1989 in einer anderen hessischen Stadt ein weiteres Mal in den Verdacht geriet, eine Straftat begangen zu haben – wieder wurde das Verfahren eingestellt -, wandte er sich im letzten Jahr an mich und bat um Unterstützung bei seinen Bemühungen um Löschung der Datenspeicherung. Es genügten zwei Telefongespräche mit den behördlichen Datenschutzbeauftragten der beiden Polizeidienststellen, in denen ich darum bat, zu prüfen, ob die in den Jahren 1983 und 1989 verfügte Aufbewahrung der Unterlagen mit den datenschutzrechtlichen Bestimmungen des Hessischen Gesetzes über die öffentliche Sicherheit und Ordnung (HSOG) vom 26. Juni 1990 in Einklang steht. Beide Stellen kamen zu dem Ergebnis, daß die Akten und erkennungsdienstlichen Unterlagen zu vernichten und die im polizeilichen Informationssystem gespeicherten Daten zu löschen sind.

Nicht alle Fälle können so schnell und unbürokratisch gelöst werden:

17.1.1

Mißachtung meiner Rechte nach § 29 HDSG durch verzögerte oder unterlassene Auskunftserteilung

- Ein Insasse einer Justizvollzugsanstalt hatte davon Kenntnis erlangt, daß die Hauptbelastungszeugin in seinem Strafverfahren während der Ermittlungen ausgesagt hatte, ihr sei ein gegen ihn ergangenes Urteil eines vorangegangenen Verfahrens "zugespielt" worden. Er vermutete, daß die Polizei oder die Staatsanwaltschaft das Urteil weitergegeben hätten und bat mich um eine datenschutzrechtliche Überprüfung. Im Februar 1991 bat ich die Staatsanwaltschaft beim Landgericht Darmstadt um eine Stellungnahme. Sie antwortete, die Akten seien derzeit versandt, sie werde auf mein Schreiben zurückkommen. Ein Jahr später teilte mir die Zweigstelle Offenbach der Staatsanwaltschaft beim Landgericht Darmstadt mit, daß sich an diesem Sachstand nichts geändert

habe; die Ermittlungen seien noch nicht abgeschlossen. Dies korrigierte sie kurz darauf: Das Verfahren sei seit März 1991 abgeschlossen. Auf meine Bitte, doch nun zu meinen Fragen Stellung zu nehmen, antwortete sie, sie habe die Staatsanwaltschaft Darmstadt gebeten, zu prüfen, ob diese mir antworten könne. Erst nachdem ich im Juli 1992 den Leitenden Oberstaatsanwalt beim Landgericht Darmstadt bat, sich der Sache persönlich anzunehmen, erhielt ich die Auskunft, aus den Akten seien keine Anhaltspunkte ersichtlich, wonach die Staatsanwaltschaft oder die Polizei der Zeugin das Urteil "zugespielt" hätten. Die von dem Betroffenen vermutete Datenübermittlung war damit datenschutzrechtlich nicht zu bewerten. Allerdings teile ich das von dem Betroffenen geäußerte Unverständnis über die zögernde Beantwortung meiner Frage durch die Staatsanwaltschaft beim Landgericht Darmstadt.

- Eine Partei in einem Zivilprozeß hatte vom Amtsgericht Frankfurt am Main Einsicht in die Strafakte des Prozeßgegners – die mit dem Zivilverfahren in keinem Zusammenhang stand – erhalten. Dieser rügte die Akteneinsichtsgewährung und bat mich um eine datenschutzrechtliche Beurteilung. Im November 1991 forderte ich das Gericht auf, mir mitzuteilen, aufgrund welcher Rechtsgrundlage die Akteneinsicht gewährt wurde. Mehrere Erinnerungen blieben erfolglos. Auf die letzte antwortete das Amtsgericht, der bearbeitende Richter sei zur Zeit nach Thüringen abgeordnet, weshalb die Beantwortung meiner Fragen noch warten müsse. Dem Betroffenen konnte ich bisher nur mitteilen, daß ich im vorliegenden Fall die Gewährung von Einsicht in die Strafakte an die gegnerische Partei im Zivilprozeß für problematisch halte. Die Frage, ob sie tatsächlich zulässig war, hängt von der immer noch ausstehenden Antwort des Amtsgericht Frankfurt ab.
- Im August 1991 wandte ich mich an die Führerscheinstelle des Landrates des Wetteraukreises und bat um Mitteilung, worauf ein Eintrag in der Führerscheinkartei, wonach einer Person im Jahre 1966 die Fahrerlaubnis entzogen wurde, beruhe. Die Führerscheinstelle antwortete erst nach mehreren Erinnerungen, allerdings nur lückenhaft. Weitere Fragen blieben trotz Hinweis auf die Verpflichtung nach § 29 Abs. 1 HDSG unbeantwortet. Erst nachdem ich die Akten bei der Führerscheinstelle einsah, konnte ich dem Betroffenen mitteilen, daß sein Verlangen nach Löschung dieses Eintrages nicht berechtigt war.
- Auf Bitten eines Bürgers hatte ich im Juni 1991 bei der Polizeidirektion Erbach dessen Kriminalakte eingesehen. Gegen den Betroffenen waren seit 1972 neun Ermittlungsverfahren geführt worden. Der Ausgang der Verfahren war der Polizei nicht bekannt. Der Betroffene war aus nicht ersichtlichem Grund erkennungsdienstlich behandelt worden. Seine Akte sollte bis 1997 aufbewahrt werden. Ich traf folgende Vereinbarung: Die Polizei überprüft, aufgrund welcher Rechtsgrundlage die erkennungsdienstliche Behandlung erfolgte und holt Auskünfte über den Ausgang des Verfahrens bei der Staatsanwaltschaft ein. Danach wird die Aufbewahrungsdauer neu festgelegt, die erkennungsdienstlichen Unterlagen evtl. vernichtet und ich über das Ergebnis informiert.

Nach mehreren Erinnerungen erhielt ich im Mai 1992 ein vorläufiges Ergebnis: Die Antwort der Staatsanwaltschaft Darmstadt zum Ausgang der Verfahren stehe noch aus. Unabhängig davon wurden die Unterlagen zu sechs der neun Ermittlungsverfahren ausgesondert, weil deren weitere Aufbewahrung nicht mehr erforderlich war. Die vorgesehene Aufbewahrungsdauer wurde auf Oktober 1993 verkürzt. Die Entscheidung über die evtl. Löschung der erkennungsdienstlichen Unterlagen wurde zurückgestellt. Im September 1992 teilte die Polizeidirektion Erbach mit, die Staatsanwaltschaft habe nun zu einem der Fälle mitgeteilt, daß das Verfahren nach § 170 Abs. 2 Strafprozeßordnung (StPO) eingestellt sei. Die Ausgänge der anderen Verfahren wurden nicht mitgeteilt. Die erkennungsdienstlichen Unterlagen seien nach § 81b 2. Alt. StPO angefertigt worden. Da keine Anhaltspunkte ersichtlich waren, wonach die erkennungsdienstlichen Unterlagen die Aufklärung künftiger Straftaten fördern könnten, habe ich deren Vernichtung verlangt. Die Polizeidirektion Erbach hat den Vorgang nun dem Hessischen Landeskriminalamt zur Entscheidung übersandt. Das Ergebnis steht noch aus.

- Das Hessische Landesamt für Verfassungsschutz verzögerte meine Prüfung der Akten über die Sicherheitsüberprüfung über ein Jahr (vgl. Ziff. 2.1).

17.1.2

Mißachtung meiner Rechte nach § 29 HDSG durch falsche Auskünfte

- Bei Prüfung der Zulässigkeit der Übersendung von Entlassungsberichten von Krankenhäusern an die Tbc-Abteilung des Gesundheitsamtes der Stadt Frankfurt am Main erklärte das Gesundheitsamt, daß nur in Einzelfällen Berichte von Krankenhäusern angefordert würden, und dies auch nur mit Einwilligungserklärung der Patienten. Im Rahmen einer Prüfung vor Ort sah einer meiner Mitarbeiter 80 Akten der Tbc-Abteilung des Gesundheitsamtes aus den Jahren 1990 bis 1992 durch und stellte fest, daß das Gesundheitsamt in allen Fällen bei den Krankenhäusern Zwischen- und Entlassungsberichte mit Vordruck angefordert hatte. Erklärungen, mit denen die Patienten in die Anforderung der Berichte einwilligen und die behandelnden Ärzte der Krankenhäuser von der ärztlichen Schweigepflicht entbinden, hatte das Gesundheitsamt in keinem Fall eingeholt.
- Die Führerscheinstelle des Rheingau-Taunus-Kreises ordnete im Dezember 1991 die medizinisch-psychologische Begutachtung eines Führerscheininhabers an. Sie stützte sich dabei auf eine Mitteilung der Staatsanwaltschaft beim Landgericht Wiesbaden, wonach der Betreffende wegen eines Verstoßes gegen das BTMG verurteilt worden sei. Der Betroffene fragte bei mir an, ob die Weitergabe seiner personenbezogenen Daten durch die Justizbehörde an die Führerscheinstelle zulässig war. Ich bat sowohl die Staatsanwaltschaft als auch die Führerscheinstelle um Stellungnahme. Die Staatsanwaltschaft antwortete mir im April 1992, sie habe das Urteil dem Jugend- und

Sozialamt des Landratsamtes des Rheingau-Taunus-Kreises übersandt, nicht aber der Führerscheinstelle. Die Führerscheinstelle antwortete, die an das Jugendamt adressierte Mitteilung sei aus Versehen zu ihr gelangt. Nach Aufklärung des Irrtums sei die Staatsanwaltschaft Wiesbaden um eine Mitteilung nach Nr. 46 der Anordnung über Mitteilungen in Strafsachen (MiStra, JMBL 1985 S. 189) gebeten worden. Erst aufgrund der dann ergangenen an die Führerscheinstelle unmittelbar gerichteten Mitteilung sei sie tätig geworden. Eine Rückfrage bei der Staatsanwaltschaft ergab, daß das letztgenannte Ersuchen erst im Mai 1992 erfolgte und somit nicht Grundlage für die Anordnung im Dezember 1991 sein konnte. Die Führerscheinstelle sah sich bislang nicht in der Lage, diesen Widerspruch aufzuklären – die dafür benötigte Akte läge dem Verwaltungsgericht vor.

17.2

Fehlende Sorgfalt bei der Organisation der Aktenführung

17.2.1

Vorgefundene Situation

Bei einem polizeiärztlichen Dienst schied der leitende Arzt aus. Neben seiner Tätigkeit als Polizeiarzt war er auch Hausarzt für einzelne seiner Mitarbeiter.

Die Unterlagen, die im Rahmen seiner Nebentätigkeit angefallen waren, wollte er mit Ausscheiden aus dem Dienst zulässigerweise an sich nehmen.

Er bewahrte diese Unterlagen jedoch nicht getrennt, sondern zusammen mit einer Vielzahl anderer Papiere in namentlich untergliederten Ordnern mit den Aufschriften "Personal" und "Auszubildende" auf. Bei seinen Mitarbeitern kam daher die Befürchtung auf, er könnte nicht nur die ihm zustehenden Unterlagen mitnehmen.

Sie baten mich um eine Sichtung der Ordner. Dabei mußte ich feststellen, daß tatsächlich die verschiedensten Unterlagen mit und ohne Personenbezug vermischt waren. Einige Beispiele:

- Fotokopien von Unterlagen, die der ärztliche Dienst über eine Mitarbeiterin des Polizeipräsidiums angefertigt hatte;
- Bescheinigungen bzw. Fotokopien über Fortbildungsmaßnahmen von Mitarbeitern des ärztlichen Dienstes;
- Meldungen über Polizeibeamte, die mit HIV-infizierten Personen in Berührung gekommen waren, einschließlich der Personalien dieser Personen;
- ärztliche Unterlagen über BtM-Abhängige;
- ärztliche Unterlagen über Inhaftierte zur Feststellung der Haftfähigkeit, zum Teil mit Kopien der gesamten staatsanwaltschaftlichen Ermittlungsakte;
- Zeugnisse und Bewerbungsunterlagen von Mitarbeitern beim ärztlichen Dienst.

Die Vermischung solcher Unterlagen ist beispielhaft für ein doch häufig auftretendes Problem: Bei der Organisation von Verfahrensabläufen, der Ausgestaltung der Aktenführung sowie den Regelungen über Aufbewahrung und Aktenzugang wird zuwenig überlegt, ob einzelne Informationen oder Unterlagen überhaupt benötigt werden, zu welchen Zwecken sie verwendet werden dürfen und wer Zugang zu diesen Daten haben muß. Verstärkt treten Schwierigkeiten auf, wenn eine Stelle unterschiedliche Aufgaben wahrnimmt. Auch nach 20 Jahren Datenschutzgesetzgebung bestimmt nicht das Recht auf informationelle Selbstbestimmung das Handeln der Verwaltung, sondern dieses ist weiterhin geprägt von langjähriger Verwaltungsübung und entsprechend eingefahrenen Denk- und Handlungsweisen ihrer Mitarbeiter.

17.2.2

Grundsätze zur Neuorganisation

Im vorliegenden Fall war es erforderlich, die komplette Aktenführung sowie den Zugang zu den einzelnen Akten neu zu gestalten. Die betroffene Dienststelle hat ein sehr breites Aufgabenspektrum, das auf unterschiedlichen Rechtsgrundlagen beruht.

Als Beispiele seien bei der ärztlichen Betreuung von Landesbediensteten genannt:

- Bewerber- und Einstellungsuntersuchungen;
- Untersuchungen zur Begutachtung der Polizeidienstfähigkeit;
- Untersuchungen für besondere polizeiliche Verwendungen;

- ärztliche Versorgung im Einsatz;
- sportärztliche Beratung;
- Gutachten im Beihilfeverfahren;
- Begutachtung bei Dienstunfällen;

sowie zur Unterstützung vollzugspolizeilicher Maßnahmen:

- Verwehr- und Verhandlungsfähigkeitsuntersuchungen;
- Blutentnahmen;
- ärztliche Betreuung der im Gewahrsam und in den Haftzellen Verwahrten;
- Untersuchungen im Rahmen des Hessischen Freiheitsentziehungsgesetzes;
- Unterstützung im Rahmen der Ermittlungen und Beweissicherung.

Für eine ordnungsgemäße Organisation dieser Dienststelle und eine entsprechende Behandlung der dabei anfallenden Daten sind – wie überall – sowohl Erforderlichkeit als auch Zweckbindung zu beachten. Das heißt, daß die verschiedenen Unterlagen differenziert nach den einzelnen Aufgaben bzw. den Rechtsgrundlagen, auf denen diese beruhen, behandelt werden müssen.

Besonderes Augenmerk ist auf die Behandlung der Daten derer zu richten, die in der Dienststelle "Polizeiärztlicher Dienst" selbst tätig sind. Es ist darauf zu achten, daß keine unzulässigen Personalnebenakten geführt werden. Soweit die personalverwaltende Behörde nicht zugleich Beschäftigungsbehörde ist, ist zwar grundsätzlich das Führen von Nebenakten zulässig; sie dürfen jedoch nur solche Unterlagen enthalten, deren Kenntnis zur rechtmäßigen Aufgabenerledigung der betreffenden Behörde erforderlich ist. Das Führen einer Personalnebenakte ist in der Hauptakte zu vermerken. Beim polizeiärztlichen Dienst sind jedoch nur wenige Informationen über die dort Beschäftigten erforderlich. Bewerbungsunterlagen, Fortbildungsmaßnahmen, Beurteilungen u.ä. sind keine Unterlagen, die dem Vorgesetzten ständig zur Verfügung stehen müssen. Soweit darüber hinaus für die Mitarbeiter des ärztlichen Dienstes auch medizinische Unterlagen anfallen, ist zudem eine Trennung von den Personalunterlagen erforderlich.

Der polizeiärztliche Dienst ist zugleich Ausbildungsstelle für Arzthelfer. Die für eine ordnungsgemäße Ausbildung notwendigen Informationen dürfen selbstverständlich bei der Ausbildungsstelle in Form einer Akte abgelegt werden. Dabei ist jedoch ebenfalls sorgfältig zu prüfen, welche Unterlagen dazu auf Dauer wirklich erforderlich sind. Auf gar keinen Fall gehören dazu Beurteilungen. Das Führen einer solchen Ausbildungsakte ist ebenfalls in den Personalhauptakten zu vermerken.

Schließlich ist ausdrücklich festzulegen, wer zu welchen Unterlagen Zugriff haben darf. Ausgangspunkt dieser Regelung muß sein, zu welchem Zweck die einzelnen Akten geführt werden, und wer mit den entsprechenden Aufgaben innerhalb des polizeiärztlichen Dienstes betraut ist. Soweit es sich um Personalunterlagen handelt, kann unter Umständen eine differenzierte Zugriffsberechtigung notwendig sein. Falls beispielsweise sensible medizinische Unterlagen über die Beschäftigten geführt werden, sind etwa eine Beschränkung der Einsichtnahme auf den Arzt sowie eine Aufbewahrung in verschlossenen Umschlägen mit Dokumentation der Einsichtnahme oder vergleichbare Maßnahmen zu prüfen.

18. Bilanz

18.1

Aufnahme des Rechts auf informationelle Selbstbestimmung und Informationsfreiheit in das Grundgesetz

Ich hatte dem Hessischen Landtag anlässlich des von ihm und der Hessischen Landesregierung am 30. und 31. Oktober 1991 veranstalteten Symposions "Verfassungsreform" einen Zwischenbericht nach § 30 Abs. 1 Hessisches Datenschutzgesetz (HDSG) "Zur Aufnahme des informationellen Selbstbestimmungsrechts und der Informationsfreiheit (Freedom of Information) in das Grundgesetz" vorgelegt, in dem ich die Gründe, die für eine Aufnahme in das Grundgesetz sprechen, ausführlich dargelegt und konkrete Textvorschläge für das Recht auf informationelle Selbstbestimmung und auf Informationsfreiheit unterbreitet habe (vollständig abgedruckt im 20. Tätigkeitsbericht, Ziff. 17.2).

Im Rahmen der im Einigungsvertrag empfohlenen Diskussion über Änderungen bzw. Ergänzungen des Grundgesetzes ist eine formelle Beteiligung der Länderparlamente nicht vorgesehen. Zunächst wurde das Thema Verfassungsreform in der Kommission Verfassungsreform des Bundesrates beraten. Das hessische Kabinett hat am 4.

Februar 1992 beschlossen, meinen Formulierungsvorschlag zum Recht auf informationelle Selbstbestimmung als Beitrag des Landes Hessen in den zuständigen Arbeitsausschuß der Kommission Verfassungsreform des Bundesrates einzubringen. Im Arbeitsausschuß wurde ein Formulierungsvorschlag zur Einfügung eines Grundrechts auf Datenschutz sowie zur verfassungsrechtlichen Verankerung der Stellung des Datenschutzbeauftragten erarbeitet; er fand jedoch lediglich eine einfache, nicht die erforderliche Zweidrittelmehrheit. Dementsprechend hat das Plenum der Verfassungskommission, das seine Arbeit am 14. Mai 1992 abgeschlossen hat, zum Thema "Datenschutz" lediglich einen Diskussionsbericht, jedoch keine eigenen Empfehlungen verabschiedet. Hinsichtlich der Aufnahme der Informationsfreiheit (Freedom of Information) in das Grundgesetz bestand in der Arbeitsgruppe offenbar überwiegend die Auffassung, daß diese Frage eher bereichsspezifisch auf einfachgesetzlicher Ebene geregelt werden sollte (Abschlußbericht BR-Drucks. 360/92).

Die Verfassungsdiskussion wird jetzt in der Gemeinsamen Verfassungskommission von Bundestag und Bundesrat, die sich am 16. Januar 1992 konstituiert hat und ihre Vorschläge bis zum 31. März 1993 vorlegen soll, fortgesetzt. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat auf einer Sonderkonferenz am 28. April 1992 eine Entschließung zur Aufnahme des Datenschutzes in das Grundgesetz verabschiedet und der Gemeinsamen Verfassungskommission von Bundestag und Bundesrat zugeleitet. In der Entschließung hat die Konferenz die Vorstellungen, die in der Verfassungskommission des Bundesrates entwickelt worden sind, begrüßt und sich dafür ausgesprochen, das Recht auf informationelle Selbstbestimmung im Grundgesetz zu verankern. Darüber hinaus hat die Konferenz empfohlen, die unabhängige Datenschutzkontrolle, die für die Verwirklichung des Grundrechts auf Datenschutz im Alltag von entscheidender Bedeutung ist, in die Verfassung aufzunehmen und in die Beratungen der Gemeinsamen Verfassungskommission darüber hinaus die folgenden weiteren Punkte einzubeziehen, die sich aus der Entwicklung der Informationstechnik ergeben:

- Stärkung der Grundrechte des Art. 10 (Brief-, Post- und Fernmeldegeheimnis) und Art. 13 (Unverletzlichkeit der Wohnung) im Hinblick auf neue Überwachungstechniken
- Recht auf Zugang zu den Daten der Verwaltung (Aktienöffentlichkeit, Informationsfreiheit) sowie
- Instrumente der Technikfolgenabschätzung.

1992 haben mehrere neue Bundesländer Verfassungen beschlossen, die auch Bestimmungen zum Recht auf informationelle Selbstbestimmung (Brandenburg, Art. 11; Sachsen, Art. 33; Sachsen-Anhalt, Art. 6), zur Informationsfreiheit (Brandenburg, Art. 21; Sachsen hinsichtlich der Daten über die Umwelt, Art. 34; Sachsen-Anhalt hinsichtlich der Daten über die Umwelt, Art. 6) sowie zum Landesbeauftragten für den Datenschutz (Brandenburg, Art. 74; Sachsen, Art. 57; Sachsen-Anhalt, Art. 63) enthalten.

18.2

EG-Richtlinie zum Datenschutz

(19. Tätigkeitsbericht Ziff. 2; 20. Tätigkeitsbericht Ziff. 16.3)

Die EG-Kommission hat dem Ministerrat der Europäischen Gemeinschaften einen neuen Vorschlag für eine Datenschutzrichtlinie vorgelegt. Der "Geänderte Vorschlag für eine Richtlinie des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr" vom 15. Oktober 1992 (KOM (92) 422 endg. – SYN 287) ist eine Reaktion auf die Stellungnahme des Europäischen Parlaments zu dem am 18. Juli 1990 vorgelegten ersten Vorschlag der Kommission (KOM (90) 314 endg. – SYN 287 oder BR-Drucks. 690/90). Das Europäische Parlament hatte am 11. März 1992 mehr als 100 Änderungsanträge zum ursprünglichen Kommissionsentwurf beschlossen (PE 160.503, Sitzungsprotokoll EP).

In der Überschrift des neuen Entwurfs kommt nun das wohl entscheidende Motiv, das die Kommission überhaupt zu einem Richtlinienvorschlag veranlaßt hat, zum Ausdruck: Es soll verhindert werden, daß unterschiedliche nationale Datenschutzgesetze und divergierende Entscheidungen der Datenschutzkontrollbehörden den freien Austausch personenbezogener Daten zwischen den Mitgliedstaaten der EG behindern und dadurch Wettbewerbsverzerrungen entstehen. Die Überschrift stellt außerdem klar, daß der Schutz nur für natürliche und nicht auch für juristische Personen gilt.

Bestärkt durch das Europäische Parlament hält die Kommission an ihrem Ziel fest, nicht den kleinsten gemeinsamen Nenner, sondern für alle Mitgliedsländer ein gleichwertig hohes Datenschutzniveau festzuschreiben.

Aufgegeben wurde die auch für das deutsche Recht charakteristische formelle Unterscheidung zwischen Datenverarbeitung im öffentlichen und privaten Bereich. Grundsätzlich gelten für beide Sektoren dieselben Regeln, notwendige Abweichungen werden in den einzelnen Vorschriften berücksichtigt.

Mit dem neuen Entwurf hat sich der Arbeitskreis Europa der Konferenz der Datenschutzbeauftragten des Bundes und der Länder ausführlich beschäftigt. Die Beratungsergebnisse hat der Bundesbeauftragte für den Datenschutz dem Bundesinnenminister in einem Schreiben vom 16. Oktober 1992 mitgeteilt und damit die Aufforderung verbunden, die Auffassung der Datenschutzbeauftragten in den bevorstehenden Verhandlungen im Ministerrat der EG zur Geltung zu bringen.

Die Datenschutzbeauftragten wollen insbesondere eine Klarstellung im Text der Richtlinie, daß die Mitgliedstaaten ein Datenschutzniveau gewährleisten dürfen, das über das der Richtlinie hinausgeht. Andernfalls könnte es passieren, daß manche bereichsspezifische restriktive Datenschutzregelung in der Bundesrepublik aufgehoben werden müßte.

Einer Präzisierung bedarf außerdem die Vorschrift über die Rechtssetzungsbefugnis der EG-Kommission (Art. 33), denn sie läßt offen, ob die Kommission die Möglichkeit haben soll, außerhalb des Anwendungsbereichs der Richtlinie für alle Datenverarbeitungsbereiche spezifische Regelungen zu erlassen. Eine solche Generalermächtigung der Kommission wäre auf keinen Fall akzeptabel.

Zu den Forderungen der Datenschutzbeauftragten zählt unter anderem auch, daß die Bundesregierung im Ministerrat sicherstellen muß, daß das in der Bundesrepublik existierende Modell der Datenschutzbeauftragten beibehalten werden kann. Probleme könnten hier durch die in der Richtlinie für die Kontrollbehörde vorgesehenen Exekutivbefugnisse entstehen, da die Datenschutzbeauftragten derzeit keine Eingriffs- und Anordnungsbefugnisse haben.

Der Entwurf steht nun zur Beratung im Ministerrat an, dem die Aufgabe obliegt, einen "gemeinsamen Standpunkt" zu formulieren, der dem Europäischen Parlament zugeleitet wird. Die Richtlinie wird mit Sicherheit nicht, wie ursprünglich geplant, zu Beginn des Europäischen Binnenmarktes am 1. Januar 1993 verabschiedet sein. Für die Umsetzung der Richtlinie in nationales Recht sieht der Entwurf sogar eine Frist bis zum 1. Juli 1994 vor.

18.3

Telefax in Krankenhäusern

(20. Tätigkeitsbericht, Ziff. 9.1)

Die Städtischen Kliniken Kassel haben mit meiner Beratung eine Dienstanweisung für den Umgang mit Telefaxgeräten erlassen, die den im letzten Tätigkeitsbericht (Ziff. 9.1) dargelegten datenschutzrechtlichen Anforderungen Rechnung trägt. Entsprechendes gilt für die Städtischen Kliniken Wiesbaden.

Unter Zugrundelegung der mit verschiedenen Kliniken geführten Diskussionen über den Einsatz der Telefaxgeräte habe ich einen Mustertext für den datenschutzrechtlichen Teil einer Dienstanweisung über die Einrichtung, den Betrieb und die Nutzung von Telefaxgeräten in einer Klinik entworfen, der gegebenenfalls – je nach Größe und besonderen Umständen der jeweiligen Klinik – zu modifizieren ist. Bei diesen Diskussionen wurde mir zum Teil von den Kliniken entgegengehalten, daß die datenschutzrechtlichen Anforderungen an den Umgang mit Telefaxgeräten erhebliche praktische Probleme in der Umsetzung aufwerfen. Diese Argumentation ist verständlich, kann aber die Notwendigkeit einer solchen Dienstanweisung im Ergebnis nicht in Frage stellen. Derartige Schwierigkeiten treten bei der Einführung neuer Techniken immer wieder auf, weil Probleme des Datenschutzes und der Datensicherheit häufig bei der Entwicklung der Produkte nicht hinreichend berücksichtigt werden. Ein typisches Beispiel hierfür ist die Entwicklung bei den PCs: Ursprünglich hatten die PCs keinerlei Schutzkomponenten; aber infolge der Diskussion über Datenschutz und Datensicherheit ist inzwischen ein Sicherheitsstandard erreicht, der ihren Einsatz – in den meisten Fällen – unproblematisch macht. Bei den Telefaxgeräten bleibt für die Übergangszeit nur die Möglichkeit, die gravierendsten Mängel so weit wie möglich durch organisatorische Maßnahmen zu kompensieren. Im übrigen sind die Hersteller aufgefordert, durch technische Maßnahmen den Sicherheitsstandard zu verbessern (vgl. 17. Tätigkeitsbericht, Ziff. 16.1).

Eine Dienstanweisung für den datenschutzgerechten Umgang mit Telefaxgeräten sollte folgende Punkte enthalten:

- Telefaxgeräte sind Fernmeldeanlagen. Die abgehenden und ankommenden Fernkopien sowie die Sende- und Empfangsprotokolle unterliegen dem Fernmeldegeheimnis. Darüber hinaus gelten § 12 Hessisches Krankenhausgesetz in Verbindung mit den Vorschriften des Hessischen Datenschutzgesetzes sowie die ärztliche Schweigepflicht i.S.v. § 203 StGB.
- Es sind alle erforderlichen Maßnahmen zu treffen, um eine Kenntnisnahme der Fernkopien durch Unbefugte zu verhindern.
- In Räumen mit Publikumsverkehr dürfen keine Fernkopien mit Patientendaten empfangen werden.
- In Verwaltungs- und Versorgungsbereichen dürfen keine medizinischen Daten über Patienten empfangen werden.
- Die Telefaxgeräte der einzelnen Fachabteilungen und Institute dürfen grundsätzlich nicht von anderen Fachabteilungen oder Instituten benutzt werden. Auf den jeweils verwendeten Briefkopfbögen muß die eigene Faxnummer der Fachabteilung bzw. des Instituts angegeben sein. Eine Benutzung durch Mitarbeiter anderer Fachabteilungen oder Institute ist nur im Einzelfall zulässig, wenn diese den Sendevorgang persönlich durchführen und das Original einschließlich des Sendeprotokolls mitnehmen.

- Der Standort des Telefaxgerätes muß so gewählt sein, daß nur Befugte von den eingehenden Fernkopien Kenntnis nehmen können.
- Bevor erstmals personenbezogene Patientendaten per Fernkopie an einen bestimmten Empfänger verschickt werden, muß sich der Absender fernmündlich erkundigen, ob der Empfänger Verfügungen getroffen hat, die sicherstellen, daß die Daten nur an die Empfangsberechtigten gelangen.
- Die Telefaxnummer des Empfängers ist vor der Übermittlung durch den Absender auf die Richtigkeit zu kontrollieren.
- Der Adressat der Patientendaten muß auf der Fernkopie konkret angegeben werden. Allgemein gehaltene Adressen sind nicht zulässig.

Sofern eine Fernkopie auf einem nicht dafür bestimmten Gerät eingeht, ist wie folgt zu verfahren:

- Der Adressat ist unverzüglich aufzufordern, die Fernkopie von einer befugten Person abholen zu lassen. Bis zur Abholung sind die Fotokopien vor einer Kenntnisnahme durch Dritte zu schützen.
- Der Absender ist unverzüglich darauf hinzuweisen, daß diese Telefaxnummer künftig nicht mehr verwendet werden darf; gegebenenfalls ist die zutreffende Faxnummer anzugeben. Ferner ist der Absender darauf hinzuweisen, daß die Fernkopie innerhalb der Kliniken weitergeleitet wurde bzw. daß die falsch eingegangene Faxsendung vernichtet wurde.
- Die Sende- und Empfangsprotokolle sind Jahre aufzubewahren.
- Bei der Einrichtung eines Telefaxgerätes ist der interne Datenschutzbeauftragte einzubeziehen.
- Für die Einhaltung der Dienstanweisung und die konkrete Umsetzung sind verantwortlich.

18.4

Verabschiedung des neunten Gesetzes zur Änderung dienstrechtlicher Vorschriften (18. Tätigkeitsbericht, Ziff. 12.3)

Die Regelungen zum Personalaktenrecht im Bundesbeamtengesetz (BBG) und Beamtenrechtsrahmengesetz (BRRG), sind am 1. Januar 1993 in Kraft getreten.

Im wesentlichen sind folgende Bereiche geregelt:

- Pflicht zur Führung von Personalakten (§ 90 Abs. 1 S. 1 BBG; § 56 Abs. 1 S. 1 BRRG);
- Grundsätze der Aktenführung, insbesondere zur Führung von Teil- und Nebenakten (§§ 90 Abs. 1 und 2, 90a BBG; §§ 56 Abs. 1 und 2, 56a BRRG);
- Zugangsrecht zur Personalakte nur für Beschäftigte der Personalverwaltung (§ 90 Abs. 3 BBG; § 56 Abs. 3 BRRG);
- Einsichtsrechte des Bediensteten, seines Bevollmächtigten oder seiner Hinterbliebenen (§ 90c BBG; § 56c BRRG);
- Vorlage und Auskunftsmöglichkeiten an Dritte (§ 90d BBG; § 56d BRRG);
- Voraussetzungen für die Entfernung von Vorgängen aus der Personalakte (§ 90e BBG; § 56e BRRG);
- Aufbewahrungsfristen (§ 90f BBG);
- Personaldatenverarbeitung in Dateien (§ 90g BBG; § 56f BRRG).

Damit hat die Bundesregierung endlich die vom Bundestag und den Datenschutzbeauftragten seit langem geforderte bereichsspezifische Regelung des Arbeitnehmerdatenschutzes jedenfalls für den Bereich des öffentlichen Dienstes realisiert.

Negativ zu vermerken ist, daß zahlreiche der in meinem 18. Tätigkeitsbericht (Ziff. 12.3) erörterten Mängel des Entwurfs Eingang in das Gesetz gefunden haben:

Das Einsichtsrecht in die Sicherheitsakten, soweit sie sich beim Dienstherrn befinden, ist nicht geregelt.

Die Einsichts- bzw. Auskunftsrechte gegenüber aufsichtsführenden Behörden, Behörden desselben Geschäftsbereichs oder auch Dritten ohne Einwilligung des Betroffenen sind nach wie vor zu weitgehend.

Ein positiver Ansatz ist in der Regelung über die Führung von Beihilfeakten zu sehen, die nunmehr stets getrennt zu führen und zu bearbeiten sind. Auch die Regelung über die Verwendung von Beihilfeakten zu anderen als Beihilfezwecken ist jetzt eingeschränkter als im Entwurf zunächst vorgesehen.

18.5

Prüfung der Datenerhebung in Krankenhäusern

(20. Tätigkeitsbericht Ziff. 9.2)

Im letzten Tätigkeitsbericht hatte ich über meine Prüfung der Datenverarbeitung bei der Patientenaufnahme in Krankenhäusern berichtet. Diese Prüfung habe ich fortgesetzt und festgestellt, daß die Aufnahmeformulare zahlreicher Krankenhäuser noch immer nicht den Anforderungen des Hessischen Krankenhausgesetzes vom 18. Dezember 1989 (HKHG, GVBl. I S. 452) entsprechen.

Einige Krankenhäuser, die ich Ende September 1992 schriftlich gebeten hatte, die aktuellen Aufnahmeformulare zu schicken, hatten bis Anfang Dezember 1992 nicht reagiert. Es waren dies das Kreiskrankenhaus in Heppenheim, das Stadtkrankenhaus in Hanau, die Universitätskliniken in Gießen sowie die Städtischen Kliniken in Kassel.

Die Krankenhäuser, mit deren Vertretern die datenschutzgerechte Neugestaltung der Aufnahmeformulare besprochen werden konnte, haben inzwischen ihre Aufnahmeformulare geändert und der Rechtslage angepaßt. Hierzu gehören der Landeswohlfahrtsverband Hessen als größter hessischer Krankenhausträger und die Dr.-Horst-Schmidt-Kliniken in Wiesbaden.

Ich werde meine Prüfungen fortsetzen.

Wiesbaden, den 26. Februar 1993

gez. Professor Dr. Hassemer

19. Materialien

19.1

Entschließungen der Konferenz der Datenschutzbeauftragten des Bundes und der Länder

19.1.1

Entschließung der 43. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 23./24. März 1992 in Stuttgart zum Arbeitnehmerdatenschutz

I.
Im Rahmen des Arbeitsverhältnisses werden personenbezogene Daten aus ganz unterschiedlichen Lebensbereichen des Arbeitnehmers erhoben und gespeichert. Diese Daten verwendet der Arbeitgeber nicht nur für eigene Zwecke. Aus dem Arbeitsverhältnis ergeben sich auch Auskunfts-, Bescheinigungs- und Meldepflichten, die der Arbeitgeber gegenüber öffentlichen Stellen zu erfüllen hat. Durch die Möglichkeit, im Arbeitsverhältnis anfallende personenbezogene Daten miteinander zu verknüpfen und sie – losgelöst vom Erhebungszweck – für andere Verwendungen zu nutzen, entstehen Gefahren für das Persönlichkeitsrecht des Arbeitnehmers. Mit der Intensität der Datenverarbeitung, insbesondere durch Personalinformationssysteme und digitale Telekommunikationsanlagen, nehmen die Kontroll- und Überwachungsmöglichkeiten des Arbeitgebers zu.

Die Datenschutzbeauftragten des Bundes und der Länder fordern deshalb bereits seit 1984 bereichsspezifische und präzise gesetzliche Bestimmungen zum Arbeitnehmerdatenschutz. Bundestag, Bundesrat und Bundesregierung haben ebenfalls eine Regelungsnotwendigkeit bejaht; gleichwohl stehen bundesgesetzliche Regelungen über den allgemeinen Arbeitnehmerdatenschutz immer noch aus.

Die Notwendigkeit zur gesetzlichen Regelung besteht unabhängig davon, ob Arbeitnehmerdaten in automatisierten Dateien, in Akten oder in sonstigen Unterlagen verarbeitet werden. Der erhöhten Gefährdung durch die automatisierte Datenverarbeitung ist durch spezifische Schutzvorschriften Rechnung zu tragen.

Angesichts der besonderen Abhängigkeit des Arbeitnehmers im Arbeitsverhältnis und während der Phase einer Bewerbung um einen Arbeitsplatz ist durch ein Gesetz zu untersagen, daß Rechte, die dem Arbeitnehmer nach einschlägigen Datenschutzvorschriften zustehen, durch Rechtsgeschäft, Tarifvertrag und Dienst- oder Betriebsvereinbarung ausgeschlossen werden. Außerdem ist durch Gesetz festzulegen, daß eine Einwilligung des Arbeitnehmers oder Bewerbers nur dann als Grundlage einer Datenerhebung, -verarbeitung oder -nutzung in Frage kommt, wenn die Freiwilligkeit der Einwilligung sichergestellt ist, also die Einwilligung ohne Furcht vor Nachteilen verweigert werden kann. Deshalb dürfen allein aufgrund einer Einwilligung z.B. keine Gesundheitszeugnisse, Ergebnisse von Genomanalysen u.ä. angefordert werden, wenn sie den Rahmen des Fragerechts des Arbeitgebers überschreiten.

II.

Die gesetzliche Ausgestaltung des Arbeitnehmerdatenschutzes muß insbesondere folgende Grundsätze beachten:

1. Die Datenerhebung muß grundsätzlich beim Arbeitnehmer erfolgen.
2. Der Arbeitgeber darf Daten des Arbeitnehmers – auch durch Befragen des Arbeitnehmers oder Bewerbers – nur erheben, verarbeiten oder nutzen, soweit dies zur Eingehung, Durchführung, Beendigung oder Abwicklung des Arbeitsverhältnisses erforderlich oder sonst gesetzlich vorgesehen ist. Dabei ist der Grundsatz der Zweckbindung zu beachten. Auch ist zwischen der Bewerbungs- und Einstellungsphase zu unterscheiden.
3. Der Arbeitgeber darf Daten, die er aufgrund gesetzlicher Vorgaben für andere Stellen (z.B. Sozialversicherungsträger) erheben muß, nur für diesen Zweck verwenden.
4. Eine Datenauswertung und -verknüpfung, die zur Herstellung eines umfassenden Persönlichkeitsprofils des Arbeitnehmers führen kann, ist unzulässig.
5. Beurteilungen und Personalauswahlentscheidungen dürfen nicht allein auf Informationen gestützt werden, die unmittelbar durch automatisierte Datenverarbeitung gewonnen werden.
6. Notwendige Datenübermittlungen zwischen Arzt und Arbeitgeber sind eindeutig zu regeln. Dem Arbeitgeber darf grundsätzlich nur das Ergebnis der ärztlichen Untersuchung zugänglich gemacht werden. Darüber hinaus dürfen ihm – soweit erforderlich – nur tätigkeitsbezogene Risikofaktoren mitgeteilt werden. Medizinische und psychologische Befunde sind getrennt von den übrigen Personalunterlagen aufzubewahren. Die Ergebnisse medizinischer oder psychologischer Untersuchungen und Tests des Beschäftigten dürfen automatisiert nur verarbeitet werden, wenn dies dem Schutz des Beschäftigten dient.
7. Dem Arbeitnehmer sind umfassende Auskunfts- und Einsichtsrechte in die Unterlagen einzuräumen, die sein Arbeitsverhältnis betreffen. Diese Rechte müssen sich auch auf Herkunft, Verarbeitungszwecke und Empfänger der Daten sowie die Art und Weise ihrer Auswertung erstrecken.
8. Dem Personal-/Betriebsrat muß ein Mitbestimmungsrecht bei der Einführung, Anwendung und der wesentlichen Änderung von automatisierten Dateien mit personenbezogenen Daten der Arbeitnehmer für Zwecke der Personalverwaltung zustehen. Das gilt auch bei sonstigen technischen Einrichtungen, mit denen das Verhalten und die Leistung der Beschäftigten überwacht werden kann.
9. Gesetzlich festzulegen ist, welche Daten der Arbeitnehmervertretung für ihre Aufgabenerfüllung zugänglich sein müssen und wie der Datenschutz bei der Verarbeitung von Arbeitnehmerdaten im Bereich der Arbeitnehmervertretung gewährleistet wird. Regelungsbedürftig ist auch das Verhältnis zwischen dem Personal-/Betriebsrat und dem behördlichen/betrieblichen Datenschutzbeauftragten.
10. Die Befugnis des Personal-/Betriebsrats, sich unmittelbar an die Datenschutzkontrollinstanzen zu wenden, ist gesetzlich klarzustellen.
11. Arbeitnehmerdaten dürfen nur dann ins Ausland übermittelt werden, wenn dort ein dem deutschen Recht vergleichbarer Datenschutzstandard gewährleistet ist oder wenn der Betroffene nach den o.g. Grundsätzen (vgl. Abschn. I Abs. 4) eingewilligt hat.

19.1.2**Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder zum Grundrecht auf Datenschutz vom 28. April 1992**

1. Seit dem Volkszählungsurteil des Bundesverfassungsgerichts im Jahre 1983 ist allgemein anerkannt, daß die Grundrechte auch die Befugnis des einzelnen umfassen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu entscheiden. Die Datenschutzbeauftragten treten dafür ein, dieses Recht ausdrücklich im Grundgesetz zu verankern. Damit würde
 - für die Bürger deutlicher erkennbar, daß unsere Verfassung ihr Recht auf Datenschutz in gleicher Weise garantiert wie die traditionellen Grundrechte,
 - der wachsenden Bedeutung des Datenschutzes für das Funktionieren der freiheitlichen Demokratie Rechnung getragen und auf die negativen Erfahrungen der DDR-Geschichte reagiert,
 - der Grundrechtskatalog dem technologischen Wandel angepaßt und
 - die Konsequenz aus den positiven Erfahrungen gezogen, die in mehreren Ländern des Bundes und im Ausland mit ähnlichen Verfassungsbestimmungen gemacht wurden.

Die Konferenz begrüßt deshalb die Vorstellungen, die in der Verfassungskommission des Bundesrates entwickelt worden sind.

Die Datenschutzbeauftragten empfehlen der Gemeinsamen Verfassungskommission des Bundestages und Bundesrates im Zusammenhang mit Art. 1 und Art. 2 GG den nachfolgenden Text zur Beratung:

“Jeder hat das Recht, über die Preisgabe und Verwendung seiner persönlichen Daten selbst zu bestimmen. Dazu gehört das Recht auf Auskunft und Einsicht in amtliche Unterlagen. Dieses Recht darf nur durch Gesetz oder aufgrund eines Gesetzes eingeschränkt werden, soweit überwiegende Interessen der Allgemeinheit es erfordern.“

2. Darüber hinaus empfiehlt die Konferenz, die unabhängige Datenschutzkontrolle, die für die Verwirklichung des Grundrechts auf Datenschutz im Alltag von entscheidender Bedeutung ist, in der Verfassung zu verankern.
3. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hält es zusätzlich für erforderlich, in die Verfassungsdiskussion folgende Punkte miteinzubeziehen, die sich aus der Entwicklung der Informationstechnik ergeben:
 - Stärkung der Grundrechte aus Art. 10 und 13 im Hinblick auf neue Überwachungstechniken
 - Recht auf Zugang zu den Daten der Verwaltung (Aktenöffentlichkeit, Informationsfreiheit)
 - Instrumente zur Technikfolgenabschätzung.

19.1.3

Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder zur Neuregelung des Asylverfahrens

(BT-Drucks. 12/2062) vom 28. April 1992

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hält Änderungen des Gesetzentwurfs zur Neuregelung des Asylverfahrens für erforderlich, insbesondere der geplanten Regelungen

1. über die erkennungsdienstliche Behandlung von Asylbewerbern zur Sicherung der Identität (§ 16 Abs. 1) und
2. über die Nutzung der dabei gewonnenen erkennungsdienstlichen Unterlagen zur Strafverfolgung und zur Gefahrenabwehr (§ 16 Abs. 5).

Zu 1.:

Nach dem geltenden Recht sind Lichtbilder und Fingerabdrucke bei Asylbewerbern nur dann zu fertigen, wenn deren Identität nicht eindeutig bekannt ist. Demgegenüber sieht der Gesetzentwurf zur Neuregelung des Asylverfahrens vor, daß von sämtlichen Asylbewerbern – bis auf wenige Ausnahmen – Lichtbilder und Fingerabdrucke zu fertigen sind. Dies ist mit dem Verfassungsgrundsatz der Verhältnismäßigkeit nicht vereinbar: Der Staat hat selbstverständlich das Recht, zu wissen, mit wem er es zu tun hat. Jeder – gleichgültig ob Deutscher oder Ausländer – muß sich deshalb durch Dokumente ausweisen können; nur wenn Zweifel an der Identität bestehen, kommen erkennungsdienstliche Maßnahmen in Betracht. Dieser Grundsatz unserer Rechtsordnung muß auch im Rahmen der Neuregelung des Asylverfahrens beachtet werden. Nur wenn feststeht, daß die Identität eines hohen Anteils der Asylbewerber – also nicht bloß diejenige einzelner oder bestimmter Gruppen – zweifelhaft ist, wäre eine erkennungsdienstliche Behandlung aller Asylbewerber gerechtfertigt. Gerade dies aber ist bisher nicht hinreichend belegt: In der amtlichen Begründung des Gesetzentwurfs ist allein davon die Rede, daß nach Feststellung niederländischer Behörden 20 v.H. der Asylbewerber unter falschem Namen einen weiteren Asylantrag stellen. Aussagekräftige Angaben, in welchem Umfang in der Bundesrepublik Deutschland Asylbewerber unter Täuschung über ihre Identität gleich bei der ersten Antragstellung oder nach dessen Ablehnung erneut versuchen, Asyl zu erhalten, fehlen bislang.

Zu 2.:

Bei der zentralen Auswertung der Fingerabdrucke von Asylbewerbern durch das Bundeskriminalamt muß – ungeachtet dessen, ob das Bundeskriminalamt dabei in eigener Zuständigkeit oder für das Bundesamt für die Anerkennung ausländischer Flüchtlinge tätig wird – unbedingt folgendes sichergestellt sein:

- Fingerabdrucke von Asylbewerbern, die unter Beachtung des zu Nr. 1 Gesagten gefertigt wurden, dürfen nur gespeichert werden, soweit dies zur Sicherung der Identität unbedingt erforderlich ist. Dazu reicht die bisher vom Bundeskriminalamt angewandte Methode der sog. Kurzsatzverformelung der Fingerabdrucke aus. Gerade aber dabei soll es nicht bleiben: Mit der bevorstehenden Einführung von AFIS – einem neuen automatisierten Fingerabdruckverfahren – sollen künftig auch die Fingerabdrucke von Asylbewerbern, die allein zur Feststellung deren Identität gefertigt wurden, genauso erfaßt und ausgewertet werden wie die Fingerabdrucke mutmaßlicher oder tatsächlicher Straftäter. Asylbewerber würden damit von vornherein wie Straftäter behandelt. Eine solche Verfahrensweise wird dem Grundsatz der Verhältnismäßigkeit, insbesondere dem Übermaßverbot, nicht gerecht. Zudem unterläuft sie die in § 16 Abs. 4 des Gesetzentwurfs vorgesehene Trennung der erkennungsdienstlichen Unterlagen von Asylbewerbern und Straftätern. Um die gebotene Differenzierung sicherzustellen, sollte – über

das Trennungsgebot des § 16 Abs. 4 hinaus – die Verformelung auf den Abdruck eines Fingers des Asylbewerbers beschränkt werden, da dies zur eindeutigen Feststellung seiner Identität genügt.

- Die Datenschutzbeauftragten verkennen nicht, daß es unter Umständen im überwiegenden Allgemeininteresse notwendig sein kann, im Rahmen asylrechtlicher Identitätsfeststellung gefertigte Fingerabdrucke für Zwecke der Strafverfolgung zu nutzen. Weil eine solche Verwendung einen neuen und zudem erheblichen Eingriff in das Grundrecht auf Datenschutz darstellt, darf sie nicht – wie es der Gesetzentwurf aber vorsieht – praktisch voraussetzungslos erfolgen. Notwendig ist vielmehr, die Voraussetzungen in einem abschließenden Straftatenkatalog aufzuführen; darin könnten auch die in der amtlichen Begründung des Gesetzentwurfs erwähnten Fälle des Sozialhilfebetrugs enthalten sein.
- Ein entsprechender Maßstab ist an die Regelung anzulegen, wann zur Identitätssicherung gefertigte Fingerabdrucke von Asylbewerbern zur polizeilichen Gefahrenabwehr genutzt werden dürfen. Eine solche Nutzung sollte nur zugelassen werden, soweit dies zur Abwehr einer gegenwärtigen erheblichen Gefahr für die öffentliche Sicherheit erforderlich ist.

19.1.4

Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 1./2. Oktober 1992 zum Datenschutz bei internen Telekommunikationsanlagen

Der zunehmende Einsatz von digitalen Telekommunikationsanlagen (TK-Anlagen) in Wirtschaft und Verwaltung birgt Datenschutzrisiken in sich, denen durch eine datenschutzfreundliche Ausgestaltung der Technik und durch geeignete bereichsspezifische Regelungen entgegengewirkt werden muß. Telefongespräche stehen – auch wenn sie von einem Dienstapparat aus geführt werden – unter dem Schutz des Grundgesetzes. Dies hat das Bundesverfassungsgericht in seiner neueren Rechtsprechung hervorgehoben.

Der Schutz des Fernmeldegeheimnisses und des nichtöffentlich gesprochenen Wortes ist gerade bei Arbeitnehmern bedeutsam, da diese sich in einem besonderen Abhängigkeitsverhältnis befinden; aber auch das informationelle Selbstbestimmungsrecht Dritter, die anrufen oder angerufen werden, muß gewahrt bleiben.

Entsprechende bundesrechtliche Regelungen für interne TK-Anlagen sind überfällig, da in diesen Anlagen – insbesondere wenn sie digital an das öffentliche ISDN angeschlossen sind – umfangreiche Sammlungen sensibler personenbezogener Daten entstehen können, die sich auch zur Verhaltens- und Leistungskontrolle eignen und zudem Hinweise auf das Kommunikationsverhalten aller Gesprächsteilnehmer geben.

Die Regelungen sollten verbindliche Vorgaben für die technische Ausgestaltung von TK-Anlagen geben und den Umfang der zulässigen Datenverarbeitung festlegen:

- Es müssen die technischen Voraussetzungen gewährleistet sein, daß Anrufer und Angerufene die Rufnummernanzeige fallweise abschalten können.
- Die automatische Speicherung der Rufnummern von externen Anrufern nach Beendigung des Telefongesprächs ist auszuschließen, es sei denn, eine sachliche Notwendigkeit besteht hierfür (z.B. bei Feuerwehr und Rettungsdiensten).
- Die Weiterleitung eines Anrufs an einen anderen als den gewählten Anschluß sollte dem Anrufer so rechtzeitig signalisiert werden, daß dieser den Verbindungsaufbau abbrechen kann.
- Das Mithören und Mitsprechen weiterer Personen bei bestehenden Verbindungen sollte nur nach eindeutiger und rechtzeitiger Ankündigung möglich sein.
- Verbindungsdaten einschließlich der angerufenen Telefonnummern sollten nach Beendigung der Gespräche nur insoweit gespeichert werden, als dies für Abrechnungszwecke und zulässige Kontrollzwecke erforderlich ist. Die Nummern der Gesprächspartner von Arbeitnehmervertretungen, internen Beratungseinrichtungen und sonstigen auf Vertraulichkeit angewiesenen Stellen dürfen nicht registriert werden.
- Die TK-Anlagen müssen durch geeignete technische Maßnahmen gegen unberechtigte Veränderungen der Systemkonfiguration und unberechtigte Zugriffe auf Verbindungs- und Inhaltsdaten geschützt werden.

Da TK-Anlagen geeignet sind, das Verhalten und die Leistung der Arbeitnehmer zu kontrollieren, und sie überdies häufig die Arbeitsplatzgestaltung beeinflussen, löst ihre Einführung in Betrieben und Behörden Mitbestimmungsrechte der Betriebsräte und überwiegend auch der Personalräte aus. Sie dürfen daher nur betrieben werden, wenn unter Beteiligung der Arbeitnehmervertretungen verbindlich festgelegt wurde, welche Leistungsmerkmale aktiviert und unter welchen Bedingungen sie genutzt werden, welche Daten gespeichert, wie und von wem sie ausgewertet werden. Die Nutzer der TK-Anlage sind über den Umfang der Datenverarbeitung umfassend zu unterrichten.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert, daß umgehend datenschutzrechtliche Regelungen für den Einsatz und die Nutzung von internen TK-Anlagen mit einer bereichsspezifischen Rechtsgrundlage für die Verarbeitung von Arbeitnehmerdaten geschaffen werden.

19.1.5**Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 1./2. Oktober 1992 zum Entwurf eines Gesetzes zur Sicherung und Strukturverbesserung der gesetzlichen Krankenversicherung – Gesundheits-Strukturgesetz 1993 – (BR-Drucks. 560/92)**

Die Bundesregierung will mit dem Gesundheits-Strukturgesetz dem Kostenanstieg in der gesetzlichen Krankenversicherung entgegenwirken. Dieses begrüßenswerte Ziel soll nach dem vorgelegten Gesetzentwurf unter anderem auch durch eine verstärkte automatisierte Datenverarbeitung erreicht werden. Die damit verbundenen Eingriffe in die Persönlichkeitsrechte der Versicherten und in die sie schützende ärztliche Schweigepflicht müssen auf das unbedingt Notwendige beschränkt werden. Die Datenschutzkonferenz hält vor allem folgende Verbesserungen des Gesetzentwurfs für notwendig:

- Der Gesetzentwurf sieht vor, daß die Krankenhäuser den Krankenkassen mehr Versichertendaten zur Verfügung stellen müssen als bisher. Es sollte deshalb eingehend geprüft werden, ob die Krankenkassen tatsächlich alle geforderten Angaben benötigen; die Aufgabenteilung zwischen Krankenkassen und Medizinischem Dienst muß aufrechterhalten bleiben.
- Für das Modellvorhaben zur Überprüfung des Krankenhausaufenthalts müssen die Erhebung, Verwendung und Löschung von Versichertendaten durch den Medizinischen Dienst präziser als bisher vorgesehen geregelt werden.
- Beim Einzug der Vergütung der Krankenhausärzte für Wahlleistungen durch Krankenhäuser sollte die Einschaltung privater Abrechnungsstellen ohne Einwilligung der Patienten nicht zugelassen werden, da dabei Abrechnungsdaten an Dritte offenbart werden. Die Daten sind gegen unbefugte Offenbarung und Beschlagnahme rechtlich besser geschützt, wenn sie – auch zur Abrechnung – im Krankenhaus verbleiben. Die Krankenhäuser sind zudem selbst in der Lage, die Vergütung einzuziehen.
- Für die neu vorgesehenen Patienten-Erhebungsbogen zur Ermittlung des Bedarfs an Pflegepersonal im Krankenhaus sollte eine strikte Zweckbindung sowie eine frühestmögliche Lösungs- oder Anonymisierungspflicht festgelegt werden. Eine Überlassung der Patienten-Erhebungsbogen in der im Gesetzentwurf vorgesehenen Fassung an die Krankenkassen ist abzulehnen.

19.1.6**Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 1./2. Oktober 1992 zum "Lauschangriff"**

Die Datenschutzbeauftragten des Bundes und der Länder erklären (bei Gegenstimme des LfD Bayern):

Nachdem erst vor kurzem mit dem Gesetz zur Bekämpfung der organisierten Kriminalität die Befugnisse der Strafverfolgungsbehörden erheblich erweitert worden sind und obwohl über den Erfolg dieser Maßnahmen noch keine Erfahrungen gesammelt werden konnten, wird gegenwärtig parteiübergreifend vielfach die Forderung erhoben, der Polizei in bestimmten Fällen das heimliche Abhören und Herstellen von Bild- und Tonaufzeichnungen in und aus Wohnungen (sog. "Lauschangriff") zu ermöglichen.

1. Das Grundgesetz gewährt jedem einen unantastbaren Bereich privater Lebensgestaltung, der der Einwirkung der öffentlichen Gewalt entzogen ist. Dem einzelnen muß um der freien und selbstverantwortlichen Entfaltung seiner Persönlichkeit willen ein "Innenraum" verbleiben, in dem er "sich selbst besitzt" und "in den er sich zurückziehen kann, zu dem die Umwelt keinen Zutritt hat, in dem man in Ruhe gelassen wird und ein Recht auf Einsamkeit genießt" (BVerfGE 27,1 ff.). Jedem muß ein privates Refugium, ein persönlicher Bereich bleiben, der obrigkeitlicher Ausforschung – insbesondere heimlicher – entzogen ist. Dies gilt gegenüber Maßnahmen der Strafverfolgung vor allem deshalb, weil davon auch unverdächtige oder unschuldige Bürger betroffen sind. Auch strafprozessuale Maßnahmen dürfen nicht den Wesensgehalt eines Grundrechts, insbesondere nicht das Menschenbild des Grundgesetzes, verletzen.
2. Die Datenschutzbeauftragten nehmen die Gefahren, die das organisierte Verbrechen für die Opfer und auch für die Demokratie und den Rechtsstaat heraufbeschwört, sehr ernst. Sie sind allerdings der Meinung, daß eine angemessene Abwägung zwischen der Verfolgung der organisierten Kriminalität und dem Schutz der Persönlichkeitsrechte der Bürger geboten und möglich ist und es eine Wahrheitserforschung um jeden Preis auch künftig im Strafprozeßrecht nicht geben darf. Daraus folgt, daß der Lauschangriff auf Privatwohnungen für Zwecke der Strafverfolgung auch in Zukunft nicht erlaubt werden darf.
3. Eine andere Frage ist, ob und unter welchen Voraussetzungen der Gesetzgeber für Räume, die allgemein zugänglich sind oder beruflichen oder geschäftlichen Tätigkeiten dienen (z.B. Hinterzimmer von Gaststätten, Spielcasinos, Saunacclubs, Bordelle), einen Lauschangriff zulassen kann. Hierfür sind Mindestvoraussetzungen ein eng begrenzter abschließender Straftatenkatalog, die Verwendung der gewonnenen Erkenntnisse ausschließlich zur Verfolgung dieser Straftaten, ein strikter Richtervorbehalt sowie die Wahrung besonderer Amts- und Berufsheimnisse.

Absender/in (Erklärende/r):

- Anlage -

Name, Vorname _____	PLZ, Ort _____
	Straße, Hausnummer _____
	Telefonnr. unter der Sie tagsüber erreichbar sind _____

Sehr geehrte Frau,
sehr geehrter Herr,

bitte füllen Sie diesen Vordruck
gut leserlich aus und senden Sie
ihn innerhalb von vier Wochen
an nebenstehende Dienststelle.'

Wenn Sie den Vordruck nicht frist-
gerecht zurückgeben und auch keine
Fristverlängerung beantragen, gilt
dies als Erklärung Ihres Einver-
ständnisses, daß Auskünfte beim

Sozialamt und der Wohngeldstelle darüber eingeholt werden, ob Sie Sozialhilfe oder Wohngeld erhalten. Wenn Sie vermeiden wollen, daß entsprechende Auskünfte beim Sozialamt oder der Wohngeldstelle eingeholt werden, sollten Sie den ausgefüllten Vordruck rechtzeitig zurücksenden.

Falls Sie weder Sozialhilfe noch Wohngeld erhalten, werden Sie bei nicht fristgerechter Rücksendung des ausgefüllten Vordrucks nach den höchsten Abgabesätzen herangezogen (bis zu 9,00 DM je m²).

Vollzug des Hessischen Gesetzes zum Abbau der Fehlsubventionierung im Wohnungswesen

E r k l ä r u n g

des Mieters/der Mieterin einer Sozialwohnung

- Ich habe die Wohnung nicht gemietet, sondern bin Eigentümer/in oder Erbauberechtigte/r. In diesem Fall genügt es, wenn Sie Abschnitt 1.1 und 3. ausfüllen, die Erklärung unterschreiben und eine Kopie des Grundbuchauszuges beifügen. Eine Einkommenserklärung müssen Sie nicht abgeben.
- Ich beziehe Wohngeld. In diesem Fall genügt es, wenn Sie Abschnitt 1.1 und 3. ausfüllen, die Erklärung unterschreiben und eine Kopie des Wohngeldbescheides beifügen. Eine Einkommenserklärung müssen Sie nicht abgeben.
- Ich erhalte laufende Leistungen zum Lebensunterhalt nach dem Bundessozialhilfegesetz (Sozialhilfe). In diesem Fall genügt es, wenn Sie Abschnitt 1.1 und 3. ausfüllen, die Erklärung unterschreiben und eine Kopie des Sozialhilfebescheides beifügen. Eine Einkommenserklärung müssen Sie nicht abgeben.
- Ich will keine Angaben zu meinem Einkommen machen. Mir ist bekannt, daß ich dann nach den höchsten Abgabesätzen herangezogen werde (bis zu 9,00 DM je m²). In diesem Fall genügt es, wenn Sie die Abschnitte 1. und 2. ausfüllen und die Erklärung unterschreiben.

Trifft auf Sie keine der oben genannten Möglichkeiten zu, dann füllen Sie bitte den ganzen Fragebogen aus und geben Sie eine Einkommenserklärung ab.

1. Angaben zur Wohnung

1.1 Die Wohnung befindet sich in:

PLZ _____	Ort _____	Zustellpostamt (falls bekannt) _____
Straße und Hausnummer _____		<input type="checkbox"/> Vorderhaus <input type="checkbox"/> Hinterhaus <input type="checkbox"/> Seitengebäude
Stockwerk _____		<input type="checkbox"/> rechts <input type="checkbox"/> Mitte <input type="checkbox"/> links

1.2 Die Wohnung ist m² groß. Die Wohnungsgröße (Wohnfläche) können Sie Ihrem Mietvertrag entnehmen.

1.3 Die Wohnung ist ausgestattet mit:

<input type="checkbox"/> Zentralheizung	<input type="checkbox"/> Etagenheizung	<input type="checkbox"/> Öleinzelföfen mit zentraler Brennstoffversorgung	<input type="checkbox"/> Gas- oder Elektro-einzelföfen
<input type="checkbox"/> Öl- oder Kohle-einzelföfen	<input type="checkbox"/> Bad oder Dusche		

Ganz wichtig: Verbesserungen der Wohnungsausstattung, die Sie auf eigene Kosten vorgenommen haben, oder für die Sie vom Vermieter nur einen Zuschuß von höchstens 50% erhalten haben, sind nicht zu berücksichtigen.

2. Angaben zum Mietverhältnis

Datum des Mietvertrages _____	Beginn des Mietverhältnisses gemäß Mietvertrag _____	Monatl. Mietzins ohne Nebenkosten _____
-------------------------------	--	---

3. Angaben zur Person des Mieters/der Mieterin bzw. der Mieter/innen

Wer Mieter oder Mieterin der Wohnung ist, entnehmen Sie bitte dem Mietvertrag.

Name, Vorname _____	ggf. Geburtsname _____
1. _____	_____
2. _____	_____

Bei mehr als zwei Mietern/Mieterinnen bitte gesondertes Blatt verwenden.

4. Angaben zur Person der Bewohner/Bewohnerinnen

4.1 Nachstehende Personen wohnen nicht nur vorübergehend in der Wohnung:

Bitte führen Sie sämtliche Personen auf, die nicht nur vorübergehend in der Wohnung wohnen (auch die unter Abschnitt 3. bereits genannten Personen). Besucher - auch bei längerer Besuchsdauer - gehören nicht dazu.

Name, Vorname	Geburtsdatum	Name, Vorname	Geburtsdatum
1. _____	_____	4. _____	_____
2. _____	_____	5. _____	_____
3. _____	_____	6. _____	_____

Bei mehr als sechs Personen bitte gesondertes Blatt verwenden.

4.2 Von den vorgenannten Personen sind miteinander verheiratet:

Name, Vorname der Ehefrau	Name, Vorname des Ehemannes	Datum der Eheschließung
_____	_____	_____

4.3 Von den in der Wohnung wohnenden Personen befinden sich in einem Aus- oder Fortbildungsverhältnis:

Name, Vorname	Art der Aus- oder Fortbildung (z.B. Studium, Lehre)	Voraussichtl. Beendigung
1. _____	_____	_____
2. _____	_____	_____
3. _____	_____	_____

4.4 Von den in der Wohnung wohnenden Personen sind folgende behindert:
(Bitte fügen Sie entsprechende Nachweise bei)

Name, Vorname	Behinderungsgrad
1. _____	<input type="checkbox"/> ab 50 <input type="checkbox"/> ab 80 <input type="checkbox"/> Schwerbehinderten gleichgestellt
2. _____	<input type="checkbox"/> ab 50 <input type="checkbox"/> ab 80 <input type="checkbox"/> Schwerbehinderten gleichgestellt

Bei mehr als zwei Personen bitte gesondertes Blatt verwenden.

5. Von den in der Wohnung wohnende Personen sind betreuungsbedürftig:

5.1 wegen Krankheit:

Name, Vorname	Angaben zur Erkrankung			Name, Vorname der betreuenden Person
	Art	Beginn	Voraussichtl. Dauer	
_____	_____	_____	_____	_____

Bei mehreren Personen bitte gesondertes Blatt verwenden.

5.2 wegen Schwerbehinderung oder Hilflosigkeit:

Schwerbehindert sind Personen mit einem Behinderungsgrad von wenigstens 50, die förmlich anerkannt sind. Die Voraussetzungen bitte durch Vorlage eines Schwerbehindertenausweises oder einer Bescheinigung über die Feststellung der Behinderung nachweisen.

Hilflos sind Personen, die aufgrund eines nicht nur vorübergehenden körperlichen, geistigen oder seelischen Zustandes nicht in der Lage sind, die für die alltägliche Lebensführung notwendigen Verrichtungen selbstständig auszuführen und deshalb dauerhaft auf Betreuung angewiesen sind. Die Hilflosigkeit bitte durch behördliche oder ärztliche Bestätigung nachweisen.

Name, Vorname	Ursache der Betreuungsbedürftigkeit	Name, Vorname der betreuenden Person
1. _____	_____	_____
2. _____	_____	_____

Bei mehr als zwei Personen bitte gesondertes Blatt verwenden.

5.3 wegen berufs- oder ausbildungsbedingter Abwesenheit:

Zu betreuende Personen:

Wegen eines Beschäftigungs- oder Aus-
bildungsverhältnisses abwesende Person:

Name, Vorname _____	
1.	_____
2.	_____
3.	_____
4.	_____

Name, Vorname _____		
Art des Beschäftigungs- oder _____ Ausbildungsverhältnisses		
Voraussichtl. Ende _____		
Tägl. Dauer _____	Tage/Woche _____	Tage/ Monat _____

Bei mehr als vier Personen
bitte gesondertes Blatt verwenden.

Alle in der Wohnung wohnenden Personen sind verpflichtet, der zuständigen Stelle
Auskünfte über ihr Einkommen zu erteilen.

- Einkommenserklärungen des Mieters/der Mieterin bzw. der Mieter/innen sind
beigefügt.
- Einkommenserklärungen für alle in der Wohnung wohnenden Personen sind beigefügt.
*Die Bewohner/innen sind nicht verpflichtet, dem Mieter/der Mieterin Angaben über
ihr eigenes Einkommen zugänglich zu machen. Sie können die Erklärung auch
unmittelbar gegenüber der zuständigen Stelle abgeben.*

Die Richtigkeit aller Angaben wird versichert.

Ort _____	Datum _____	Unterschrift des/der Absenders/Absenderin _____
-----------	-------------	---