

8. Wahlperiode

31. 12. 82

Mitteilung

der Landesbeauftragten für den Datenschutz

Dritter Tätigkeitsbericht

der Landesbeauftragten für den Datenschutz

Schreiben der Landesbeauftragten für den Datenschutz vom 30. Dezember 1982 Nr. C 2310:

Anbei übersende ich Ihnen meinen dritten Tätigkeitsbericht, den ich nach § 16 Abs. 2 des Landesdatenschutzgesetzes dem Landtag von Baden-Württemberg zum 31. Dezember 1982 zu erstatten habe.

Dr. Ruth Leuze

**Dritter Tätigkeitsbericht
der
Landesbeauftragten für den Datenschutz
in Baden-Württemberg**

INHALTSVERZEICHNIS

	Seite
1. Teil: Zur Lage	8
1. Abschnitt: Reaktionen auf den 2. Tätigkeitsbericht	8
1. Allgemeine Reaktionen	8
2. Reaktionen im parlamentarischen Raum	8
3. Reaktionen der Landesregierung	8
2. Abschnitt: Änderungen des Landesdatenschutzgesetzes	10
1. Erstes Gesetz zur Änderung des Landesdatenschutzgesetzes	10
2. Entwurf eines zweiten Gesetzes zur Änderung des Landesdatenschutzgesetzes	12
3. Abschnitt: Datenschutz in Gefahr	13
1. Vom Wandel im Rechtsdenken und falsch praktiziertem Datenschutz	13
2. Ideologische Vorbehalte gegen den Datenschutz	15
3. Das Ärgernis „Unabhängige Datenschutzkontrolle“	16
4. Abschnitt: Aufgabe des Datenschutzes	16
2. Teil: Forschung	19
1. Abschnitt: Zur Situation	19
1. Entwicklung seit dem 2. Tätigkeitsbericht	19
2. Gesetzentwurf der Landesregierung zur zweiten Änderung des Landesdatenschutzgesetzes (Stand: 26. Oktober 1982)	21
2.1 Gesetzestechnik	21
2.2 Inhalt des Gesetzentwurfs und Bewertung	22
2.2.1 Datenzugang	22
2.2.2 Krankheitsdatenregister	25
2.2.3 Beseitigung der Auskunftspflicht	26
2.3 Gesetzgebungskompetenz	26
2.3.1 Privater Bereich	26
2.3.2 Berufs- und besondere Amtsgeheimnisse	26
3. Vorschläge	27
3.1 Mehr Information	27
3.2 Verstärkter Einsatz der Möglichkeiten der Anonymisierung und Aggregierung	28
3.3 Bemühen um Einwilligung	28
4. Zur Notwendigkeit neuer Gesetze	28

	Seite
2. Abschnitt: Medizinische Forschung	30
1. Studie über Morbus Crohn und Colitis ulcerosa	30
2. Krebsregister Nordbaden	30
3. Auskünfte aus Personenstandsbüchern zur Erforschung von Krankheiten des Nervensystems	32
3. Abschnitt: Sozialforschung	32
1. Erfahrungen aus den Kontrollbesuchen bei den Universitäten Konstanz und Karlsruhe	32
1.1 Beschaffung von Adreßdaten	33
1.2 Datenverarbeitung für wissenschaftliche Zwecke	34
2. Einzelne Forschungsvorhaben	35
2.1 Befragung der Technischen Lehrer im Berufsfeld Holztechnik	35
2.2 Forschungsvorhaben „Informelle Reaktionen nach Jugendstrafrecht“	36
4. Abschnitt: Archivwesen	37
1. Allgemeines	37
2. Empfehlungen zum Inhalt eines Landesarchivgesetzes	38
3. Teil: Öffentliche Sicherheit und Strafrechtspflege	39
1. Abschnitt: Verfassungsschutz	39
1. Registrierung von Auskunftersuchen der Bürger und Anfragen des Landesbeauftragten für den Datenschutz	39
2. Personenüberprüfung	41
2.1 Überprüfung von Personen mit Zugangsberechtigung zu Sicherheitsbereichen auf dem Flughafen Stuttgart	41
2.1.1 Regelung des Personenüberprüfungsverfahrens	41
2.1.2 Beurteilung des bisherigen Verfahrens	41
2.1.3 Neuregelung	42
2.1.4 Bewertung der Neuregelung	43
2.2 Überprüfung von Beschäftigten der Regionalen Rechenzentren	44
3. Eingaben	45
2. Abschnitt: Polizei	46
1. Zur Situation	47
1.1 Neue Verwaltungsvorschriften	47
1.2 Neue Dateien	47
1.2.1 Allgemeines	47
1.2.2 Datei „Landfriedensbruch und verwandte Straftaten“	48

	Seite
1.3 Vollzug datenschutzrechtlicher Vorschriften	49
1.3.1 Bereinigung der Personenauskunftsdatei und anderer kriminalpolizeilicher Sammlungen	49
1.3.2 Abweichen von Regelfristen der KpS-Richtlinien	50
1.3.3 Mißbräuchliche PAD-Abfrage	51
1.4 Verhältnis von Polizei und Datenschutz	51
2. Eingeschränkte Kontrollmöglichkeit im Bereich der Polizei	53
2.1 Generelle Kontrollen	54
2.1.1 Keine Kontrolle interner Dateien und Akten	54
2.1.2 Im Zweifel kein Prüfungseinstieg über Akten	54
2.2 Prüfung aus Anlaß von Eingaben	56
3. Prüfung der Abteilung Staatsschutz des Landeskriminalamts	58
3.1 Gegenstand der Prüfung	58
3.2 Feststellungen und Schlußfolgerung	59
4. Eingaben	62
 3. Abschnitt: Strafrechtspflege	 67
1. Registrieren von Prozeßbesuchern	67
2. Mitteilungen von Staatsanwaltschaften oder Gerichten an Empfänger von Geldauflagen	68
3. Nennung des Beschuldigten in der Einstellungsverfügung der Staatsanwaltschaft	69
4. Versendung sensibler Unterlagen durch die Justiz an den Arbeitgeber eines Scheidungswilligen	70
5. Offenbarung von Sozialdaten für Zwecke der Straf- verfolgung	70
6. Strafvollzugsstatistik	71
 4. Teil: Personalwesen	 72
1. Personalbogen	72
1.1 Inhalt der Personalbogen	72
1.2 Rückgabe der Personalbogen	73
2. Vertraulichkeit der Personalakten	74
3. Bekanntgabe von Personaldaten für Organisations- untersuchungen	74
4. Unterrichtung über Nebentätigkeiten	75
5. Bekanntgabe von Personaldaten an Personalräte	75
6. Automatisiertes Verfahren zur Unterstützung der Personalverwaltung	76
6.1 Keine Gewähr für die Vollständigkeit von Aus- wertungen	76
6.2 Sperrung und Löschung	77
7. Eingaben	77

	Seite
5. Teil: Statistik	78
1. Allgemeines zum Datenschutz beim Statistischen Landesamt	78
2. Statistikgeheimnis	79
3. Einzelne Statistiken	80
3.1 Volkszählung 1983	80
3.2 Hochschulstatistik	81
6. Teil: Kommunalwesen	83
1. Kommunalwahlrecht	83
2. Meldewesen	86
7. Teil: Sorgen der Bürger	86
1. Zur Situation	86
2. Einzelne Sorgen	87
2.1 Gesundheitswesen	87
2.2 Sozialwesen	89
2.3 Schulen und Hochschulen	92
2.4 Verkehrswesen	94
2.5 Bauwesen	96
2.6 Steuerwesen	97
2.7 Kommunalabgaben	98
2.8 Justizverwaltung	100
8. Teil: Elektronische Datenverarbeitung	100
1. Abschnitt: Möglichkeiten und Grenzen der Datenschutzkontrolle	100
1. Programmkontrolle	101
2. Kontrolle des Programmeinsatzes	102
3. Kontrolle flexibler Verfahren	102
2. Abschnitt: Erfahrungen aus der Praxis	103
1. Verfahrensentwicklung	103
1.1 Verfahrensdokumentation	103
1.2 Programmtests	104
2. Verfahrensanwendung	104
2.1 Datenerfassung	105
2.2 Kennworte	106
2.2.1 Einsatz von Kennworten	106
2.2.2 Kennworte bei polizeilichen Informationssystemen	107
2.3 Löschen und Auslagern	108
3. Archivverwaltung	109
4. Auftragsdatenverarbeitung	109
5. Dienstprogramme	110

	Seite
3. Abschnitt: Entwicklungstrends	110
1. Pflege von Programmen	111
2. Fernwartung	111
3. Reduzierung von Akten	112
4. Abschnitt: Bildschirmtext	113
1. Beschreibung von Bildschirmtext	113
2. Vorhaben der Deutschen Bundespost	114
3. Datenschutzprobleme	114
4. Zielvorstellungen des Datenschutzes	115
5. Entwurf eines Staatsvertrags über Bildschirmtext	115
Schlußbemerkung	116

1. Teil: Zur Lage

1. Abschnitt: Reaktionen auf den 2. Tätigkeitsbericht

1. Allgemeine Reaktionen

Berichte von Behörden stoßen im allgemeinen in der Öffentlichkeit nicht gerade auf gesteigertes Interesse. Das Gegenteil war bei meinem 2. Tätigkeitsbericht der Fall. Er fand ein bundesweites Echo. Viele Bürger, Organisationen, Behörden, politische Gruppen und Medien befaßten sich eingehend mit ihm.

2. Reaktionen im parlamentarischen Raum

Während die Opposition in ihren ersten Stellungnahmen den 2. Tätigkeitsbericht begrüßte, tat sich die Regierungsfraktion damit schwerer. Kaum lag der Bericht vor, sprach sie schon von Gesetzesänderungen, die zuvor bereits Polizei und Kreise der medizinischen Forschung gefordert hatten. Ihr Ziel müsse sein, „insbesondere einen sachgerechten Ausgleich zwischen den Belangen des Datenschutzes und denjenigen der medizinischen Forschung und denen der Polizei und des Datenschutzes sicherzustellen“ und eine „Klarstellung des Tätigkeitsfelds der Datenschutzbeauftragten und seiner Grenzen“ herbeizuführen (Pressemitteilung vom 12. Jan. 1982). Damit war der Startschuß für eine Auseinandersetzung gegeben, die das ganze Berichtsjahr beherrschte.

3. Reaktionen der Landesregierung

Wie sich die Landesregierung mit meinem 2. Tätigkeitsbericht auseinandersetzen würde, zeigte schon die erste Äußerung des Herrn Innenministers (Pressemitteilung Nr. 2/1982 vom 12. Jan. 1982). Er warf mir außer einem „teilweise überanstrengten Datenschutzverständnis“ vor, ich hätte mit meiner Darstellung der Einsichtnahme des Verfassungsschutzes in das Melderegister „unter Sicherheitsgesichtspunkten erforderliche Geheimhaltungsbestimmungen nicht beachtet“. Wenn ein Innenminister einen solch schwerwiegenden Vorwurf erhebt, müßte man eigentlich erwarten, daß er daraus dienst- und strafrechtliche Konsequenzen zieht oder aber den Vorwurf zurücknimmt. Nichts dergleichen geschah. Der Vorwurf steht bis heute im Raum, obwohl das Innenministerium sehr wohl weiß, daß er absolut ungerechtfertigt ist.

Diesem wenig verheißungsvollen Auftakt folgte die nicht minder enttäuschende offizielle Stellungnahme der Landesregierung vom März 1982. Ich erwartete nicht, daß sie sich in vollem Umfang meinen Rechtsauffassungen anschließt und allen meinen Vorschläge und Empfehlungen folgt. Ich nahm aber an, die Ministerien würden sich sachlich und fair mit meinem Tätigkeitsbericht auseinandersetzen, die Probleme nicht verharmlosen, den aktuellen Stand der datenschutzrechtlichen Diskussion berücksichtigen und die Sachverhalte korrekt wiedergeben. Diese Erwartung erfüllte sich nicht. Ganz offensichtlich behielt ihr Bestreben, rechtzubehalten und den Datenschutz soweit es irgend geht zurückzudrängen, die Oberhand vor allen anderen Überlegungen. Zum Beleg dafür mögen einige Beispiele dienen:

- Die Landesregierung schließt sich zwar in ihren grundsätzlichen Bemerkungen zur Forschung meiner Auffassung an, § 20 LDSC erlaube nicht, ohne Einwilligung der Patienten Krankheitsdatenregister zu reinen Forschungszwecken anzulegen und zu führen. Sie sieht darin jedoch lediglich eine Gesetzeslücke, die

- es alsbald zu schließen gilt. Kein Wort fand sie für die besondere Problematik solcher Register und deren besondere Gefahren. Statt dessen behauptet sie wahrheitswidrig, auf Bundesebene bestünden ähnliche Bestrebungen zur Legalisierung von Krankheitsdatenregistern. Verschwiegen wird, daß das Bundesgesundheitsministerium in der Gesundheitsministerkonferenz nur ein — dort zudem umstrittenes — Muster eines Krebsregistergesetzes der Länder zur Diskussion stellte und bewußt davon absah, generelle Regelungen für Krankheitsdatenregister vorzuschlagen.
- Das Wissenschaftsministerium setzt sich im Bestreben, die von mir kritisierten Praktiken auf dem Gebiet der medizinischen Forschung selbst um den Preis juristischer Glaubwürdigkeit zu rechtfertigen, souverän über den klaren Wortlaut der ärztlichen Berufsordnung und die Äußerungen in der arzt- und datenschutzrechtlichen Literatur hinweg und verneint selbst dann eine Verletzung der ärztlichen Schweigepflicht, wenn ein behandelnder Arzt Daten seiner Patienten ohne deren Wissen unter vollem Namen und vollständiger Adresse an ein Krankheitsdatenregister bei einer anderen Einrichtung weitergibt. Offenbar traut das Wissenschaftsministerium inzwischen dieser These selbst nicht mehr. Denn ein Kernpunkt des Entwurfs eines 2. Gesetzes zur Änderung des Landesdatenschutzgesetzes ist die Regelung, wonach Patientendaten ohne Einwilligung an forschende Einrichtungen weitergegeben werden können. Nach der bisherigen Rechtsauffassung des Wissenschaftsministeriums wäre eine solche Vorschrift eigentlich überflüssig.
 - Während noch im Juni 1982 das Innenministerium als Aufsichtsbehörde für den Datenschutz im privaten Bereich die Datenspeicherung des Krebsverbands Baden-Württemberg für Zwecke seines Krebsregisters als unzulässig bezeichnete und dabei vor allem betonte, § 36 BDSG sei keine Erlaubnisvorschrift für die Speicherung personenbezogener Daten zu Forschungszwecken, behauptet es in der Stellungnahme der Landesregierung ohne jede Begründung das Gegenteil und führt aus, die Speicherung der Daten beim Krebsverband sei nach § 36 BDSG zulässig.
 - In meinem 2. Tätigkeitsbericht hatte ich ausgeführt, einige Polizeidienststellen hätten zur Feststellung der Glaubwürdigkeit kindlicher/jugendlicher Zeugen einen in meinen Augen bedenklichen Fragebogen verwendet, und die Kriminalpolizei hätte sofort ihre Bereitschaft erklärt, künftig auf solche Fragebogen zu verzichten. Um ja jeden Anschein zu vermeiden, die Kriminalpolizei habe aufgrund einer Intervention des Landesbeauftragten für den Datenschutz eine bedenkliche Praxis aufgegeben, behauptet das Innenministerium in der Stellungnahme, die Kriminalpolizei habe auf den Einsatz des Fragebogens bereits verzichtet, bevor ich die Angelegenheit aufgegriffen hätte. Wahr ist, daß ich mich mit Schreiben vom 10. Okt. 1980 an das Landeskriminalamt wandte und sich die Polizei erst in einer Dienstbesprechung am 14./15. Jan. 1981 darauf verständigte, auf den Fragebogen zu verzichten, weil er für ihre Arbeit nicht erforderlich sei. Dieser Einzelfall ist für sich gesehen sicherlich nicht von besonderer Bedeutung. Er ist aber typisch für die Art und Weise, wie versucht wird, die Ausführungen im 2. Tätigkeitsbericht zu entkräften und zu relativieren.
 - Geradezu ein Musterfall für die Vorgehens- und Argumentationsweise der Landesregierung ist ihre Auseinandersetzung mit meiner Forderung, dem Bediensteten vor Ort einfache, verständliche, auf seine konkrete Tätigkeit zugeschnittene Erläu-

terungen zu geben. Sie behauptet, die Anwendung solcher Vorschriften setze eine Klärung und Erläuterung von Grundbegriffen und Grundfragen des Datenschutzes durch eine allgemeine Verwaltungsvorschrift zum Landesdatenschutzgesetz voraus, an deren Ausarbeitung ich bisher meine Mitarbeit verweigert habe. Auch diese Aussage ist falsch. Richtig ist, daß mir das Innenministerium im Juni 1981 ebenso wie den anderen Ministerien ein vorläufiges Verzeichnis des Regelungsinhalts allgemeiner Verwaltungsvorschriften zur Stellungnahme zuleitete. Diese Stellungnahme gab ich ab. Dabei vertrat ich u. a. die Auffassung, man solle mit dem Erlaß solcher Vorschriften aus einer Reihe von Gründen zuwarten. Dies sei vertretbar, weil die Bekanntmachung des Innenministeriums über den Vollzug der Datenschutzregisterverordnung vom 4. Febr. 1981 (GABl. S. 153) zu den dringendsten allgemeinen Fragen bereits Klarstellungen gebracht habe. Von einer Verweigerung kann also keine Rede sein. Im übrigen hörte ich bis heute vom Innenministerium in dieser Angelegenheit nicht mehr das geringste.

Diese Einwände gegen die Stellungnahme der Landesregierung teilte ich dem Herrn Ministerpräsidenten mit. Das Staatsministerium ließ mich dazu wissen, es habe die berührten Ressorts hiervon unterrichtet.

2. Abschnitt: Änderungen des Landesdatenschutzgesetzes

1. Erstes Gesetz zur Änderung des Landesdatenschutzgesetzes

Die Regierungsfraktion wartete die Beratungen meines 2. Tätigkeitsberichts nicht ab. Bereits im März 1982 brachte sie den Entwurf eines 1. Gesetzes zur Änderung des Landesdatenschutzgesetzes ein und zog die parlamentarischen Beratungen in bemerkenswerter Eile durch. Dieses Änderungsgesetz ist ein empfindlicher Rückschlag für den Datenschutz:

- Es entläßt die datenspeichernden Behörden aus jeder Verantwortung für die Zulässigkeit einer Datenübermittlung an andere Behörden. Praktisch ermöglicht es damit im Anwendungsbereich des Landesdatenschutzgesetzes einen unbegrenzten Datenaustausch unter Behörden.
- Es beschränkt die Kontrollbefugnis des Landesbeauftragten für den Datenschutz im Bereich der „anderen Vorschriften über den Datenschutz“ auf Vorgänge in Dateien. Die „anderen Vorschriften über den Datenschutz“ gelten aber durchweg auch, wenn die Daten nicht in einer Datei gespeichert sind. Deshalb ist dem Landesbeauftragten für den Datenschutz deren Kontrolle nur noch möglich, wenn eine Datenspeicherung in einer Datei stattfindet. Diese Neuregelung gefährdet die Einhaltung der sonstigen Datenschutzvorschriften und beeinträchtigt den Datenschutz in den Augen der Bürger.
- Es gestattet den Ministerien, zur Wahrung „übergeordneter Gesichtspunkte“ einer anderen als der speichernden Stelle die Aufgabe zu übertragen, dem Bürger Auskunft über seine gespeicherten Daten zu geben. Machen die Ministerien von dieser Ermächtigung Gebrauch, führt dies zu unnötigen Datenübermittlungen. Zugleich sprechen sie damit den betroffenen Behörden die Fähigkeit ab, „übergeordnete Gesichtspunkte“ zu berücksichtigen.
- Es privilegiert die Polizei gegenüber allen übrigen Behörden bei der Meldung zum Datenschutzregister. Sie muß nur noch

automatisierte Dateien melden, die anderen Behörden dagegen auch manuell geführte Dateien. Einen sachlichen Grund dafür gibt es nicht.

Niemand wird behaupten, das Landesdatenschutzgesetz von 1980 sei der Weisheit letzter Schluß und niemand will der Regierungsfraktion das Recht absprechen, Änderungen vorzuschlagen und durchzusetzen, die sie für richtig hält. Nicht enttäuschte vor allem die Art und Weise, wie die Regierungsfraktion in der Öffentlichkeit und gegenüber einzelnen Bürgern ihre dem Datenschutz abträgliche Gesetzesinitiative begründete, und wie wenig sie bereit war, sich mit Gegenargumenten auseinanderzusetzen. Anstatt ihre Gründe klar zu sagen, segelte die Gesetzesinitiative von Anfang an unter der Flagge „Klarstellung“. Unter Klarstellung versteht man im allgemeinen das Herstellen eines ursprünglich gewollten, aber im Gesetz nicht hinreichend deutlich zum Ausdruck gekommenen Zustands. Dies läßt sich von der Gesetzesnovelle sicherlich nicht behaupten. Sie schreibt zum Beispiel in der Übermittlungsvorschrift des § 10 Abs. 1 LDSG eine extrem datenschutzfeindliche Position fest, die zuvor noch keine Seite vertreten hat. Nichts anderes gilt für die neue Umschreibung der Kontrollbefugnis des Landesbeauftragten für den Datenschutz. Hier wurde eine in Bund und Ländern kontrovers diskutierte Frage einseitig zu Gunsten der keineswegs in den eigenen Reihen unangefochtenen Auffassung der Landesregierung zementiert.

Welche Argumente die Regierungsfraktion verwandte, zeigte folgender Auszug aus einem ihrer Schreiben vom Frühjahr 1982 an einen mir persönlich nicht bekannten Bürger unseres Landes:

„Inhaltlich treffen die Presseinformationen, auf die Sie sich stützen, nicht zu. Mit dem von uns eingebrachten Gesetzentwurf werden die Kontrollkompetenzen der Datenschutzbeauftragten nicht eingeschränkt. Das Datenschutzrecht stellt eine neue Materie dar, mit der erst Erfahrungen gewonnen werden müssen. Baden-Württemberg war eines der ersten Länder, das ein Datenschutzgesetz geschaffen hat. Es hat sich damals weitgehend an das Bundesgesetz angelehnt. Die ersten praktischen Erfahrungen mit unserem Gesetz haben gezeigt, daß das Gesetz in einigen Punkten so formuliert war, daß es Auslegungsschwierigkeiten gegeben hat — und zwar trotz weitgehend gleicher Formulierung in Bund und Ländern nur bei uns in Baden-Württemberg. In den anderen Ländern und beim Bund haben sich offensichtlich die Datenschutzbeauftragten mit den Regierungen einigen können. Dort wird das Gesetz so praktiziert, wie es nach Auffassung unserer Regierung und nach Auffassung des Landtags auszulegen ist. Die Datenschutzbeauftragte des Landes Baden-Württemberg vermochte sich jedoch dieser Auslegung nicht anzuschließen.“

An diesen Ausführungen ist nahezu alles falsch:

- Baden-Württemberg war nicht eines der ersten, sondern das vorletzte Bundesland, das ein Datenschutzgesetz erließ. Die unterschiedlichen Rechtsauffassungen über den Umfang der Kontrollkompetenz der Datenschutzbeauftragten waren bei Erlaß des Landesdatenschutzgesetzes bereits bekannt.
- Es existieren keine Auslegungsprobleme, die nur in Baden-Württemberg auftraten.
- Keine Rede kann davon sein, im Bund und in den anderen Ländern hätten sich die Datenschutzbeauftragten mit den Regierungen auf eine Praxis geeinigt, die der Auffassung der Landesregierung von Baden-Württemberg entspricht. Im Gegenteil: Zwar gibt es auch dort unterschiedliche Rechtsauffassungen über den Umfang der Kontrollzuständigkeit der Datenschutzbeauftragten. Doch wird in der Verwaltungspraxis fast überall entsprechend meiner Rechtsauffassung verfahren. In-

soweit kann man tatsächlich von einer Einigung zwischen den Datenschutzbeauftragten und den Regierungen sprechen.

- Falsch und besonders diskriminierend ist daher auch die Behauptung, allein die Datenschutzbeauftragte des Landes Baden-Württemberg habe sich dieser Auslegung nicht anschließen vermocht.

Als ich von diesem Vorgang erfuhr, wandte ich mich an die Regierungsfraktion. Sie antwortete mir auf mein Schreiben nicht.

Mit fast denselben Argumenten wie sie verteidigte das Innenministerium in Schreiben an Bürger die vorgenommene Änderung des Landesdatenschutzgesetzes. Auch hier wird behauptet, die Landesbeauftragte für den Datenschutz habe Kompetenzen für sich in Anspruch genommen, die sie noch nie besessen habe. Die im Gesetz festgeschriebene Rechtsauffassung werde von Bund und den übrigen Bundesländern geteilt. Auch hier findet sich kein Wort von der überwiegend gegenteiligen Verwaltungspraxis im Bund und in den meisten Bundesländern. Kein Wort verliert es, daß beispielsweise das Bayerische Staatsministerium des Innern seit eh und je die vom Bundes- und den Landesbeauftragten für den Datenschutz vertretene Rechtsauffassung zum Umfang ihrer Kontrollkompetenz teilt. Diese Argumentationskette gipfelt in folgendem Satz aus einem Schreiben des Innenministeriums vom Herbst 1982: „Es ist meine Überzeugung, daß die Änderung des Datenschutzgesetzes bei wohlverstandener Würdigung beim Bürger nicht zur weiteren Staatsverdrossenheit beiträgt, sondern im Gegenteil das Vertrauen in die rechtsstaatliche Ordnung und die bürgerfreundliche Verwaltung im Land stärkt.“ So sah es der Empfänger des Briefes nicht.

2. Entwurf eines 2. Gesetzes zur Änderung des Landesdatenschutzgesetzes

Die weitere Forderung der Regierungsfraktion, das Landesdatenschutzgesetz zu Gunsten der Forschung zu ändern, ist noch nicht vollzogen. Die Landesregierung erklärte vor kurzem, sie wolle den Gesetzentwurf Anfang 1983 im Landtag einbringen. Im Rahmen seiner Ausarbeitung machte ich zwei Beobachtungen, die typisch für die herrschende Einstellung im Lande zum Datenschutz sind. Zum einen bemühten sich die Ministerien nach Kräften, mich beim Ausarbeiten des Gesetzentwurfs auszuschalten und den Landesbeauftragten für den Datenschutz als einen von vielen Interessenvertretern zu behandeln. Zum anderen tendieren Regierung und Fraktion zur Radikallösung. Man will mit dem berühmten Federstrich des Gesetzgebers die rechtswidrige Praxis bei der Datenweitergabe und -speicherung nachträglich legalisieren, die meine Kontrolltätigkeit im wesentlichen aufdeckte. Ich frage mich, ob die Befürworter dieser Pläne die ganze Tragweite einer solchen Legalisierung rechtswidriger Zustände bedachten. Im vergangenen Jahr wiesen gerade führende Vertreter des Landes Baden-Württemberg auf das schwindende Rechtsbewußtsein in der Bevölkerung, die Bedeutung der Bindung an das Recht und dessen friedensstiftende Funktion für unser Gemeinwesen hin und warnten vor einer nachträglichen Legalisierung rechtswidriger Zustände. Diese Warnungen bezogen sich auf Rechtsverstöße auf ganz anderen Gebieten. Müssen diese Überlegungen nicht für unser Recht insgesamt gelten? Ich meine, wer das schwindende Rechtsbewußtsein in der Bevölkerung beklagt, darf nicht übersehen, daß diese Entwicklung auch in der öffentlichen Verwaltung spürbar ist. Auch die öffentliche Verwaltung sollte sich wieder stärker auf ihre ver-

fassungsrechtliche Bindung an Gesetz und Recht besinnen. Die Sache wäre es wert, diesen Gedanken nachzugehen, ehe sich der Gesetzgeber entschließt, gesetzwidrige Praktiken der Verwaltung zu legalisieren.

3. Abschnitt: Datenschutz in Gefahr

Der Datenschutz ist in großer Gefahr. Daran kann niemand zweifeln, der die geschilderten Reaktionen auf meinen 2. Tätigkeitsbericht und die Gesetzesinitiativen zum Abbau des Datenschutzes bedenkt. Gewiß nimmt Baden-Württemberg damit eine unrühmliche Spitzenposition ein. Dies darf aber nicht den Blick dafür trüben, daß dem Datenschutz auch andernorts der Wind ins Gesicht bläst. Längst vorbei sind die Zeiten, da alle politischen Kräfte in den Parlamenten Vorschriften des Datenschutzes einmütig beschlossen. Bekenntnisse zum Datenschutz sind rar geworden. Häufig ist nur noch vom „recht verstandenen Datenschutz“ die Rede. Dahinter verbirgt sich meist ein sehr reduzierter Persönlichkeitsschutz. Für diese Entwicklung gibt es eine Reihe von Gründen. Wer sich ihnen entgegenstellen will, muß sie kennen und damit auseinandersetzen.

1. Vom Wandel im Rechtsdenken und falsch praktiziertem Datenschutz

Beim Erlaß der Datenschutzgesetze in der zweiten Hälfte der sechziger Jahre waren sich viele, die diese Gesetze beschlossen, und viele, die sie anwenden, über deren tatsächliche Konsequenzen nicht im klaren. Erst allmählich bemerkten sie: Das Datenschutzgesetz ist nicht eines von vielen Gesetzen, das man zur Kenntnis nimmt und mehr schlecht als recht beachtet, sondern ein Gesetz, das Auswirkungen zeitigt und zu neuen Überlegungen nötigt. Diese Tatsache ist eine der wichtigsten Ursachen der jetzigen Situation. Gewiß hatte die Verwaltung schon vor Erlaß der Datenschutzgesetze Erfahrung mit einer Reihe besonderer Geheimhaltungsbestimmungen. Manche hielt sie — zum Beispiel das Steuergeheimnis — auch sehr genau ein. Bei anderen — zum Beispiel der allgemeinen Verschwiegenheitspflicht der Beamten — nahm und nimmt sie es nicht so genau. All diese Regelungen aber betreffen nur Teilaspekte der Informationsverarbeitung in Teilbereichen des Lebens. Das Neue an den allgemeinen Datenschutzgesetzen war, daß sie generell, also für alle Lebensbereiche gelten und alle Arten persönlicher Daten in ihren Schutz einbeziehen. Ihr Grundsatz, daß jede Phase der Datenverarbeitung einer gesetzlichen Legitimation oder des Einverständnisses des betroffenen Bürgers bedarf, ist in meinen Augen eine der bedeutendsten Entscheidungen des Gesetzgebers. Dieser Grundsatz entspricht ganz sicherlich nicht dem traditionellen Rechtsverständnis der Verwaltung. Es besagte: die öffentliche Hand braucht nur für Maßnahmen eine Rechtsgrundlage, die dem Bürger ein bestimmtes Tun, Dulden oder Unterlassen abverlangen und gegen die er mit den traditionellen Rechtsmitteln vorgehen kann. Weil die Verwaltung damit rechnen mußte, bemühte sie sich, insoweit dem geltenden Recht zu entsprechen. Ganz anders war ihre Betrachtungsweise beim Sammeln, Aufbewahren und Weitergeben von Informationen über einzelne Personen. Darin sah sie überwiegend nur tatsächliches Handeln, das im Regelfall die Rechtsstellung des betroffenen Bürgers nicht berührt. Deswegen fühlt sie sich dabei auch weitgehend frei. Genau in diesem Punkt brachten die allgemeinen Datenschutzgesetze dann unter dem Einfluß der Rechtsprechung des Bundesverfassungsgerichts zum allgemeinen Persönlichkeitsrecht eine grundle-

gende Wende. Plötzlich war es nicht mehr zulässig, innerhalb der Verwaltung Daten frei fließen zu lassen. Plötzlich mußte man bei der Weitergabe von Daten an Private überlegen, ob dies schutzwürdige Belange von Bürgern beeinträchtigen konnte. Plötzlich war es nicht mehr bloß eine Frage der Zweckmäßigkeit sondern auch des Rechts, ob bestimmte Daten benötigt und deshalb aufbewahrt werden dürfen oder nicht. Daß es dabei zu Friktionen kam, war nahezu unvermeidlich. Der hohe Abstraktionsgrad der Datenschutzgesetze tat sein übriges. Er erschwerte ihr Verständnis sehr und bereitete der Verwaltungspraxis ganz erhebliche Schwierigkeiten. In dieser Situation hätte es klarer Vorgaben bedurft. Die verantwortlichen Ministerien ließen aber die Behörden vor Ort im eigenen Saft schmoren, anstatt ihnen konkrete Hilfen an die Hand zu geben und damit ihre Arbeit zu erleichtern. Das Resultat war verheerend. Zum Teil kam es zu haarsträubenden Interpretationen der Datenschutzgesetze. Sie trieben Behörden, welche bestimmte Daten zu Recht für sich beanspruchten, verständlicherweise auf die Barrikaden. Solche Fehlinterpretationen leisteten sich keineswegs nur Stellen, die mit geringer Verwaltungskraft ausgestattet sind. Überraschenderweise kommen sie auch bei Verwaltungen bis hinauf zu den Ministerien vor, die eigentlich in der Lage sein sollten, Gesetze zu interpretieren. Ganz offensichtlich ist diese Kunst — aus welchen Gründen auch immer — im Schwinden begriffen. Eine große Rolle spielt dabei sicherlich folgender Umstand: Manche Mitarbeiter der Verwaltung sind heute noch so der herkömmlichen Denkweise verhaftet, daß sie die möglichen Auswirkungen einer Informationsverarbeitung auf die Persönlichkeitssphäre des Bürgers nicht bedenken. Sie betrachten deshalb die Datenschutzgesetze als unnötiges Beiwerk, das ihnen die Arbeit erschwert und sich nicht näher anzuschauen lohnt. Für viele Behörden waren die Datenschutzgesetze auch eine willkommene Gelegenheit, berechnete Informationswünsche abzublocken. Sie kalkultierten die weit verbreitete Unsicherheit teils bewußt ein und beriefen sich auf das Schlagwort Datenschutz, obwohl sie in Wirklichkeit die Information aus ganz anderen Motiven verweigerten. Häufig waren dies finanzielle Überlegungen oder der entstehende Arbeitsaufwand. Weil man dies aber nicht sagen wollte, machte man lieber den Datenschutz verantwortlich.

All diese Umstände führten zu zum Teil durchaus verständlichem Unmut und Vorbehalt gegenüber dem Datenschutz als solchem. Anstatt nun aber durch mehr Information, also konkrete Hilfen sicherzustellen, daß die Verwaltung das Landesdatenschutzgesetz richtig anwendet, lenkten die verantwortlichen Behörden den entstandenen Unmut bewußt auf das Landesdatenschutzgesetz mit den bekannten Folgen. Sie stellten Politikern die angeblich schlimmen Folgen des Gesetzes in den schwärzesten Farben anhand von Fällen dar, die samt und sonders allenfalls ein Beweis für die unrichtige Anwendung des Gesetzes und damit für die mangelnde Qualität der Verwaltung sind, nicht aber für die Schädlichkeit des Datenschutzgesetzes. Dies zeigte sich besonders deutlich während der parlamentarischen Beratungen des Entwurfs eines 1. Gesetzes zur Änderung des Landesdatenschutzgesetzes. Die Regierungsfraktion begründete zum Beispiel die Notwendigkeit, die Übermittlungsvorschrift des § 10 Abs. 1 LDSG vornehmlich im Interesse der Polizei zu ändern, ausschließlich mit Beispielen, denen eine unrichtige Anwendung dieser Vorschrift zugrunde lag. Vor allem wäre es Aufgabe des Innenministeriums, des für den Datenschutz federführenden Ressorts gewesen, für eine korrekte Information der Parlamentarier zu sorgen, die naturgemäß mit den Besonderheiten des Datenschutzrechts nicht vertraut sind. Dies geschah bedauerlicherweise nicht. Das Fachministerium für die Polizei behielt die Oberhand; der Datenschutz blieb zweiter Sieger.

2. Ideologische Vorbehalte gegen den Datenschutz

Der beschriebene Ärger mit dem unmittelbaren Vollzug des Datenschutzes reicht nicht aus, um die gegenwärtige Stimmung innerhalb der Verwaltung zu erklären. Seit geraumer Zeit sind hier und auch im politischen Raum, den die Verwaltung mit Argumenten unterstützt, konservative Strömungen zu beobachten, die den Datenschutz grundsätzlich in Frage stellen. Diese Strömung fand meines Wissens bislang ihren unmittelbarsten Ausdruck in der Stellungnahme des Wissenschaftsministeriums zum Referentenentwurf eines Gesetzes zur Änderung des Bundesdatenschutzgesetzes. Sie greift zunächst einmal die Grundentscheidung der allgemeinen Datenschutzgesetze an, daß jede Phase der Datenverarbeitung einer gesetzlichen Grundlage oder des Einverständnisses des Bürgers bedarf. Darin sieht das Ministerium eine Überbetonung des individuellen Rechtsstatus, der die Vorstellung suggeriere, „daß insbesondere Behörden und öffentliche Stellen Personendaten typischerweise eher zu Lasten als zu Nutzen des Betroffenen verwenden und auch ein wirksamer Rechtsschutz nicht gewährleistet sei.“ Die Bindung der Informationsweitergabe an die Erlaubnis durch eine Rechtsvorschrift führe „bei Gesellschaftsbereichen, bei denen ungehinderter Datenzugang und verantwortungsvolle Datenverwendung in der Natur der Sache liegen (Forschung, Statistik), zu von vornherein überflüssigen Problematisierungen.“ Gerade dieser Aussage kommt besondere Bedeutung zu. Schließlich ist vor allem das Wissenschaftsministerium wesentlich an der Erarbeitung des Gesetzentwurfs zur 2. Änderung des Landesdatenschutzgesetzes beteiligt, der die Forschung weitgehend freistellen will von der Einhaltung datenschutzrechtlicher Bestimmungen. Für das Wissenschaftsministerium ist es also eine unnötige Problematisierung, wenn man die Frage nach dem Verhältnis von Datenschutz und Forschung überhaupt aufgreift. Seinen Höhepunkt findet diese Polemik gegen den Datenschutz in der Aussage, die Datenschutzgesetzgebung gehöre möglicherweise zu jenen mißglückten Gesetzen, die zum Teil zurückzuführen sind „auf den Einfluß von Ideologien, deren theoretischer Gehalt nicht hinreichend realadäquat (lebens- und praxisnah) ist“. Schließlich behauptet das Ministerium noch, man könne von einem Datenschutzbedürfnis der Allgemeinheit allenfalls insoweit sprechen, als es ihr interessierte Seiten mit Erfolg aufdrängen“. Bei der Datenschutzgesetzgebung werde auf vielen Strecken nicht Bedarfsdeckung, sondern Bedarfsweckung betrieben.

Diese Ausführungen bauen letztlich auf der Position des ach so anständigen Menschen auf, der nichts zu verbergen hat und deshalb keinen Datenschutz braucht. Diese These vertreten vor allem Leute, die das Glück und das Geschick haben, auf der Sonnenseite des Lebens zu stehen, und auf Grund ihrer Stellung oder Verbindungen in der Lage sind, alle erdenklichen Vorteile für sich auszunutzen. Bohrt man in solchen Fällen etwas nach, dann treten häufig sehr einseitige, von wenig Sachkenntnis getrübe Vorstellungen über den Datenschutz zutage. Oft verengt sich das Thema Datenschutz auf Teilbereiche, insbesondere auf das Verhältnis von Datenschutz und Polizei. Dabei fallen dann Schlagworte wie „der Datenschutz privilegiert Rechtsbrecher“. In anderen Bereichen ist der Wunsch nach absoluter Transparenz bei weitem nicht so stark ausgeprägt. Insbesondere findet das Steuergeheimnis in diesen Kreisen glühende Verfechter. Überhaupt ist es ein sehr interessantes Phänomen, daß das Steuergeheimnis praktisch alle akzeptieren, während beispielsweise das Sozialgeheimnis sehr starken Angriffen ausgesetzt ist. Die selbstgerechten Absagen an den Datenschutz übersehen die zahlreichen Mißbrauchsmöglichkeiten und die Möglichkeiten der Verwendung von für bestimmte Zwecke er-

hobenen Daten zu ganz anderen Zwecken, die auch der „anständige Bürger“ nicht immer wünscht. Sie bedenken auch nicht, daß die Schutzbedürftigkeit manchmal schneller eintreten kann als man glaubt. Niemand ist vor Problemen und Schwierigkeiten im persönlichen Bereich geschützt, die er nicht auf dem offenen Markte ausgetragen sehen will. Schließlich aber erscheint mir ein weiterer Gesichtspunkt von Bedeutung. Die These, der „anständige Bürger“ brauche keinen Datenschutz, macht diesen sozusagen zum Maß aller Dinge. Personen, die dieser — von wem auch immer festgestellten — Norm nicht entsprechen, werden damit schutz- und rechtlos gestellt. Außenseiter und Randgruppen, Gefährdete und Gestrauchelte usw. drückt man damit an den Rand. Die Möglichkeit zu individuellem Rollenverhalten wird über Gebühr eingeschränkt. Diese Vorstellung von einer Gesellschaft hatten sicher die Schöpfer unseres Grundgesetzes nicht vor Augen.

3. Das Ärgernis „Unabhängige Datenschutzkontrolle“

Vielleicht noch mehr als das materielle Datenschutzrecht und seine Auswirkungen fordert die unabhängige Datenschutzkontrolle die Verwaltung zu Abwehrreaktionen heraus. Allein schon die Tatsache, daß diese Institution außerhalb der üblichen Verwaltungshierarchie steht, verursacht Irritationen. Die Ministerien sinnieren und trachten deshalb ständig, den Einfluß dieser Institution, auf die sie selbst keinen Einfluß haben, möglichst klein zu halten. Wenn man schon mit ihr leben muß, soll ihr Aktionsradius wenigstens auf das Mindestmaß beschränkt bleiben. Dies ist der eigentliche Grund, warum sich die Ministerien und in ihrem Gefolge zum Beispiel auch das Landeskriminalamt seit meinem Amtsantritt bemühen, meine Zuständigkeit so restriktiv wie irgend möglich festzulegen. Unbequem und lästig ist die unabhängige Datenschutzkontrolle aber auch aus einem anderen Grund. Sie arbeitet unabhängig von den üblich gewordenen Opportunitätsüberlegungen. Sie führten in der Vergangenheit dazu, daß eine Reihe besonderer Geheimhaltungsvorschriften in bestimmten Bereichen kaum mehr Wirkung entfalteten. Verstößen ging man allenfalls dann nach, wenn eine konkrete Beschwerde vorlag. Solche aber kamen nur höchst selten vor aus dem einfachen Grund, weil der betroffene Bürger von den Informationsvorgängen nichts erfährt. Mit der Datenschutzkontrolle entstand eine Institution, die von sich aus ohne konkreten Anlaß das Behördenhandeln überprüft, die Verstöße nicht unter den Teppich kehrt, sondern aufdeckt und sie beim Namen nennt. Jahrelang geübte Verhaltensweisen, über deren Rechtmäßigkeit man sich zuvor wenig Gedanken machte, werden in Frage gestellt. Die Verwaltung ist gezwungen, sich für Arbeitsweisen zu rechtfertigen, die sie schon immer hatte. Genau dies kann sie offenbar nur schwer ertragen. Dieser Last will sie sich deshalb nach Möglichkeit entledigen.

4. Abschnitt: Aufgabe des Datenschutzes

Wegen dieser vielfältigen Bedrohungen des Datenschutzes genügt nicht, wie ein Kaninchen auf die Schlange zu starren und darauf zu warten, wie sie reagiert. Gerade in schwieriger Lage ist es wichtig, das Anliegen und die Ziele des Datenschutzes offensiv zu vertreten. Am besten geschieht dies durch eine noch stärkere Information der breiten Öffentlichkeit darüber, was der Datenschutz eigentlich will. Worum geht es? Der Mensch lebt nicht isoliert für sich auf der Welt, sondern ist Mitglied einer Gemeinschaft. Er hat freiwillig und unfreiwillig Kontakte mit anderen Menschen und Stellen. Er teilt diesen Informationen über sich mit und holt Informationen über andere ein. Sozusagen von der Wiege bis zur Bahre werden Informationen abge-

fragt, gesammelt und ausgewertet. Je arbeitsteiliger und damit auch komplizierter unser Leben wird, desto häufiger geschieht dies. Die modernen Kommunikations- und Informationsmittel, vor allem die Computer, tun ein übriges dazu, diese Entwicklung rasant zu beschleunigen. Das Registrieren beginnt bereits mit der Geburt im Krankenhaus und setzt sich fort im Standesamt und der Meldebehörde. Von diesem Zeitpunkt an hinterläßt nahezu jeder soziale Kontakt mit anderen Personen und Stellen Spuren. Schon im Kindergarten werden Karteien geführt, die Familienverhältnisse erfragt und gespeichert. Die Entwicklung setzt sich fort in Schule, Ausbildung und im Beruf. Schon bei der Geburt setzt das ein, was den Menschen in unserem Wirtschaftssystem zeitlebens begleiten wird: die — wie es der Württ. Sparkassen- und Giroverband mir gegenüber sehr vornehm und zurückhaltend umschrieben hat — „Umwerbung und akquisitorische Betreuung“ durch die Wirtschaft. Schon zu diesem Zeitpunkt interessieren sich Wirtschaftsunternehmen für die Daten von Kindern, um Werbung zu treiben, und bemühen sich, diese von Krankenhäusern und Standesämtern zu erhalten. Schon hier wird ein Phänomen erkennbar, das uns später auf Schritt und Tritt begleitet. Ich meine den Umstand, daß die Daten, die eine bestimmte Stelle zur Erfüllung ihrer Aufgaben sammelte, auch andere Stellen und Personen wünschen, an die der einzelne Bürger bei der Datenabgabe nicht im Traume dachte. Die Zahl der Stellen und Bereiche, für die Angaben über einzelne Personen gesammelt werden, läßt sich beliebig steigern:

- Man denke nur an die vielen statistischen Erhebungen, die Parlament, Regierung und Verwaltung die Möglichkeit geben sollen, die gesellschaftlichen und wirtschaftlichen Entwicklungen zu verfolgen und Grundlagen für Entscheidungen und Planungen zu erhalten. Die 1982 angelaufene Volkszählung mit ihren zahlreichen Fragen zur Person, über die Wohnverhältnisse und sonstigen Lebensumstände ist ein besonders herausragendes Beispiel für den Bedarf an Informationen, der für unsere Gesellschaft geradezu typisch ist. An dieser Volkszählung zeigt sich aber auch für jeden einsehbar das Schutzbedürfnis des einzelnen und sein Interesse daran, daß solche Angaben nicht auch zum Beispiel für steuerliche Zwecke oder sonstige Maßnahmen der Verwaltung gegen ihn verwendet oder gar Privaten zur Verfügung gestellt werden.
- In großem Umfang werden auch Daten im Arbeitsleben gesammelt. Der Arbeitgeber muß allein schon deshalb zahlreiche Angaben über den einzelnen Arbeitnehmer aufzeichnen, weil er sie zur Erfüllung gesetzlich festgelegter Mitteilungspflichten gegenüber Krankenkassen, Berufsgenossenschaften, Rentenversicherungen, Arbeitsamt, Finanzamt, Gewerbeaufsichtsamt, Gesundheitsamt, Industrie- und Handelskammer, Handwerkskammer benötigt. Dazu kommen selbstverständlich noch die Angaben, die der Arbeitgeber in seinem eigenen Interesse erhebt, etwa um das Unternehmen möglichst rentabel und effektiv zu führen. Es liegt auf der Hand, daß bei dieser Datenerhebung die Interessen der Arbeitnehmer zumindest teilweise entgegengesetzt sind. Gerade im Bereich des Arbeitslebens bedeutet in besonderem Maße Wissen Macht. Je mehr der Arbeitgeber über seine Mitarbeiter weiß, desto größer ist die Möglichkeit der Kontrolle und der Verfügbarkeit über den Arbeitnehmer. Schließlich zeigt sich hier eine weitere Gefahr der Datenverarbeitung. Daten, die der Arbeitgeber im Interesse des Arbeitnehmers für einen ganz bestimmten Zweck sammelte, können, wenn der Arbeitgeber sie zu einem anderen Zweck verwendet, zu erheblichen Nachteilen für den Arbeitnehmer führen. So können zum Beispiel arbeitsmedizinische Aussagen über die Eignung eines Arbeitnehmers für einen be-

stimmten Arbeitsplatz zunächst einmal sicherstellen, daß der Arbeitnehmer so eingesetzt wird, daß seine Gesundheit keinen Schaden erleidet. Diese Angaben können aber auch bei Entlassungen als Auswahlkriterien benutzt werden und damit dem Arbeitnehmer zum Nachteil gereichen.

- Ganz enorme Bedeutung hat das Sammeln von Informationen auf dem Gebiet der Sozialleistungen der öffentlichen Hand, insbesondere auf dem Gebiet der Sozialversicherung. Die Sozialversicherten müssen den einzelnen Versicherungsträgern in großem Umfang Angaben sensibelster Art offenbaren, damit diese prüfen können, ob die Voraussetzungen für die beantragten Leistungen gegeben sind. Kaum anders stellt sich die Situation auf dem Gebiet der privaten Kranken- und Lebensversicherungen dar. Auch hier müssen die Versicherten den Versicherungen häufig detaillierte Angaben über ihren Gesundheitszustand machen, an deren Geheimhaltung jeder einzelne von ihnen ein evidentes Interesse hat.
- Umfangreiche Datensammlungen bestehen auch bei den Sicherheitsbehörden. Insbesondere die Polizei ist zur Erfüllung ihrer Aufgaben auf dem Gebiet der Strafverfolgung und der Gefahrenabwehr auf personenbezogene Informationen angewiesen. Jeder, der in den Datensammlungen der Sicherheitsbehörden gespeichert ist, läuft Gefahr, über den konkreten Anlaß der Speicherung hinaus auch später noch ständig mit Ermittlungsmaßnahmen überzogen zu werden. Außerdem muß er befürchten, daß die Sicherheitsbehörden bei Behördenanfragen auf die Speicherung hinweisen mit all den nachteiligen Folgen, die eine Bekanntgabe dieser Angaben mit sich bringen kann.
- Wer wissen will, wieviel die Banken über ihn wissen, muß sich nur einmal seine Kontoauszüge genauer anschauen. Mit der Zunahme des bargeldlosen Zahlungsverkehrs erhalten die Banken Kenntnis von einer großen Zahl von Aktivitäten. Die Bank kennt die Höhe des Gehalts und die Abzüge. Sie weiß, welche Zeitungen abonniert und welche Versicherungen abgeschlossen sind, welche Leistungen von Versicherungen, vom Sozialamt, von der Wohngeldstelle oder vom Arbeitsamt kommen, an welche Vereine und Berufsverbände Mitgliedsbeiträge bezahlt werden und vieles mehr. Sie kann unter bestimmten Voraussetzungen Auskunft bei Kreditschutzorganisationen abrufen und gibt ihrerseits dorthin Daten weiter. Die Datenspeicherungen solcher Kreditschutzorganisationen und Auskunftsteile enthalten Aussagen über die Kreditfähigkeit und Kreditwürdigkeit von Einzelpersonen und Firmen. Diese Informationen werden Interessenten auf Anfrage zur Verfügung gestellt. Auch hier bedarf es keiner großen Phantasie zu ermesen, welcher Schaden eintreten kann, wenn beispielsweise Interessenten auf Grund einer Namensverwechslung unrichtige Daten erhalten.

Hört man manche Kritiker des Datenschutzes, so könnte man fast meinen, der Datenschutz fordere, all diese beispielhaft geschilderten Informationsverarbeitungsvorgänge ganz abzuschaffen und jegliche Datenweitergabe zu verbieten. Dies ist eine der Strategien, mit denen versucht wird, den Datenschutz dadurch zu bekämpfen, daß man ihn ad absurdum führt. Es kann selbstverständlich keine Rede davon sein, daß der Datenschutz eine solche Zielsetzung hat. Er geht aus von der in Art. 1 und 2 Abs. 1 des Grundgesetzes zum Ausdruck kommenden Wertentscheidung unserer Verfassung zum Schutz der Persönlichkeitssphäre des Bürgers. Die Wahrung seiner Individualität steht im Vordergrund. Der Datenschutz sieht von vornherein aber auch Grenzen, die der freien Entfaltung der Persönlichkeit durch legitime Interessen der Gemeinschaft und Rechte anderer gesetzt sind.

Jede Datengewinnung, jedes Sammeln, jede Weitergabe, jedes Löschen personenbezogener Daten steht unter diesem Vorbehalt. Beschränkungen der Persönlichkeitssphäre durch Informationsverarbeitung dürfen dann, aber auch nur dann erfolgen, wenn legitime Interessen der Gemeinschaft oder Rechte anderer dies zwingend erfordern. Innerhalb dieser Grenzen muß es dem einzelnen Bürger jedoch möglich sein, Freiräume zu erhalten, sich seinen individuellen Neigungen entsprechend zu verhalten und vor allem auch frei darüber zu entscheiden, mit wem er in Kontakt treten will, wem und wann er sich offenbart und wer über ihn wie lange Daten sammeln und aufbewahren darf. Bei der Festlegung der Grenzen darf man nicht pauschal dem öffentlichen Interesse den Vorrang geben. Vielmehr muß man hierbei unter strikter Beachtung des Verfassungsgrundsatzes der Verhältnismäßigkeit vorgehen. Dies kann den Verzicht auf absolute Perfektion bedeuten, wenn die dazu erforderlichen Eingriffe in die Persönlichkeitssphäre unverhältnismäßig wären, wenn also der erzielbare Erfolg außer Verhältnis zu der damit verbundenen Belastung des einzelnen stünde. Auf diesen Grundsätzen baut unser geltendes Datenschutzrecht auf. Dafür zu sorgen, daß dieser Rechtszustand erhalten bleibt und auch nicht im Wege der Interpretation der einzelnen Bestimmungen aufgeweicht, sondern eine wirksame Kontrolle gesichert wird, muß allen ein Anliegen sein, die im Menschen nicht nur das Objekt staatlichen und gesellschaftlichen Handelns, sondern ein der Selbstverantwortung fähiges Individuum sehen, das geachtet und beachtet werden muß. Ich meine, daß es sich lohnt, sich dafür einzusetzen. Dabei bin ich mir im klaren, daß dies nicht einfach ist. In einer Zeit des Wettrüstens, der Arbeitslosigkeit und der leeren öffentlichen Kassen fällt schwer, die notwendigen Informationen zur Erkennung der anstehenden Probleme des Datenschutzes zu vermitteln. Die Auswirkungen der Datenschutzverstöße lassen sich meist nicht in Mark und Pfennig ausdrücken. Was bleibt, ist vielmehr häufig ein Gefühl der Diskriminierung, der Mißachtung, des enttäuschten Vertrauens oder der Angst. Kritiker des Datenschutzes weisen, wenn ich altgewohnte Informationsweitergaben beanstande, immer wieder darauf hin, hierüber habe sich bisher noch niemand beschwert. Sie lassen dabei völlig außer acht, daß viele Bürger diese Datenübermittlungen mit dem Gefühl der Ohnmacht hinnahmen, weil sie keine Möglichkeit sahen, sich dagegen zu wehren. Ganz besonders galt dies, wenn Randgruppen unserer Gesellschaft, Alte und Schwache und Hilfsbedürftige betroffen waren. Gerade der Schutz solcher Minderheiten unter Umständen auch vor der Mehrheit ist ein wesentliches Ziel des Datenschutzes. Ich meine, von einem so verstandenen Datenschutz kann es keine Abstriche geben, wollen wir uns die Chance für eine menschliche Gesellschaft erhalten. Das Gebot der Stunde kann angesichts der Entwicklung der Informationstechnik und der immer stärkeren Einflußnahme von Staat und Gesellschaft auf unser Leben nur sein, den Datenschutz zu sichern und auszubauen.

2. Teil: Forschung

1. Abschnitt: Zur Situation

1. Entwicklung seit dem 2. Tätigkeitsbericht

Meine Ausführungen im 2. Tätigkeitsbericht über das Verhältnis von Datenschutz und Forschung hatten eine ganz erstaunliche Resonanz. Der aufgezeigte Widerspruch zwischen Sollen und Sein im Bereich der medizinischen Forschung erregte großes Aufsehen. Die Reaktionen waren sehr unterschiedlich. Weder fehlte es an Zustimmung noch an Kritik, die manchmal sogar in persönliche

Angriffe mündete. Vor allem trug mein 2. Tätigkeitsbericht dazu bei, das Problembewußtsein zu schärfen und die zuvor sehr allgemein geführte Diskussion über Notwendigkeit und Grenzen des Datenschutzes im Bereich der medizinischen Forschung wesentlich konkreter und anschaulicher zu machen. Am meisten überraschte mich, daß die überwiegende Zahl der betroffenen Forscher und Institutionen ebenso wie viele Stimmen in Politik und Publizistik nicht zur Kenntnis nehmen wollten, daß nicht das Landesdatenschutzgesetz den Zugang der medizinischen Forschung zu Patientendaten einschränkt, sondern die ärztliche Schweigepflicht. Sie sprachen immer wieder von der neuen, durch das Landesdatenschutzgesetz geschaffenen Rechtslage und ließen dabei völlig außer acht, daß es seit eh und je eine Verletzung der ärztlichen Schweigepflicht darstellt, wenn ein Arzt personenbezogene Daten seines Patienten ohne dessen Einwilligung an Forscher weitergibt. Inzwischen vollzog sich ein gewisser Wandel, den ich als das wichtigste Ergebnis der Diskussion im vergangenen Jahr betrachte: Die Bedeutung der ärztlichen Schweigepflicht ist wieder stärker in das öffentliche Bewußtsein und ganz besonders in das Blickfeld der Ärzteschaft gerückt. Dieser Bewußtseinswandel fand seinen deutlichen Ausdruck auf dem Deutschen Ärztetag 1982 in Münster, der ein nachhaltiges Bekenntnis zur ärztlichen Schweigepflicht auch im Verhältnis zur Forschung ablegte.

Weniger erfreulich gestaltete sich die Entwicklung in Baden-Württemberg selbst. Während auf einer Reihe von Veranstaltungen im gesamten Bundesgebiet Forscher, Ärzte und Datenschützer die zweifellos bestehenden Probleme sehr offen und sachlich miteinander erörterten und gemeinsam nach Lösungen suchten, glaubte man in Baden-Württemberg, auf einen solchen Meinungsaustausch verzichten zu können. Die Ministerien hielten es auch nicht für erforderlich, der zweifellos vorhandenen Rechtsunsicherheit bei Forschungseinrichtungen und Behörden entgegenzuwirken. Anstatt sich hierum im Interesse des Persönlichkeitsschutzes und der Forschung zu bemühen, faßte man den Plan für eine Radikalkur: Eine Änderung des Landesdatenschutzgesetzes soll sicherstellen, daß in Zukunft jedermann — wie es schon jetzt im Bereich der medizinischen Forschung leider vielfach entgegen geltendem Recht geschieht — personenbezogene Daten ohne Rücksicht, ob sie die ärztliche Schweigepflicht oder andere Berufsgeheimnisse besonders schützen, an Forscher ohne Einwilligung der Patienten weitergeben kann und die Forscher mit diesen Daten Krankheitsregister jeglicher Art anlegen und führen dürfen. Bereits Ende März 1982 lag ein von Wissenschafts-, Innen- und Sozialministerium erarbeiteter Gesetzentwurf vor. Meiner wiederholt vorgetragenen Bitte, ihn mir zu überlassen, entsprachen die Ministerien nicht — geschweige denn meinem Wunsch, mich an ihren Überlegungen zu beteiligen. Statt dessen hatte ich die Möglichkeit, den wesentlichen Inhalt des Gesetzentwurfs der Presse zu entnehmen. In einem Gespräch mit dem Herrn Ministerpräsidenten und Mitgliedern der Landesregierung konnte ich dann wenigstens erreichen, daß die Regierung von der Einleitung des offiziellen Gesetzgebungsverfahrens vorerst absah und sich entschied, als nächsten Schritt eine Expertenanhörung durchzuführen. Auf diese Weise wollte sie in Erfahrung bringen, inwieweit überhaupt ein Bedürfnis für gesetzliche Regelungen besteht. So sehr ich diese Entscheidung begrüße, so sehr bedauere ich, auf welche Art und Weise die Ministerien diesen Auftrag ausführten.

Das Hearing fand am 15. Juni 1982 statt. Es beschränkte sich auf die medizinische Forschung. Seine Ergebnisse sind nur bedingt verwertbar. Zum einen fehlte die gemeinsame Ausgangslage, weil sich die Sachverständigen nicht darüber im klaren waren, was

nach geltendem Recht zulässig ist und was nicht. Wegen dieses Umstands sahen sie gelegentlich Probleme, die in Wirklichkeit keine sind, und gingen auf die eigentliche Problematik nicht ein. Ihre Unsicherheit verstärkte der von den Ministerien vorgegebene Fragenkatalog; er war viel zu allgemein und schwer verständlich formuliert, so daß die Antworten dementsprechend allgemein und unpräzise ausfielen. Dieser Mangel ließ sich nur schwer durch gezielte Einzelfragen ausgleichen. Eine maßgebliche Rolle spielte auch die Zusammensetzung der angehörten Experten. So waren verschiedene Forscher eingeladen, deren Methoden der Datenverarbeitung ich bereits 1981 wegen Verstoßes gegen das Arztgeheimnis ausdrücklich beanstandet hatte. Daß diese sich von ihren bisherigen Arbeitsmethoden distanzieren würden, konnte man schlechterdings nicht erwarten. Ähnliches gilt auch für die in großer Zahl vertretenen Epidemiologen und Forscher, die mit Methoden der Epidemiologie arbeiten. Ihren Stimmen, die sich für einen weitgehenden ungehinderten Zugang zu medizinischen Daten aussprachen, standen auf der anderen Seite Aussagen von Ärztevertretern gegenüber, die zum Teil vehement gegen flächendeckende Krankheitsregister Stellung bezogen und die bestehenden Möglichkeiten des Datenzugangs für ausreichend halten.

Wegen dieser Umstände konnten sich die beteiligten Ministerien durch das Hearing keineswegs in ihren gesetzgeberischen Plänen bestätigt fühlen. Einen Beweis dafür sehe ich darin, daß sich die Landesregierung erst Ende Oktober 1982, also vier Monate später auf Drängen von Teilen des Landtags entschloß, den bereits seit März 1982 vorliegenden Gesetzentwurf praktisch unverändert in das offizielle Anhörungsverfahren zu geben. Erst zu diesem Zeitpunkt hielt man es für opportun, mir den Gesetzentwurf zuzuleiten. Obwohl der Gesetzentwurf nicht nur das Arztgeheimnis zu Gunsten der medizinischen Forschung, sondern alle Berufs- und besonderen Amtsgeheimnisse zu Gunsten aller Forschungsbereiche weitestgehend aufheben will, hörten die Ministerien im offiziellen Anhörungsverfahren neben den Universitäten des Landes nur Persönlichkeiten und Organisationen, die dem medizinischen Bereich nahe stehen. Sie hielten nicht für erforderlich, die Haltung der Berufs- und Standesorganisationen der Gruppen kennenzulernen, die die sonstigen Berufs- und besonderen Amtsgeheimnisse beachten müssen, beispielsweise die Verbände der Berufspsychologen und Sozialarbeiter, der Steuerberater, die Ehe-, Erziehungs- und Drogenberatungsstellen und deren Träger. Das aber ist unerlässlich, wenn sich Landesregierung und Landtag eine alle Interessen in Rechnung stellende Meinung bilden wollen.

2. Gesetzentwurf der Landesregierung zur 2. Änderung des Landesdatenschutzgesetzes (Stand: 26. Okt. 1982) — Anlage

2.1 Gesetzestechnik

Jeder Leser des Gesetzentwurfs hat, ehe er sich mit dessen Inhalt befassen kann, eine Hürde besonderer Art zu überwinden: die Gesetzessprache. Sie ist ein zwar mehr formaler, in ihren negativen Auswirkungen aber nicht zu unterschätzender Fehler des Entwurfs. Schon jetzt führen viele Stellen beredete Klage, wie schwer es ihnen die abstrakte Sprache der Datenschutzgesetze macht, den Bedeutungsinhalt ihrer einzelnen Vorschriften zu verstehen. Diese Schwäche der Datenschutzgesetze übertrifft der Gesetzentwurf bei weitem. Er verwendet nicht nur zahlreiche, sehr unbestimmte und deshalb auch vielseitig interpretierbare Begriffe, sondern arbeitet zusätzlich im

Übermaß mit Verweisungen. Als besonders abschreckendes Beispiel zitiere ich seinen § 20 a Abs. 5 im Wortlaut:

„Die Registerstelle ist berechtigt, unter den Voraussetzungen des § 20 Abs. 1 Nr. 1 und 2 Buchst. a und nach Maßgabe der Rechtsverordnung nach den Absätzen 1 und 2 die für bestimmte Forschungsvorhaben erforderlichen personenbezogenen Daten ohne Einwilligung des Betroffenen an wissenschaftliche Einrichtungen zu übermitteln. § 20 Abs. 3 Satz 2 gilt entsprechend. Eine weitere Übermittlung durch die wissenschaftliche Einrichtung an Dritte ist unzulässig.“

Wegen dieser Gesetzessprache fällt es selbst mit dem Datenschutzrecht vertrauten Juristen schwer, den Gesetzentwurf zu verstehen. Erst recht muß dies für die unmittelbaren Adressaten des Gesetzentwurfs, insbesondere für Forscher und potentielle Datenlieferanten, gelten. Mir ist schlechterdings nicht verständlich, wie in der Erarbeitung von Gesetzentwürfen erfahrene Ministerien verantworten können, einen so schwer verständlichen Gesetzentwurf in das Anhörverfahren zu geben. Die Folge kann nur sein, daß eine sachgerechte Auseinandersetzung mit der vorgeschlagenen Regelung nicht erfolgt und damit die Anhörung ihren eigentlichen Sinn verliert. Würde der Gesetzentwurf gar noch Gesetz, wäre schon allein wegen seiner Sprache der Rechtsunsicherheit Tür und Tor geöffnet und der Unmut über den Datenschutz und das Unverständnis seiner Regelungen vorprogrammiert.

2.2 Inhalt des Gesetzentwurfs und Bewertung

2.2.1 Datenzugang

Bisher regelt das Landesdatenschutzgesetz nur, unter welchen Voraussetzungen öffentliche Stellen personenbezogene Daten aus Dateien an öffentliche Forschungseinrichtungen weitergeben dürfen. Keine Aussage macht es über private Datenlieferanten und private Forschungseinrichtungen. Es berührt auch nicht die in anderen Gesetzen enthaltenen Vorschriften über besondere Amts- und Berufsgeheimnisse, zum Beispiel die ärztliche Schweigepflicht, die Schweigepflicht der Rechtsanwälte, das Steuergeheimnis, das Sozialgeheimnis oder das Statistikgeheimnis. Diese Geheimhaltungsvorschriften gelten deshalb stets neben dem Landesdatenschutzgesetz. Sie erlauben im Regelfall eine Weitergabe der Daten nur mit Einwilligung des Betroffenen.

Der Gesetzentwurf erleichtert demgegenüber die Voraussetzungen für die Datenweitergabe zu Forschungszwecken ganz generell. Er bezieht in diese Regelung alle privaten Stellen ein, die Daten liefern oder die Forschungsarbeit betreiben. Bei der Weitergabe der Daten soll es nicht mehr darauf ankommen, ob die Stellen die Daten in einer Datei speichern oder nicht. Die gravierendste Änderung des Gesetzentwurfs ist freilich, daß öffentliche und private Stellen personenbezogene Daten ohne Einwilligung des Betroffenen auch weitergeben dürfen, wenn sie ein Berufs- oder besonderes Amtsgeheimnis schützt. Damit setzen die Gesetzesverfasser im Verhältnis zur Forschung praktisch alle Geheimhaltungsvorschriften außer Kraft.

Ich halte diese Regelung für völlig unannehmbar:

- Sie berechtigt Ärzte, Zahnärzte, Apotheker und andere Angehörige von Heilberufen, Berufspsychologen, Anwälte, Steuerberater, Wirtschaftsprüfer, Ehe-, Er-

ziehungs-, Jugend- und Drogenberater, Mitarbeiter von Beratungsstellen nach § 218 b Abs. 2 Nr. 1 StGB, Sozialarbeiter und Sozialpädagogen alle Angaben, die ihnen hilfe- und ratsuchende Menschen in ihrer Not anvertrauen, ohne deren Wissen und unter voller Nennung ihres Namens an Forscher aller Forschungsrichtungen weiterzugeben. Entgegen der amtlichen Begründung läßt dies die jetzige Fassung des Gesetzentwurfs allein schon zu, wenn die wissenschaftliche Einrichtung die Identifizierungsdaten getrennt von den übrigen Daten speichert und sichert. Dieses Trennungsgebot ist eine Minimalforderung, welche die wissenschaftliche Forschung heute schon weitgehend erfüllt. Der Gesetzentwurf erlaubt also im Ergebnis, selbst sensibelste Daten ohne jede Einschränkung weiterzugeben und verletzt damit das durch Art. 1 und Art. 2 Abs. 1 GG geschützte allgemeine Persönlichkeitsrecht in offenkundiger Weise. Gesetzt den Fall, die Gesetzesverfasser passen den Wortlaut ihres Entwurfs ihrer Begründung an und machen, wie sie dort ausführen, die Datenweitergabe ohne Einwilligung davon abhängig, daß das öffentliche Interesse am Forschungsvorhaben das Geheimhaltungsinteresse des Betroffenen erheblich überwiegt und das Einholen seiner Einwilligung wegen seiner Gefährdung oder der des Forschungszwecks oder wegen des damit verbundenen Aufwands nicht zumutbar oder möglich ist: Auch eine solche Generalklausel wäre unververtretbar. Sie ist mit so vielen unbestimmten Gesetzesbegriffen gespickt, daß sie je nach der individuellen Einstellung der beteiligten Personen praktisch jedes gewünschte Ergebnis ermöglicht. Ich frage bloß: Wann ist Art und Umfang des Aufwands für das Einholen der Einwilligung nicht mehr zumutbar? Richtet sich dies jeweils nach der Situation der öffentlichen Finanzen? — Wann läßt das Forschungsvorhaben „einen wesentlichen Nutzen für die Allgemeinheit“ erwarten? Welcher Forscher würde dies je bei seinem Forschungsvorhaben verneinen? Über diese Formeln läßt sich trefflich streiten; damit wäre der künftige Konflikt schon vorprogrammiert.

- Der Gesetzesvorschlag geht wie ein Rasenmäher über die Berufs- und Amtsgeheimnisse hinweg und behandelt alle personenbezogenen Daten ohne Rücksicht auf ihre Schutzbedürftigkeit gleich. Völlig unberücksichtigt läßt er die Gründe, die einst Anlaß waren, die einzelnen Geheimhaltungsvorschriften zu schaffen. Sie sind unterschiedlicher Art. Teils sind die Geheimhaltungsvorschriften Grundvoraussetzung für ein rückhaltloses Sich-Anvertrauen gegenüber beratenden und betreuenden Stellen; man denke bloß an das Arztgeheimnis, Sozialgeheimnis oder Anwaltgeheimnis. Teils sind sie das Äquivalent für gesetzliche Pflichten der Bürger, umfangreiche und zudem richtige Auskünfte über private Angelegenheiten zu geben; ich erinnere an das Statistik- und Steuergeheimnis. Der Gesetzentwurf ignoriert dies alles und schafft neue Offenbarungstatbestände, ohne nachzuweisen, warum dies notwendig ist und die Regelung alle Forschungsbereiche und nicht nur — wie die Öffentlichkeit noch vielfach glaubt — die medizinische For-

schaft erfassen soll. Auch bedachten die Gesetzesverfasser nicht die fatale Folge ihres Gesetzentwurfs, daß er die Daten Toter besser schützt als die der Lebenden. Denn seine Regeln gelten nur für Lebende; unberührt lassen sie die Vorschrift des § 203 Abs. 4 des Strafgesetzbuchs, wonach die Berufs- und Amtsgeheimnisse über den Tod hinauswirken.

- Das Freistellen der Forschung vom Beachten aller Amts- und Berufsgeheimnisse würde das Vertrauen der Bürger in die Diskretion der von ihnen aufgesuchten beratenden und betreuenden Stellen gefährden, ja zerstören oder gar nicht mehr erst entstehen lassen. Solches Vertrauen ist aber die wichtigste Voraussetzung für deren Arbeit überhaupt und damit für richtige und wirksame Hilfe. Deshalb schützt es unsere Rechtsordnung bislang ganz besonders.
- Der Gesetzesvorschlag stellt nicht sicher und kann es wegen der mangelnden Kompetenz des Landesgesetzgebers auch nicht, daß der Forscher die erhaltenen Daten nur für seinen ursprünglichen beabsichtigten Forschungszweck verwendet. Selbst wenn der Gesetzentwurf ein generelles Übermittlungsverbot aufgestellt hätte — was nicht einmal der Fall ist —, könnten die Strafverfolgungsorgane oder die Steuerverwaltung immer noch auf Grund der Ermächtigungsnormen der Strafprozeß- und Abgabeordnung auf diese Daten zugreifen. Diese Möglichkeit bestünde selbst bei Daten, die ursprünglich Berufs- oder besondere Amtsgeheimnisse schützen. Denn sie verlieren mit der Weitergabe an wissenschaftliche Einrichtungen diesen Schutz. Für diese Einrichtungen gelten die Zeugnisverweigerungsrechte und Beschlagnahmeverbote der Strafprozeßordnung sowie die Auskunftsverweigerungsrechte der Abgabenordnung nicht mehr. Würde beispielsweise eine Beratungsstelle nach § 218b Abs. 2 Nr. 1 StGB Angaben aus ihrer Beratungstätigkeit an einen Forscher weitergeben, dann könnten ab diesem Zeitpunkt die Strafverfolgungsorgane auf diese Daten zugreifen. Anders als die Mitarbeiter der Beratungsstelle hätte der Forscher kein Zeugnisverweigerungsrecht. Auch bestünde anders als bei der Beratungsstelle kein Beschlagnahmeverbot. Nichts anderes gilt auch für alle übrigen Forschungsbereiche und Forschungsvorhaben. Ich meine, man sollte auch diese Konsequenzen für die Betroffenen bedenken, ehe man daran geht, der Forschung einen Freibrief einzuräumen.
- Der Gesetzentwurf gestattet die schrankenlose Weitergabe von Daten unabhängig davon, ob sie in Dateien oder anderswo, zum Beispiel in Akten geführt werden. Damit vollzog die Landesregierung eine Kehrtwendung um 180 Grad gegenüber ihrer bisherigen Haltung. Bislang bezeichnete sie die Beschränkung des Anwendungsbereichs des Landes- und Bundesdatenschutzgesetzes auf die dateibezogene Datenverarbeitung als unverzichtbar und verneinte ein darüber hinausgehendes Regelungsbedürfnis. Ebenso nahm sie letztlich diese Haltung in der Frage der Kontrollbefugnis des Landesbeauftragten für den Datenschutz ein. Es überrascht, daß dies alles plötzlich nicht mehr gelten soll.

2.2.2 Krankheitsdatenregister

Bisher erlaubt das Landesdatenschutzgesetz nur, personenbezogene Daten ohne Einwilligung des Betroffenen zu speichern, wenn die Speicherung einem konkreten Forschungsvorhaben mit einer definierten Fragestellung dient. Nicht zulässig ist dagegen, ohne Einwilligung der Patienten Krankheitsdatenregister anzulegen, die lediglich die Grundlage für eine ganze Reihe noch gar nicht feststehender Forschungsvorhaben bilden sollen. Trotz dieser klaren Gesetzeslage legten Forscher in der Vergangenheit eine ganze Reihe solcher Krankheitsdatenregister an. Ich erinnere an die verschiedenen Krebsregister und an das Kumulative psychiatrische Fallregister des Zentralinstituts für Seelische Gesundheit in Mannheim. Um diese Register zu legalisieren und weitere Register zu ermöglichen, ermächtigt der Gesetzesvorschlag die zuständige oberste Landesbehörde — in der Regel also das Wissenschaftsministerium —, durch Rechtsverordnung das Anlegen und Führen solcher Krankheitsdatenregister zu erlauben, „wenn dies im öffentlichen Interesse erforderlich ist“. In diesem Fall dürfen alle Stellen dem Register Daten ohne Einwilligung des Kranken überlassen, auch wenn sie einem Berufs- oder besonderen Amtsgeheimnis unterliegen.

Diese Regelung geht viel zu weit. Die Aufnahme von Krankheitsdaten einer Person in ein solches Register ist ein schwerwiegender Eingriff in die Rechtsstellung des Kranken. Hierzu bedarf es einer Entscheidung des Gesetzgebers im Einzelfall. Deshalb geht es nicht an, die Entscheidung über solche Register der Exekutive zu überlassen — selbst wenn dies in Form einer Rechtsverordnung zu geschehen hat. Auch dann besteht die Gefahr, daß die Verwaltung viel zu großzügig Register zuläßt. Man bedenke bloß, wie sehr das Wissenschaftsministerium schon bisher die Forschungsinteressen gegenüber dem Persönlichkeitsschutz bevorzugte. Einzige Voraussetzung für den Aufbau solcher Register wäre in Zukunft, daß das einzelne Register „im öffentlichen Interesse erforderlich“ ist. Diese vage Zulässigkeitsvoraussetzung ist keine wirksame Schranke gegen ein uferloses Ausdehnen von Krankheitsdatenregistern. Zum einen speichern diese Register auf viele Jahre hinaus die Daten und werten sie für eine Vielzahl von noch unbekannten Forschungsvorhaben aus. Zum anderen unterliegen die gespeicherten Daten nicht mehr der ärztlichen Schweigepflicht mit der Folge, daß zum Beispiel Strafverfolgungsorgane auf sie zugreifen können. Man denke bloß, dies geschähe bei einer Registerstelle für Suchtkranke. Die medizinische Versorgung der darin erfaßten Menschen würde darunter ebenso leiden wie die wissenschaftliche Arbeit der Registerstelle. Schließlich bietet die geforderte getrennte Speicherung der Identifizierungsdaten von den übrigen Daten in Wirklichkeit nur einen sehr geringen Schutz für den Betroffenen. Etwaige Interessenten sind im allgemeinen nicht daran interessiert, die eigentlich medizinischen Daten zu erhalten. Sie wollen bloß wissen, welche Personen überhaupt das Krankheitsdatenregister speichert. Dazu genügt aber die Kenntnis der Identifizierungsdaten. Schon jetzt sind Fälle bekannt, in denen solche Registerstellen Abfragen bei Meldebehörden und Standesämtern durchführen oder durchzuführen versuchen.

2.2.3 Beseitigung der Auskunftspflicht

Bislang verpflichten das Landes- oder das Bundesdatenschutzgesetz wissenschaftliche Einrichtungen, dem Betroffenen Auskunft über seine gespeicherten Daten zu geben. Der Gesetzentwurf will diese Auskunftspflicht beseitigen.

Das Auskunftsrecht des Bürgers ist eines der elementarsten Datenschutzrechte. Es gibt ihm die Möglichkeit, sich zu informieren, wer über ihn welche Daten speichert, und versetzt ihn in die Lage, von seinen Rechten auf Berichten, Sperren und Löschen Gebrauch zu machen. Es besteht nicht das geringste Bedürfnis, dies zu ändern. Entgegen der Gesetzesbegründung kann keine Rede davon sein, daß die Auskunftspflichtung die wissenschaftliche Forschung beeinträchtigt. Dafür ist keinerlei Nachweis erbracht. Die geplante Regelung ist unmittelbarer Ausdruck der Tendenz des gesamten Gesetzentwurfs, die wissenschaftliche Forschung so weit es irgend geht auch gegenüber dem Betroffenen abzuschotten und ihn als möglichen Störfaktor auszuschalten. Darin liegt eine Entmündigung des Bürgers, die mit dem Menschenbild unseres Verfassungs- und Rechtssystems unvereinbar ist.

2.3 Gesetzgebungskompetenz

Der Gesetzentwurf will das Verhältnis von Datenschutz und Forschung abschließend regeln. Wegen der Aufteilung der Gesetzgebungszuständigkeiten zwischen Bund und Ländern im Grundgesetz kann der Landesgesetzgeber dies nicht in vollem Umfang.

2.3.1 Privater Bereich

Fraglich ist, ob der Landesgesetzgeber regeln kann, unter welchen Voraussetzungen private Personen und Stellen personenbezogene Angaben aus Dateien an wissenschaftliche Einrichtungen übermitteln dürfen. Bisher richten sich solche Übermittlungen nach den Bestimmungen des dritten und vierten Abschnittes des Bundesdatenschutzgesetzes. Soweit sie abschließend sind, hat der Landesgesetzgeber keinen Gestaltungsspielraum.

2.3.2 Berufs- und besondere Amtsgeheimnisse

Fraglich ist auch, wie weit der Gesetzgeber eine Mitteilungsberechtigung für personenbezogene Daten schaffen kann, die Berufs- und besondere Amtsgeheimnisse schützen. Mit Sicherheit ist dies nicht bei allen diesen Geheimnissen zulässig. So steht das Statistikgeheimnis nach § 11 des Bundesstatistikgesetzes oder das Sozialgeheimnis nach § 35 SGB I nicht zur Disposition des Landesgesetzgebers. Diese Bestimmungen regeln abschließend, wie mit den personenbezogenen Daten verfahren werden darf, die bei der Durchführung von Bundesstatistiken und der Gewährung von Sozialleistungen angefallen sind. Aber auch bei einer Reihe weiterer Berufs- und besonderer Amtsgeheimnisse ist sehr fraglich, ob der Landesgesetzgeber überhaupt einen Spielraum hat. Leider hielten die Verfasser des Gesetzentwurfs es nicht einmal für nötig, ein Wort über diese heikle Verfassungsfrage zu verlieren. Von der Klärung des Umfangs der Gesetzgebungskompetenz des Landes hängt aber letztlich ab, welche konkreten Auswirkungen der Gesetzentwurf im

einzelnen tatsächlich hat. Mit Gewißheit läßt sich schon jetzt sagen: Die Aufteilung der Gesetzgebungszuständigkeit zwischen Bund und Land führt jedenfalls dazu, daß im Falle einer Verwirklichung des Gesetzentwurfs besonders schutzwürdige Daten wesentlich geringer geschützt wären als weit weniger sensible Daten, deren Schutz der Bundesgesetzgeber abschließend regelte. Angaben über das Wohngeldverfahren wären beispielsweise besser geschützt als alle Daten, die Kranke in ihrer Suche nach Hilfe Ärzten anvertrauen.

Zusammenfassend stelle ich fest: Der Gesetzentwurf hebt elementare Grundrechte der Bürger weitgehend aus den Angeln. Er löst im Forschungsbereich alle Amts- und Berufsgeheimnisse zu Lasten des Persönlichkeitsschutzes auf. Für diesen Bruch mit der Rechts tradition der Bundesrepublik besteht keinerlei Notwendigkeit. Ich appelliere deshalb an die Landesregierung, ihre gesetzgeberischen Pläne zu überdenken und davon abzusehen, der wissenschaftlichen Forschung auf Kosten aller Bürger in Baden-Württemberg einen solchen Freibrief auszustellen.

3. Vorschläge

3.1 Mehr Information

Ähnlich weitreichende Gesetzgebungspläne, wie sie die Landesregierung von Baden-Württemberg hegt, gibt es nirgendwo sonst im Bundesgebiet. Auch der Wissenschaftsrat ging in seiner Entschließung vom 5. Nov. 1982 nicht so weit zu verlangen, man solle alle Berufs- und besonderen Amtsgeheimnisse im Wege einer sehr vagen Generalklausel zu Gunsten der Forschung außer Kraft setzen. Dieser Weg ist zwar für Gesetzesverfasser bequem. Denn er enthebt sie der Mühe, für jeden einzelnen Forschungszweck und für jedes einzelne Berufs- und besondere Amtsgeheimnis sorgfältig zu prüfen, ob die gegenwärtige Rechtslage tatsächlich so unbefriedigend ist, daß sie eine Änderung rechtfertigen könnte. Eine solche Prüfung ist zeitaufwendig und mühsam. Aber so beschwerlich sie sein mag, so unentbehrlich ist sie. Nach meinen Erfahrungen, die ich im vergangenen Jahr durch Kontrollbesuche bei zwei Universitäten weiter vertiefte, traten ernsthafte Probleme bislang nur im Bereich der medizinischen Forschung auf. Gewiß kam es auch in anderen Bereichen vor, daß Forscher nicht die gewünschten Daten in der gewünschten Zeit erhielten. Ging man den Dingen auf den Grund, ergab sich rasch, daß die eigentliche Ursache die weitverbreitete Unsicherheit über das maßgebende Datenschutzrecht und vor allem die vorherrschende Unklarheit über den Inhalt der Forschungsklausel des § 20 LDSG sind. Ich habe auf diese Gefahr und auf ihre negativen Auswirkungen bereits in meinem 2. Tätigkeitsbericht hingewiesen und die Ministerien aufgefordert, den Behörden und wissenschaftlichen Einrichtungen Informationen an die Hand zu geben. Leider blieb dieser Appell ohne jedes Echo. Vor allem ergriff das Wissenschaftsministerium nicht die geringste eigene Initiative, dieser Rechtsunsicherheit ein Ende zu bereiten. Hier liegt nach wie vor ein weitgehend unbeackertes Feld, auf dem sehr viel getan werden kann und im Interesse der Forschung auch getan werden muß. Ganz besonders gilt dies für die medizinische Forschung, wo die aufgetretenen Probleme am ernsthaftesten sind. Eine Reihe von Fragen des Datenzugangs ließe sich allein schon dadurch lösen.

3.2 Verstärkter Einsatz der Möglichkeiten der Anonymisierung und Aggregierung

Bei Kontrollbesuchen, Anfragen und Diskussionen stellte ich laufend fest, daß die Forschung noch viel zu wenig die Möglichkeiten der Anonymisierung und Aggregierung von Daten einsetzt. Immer wieder sagte man mir, die Datenlieferanten seien nicht in der Lage, die Anonymisierung oder Aggregierung selbst vorzunehmen und auf diese Weise sicherzustellen, daß der Forscher nur die tatsächlich benötigten anonymen Daten erhält. Hier gilt es anzusetzen und die Zusammenarbeit zwischen Forschern und den Stellen zu verbessern, die im Besitz der gewünschten Daten sind. Erforderlich ist weiter, wie auch eine Empfehlung des Wissenschaftsrats fordert, die Entwicklung geeigneter Anonymisierungs- und Aggregationsmethoden voranzutreiben. Mir scheint, die Forschung bemühte sich bislang viel zu wenig darum, die Erkenntnisse der modernen Mathematik, vor allem die entwickelten Verschlüsselungstechniken für ihre Zwecke fruchtbar zu machen. Darum muß sie sich bemühen. Die Experten müssen ihr dabei helfen und versuchen, die Verschlüsselungstechniken so praktikabel zu gestalten, daß sie auch die Forschungspraxis anwenden kann.

3.3 Bemühen um Einwilligung

Eines vom Wichtigsten ist, auch in der Forschung nicht den Weg des geringsten Widerstands zu gehen. Sehr viel häufiger und intensiver als bislang muß sie sich um die Einwilligung der Betroffenen bemühen. Dies gilt für alle Forschungsbereiche, ganz besonders aber für die medizinische Forschung. Die Bereitschaft der Patienten, die Einwilligung zu erteilen, ist weit aus größer als viele glauben. Der Weg zur Einwilligung ist nicht immer bequem und manchmal gewiß auch aufwendig. Er erfordert häufig ein stärkeres Ein- und Zugehen auf den Patienten. Behandelnde und forschende Ärzte müssen ihn jedoch beschreiten, wenn sie im Patienten nicht nur das Patientengut, sondern den Menschen sehen, dem trotz seiner durch Krankheit bedingten Schwäche das Recht zusteht, selbst darüber zu entscheiden, ob er seine Daten der wissenschaftlichen Forschung zur Verfügung stellen will oder nicht.

4. Zur Notwendigkeit neuer Gesetze

Das Verhältnis von Forschung und Datenschutz beschäftigt mich seit Beginn meiner Amtszeit. Ich hatte zahlreiche Kontakte mit Forschern und Stellen, die der Forschung Daten liefern. Dabei stellte ich immer wieder fest, daß es außerhalb der medizinischen Forschung keine Probleme gibt, deretwegen ernsthaft an eine Gesetzesänderung zu denken wäre. Eine Ausnahme bildet lediglich die Zeitgeschichte. Diese ist, wie ich bereits in meinem 2. Tätigkeitsbericht ausführte, durch das Verbot des § 20 Abs. 3 LDSG, personenbezogene Daten ohne Einwilligung zu veröffentlichen, stark behindert.

Für die medizinische Forschung halte ich eine Änderung des geltenden Rechts nur für gerechtfertigt, wenn sich zeigen sollte, daß ihr trotz Beschreitens der aufgezeigten Wege ernsthafte Gefahren drohen. Der Nachweis, wir hätten in Baden-Württemberg eine solche Situation, ist nicht erbracht. So sieht die Dinge auch die Landesregierung von Rheinland-Pfalz. Sie legte jüngst ihrem Landtag ausführlich dar, warum das geltende Datenschutzrecht grundsätzlich geeignet ist, den Zielkonflikt zwischen den Erfor-

dernissen der medizinischen Forschung und dem Recht des Patienten auf Wahrung seiner Privatsphäre sachgerecht zu lösen (Landtags-Drucksache 9/2504). Diese Äußerung hat für Baden-Württemberg besondere Bedeutung. Denn das rheinland-pfälzische Landesdatenschutzgesetz enthält eine mit unserer Forschungsklausel des § 20 LDSG identische Regelung. Rechtsänderungen zugunsten der medizinischen Forschung halte ich allenfalls für Teilbereiche nach sorgfältigem Abwägen des Für und Wider für denkbar. Ich verweise dazu auf die Diskussion über ein zentrales Krebsregister. Sollten Landtag und Landesregierung von Baden-Württemberg tatsächlich im Gegensatz etwa zur Auffassung des Deutschen Ärztetages 1982 ein Krebsregister für unerlässlich halten, müßten sie wegen der Schwere des damit verbundenen Eingriffs ein spezielles Krebsregistergesetz erlassen. Nicht begnügen dürfen sie sich mit dem Schaffen von Generalklauseln, die eine nahezu ungehinderte Anlegung zentraler Krankheitsdatenregister ermöglichen.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder entwickelte konkrete Vorschläge für den etwaigen Inhalt eines Gesetzes über ein Krebsregister. Sie sind dem Sozialministerium seit längerem bekannt. Aus meiner Sicht sollte ein Krebsregistergesetz folgenden Inhalt haben:

- Die Aufgaben des Krebsregisters sind konkret zu umschreiben; seine Führung ist einer öffentlichen Stelle zu übertragen.
- Meldungen zum Krebsregister dürfen grundsätzlich nur mit Einwilligung der Krebskranken erfolgen. Ausnahmen hiervon sollten möglich sein, wenn die Meldung für den Zweck des Registers wesentlich erscheint und der Krebspatient gesundheitliche Nachteile erleiden könnte, wenn der Arzt ihn wegen Einwilligung über seine Krankheit weiter aufklären müßte.
- Die Angaben, die der behandelnde Arzt dem Krebsregister meldet, sind konkret festzulegen.
- Die registerführende Stelle soll in begrenztem Umfang Leichenschauscheine auswerten können.
- Die registerführende Stelle muß die Daten getrennt nach Datengruppen speichern. Zu regeln ist, wann und unter welchen Voraussetzungen sie die Daten der einzelnen Gruppen zusammenführen kann.
- Die Dauer der Speicherung der Daten ist festzulegen.
- Das Register darf personenbezogene Daten an wissenschaftliche Einrichtungen zur Durchführung bestimmter Forschungsvorhaben grundsätzlich nur mit Einwilligung der Krebskranken weitergeben. Ohne Einwilligung darf sie nur so verfahren, wenn die Meldung zum Register ohne Einwilligung erfolgte.
- Befragungen der Krebskranken und Dritter zur Durchführung bestimmter Forschungsvorhaben sind nur mit Einwilligung des Patienten zulässig.
- Jedermann hat das in § 12 LDSG festgelegte Recht auf Auskunft, ob das Krebsregister über ihn Daten speichert. Jede gespeicherte Person kann jederzeit die Löschung ihrer Daten im Krebsregister verlangen.
- Straf- und Bußgeldtatbestände sollten zur Einhaltung der Vorschriften des Gesetzes beitragen.

2. Abschnitt: Medizinische Forschung

1. Studie über Morbus Crohn und Colitis ulcerosa

Eines Tages las ich im Ärzteblatt Baden-Württemberg, die Universität Tübingen wolle durch eine epidemiologische Untersuchung Häufigkeit und mögliche örtliche Trends von Morbus Crohn und Colitis ulcerosa feststellen — also von zwei chronisch entzündlichen Darmerkrankungen, deren Ursache die Medizin bis heute weitgehend nicht kennt. Diese Veröffentlichung und ein Rundschreiben des Forscherteams forderten die niedergelassenen Ärzte auf, die Namen ihrer von diesen Krankheiten befallenen Patienten dem Chefarzt der Inneren Abteilung des Krankenhauses mitzuteilen, mit dem sie jeweils zusammenarbeiten, und dabei anzugeben, wo sich die Krankenakten der einzelnen Patienten befinden. Das Forscherteam beabsichtige, durch Vermittlung dieser Chefarzte die Krankenakten einzusehen und daraus folgende Daten zu entnehmen: Namen des Patienten, Wohnort, Alter, Beruf, Nationalität, Art der Erkrankung, Beschwerden, Erkrankungsbeginn, diagnostische Eingriffe und deren Befunde, die zur Diagnosestellung geführt haben.

An dieser Aufforderung erstaunte mich sehr, daß sie mit keinem Wort auf die aus dem Arztgeheimnis folgende Notwendigkeit einging, die Einwilligung der Patienten einzuholen. Sie begnügten sich mit dem Hinweis, man werde Arztgeheimnis und Datenschutz durch ein Verschlüsselungssystem Rechnung tragen. Die Universität halte die Namen der Patienten und deren Adresse unter Verschuß und vernichte sie nach Abschluß der etwa 3½ Jahre laufenden Studie. Wie spätere Kontakte zeigten, dachte in der Tat niemand daran, die Einwilligung der Patienten einzuholen.

Gemeinsam mit der Landesärztekammer konnte ich das Forschungsteam überzeugen, daß dies notwendig ist. Die Bezirksärztekammer wies in einem Rundschreiben die niedergelassenen Ärzte darauf hin. Außerdem zeigte ich der Universität Möglichkeiten auf, wie sie das Forschungsvorhaben in Einklang mit dem Landesdatenschutzgesetz durchführen kann. Die Forscher gingen mit großer Bereitschaft auf diese Vorschläge ein und trugen so entscheidend dazu bei, daß das Forschungsvorhaben unter Wahrung des Persönlichkeitsschutzes der Patienten abläuft.

Dieses Forschungsvorhaben erscheint mir aus zwei Gründen erwähnenswert. Zum einen zeigt es, wie wenig sich noch bis vor kurzem Forscher bewußt waren, daß das Arztgeheimnis auch unter Ärzten gilt und deshalb behandelnde Ärzte unter das Arztgeheimnis fallende Angaben nur anonymisiert oder mit Einwilligung ihrer Patienten an eine wissenschaftliche Einrichtung weitergeben dürfen. Die Landesärztekammer sollte sich fragen, warum ihre Berufsordnung in dieser Frage so wenig beachtet wurde und ob sie mit dem nötigen Nachdruck ihren Aufgaben nachkam, für die Einhaltung dieser Regelung zu sorgen. Zum anderen zeigt das Vorhaben erneut, daß es durchaus möglich ist, medizinische Forschung im Rahmen des geltenden Rechts zu betreiben und welche erfreuliche Bereitschaft besteht, seinen Anforderungen gerecht zu werden. Voraussetzung dafür ist jedoch, die vorhandene Unsicherheit durch geeignete Informationen zu beseitigen.

2. Krebsregister Nordbaden

Auf eine zum Glück ziemlich einzigartige Weise erfuhr ich vom Krebsregister Nordbaden. Eines Tages suchte ein junger Doktorand meine Dienststelle auf und bat um Beratung. Er brachte

eine dicke Computerliste mit, auf der neben einer Reihe von zunächst nichtssagenden Zahlen Name, Vorname, Geburtsdatum, Geschlecht und Postleitzahl von ca. 15 000 Personen eingetragen waren. Auch hatte er ein Schreiben in Besitz, das dem Inhaber bescheinigt, Mitarbeiter des Regionalen Krebsregisters Nordbaden zu sein. Die Unterzeichner des Schreibens bitten darin, den Inhaber zu unterstützen, der im Rahmen einer Doktorarbeit speziell die Überlebensrate krebskranker Patienten zu untersuchen habe. Mit dieser Bescheinigung und der Computerliste hatte der Doktorand bei einem Standesamt vorgesprochen und nachgefragt, ob er dort erheben kann, welche der in der Computerliste genannten Personen bereits und zu welcher Zeit gestorben sind. Das Standesamt hatte offensichtlich Bedenken, dieser Bitte nachzukommen und verwies den Doktoranden an mich. Meine Ermittlungen ergaben:

Das Pathologische Institut der Universität Heidelberg führt das Regionale Krebsregister Nordbaden. Ziel dieses Registers ist in erster Linie, Patienten zu erfassen, die ihren Hauptwohnsitz innerhalb des ehemaligen Regierungsbezirks Nordbaden und des Stadt- und Landkreises Heilbronn haben und bei denen die Diagnose eines bösartigen Magen-Darm-Tumors histologisch gesichert ist. Die hierfür benötigten Daten erhebt das Krebsregister Nordbaden bei Pathologischen Instituten seines Einzugsgebiets. Die Erhebung erfolgt formlos durch Überlassen von Abschriften der Befundberichte, auf denen neben dem Befund Name, Vorname, Geburtsdatum und häufig auch noch der Wohnort mit Postleitzahl des Patienten angegeben sind. Diese Daten erfaßt dann das Pathologische Institut der Universität Heidelberg, indem es die eigentlichen Befunddaten in codierter Form getrennt von den die Identifizierung der Krebskranken ermöglichenden Daten speichert. Die Klartextspeicherung der Identifizierungsdaten hält es für erforderlich, um sicherzustellen, daß jeder Patient und die dazugehörigen Befunde nur einmal gespeichert werden. Insgesamt enthält das Krebsregister Nordbaden zur Zeit ca. 23 000 Fälle aus der Zeit ab 1971.

In rechtlicher Hinsicht wirft das Register die vor allem im 2. Tätigkeitsbericht bereits eingehend dargelegten Probleme auf. Die beteiligten Pathologischen Institute holen weder für die Überlassung der Befundberichte noch für die Speicherung der Daten im Register die Einwilligung der Patienten ein. Das Überlassen der Befundberichte ohne Einverständnis der Patienten ist aber bekanntlich eine Verletzung der ärztlichen Schweigepflicht. Allein schon aus diesem Grunde ist die Speicherung im Register ebenfalls rechtswidrig.

Ich beanstandete diese Datenverarbeitung bisher noch nicht, weil ich zunächst trotz des damit verbundenen Zeitaufwands alle Möglichkeiten erkunden möchte, ob sich das Ziel des Registers auf andere, rechtlich zulässige Weise erreichen läßt. Das Krebsregister Nordbaden könnte seine Aufgabe als Inzidenzregister nämlich auch mit anonymisierten Angaben erfüllen, wenn sich sicherstellen läßt, daß jeder Patient nur einmal gespeichert wird. Wegen der wenigen Datenlieferanten frage ich mich, ob dies durch Vergabe eines Ordnungsmerkmals geschehen kann, das die meldenden Stellen selbst durch Verschlüsseln der Identifizierungsdaten bilden. Ob und inwieweit dies realisierbar ist, prüfe ich zur Zeit. Erweist sich der Weg über das Ordnungsmerkmal als gangbar, kommt es ganz entscheidend darauf an, inwieweit die beteiligten Pathologischen Institute bereit sind, solche zu vergeben und damit dazu beizutragen, daß das Krebsregister weitergeführt werden kann.

3. Auskünfte aus Personenstandsbüchern zur Erforschung von Krankheiten des Nervensystems

Bitter beklagte sich über die Standesämter bei mir ein Arzt, der sich neben seiner Arbeit im Krankenhaus wissenschaftlich betätigt. Die Standesämter verweigern ihm zunehmend unter Hinweis auf den Datenschutz Auskünfte aus Personenstandsbüchern. Zur Durchführung seines Forschungsvorhabens auf dem Gebiet der Gehirn- und Nervenerkrankungen benötigt er aber die Geburtsdaten der Vorfahren von Patienten, die an einer bestimmten erblichen Krankheit leiden. Leider habe ihn auch das zuständige Regierungspräsidium nach anfänglicher Unterstützung im Stich gelassen. Es habe dabei auf das Datenschutzgesetz und die Datenschutzbeauftragte des Landes verwiesen und ihm gleichzeitig bedeutet, daß von dort kein Verständnis für seine Forschung zu erwarten sei.

Dieser Fall ist bis zu einem gewissen Grade symptomatisch dafür, wie sich einzelne Behörden im Lande mit dem Datenschutz auseinandersetzen. Obwohl sich Auskünfte aus Personenstandsbüchern ausschließlich nach § 61 des Personenstandsgesetzes und nicht nach dem Landes- oder Bundesdatenschutzgesetz richten, verweigern Standesämter offenbar wesentlich häufiger als früher Auskünfte mit dem Hinweis auf den Datenschutz. Ein mit der Rechtslage nicht Vertrauter muß daraus den Eindruck gewinnen, die neuere Datenschutzgesetzgebung habe die Erteilung von Auskünften gegenüber früher wesentlich eingeschränkt. Verborgen bleibt, daß die geltende Fassung des § 61 des Personenstandsgesetzes aus dem Jahr 1958 stammt und sich seit dieser Zeit die Rechtslage nicht im geringsten geändert hat. Ein solches Verhalten ist sehr wohl geeignet, den Datenschutz in Mißkredit zu bringen. Nicht zuletzt in diesem Zusammenhang fällt häufig das böse Wort vom überzogenen Datenschutz. Verstärkt wird diese Wirkung gar noch, wenn die Behörden zur Begründung ihrer Ablehnung gleichzeitig auf die Landesbeauftragte für den Datenschutz verweisen und mir die Rolle des Buhmanns zudiktieren. Dies kommt nach meinen Erfahrungen gar nicht selten vor.

In der Sache selbst konnte ich dem Arzt sagen, daß er als privater Forscher nicht unmittelbar Auskunft vom Standesamt erhalten kann. Die Standesbeamten dürfen ihm nur die erbetene Auskunft geben, wenn er eine Vollmacht dessen, auf den sich der Eintrag im Personenstandsbuch bezieht, oder seines Ehegatten oder eines seiner Verwandten in gerader Linie vorlegen kann. Nicht bestätigen konnte ich dem Arzt seine weitere Befürchtung, er müsse dem Standesamt auch mitteilen, daß er die Angaben zur Erforschung von erblichen Krankheiten des Nervensystems benötigt.

Unabhängig von diesem konkreten Fall befriedigt die Regelung des § 61 des Personenstandsgesetzes nicht durchweg. Der Schutz der Daten Verstorbener könnte gelockert werden. Mir ist bekannt, daß solche Bestrebungen im Interesse der genealogischen Forschung im Gange sind.

3. Abschnitt: Sozialforschung

1. Erfahrungen aus den Kontrollbesuchen bei den Universitäten Konstanz und Karlsruhe

Die Sozialforschung arbeitet ebenso wie die medizinische Forschung in sehr starkem Maße mit teilweise höchst sensiblen persönlichen Daten. Aus diesem Grunde ging ich im vergangenen Jahr gezielt der Frage nach, in welcher Weise die Sozialforschung

an den Universitäten des Landes Daten erhebt und nutzt und wie sich das Landesdatenschutzgesetz auf diesen Forschungsbereich auswirkt. Ich führte an den Universitäten Konstanz und Karlsruhe Kontrollbesuche durch und überprüfte dabei eine Reihe von Forschungsvorhaben. Gegenstand meiner Kontrolle waren im wesentlichen Projekte, bei denen die Forscher einen nach bestimmten Kriterien ausgewählten Personenkreis gezielt angingen, schriftlich oder mündlich befragten und/oder untersuchten und die dabei gewonnenen Daten auswerteten. Bei diesen Kontrollbesuchen stellte sich heraus, daß es im wesentlichen zwei Problembereiche sind, vor die sich der Forscher in bezug auf den Datenschutz gestellt sieht, nämlich die Beschaffung von Adreßdaten und die Datenverarbeitung durch den Forscher selbst.

1.1 Beschaffung von Adreßdaten

Wollen Forscher nach bestimmten Kriterien ausgewählte Personen ansprechen — man denke an Schüler, Studenten, Eltern mit Kindern, Senioren usw. —, sind sie vielfach darauf angewiesen, daß ihnen öffentliche Stellen Namen und Anschriften der betroffenen Personengruppen überlassen. Ganz offensichtlich führte die Diskussion über das Verhältnis von Datenschutz und Forschung bei Forschern und Behörden zu einer gewissen Verunsicherung darüber, was noch zulässig ist und was nicht. Vor allem fühlen sich die Behörden in dieser Frage allein gelassen. Das zeigte sich nicht nur bei den Kontrollbesuchen selbst, sondern auch bei einer Reihe von Anfragen von Behörden und Forschern im Laufe des Berichtsjahres. Eine nähere Analyse der Fälle ergab, daß jedenfalls das Landesdatenschutzgesetz berechtigten Wünschen der wissenschaftlichen Forschung nach Adreßdaten nicht im Wege steht.

Jede öffentliche Stelle im Land darf nach § 20 Abs. 1 Satz 2 LDSG Adreßdaten zur Befragung oder Untersuchung bestimmter Personengruppen an Hochschulen und andere öffentliche Einrichtungen mit der Aufgabe unabhängiger Forschung übermitteln, wenn der betroffene Bürger einverstanden ist oder wenn die Art der Verwendung der Daten seine schutzwürdigen Belange nicht beeinträchtigt.

Unproblematisch sind die Fälle der Einwilligung. Sie kommen freilich nur selten vor, da die öffentlichen Stellen im Regelfall nicht bereit sind, den mit der Einholung der Einwilligung verbundenen Arbeitsaufwand zu übernehmen. Aber auch ohne Einwilligung ist die Weitergabe von Adreßdaten von Personengruppen zulässig, wenn die öffentlichen Stellen durch Auflagen oder Vereinbarungen mit den wissenschaftlichen Einrichtungen sicherstellen, daß folgenden Anforderungen entsprochen wird:

- Der Forscher darf die Adreßdaten nur zur Durchführung eines konkreten Forschungsprojekts speichern.
- Der Forscher muß die Adreßdaten der Bürger, die die Teilnahme an der Befragung verweigern, unverzüglich löschen und die der übrigen Bürger, sobald er sie zur Durchführung seines Projekts nicht mehr benötigt.
- Der Forscher muß die ausgewählten Bürger im Anschreiben oder vor dem Interview bzw. der Untersuchung ausdrücklich darauf hinweisen, daß ihre Teilnahme freiwillig ist und daß ihnen aus der Verweigerung der Teilnahme keine Nachteile entstehen.

- Der Forscher muß die mitwirkenden Bürger über das Forschungsprojekt und über die weitere Verwendung der erhobenen Daten und ihrer Adreßdaten aufklären, weil sie nur auf dieser Basis frei entscheiden können, ob sie teilnehmen wollen oder nicht. Der Forscher sollte auch darüber informieren, ob es sich um ein Projekt mit einmaliger oder mehrmaliger Befragung handelt und wie lange der Forscher bei den erhobenen Daten den Bezug zum Befragten herstellen kann. Schließlich sollte er auch darüber unterrichten, woher die Adreßdaten stammen.
- Verarbeitet der Forscher die personenbezogenen Daten, muß er die Vorschriften des Landesdatenschutzgesetzes, insbesondere § 20 Abs. 1 Satz 1 und § 8 LDSG beachten.

Werden die gewünschten Adreßdaten durch besondere Berufsgeheimnisse geschützt, sind diese Geheimhaltungsbestimmungen zusätzlich zu beachten. Deshalb können z. B. öffentliche Stellen Adressen einer Gruppe von Personen, die an einer bestimmten Krankheit leiden, nur im Rahmen der Regeln über die ärztliche Schweigepflicht, also nur mit deren Einwilligung weitergeben. Nicht nach § 20 LDSG sondern nach § 75 des Zehnten Buchs des Sozialgesetzbuchs (SGB X) richtet sich die Weitergabe von Adreßdaten, die durch das Sozialgeheimnis geschützt werden. Dies gilt z. B. für Adreßdaten von Sozialhilfempfängern oder Empfängern sonstiger Sozialleistungen. Dabei ist es wichtig, daß zunächst die öffentliche Stelle die Genehmigung des für sie zuständigen Ministeriums einholen muß, sofern sie Sozialdaten ohne Einwilligung des Betroffenen weitergeben will. Mir ist kein einziger Fall bekannt, in dem Forscher auf solche Weise Adreßdaten erhielten.

1.2 Datenverarbeitung für wissenschaftliche Zwecke

Die Verarbeitung der personenbezogenen Daten, die zur Durchführung eines bestimmten Forschungsvorhabens erhoben worden sind, richtet sich bei Hochschulen und sonstigen öffentlichen Einrichtungen mit der Aufgabe unabhängiger Forschung nach § 20 LDSG. Danach dürfen Forscher solche Daten dann ohne Einwilligung des Betroffenen speichern oder verändern, wenn seine schutzwürdigen Belange wegen der Art ihrer Verwendung nicht beeinträchtigt werden.

Daraus ergeben sich konkret folgende Anforderungen:

- Der Forscher muß die Daten in rechtlich zulässiger Weise erhoben haben. Bei Befragungen muß er den bereits geschilderten Anforderungen Rechnung getragen haben.
- Der Forscher muß die Identifizierungsdaten der befragten Bürger nach der Erhebung unverzüglich gesondert von den übrigen Daten speichern. Dieser Anforderung muß bereits bei der Ausgestaltung der Fragebogen Rechnung getragen werden.
- Diese Datensammlungen dürfen nur zusammengeführt werden, soweit dies für das Forschungsvorhaben unerlässlich ist.
- Der Forscher muß den Kreis der Personen, die die Zusammenführung für ihn durchführen können, konkret festlegen und auf das unbedingt notwendige Maß beschränken.
- Der Forscher muß den Anforderungen des § 8 LDSG an die Datensicherung Rechnung tragen. Vor allem gilt es sicherzustellen, daß Unbefugte nicht auf die Daten zugreifen können.

- Der Forscher darf den Personenbezug nur so lange aufrecht-erhalten, wie dies zur Durchführung seines Forschungsvorhabens und für sich unmittelbar anschließende Nachunter-suchungen erforderlich ist. Ein Aufrechterhalten des Per-sonenbezugs allein deshalb, weil möglicherweise zu einem späteren Zeitpunkt eine Nachuntersuchung in Frage kom-men könnte, ist keine Datenspeicherung für ein bestimm-tes Forschungsvorhaben im Sinne von § 20 Abs. 1 Satz 1 LDSG mehr und damit, sofern für diese Vorratsspeicherung keine Einwilligung der Befragten vorliegt, nach § 5 Abs. 1 in Verbindung mit § 20 Abs. 1 Satz 1 LDSG unzulässig.

Die überprüften, zum Teil schon vor Inkrafttreten des Landes-datenschutzgesetzes begonnenen Forschungsvorhaben tragen, wie sich an Ort und Stelle zeigte, diesen Anforderungen schon weitgehend Rechnung. Insbesondere speichern die Forscher die Identifizierungsdaten durchweg getrennt von den sonstigen Forschungsdaten. Nicht immer befriedigte dagegen die Infor-mation der befragten Personen. Bei verschiedenen Vorhaben erfuhren sie nicht deutlich genug, wie lange das Forschungs-team die Daten voraussichtlich personenbezogen speichert und daß es Wiederholungsbefragungen plant. Eine solch umfas-sende Information ist aber nicht nur aus Gründen des Daten-schutzes erforderlich, sondern liegt mindestens ebenso im In-teresse der Forschung. Denn die Bereitschaft der Bürger, an solchen Forschungsvorhaben teilzunehmen, hängt sehr stark davon ab, ob sie Vertrauen in die Art und Weise, wie die Forscher ihr Projekt durchführen, gewinnen. Solches Vertrauen entsteht keineswegs von selbst. Wesentlich trägt dazu eine umfassende Information des Befragten über das Forschungs-vorhaben bei. Keine Seite brachte mir gegenüber zum Aus-druck, die geschilderten datenschutzrechtlichen Anforderungen würden die Sozialforschung in unzumutbarer Weise beein-trächtigen. Die Forscher empfanden meine Verbesserungsvor-schläge durchweg als hilfreich. Sie zeigten eine große Aufge-schlossenheit und Bereitschaft, den datenschutzrechtlichen An-forderungen Rechnung zu tragen. Deutlich spürte ich aber auch eine gewisse Unsicherheit über die Auswirkungen des gelten-den Datenschutzrechts. Bezeichnend dafür ist die Anregung einer Universität, man möge doch einmal „alle relevanten datenschutzrechtlichen Bestimmungen und Regelungen, die im Zusammenhang mit der Durchführung von Forschungsprojek-ten (mit Personenbezug) regelmäßig auftreten, in überschau-barer Form zusammenstellen“. Damit könne man sich viel Zeit und Beratungsaufwand ersparen. Ich kann nur hoffen, daß das Wissenschaftsministerium diese Anregung baldmöglichst auf-greift.

2. Einzelne Forschungsvorhaben

Beispielhaft schildere ich zwei einer ganzen Reihe untersuchter Forschungsvorhaben.

2.1 Befragung der Technischen Lehrer im Berufsfeld Holztechnik

Immer wieder trifft man auf die Vorstellung, eine Befragung sei schon anonym, wenn auf dem Fragebogen Name und An-schrift des Befragten fehlen. Deshalb fände auf eine solche Be-fragung das Landesdatenschutzgesetz keine Anwendung. Wer dies meint, übersieht, daß personenbezogene Daten nicht nur Einzelangaben über eine bestimmte, sondern auch über eine bestimm-bare Person sind. Bestimmbar ist eine Person, wenn zwar ihr Name unbekannt ist, sich aber aus den sonstigen An-

gaben entweder unmittelbar oder in Verbindung mit vorhandenem oder beschaffbarem Zusatzwissen ableiten läßt, wer die konkrete Person ist. Ein typischer Fall einer solchen vermeintlichen anonymen Befragung ist eine Befragungsaktion der Landesanstalt für Erziehung und Unterricht aus dem Jahre 1981. Die Umfrage erfolgte im Rahmen einer Untersuchung zur Gestaltung der praktischen Fachkunde in der Grundstufe des Berufsfeldes Holztechnik. Die Landesanstalt für Erziehung und Unterricht befragte ca. 150 Technische Lehrer an 40 beruflichen Schulen im Lande. Ihr Fragebogen enthielt u. a. Fragen nach der individuellen Einstellung des Befragten zu didaktischen Aussagen, nach der Gestaltung des Unterrichts und nach Kritik und Vorschlägen über die Gestaltung der praktischen Fachkunde. Daneben erfragte er auch noch eine Reihe von Angaben zur Person, u. a. das Alter des Lehrers, Einzelheiten seiner Ausbildung, seine Tätigkeiten in der betrieblichen Praxis, Teilnahme an Fortbildungsveranstaltungen und Ausbildertätigkeit bei der Innung. Schließlich war auf jedem Fragebogen eine Nummer eingetragen, die zuvor die Landesanstalt für Erziehung und Unterricht für die einzelnen Schulen vergeben hatte. Auf diese Weise wußte sie zusätzlich, an welcher Schule der Lehrer beschäftigt war, der den Fragebogen ausgefüllt hatte. Mit diesen Informationen hätte die Landesanstalt für Erziehung und Unterricht — wie sie selbst auch einräumt — ohne größere Schwierigkeiten die einzelnen Lehrer identifizieren können, die den Fragebogen beantwortet haben. Eine solche Identifizierungsmöglichkeit führt allerdings nicht, wie auch gelegentlich manche meinen, von vornherein zur Unzulässigkeit der Untersuchung. Sie bedeutet zunächst nur, daß beim Erheben und Verarbeiten der Daten das Landesdatenschutzgesetz zu beachten ist. Dieses läßt solche Befragungen und die anschließende Datenverarbeitung durchaus auch dann zu, wenn die Daten nicht völlig anonym sind. Vor allem geht dies bei Einwilligung der Befragten. Sie ist bei Untersuchungen der geschilderten Art wirksam, wenn die forschende Stelle die Befragten hinreichend deutlich auf ihre Freiwilligkeit, an der Untersuchung mitzuwirken, und die vorgesehenen Auswertungen informierte. Nicht notwendig ist bei dieser Vorgehensweise, die Einwilligung schriftlich einzuholen. Dies wäre in der Tat überzogener Formalismus, der zu einer sachlich nicht zu rechtfertigenden Behinderung der Untersuchung führen könnte. Die Landesanstalt für Erziehung und Unterricht beachtete die geschilderten Anforderungen an die Einwilligung im wesentlichen. Wünschenswert wäre es allerdings, wenn sie in Zukunft deutlicher als dies bei der konkreten Untersuchung der Fall war, auf die Freiwilligkeit und die beabsichtigte Verwendung der Daten hinweisen würde. Eine klare Information ist nicht nur für die Betroffenen von entscheidender Bedeutung. Sie kann auch verhindern, daß Mißverständnisse entstehen, und damit die Bereitschaft steigern, an solchen Befragungen teilzunehmen.

2.2 Forschungsvorhaben „Informelle Reaktionen nach Jugendstrafrecht“

Wie unbegründet der pauschale Vorwurf ist, der Datenschutz behindere die Forschung in unververtretbarer Weise, zeigt ein Forschungsvorhaben eines Universitätsinstituts für Rechtstatensachenforschung besonders deutlich. Es will erstmals auf wissenschaftlicher Basis feststellen,

— in welchem Umfang Staatsanwaltschaften und Gerichte bei Jugendlichen, die einer Straftat überführt sind, erzieheri-

sche Maßnahmen anordnen, anstatt ein förmliches Verfahren nach dem Jugendgesetz mit dem Ziel der Bestrafung durchzuführen,

- wie sich dieses Vorgehen auf Verfahrensdauer und Erledigungsökonomie der Strafverfolgungsorgane auswirkt,
- welcher Art die angeordneten erzieherischen Maßnahmen sind,
- ob und bei welchen Tätergruppen sie so erfolgreich verlaufen, daß der Jugendliche eine weitere straffreie Lebensführung erwarten läßt.

Für die Durchführung dieses Forschungsvorhabens benötigt das Universitätsinstitut Daten verschiedener Behörden. Sie will sie sich in mehreren Schritten beschaffen. Zunächst stellt das Statistische Landesamt anhand seiner Staatsanwaltsstatistik die einschlägigen Verfahren fest und teilt sie dem Universitätsinstitut unter Angabe der Art des Verfahrensabschlusses, der Verfahrensdauer, Region und des Aktenzeichens der Staatsanwaltschaft mit. Das Universitätsinstitut bittet sodann die Staatsanwaltschaften, zu den Verfahrensaktenzeichen die Personalien der Jugendlichen mitzuteilen. Mit deren Hilfe will das Universitätsinstitut vom Bundeszentralregister erfahren, ob der Jugendliche erneut straffällig wurde, und bejahendenfalls die Art der abgeurteilten Straftat und die Art der verhängten Sanktion. Die so erhobenen Daten will das Institut auf zwei getrennt aufbewahrten Datenträgern speichern, die ein gemeinsames Verbindungsmerkmal haben. Auf den ersten Datenträger kommt eine laufende Nummer, die Art des Verfahrensabschlusses, die Verfahrensdauer und Angaben über eine etwaige erneute Straffälligkeit (Art der abgeurteilten Straftat, Art der verhängten Sanktion). Auf dem zweiten Datenträger werden die Personalien der Jugendlichen und die Verfahrensaktenzeichen der Staatsanwaltschaften erfaßt. Diese Daten will das Institut jedoch löschen, sobald es die erhaltenen Daten aus dem Bundeszentralregister codiert hat.

Gegen dieses Forschungsvorhaben bestehen aus der Sicht des Datenschutzes keine Bedenken. Die Datenübermittlungen durch das Statistische Landesamt und die Staatsanwaltschaften und die Datenspeicherungen des Universitätsinstituts sind durch § 20 Abs. 1 LDSG gedeckt. Nichts einzuwenden habe ich auch gegen die vorgesehene Übermittlung von Daten aus dem Bundeszentralregister. Nach § 40 Abs. 2 des Bundeszentralregistergesetzes darf der Generalbundesanwalt nämlich für wissenschaftliche Forschungsvorhaben unbeschränkt Auskunft aus dem Register erteilen, wenn und soweit die Bedeutung des Forschungsvorhabens dies rechtfertigt und die Gewähr besteht, daß ein Mißbrauch der bekanntzugebenden Eintragungen nicht zu befürchten ist. Ob dies im konkreten Fall so ist, unterliegt allerdings letztlich nicht meiner Beurteilung, da der Generalbundesanwalt eine Bundesbehörde ist.

4. Abschnitt: Archivwesen

1. Allgemeines

An den vor allem im 2. Tätigkeitsbericht geschilderten Problemen im Verhältnis von Datenschutz und Archivwesen änderte sich im vergangenen Jahr nichts. Die Archivverwaltung hat nach wie vor Schwierigkeiten, alle archivwürdigen Unterlagen zu erhalten. Der Grund dafür ist nicht das Landesdatenschutzgesetz oder gar, wie

das Wissenschaftsministerium in der Beantwortung einer Kleinen Anfrage zur Frage des Datenschutzes im Archivwesen (Landtags-Drucksache 8/2048) meinte, die Landesbeauftragte für den Datenschutz. Das Haupthindernis sind die Berufs- und besonderen Amtsgeheimnisse, wie zum Beispiel das Statistik-, das Steuer- und das Arztgeheimnis. Bei diesen besonderen Geheimhaltungsvorschriften kann man sich in der Tat fragen, ob sie das von den Archiven zu verfolgende öffentliche Interesse, für die Erforschung und Darstellung der Geschichte und des Zeitgeschehens aufschlußreiche Unterlagen zu sammeln und aufzubewahren, in ausreichendem Maße berücksichtigen. Nach wie vor besteht auch noch eine große Unsicherheit bei den Behörden und Archiven darüber, ob und unter welchen Voraussetzungen sie zeitgeschichtlich interessierten Personen und Stellen Unterlagen zur Verfügung stellen dürfen. Noch allzu oft wird dabei mit dem Schlagwort Datenschutz gearbeitet, auch wenn das Landesdatenschutzgesetz auf diesen Sachverhalt überhaupt keine Anwendung findet. Allerdings glaube ich, eine gewisse Entspannung und Entkrampfung der Diskussion feststellen zu können. Insbesondere erkennen die Archivare selbst die wahren Probleme und ihre Ursachen deutlicher als bisher. Der Datenschutz wird auch nicht mehr pauschal zum Sündenbock gestempelt. Leider trug das für das Archivwesen zuständige Wissenschaftsministerium selbst bisher kaum etwas Wesentliches zur Problemlösung bei. Die einzige mir bekannte Initiative ist sein Vorschlag für eine Änderung des § 13 Abs. 3 des Landesdatenschutzgesetzes und des § 2 Abs. 2 des Gesetzes über die Gliederung der Archivverwaltung, die in dem Gesetzentwurf der Landesregierung eines 2. Gesetzes zur Änderung des Landesdatenschutzgesetzes (Stand: 26. Okt. 1982) enthalten ist. Ziel der angestrebten Änderung des § 13 des Landesdatenschutzgesetzes ist, in dieses Gesetz eine sog. Archivklausel aufzunehmen. In § 2 Abs. 2 des Gesetzes über die Gliederung der Archivverwaltung will man klarstellen, daß zum Archivgut auch Dateien zählen, die nicht in Schriftform vorliegen. Dieser Gesetzesvorschlag ist nicht geeignet, die Probleme zu lösen, vor denen die Archivverwaltung steht. Notwendig ist nach wie vor eine bessere Information der Behörden und sonstigen Stellen über die derzeitige Rechtslage. Notwendig ist aber vor allem auch der Erlass eines Archivgesetzes. Das Wissenschaftsministerium hat zwar in seiner Antwort auf die bereits erwähnte Kleine Anfrage die Vorlage eines Gesetzentwurfs angekündigt. Es konnte sich aber bis jetzt, wie es mich wissen ließ, noch nicht zu einer endgültigen Entscheidung durchringen, ob es tatsächlich einen solchen Gesetzentwurf ausarbeitet.

2. Empfehlungen zum Inhalt eines Landesarchivgesetzes

Meine Kollegen in Bund und Ländern teilen meine Auffassung über die Notwendigkeit eines Archivgesetzes, das einerseits die Voraussetzungen für eine sachgerechte Archivtätigkeit schaffen und andererseits den gebotenen Schutz der Persönlichkeitsrechte der Betroffenen gewährleisten soll. Wir erarbeiteten deshalb in der Konferenz der Datenschutzbeauftragten eine Reihe von Empfehlungen zum Inhalt eines Archivgesetzes. Im wesentlichen geht es um folgendes:

- Die Aufgaben der Archive sind klar zu umschreiben. Festzulegen ist auch, welches Archiv jeweils für welche Stelle zuständig ist.
- Der Zugang der Archive zu den Daten ist sicherzustellen. Soweit Daten durch besondere Geheimhaltungsvorschriften geschützt sind, ist dabei dem Schutzzweck dieser Regelungen Rechnung zu tragen.

- Die Auswirkungen der Sperrungs- und Löschungsvorschriften der Datenschutzgesetze auf die Verwaltung dürfen nicht durch Überlassen von Unterlagen an die Archive umgangen werden. Auszugehen ist vielmehr von einer grundsätzlichen Trennung von Verwaltungs- und Archivtätigkeit.
- Jeder Betroffene hat zur Wahrung seines Persönlichkeitsrechts ein Auskunftsrecht über seine in Dateien gespeicherten personenbezogenen Daten. Im übrigen ist jedem Betroffenen ein Recht auf Akteneinsicht und ein Recht auf Gegendarstellung einzuräumen, soweit aus Gründen der historischen Wahrheit ein Berichtigungsanspruch ausscheiden muß.
- Sicherzustellen ist, daß die Benutzung der Archive schutzwürdige Belange der Betroffenen nicht beeinträchtigt. Dazu eignen sich vor allem Fristen, innerhalb derer die Nutzung grundsätzlich ausgeschlossen ist. Die zeitgeschichtliche Forschung sollte jedoch die Möglichkeit erhalten, schon vor deren Ablauf unter genau festzulegenden Voraussetzungen das Material nutzen zu können.

3. Teil: Öffentliche Sicherheit und Strafrechtspflege

1. Abschnitt: Verfassungsschutz

1. Registrierung von Auskunftersuchen der Bürger und Anfragen des Landesbeauftragten für den Datenschutz

Bei einem Kontrollbesuch des Landesamts für Verfassungsschutz stellte ich ein ungewöhnliches Verfahren fest. Das Landesamt für Verfassungsschutz bringt in der Karteikarte des Bürgers, der bei ihm einen Antrag auf Auskunft über seine gespeicherten Daten stellt oder in dessen Sache ich auf Grund einer Eingabe des Bürgers tätig werde, einen entsprechenden Vermerk an. Um Mißverständnisse zu vermeiden, will ich dazu gleich sagen: Karteikarten führt das Landesamt für Verfassungsschutz nur über solche Personen, die — wie es mir schreibt — „dreimal oder öfter im Sinne des gesetzlichen Auftrags des Verfassungsschutzes konkret und relevant in Erscheinung getreten sind“. Das bedeutet: Es erfaßt Auskunftersuchen der Bürger und meine Anfragen dann, wenn bereits über den Betroffenen wegen mindestens drei Vorgängen beim Verfassungsschutz eine Karteikarte angelegt ist. Seine Maßnahme begründet es mit der Gefahr der Ausforschung. Bei dem beschriebenen Personenkreis liegt nach Auffassung des Landesamtes für Verfassungsschutz und des Innenministeriums „nahe, daß es sich um Ausforschungsbemühungen handelt“.

Ich habe über Monate hinweg, zuletzt in einem persönlichen Gespräch mit dem Herrn Innenminister, versucht, eine Änderung dieser Praxis herbeizuführen. Leider war dies vergeblich. Ich meine, daß es bei der Frage der Registrierung dieser Vorgänge abseits aller rechtlichen Überlegungen zwei Aspekte zu bedenken gilt:

- Der eine ist datenschutzrechtlicher Natur. Das Landesdatenschutzgesetz räumt dem Bürger zwei ganz wesentliche Rechte ein: Zum einen kann er nach § 12 von der speichernden Stelle Auskunft über seine gespeicherten Daten verlangen. Die Auskunft hierüber versetzt ihn oftmals überhaupt erst in die Lage, weitergehende Anträge zu stellen, beispielsweise auf Löschung seiner Daten. Daß die Sicherheitsbehörden nach Prüfung des Einzelfalls die Auskunft verweigern dürfen, ändert an dieser

grundsätzlich bestehenden Möglichkeit nichts. Zum zweiten hat der Bürger nach § 19 des Landesdatenschutzgesetzes das Recht, sich an mich zu wenden, wenn er der Ansicht ist, bei der Verarbeitung seiner personenbezogenen Daten durch eine Behörde in seinen Rechten verletzt zu sein.

Die geschilderte Praxis des Landesamts für Verfassungsschutz erschwert die legitime Ausübung dieser beiden Rechte faktisch erheblich. Der Bürger wird sich künftig zweimal überlegen, ob er einen Auskunftsantrag stellen oder sich in einer Eingabe an mich wenden soll, wenn er gewärtigen muß, daß dies für ihn zu einer besonderen Kennzeichnung beim Verfassungsschutz führt. Nicht nur dies wird ihn abschrecken. Er wird darüber hinaus befürchten, daß er mit einem Auskunftsantrag oder einer Eingabe ein zusätzliches Verdachtsmoment gegen sich schafft und möglicherweise weitere Aktivitäten des Verfassungsschutzes auslöst. Solche Befürchtungen sollte der Bürger nicht haben müssen. Er sollte sich insbesondere jederzeit vertrauensvoll an mich wenden können, ohne mit irgendwelchen Nachteilen rechnen zu müssen. Dies ist in einem Bereich, der dem Bürger weitgehend verschlossen ist und in dem viele — oft zu Unrecht — skeptischer sind als in anderen Bereichen, besonders wichtig. Es liegt nicht zuletzt auch im Interesse der Behörden, daß der Landesbeauftragte für den Datenschutz gerade hier ungestört seiner Rolle als Mittler zwischen Bürger und Verwaltung gerecht werden und zum Abbau unbegründeten Mißtrauens beitragen kann.

- Der zweite Aspekt betrifft die Sicherheitsinteressen des Staates. Selbstverständlich muß man verhindern, daß bei Auskunftsanträgen oder Bürgereingaben der Verfassungsschutz ausgeforscht wird. Ob man allerdings — wie es das Landesamt für Verfassungsschutz und das Innenministerium tun — bei jedem, über den der Verfassungsschutz bereits eine Karteikarte angelegt hat, eine solche Ausforschungsabsicht unterstellen kann, halte ich in tatsächlicher Hinsicht für mehr als zweifelhaft und damit auch in rechtlicher Hinsicht für problematisch. Denn eine Auskunftsverweigerung läßt sich nur auf konkrete Anhaltspunkte für eine Ausforschungsabsicht stützen. Wichtig erscheint mir, daß der Verfassungsschutz schon nach dem Landesdatenschutzgesetz einer Ausforschung wirksam begegnen kann. Er kann in diesem Fall nämlich einen Auskunftsantrag nach § 12 Abs. 2 des Landesdatenschutzgesetzes ablehnen. Weitergehender Maßnahmen aus Sicherheitsgründen bedarf es gegenwärtig nicht. Nicht möglich ist auch eine Ausforschung auf dem Umweg über meine Dienststelle. Stellt der Bürger bei mir einen Antrag auf Auskunft über seine beim Verfassungsschutz gespeicherten Daten, verweise ich ihn unter Darlegung der Rechtslage an das dafür allein zuständige Landesamt für Verfassungsschutz. Wendet sich der Bürger mit einer Eingabe nach § 19 LDSG an mich, prüfe ich die Rechtmäßigkeit einer etwaigen Datenverarbeitung durch den Verfassungsschutz. Dabei erfahre ich natürlich, ob das Landesamt für Verfassungsschutz Daten des Bürgers speichert oder nicht. Ich teile dem Bürger nur das Ergebnis meiner Prüfung mit, nicht auch, ob und gegebenenfalls welche Daten über ihn gespeichert sind, sofern das Landesamt für Verfassungsschutz in rechtlich zulässiger Weise der Auskunftserteilung widersprochen hat oder widersprechen könnte. In jedem Fall tausche ich meine Überlegungen darüber mit dem Landesamt für Verfassungsschutz aus.

Dies zeigt einmal mehr, daß sich in der Praxis die Interessen des Datenschutzes und Sicherheitsbelange ohne weiteres miteinander vereinbaren lassen. Ich hoffe sehr, daß sich das Landesamt für

Verfassungsschutz und das Innenministerium doch noch der Praxis anderer Verfassungsschutzbehörden anschließen, die nach einer von mir durchgeführten Umfrage bei meinen Kollegen in Bund und Ländern auf eine Registrierung von Auskunftsanträgen und Bürgereingaben in der geschilderten Form verzichten.

2. Personenüberprüfung

2.1 Überprüfung von Personen mit Zugangsberechtigung zu Sicherheitsbereichen auf dem Flughafen Stuttgart

Bereits in meinem 2. Tätigkeitsbericht stellte ich einige aus der Sicht des Datenschutzes bedenkliche oder verbesserungsbedürftige Personenüberprüfungsverfahren dar, an denen das Landesamt für Verfassungsschutz mitwirkt. Ein weiteres Verfahren dieser Art ist die Überprüfung von Personen mit Zugangsberechtigung zu Sicherheitsbereichen auf dem Flughafen Stuttgart. Dazu muß man folgendes wissen: Auf dem Flughafen Stuttgart sind aus Sicherheitsgründen auf Grund eines vom Bundesminister des Innern erstellten Plans Sicherheitsbereiche eingerichtet. Zu diesen haben nur Personen mit einem besonderen Ausweis Zutritt. Den Ausweis stellt die Stuttgarter Flughafen GmbH, die Betreiberin des Flughafens, auf Zeit oder auf Dauer aus. Zeitausweise erhalten vor allem Personen, die vorübergehend — beispielsweise wegen dringender Reparaturen oder Wartungsarbeiten — den Sicherheitsbereich betreten müssen. Vor Ausstellung des Ausweises wird ein behördliches Personenüberprüfungsverfahren durchgeführt.

2.1.1 Regelung des Personenüberprüfungsverfahrens

Früher lief das Personenüberprüfungsverfahren wie folgt ab: Die Stuttgarter Flughafen GmbH stellte beim Polizeirevier Flughafen Stuttgart per Vordruck einen Antrag auf Personenüberprüfung. Aus dem Vordruck ergaben sich die Personalien des Betroffenen und seine Aufgabe. Das Polizeirevier leitete diese Unterlagen an die Polizeidirektion Esslingen, die die polizeilichen Informationssysteme abfragte. Außerdem übermittelte sie die Personalien dem Landesamt für Verfassungsschutz, das in seinem Bereich eine Erkenntnisabfrage durchführte und erforderlichenfalls weitergehende Sicherheitsermittlungen anstellte. Es beteiligte ferner das Landeskriminalamt, das das PIOS-System abfragte und die Erkenntnisse dem Landesamt für Verfassungsschutz mitteilte. Dieses bewertete sodann alle ihm vorliegenden Erkenntnisse und gab das Ergebnis über die Polizeidirektion Esslingen dem Polizeirevier Flughafen Stuttgart bekannt. Dieses teilte der Stuttgarter Flughafen GmbH dann mit, ob das Ausstellen des Ausweises befürwortet wird oder nicht. Die Anhörung des Betroffenen vor einer beabsichtigten Ablehnung war nicht vorgesehen.

2.1.2 Beurteilung des bisherigen Verfahrens

Gegen eine Sicherheitsüberprüfung von Personen, die Sicherheitsbereiche auf einem Flughafen betreten wollen, bestehen keine grundsätzlichen Bedenken. Sie muß jedoch in rechtlich einwandfreier Weise geschehen. Ausdrücklich betonen möchte ich auch, daß das Polizeirevier Flughafen Stuttgart nach meinem Eindruck die ihm zugewiesene Aufgabe verantwortungsbewußt und sach-

gerecht wahrnahm. Gleichwohl war das Überprüfungsverfahren aus meiner Sicht in einigen Punkten problematisch und zumindest verbesserungsbedürftig:

- So war nicht gewährleistet, daß der Betroffene von der Durchführung der Sicherheitsüberprüfung überhaupt Kenntnis erhielt.
- Die Übermittlung von Erkenntnissen des Landeskriminalamts an das Landesamt für Verfassungsschutz war nicht erforderlich. Dem Landesamt für Verfassungsschutz kommt in Personalüberprüfungsverfahren keinesfalls generell die Rolle zu, die Erkenntnisse der Sicherheitsbehörden zusammenzufassen. Eine solche Praxis läßt das unter anderem in den Verfassungsschutzgesetzen enthaltene Trennungsprinzip von Verfassungsschutz und Polizei außer acht, das auch zu einer Einschränkung des Informationsflusses zwischen beiden führen muß.
- Nicht korrekt war die Übermittlung personenbezogener Daten an das Polizeirevier Flughafen Stuttgart. § 10 Abs. 1 LDSG verlangt nämlich, daß der Datenempfänger Daten zur Erfüllung der in seiner „Zuständigkeit“ liegenden Aufgaben benötigt. Abgesehen von Eilfällen war der Polizeivollzugsdienst nicht zuständig. Die Personenüberprüfung ist nämlich eine Maßnahme, die dem Schutz vor Angriffen auf die Sicherheit des Luftverkehrs dient. Sie obliegt nach dem 1980 eingeführten § 29 c des Luftverkehrsgesetzes der Luftfahrtbehörde, also dem Regierungspräsidium Stuttgart.
- Problematisch war schließlich, daß das Überprüfungsverfahren dem Überprüften keine ausreichende Möglichkeit zur Rechtfertigung gab. Daß ein bei einer bestimmten Firma Beschäftigter unter Umständen mit erheblichen Nachteilen rechnen mußte, wenn die Polizei Sicherheitsbedenken gegen ihn erhob, liegt auf der Hand. Es ist deshalb ein rechtsstaatliches Gebot, ihn bei Vorliegen relevanter Erkenntnisse vor einer Entscheidung anzuhören.

Einen Teil dieser Bedenken sahen auch das Wirtschafts- und das Innenministerium. Meine Ausführungen zur Sicherheitsüberprüfung bei bau- und betriebstechnischen Anlagen im Jahre 1981 waren für sie Anlaß, den Entwurf einer neuen Verwaltungsvorschrift zu erarbeiten und mir zur Stellungnahme zuzuleiten. Ich schlug einige Änderungen vor, die teilweise in die endgültige Regelung einfließen.

2.1.3 Neuregelung

Die neue, im August 1982 erlassene Verwaltungsvorschrift regelt das Überprüfungsverfahren für die Ausstellung von Dauerausweisen und von Ausweisen mit beschränkter Gültigkeitsdauer unterschiedlich. Im letzteren Fall führt allein das Polizeirevier Flughafen Stuttgart die Überprüfung durch. Es fragt die polizeilichen Informationssysteme ab. Liegen Eintragungen vor, aus denen sich Bedenken gegen den Zutritt des Betroffenen zu Sicherheitsbereichen ergeben, teilt es der Stuttgarter Flughafen GmbH nur diese Tatsache mit.

Bei der Ausstellung von Dauerausweisen gibt es gegenüber dem bisherigen Personenüberprüfungsverfahren folgende datenschutzrechtlich bedeutsame Abweichungen:

- Die Stuttgarter Flughafen GmbH eröffnet der zu überprüfenden Person gegen Unterschrift, daß sie einer Sicherheitsüberprüfung unterzogen wird. Damit wird das Verfahren für den Betroffenen transparenter.
- Die Sicherheitsüberprüfung führt das Regierungspräsidium Stuttgart als zuständige Luftfahrtbehörde durch.
- Es beteiligt das Landesamt für Verfassungsschutz und das Landeskriminalamt, die ihre Erkenntnisse getrennt zurückleiten.
- Das Landesamt für Verfassungsschutz übermittelt dabei nur solche personenbezogenen Daten, die für die Entscheidung des Regierungspräsidiums von Bedeutung sein können. Wie bisher verfährt hingegen die Polizei. Das Landeskriminalamt leitet nach wie vor alle in den Systemen PIOS, INPOL und PAD und in den Staatsschutzunterlagen erfaßten Erkenntnisse an das Regierungspräsidium weiter.
- Das Regierungspräsidium gibt dem Überprüften Gelegenheit, sich zu den vorliegenden Erkenntnissen zu äußern, wenn unter Berücksichtigung des Ausgangs von Ermittlungs- und Strafverfahren voraussichtlich Bedenken gegen den Zutritt zu Sicherheitsbereichen auf dem Flughafen bestehen.
- Das Regierungspräsidium teilt der Stuttgarter Flughafen GmbH lediglich das Ergebnis seiner Überprüfung, nicht jedoch die Erkenntnisse mit.

2.1.4 Bewertung der Neuregelung

Die Neuregelung entspricht überwiegend meinen Vorstellungen. Sie sollte jedoch unbedingt in einem wichtigen Punkt nochmals überdacht werden. Ich meine, nicht nur das Landesamt für Verfassungsschutz, sondern auch das Landeskriminalamt muß vor der Weitergabe seiner Daten eine Relevanzprüfung vornehmen. Dies ergibt sich aus § 10 Abs. 1 LDSG und den KpS-Richtlinien. Kriminalpolizeiliche Sammlungen sind nun einmal vertraulich und grundsätzlich nur für den Dienstgebrauch innerhalb der Polizeien des Bundes und der Länder bestimmt. Dies gilt in besonderer Weise für das PIOS-System, bei dem die Datenspeicherung sehr weit in den Vorfeldbereich hinein-geht und auch Personen umfaßt oder umfaßte, die weder Beschuldigte noch Tatverdächtige sind, sondern beispielsweise Zeugen oder Geschädigte oder „sonstige Personen“. Hier kann nicht einfach jede Erkenntnis an eine andere Behörde weitergegeben werden. Eine Prüfung ist aber auch deshalb geboten, weil weder die Personenauskunftsdatei noch das PIOS-System oder die Staatsschutzunterlagen bisher so bereinigt sind, daß sie datenschutzrechtlichen Erfordernissen in vollem Umfang genügen. Eine Erkenntnis darf aber nach den einschlägigen Verwaltungsvorschriften nur weitergegeben werden, wenn

feststeht, daß sie überhaupt noch gespeichert/aufbewahrt werden darf. Ich hoffe, daß sich mit den zuständigen Ministerien über diesen Punkt noch Einigung erzielen läßt.

2.2 Überprüfung von Beschäftigten der Regionalen Rechenzentren

Beim Kontrollbesuch eines Regionalen Rechenzentrums erfuhr ich, daß das Landesamt für Verfassungsschutz zum Teil auch die Beschäftigten der Regionalen Rechenzentren und sogar der damit organisatorisch verbundenen Gesellschaften privaten Rechts einer Personenüberprüfung unterzieht. Da die Aussagen der beteiligten Stellen über die Handhabung des Verfahrens zunächst sehr widersprüchlich waren, entstanden bei mir Zweifel, ob dieser Personenkreis in rechtlich zulässiger Weise überprüft wird. Meine umfangreichen Nachforschungen ergaben jedoch keine Verstöße gegen datenschutzrechtliche Vorschriften. Es zeigte sich allerdings eine erhebliche Unsicherheit bei den Regionalen Rechenzentren darüber, ob und gegebenenfalls unter welchen Voraussetzungen sie Beschäftigte durch das Landesamt für Verfassungsschutz überprüfen lassen können. Ich habe deshalb meine Auffassung hierzu allen Regionalen Rechenzentren dargelegt. Um sie zu verstehen, muß man folgendes wissen: Die Regionalen Rechenzentren werden in unterschiedlicher Rechtsform betrieben. Auch soweit sie Zweckverbände sind, führen sie ihr Rechenzentrum aus steuerlichen Gründen in Form einer GmbH.

- Ein Regionales Rechenzentrum in der Rechtsform eines Zweckverbandes darf Personen, die es einstellen will, auf ihre Verfassungstreue hin überprüfen (§ 3 Abs. 2 Nr. 4 des Landesverfassungsschutzgesetzes in Verbindung mit dem Beschluß der Landesregierung über die Pflicht zur Verfassungstreue im öffentlichen Dienst vom 2. Okt. 1973). Aus datenschutzrechtlicher Sicht ist zu wünschen, daß das Rechenzentrum die Betroffenen über die Durchführung der Überprüfung unterrichtet.
- Fraglich ist hingegen, ob auch Personen, die ein als BGB-Gesellschaft geführtes Rechenzentrum oder eine mit einem Zweckverband organisatorisch verbundene GmbH beschäftigen wollen, durch den Verfassungsschutz überprüft werden dürfen. § 3 Abs. 2 Nr. 4 des Landesverfassungsschutzgesetzes sieht eine solche Mitwirkung nicht vor, weil es sich hier nicht um Personen handelt, die sich um eine Einstellung in den öffentlichen Dienst bewerben. Ob die gesetzlich festgelegten Aufgaben des Landesamtes für Verfassungsschutz durch Einwilligung der Betroffenen erweitert werden können, erscheint mehr als zweifelhaft, ist jedoch keine Datenschutzfrage und deshalb allein vom Innenministerium zu klären. Den Erfordernissen des Datenschutzes wird jedenfalls genügt, wenn das Rechenzentrum die Betroffenen über die Überprüfung und die Art der an die Sicherheitsbehörden übermittelten Daten informiert und ihre Einwilligung hierzu einholt.
- Personen, die außerhalb des Rechenzentrums oder der damit verbundenen Gesellschaft stehen, dürfen in keinem Fall — also auch nicht mit ihrer Einwilligung — einer Personenüberprüfung durch das Landesamt für Verfassungsschutz unterzogen werden. Zu dieser Äußerung sah ich mich veranlaßt, weil ein zwischen einem Rechenzentrum und einem Taxiunternehmen geschlossener Beförderungsvertrag die Überprüfung der eingesetzten Taxifahrer durch den Ver-

fassungsschutz vorsah. In der Praxis macht man davon allerdings keinen Gebrauch. Die betreffende Vertragsregelung ist inzwischen ersatzlos gestrichen.

3. Eingaben

Im vergangenen Jahr erhielt ich nur sechs Eingaben zum Bereich des Verfassungsschutzes. Vier davon waren unbegründet. In zwei Fällen löschte das Landesamt für Verfassungsschutz die gespeicherten Daten, weil sie zur rechtmäßigen Erfüllung seiner Aufgaben nicht mehr erforderlich waren.

— In dem einen Fall war der Betroffene vor Jahren im Zuge einer Fahndungsaktion nach Terroristen überprüft worden. Damals lag ein Hinweis vor, in seiner Wohnung verkehrten Sympathisanten. Der genaue Anlaß der Überprüfung ergibt sich aus den Akten des Landesamtes für Verfassungsschutz nicht. Die Überprüfung erbrachte keinen Beweis für die Anschuldigung. Zur Datenspeicherung beim Verfassungsschutz kam es vier Jahre später, als im Zuge einer größeren Aktion auch die Wohngemeinschaft überprüft wurde, in der der Betroffene wohnt. Das Landesamt für Verfassungsschutz meint, die Datenspeicherung sei damals gerechtfertigt gewesen, inzwischen bestehe dafür jedoch keine Notwendigkeit mehr. Es nahm den Vorgang zum Anlaß, in ähnlichem Zusammenhang erfolgte Datenspeicherungen einer Überprüfung zu unterziehen.

— Im anderen Fall hatte der Verfassungsschutz 1973 die Daten einer Medizinstudentin gespeichert, weil sie einen vom „Komitee gegen Isolationsfolter“ herausgegebenen „Offenen Brief an den Bundesgerichtshof“ mit unterzeichnet hatte. Mit dieser Aktion wandten sich damals verschiedene Ärzte gegen eine angeblich beabsichtigte „Zwangsuntersuchung“ von Ulrike Meinhof. Wegen dieser Datenspeicherung hatte die Betroffene erhebliche Schwierigkeiten in ihrem beruflichen Fortkommen. Als sie sich 1976 um eine Stelle im öffentlichen Dienst bewarb, wurde ihr die Erkenntnis vorgehalten. Erst nach zwei Kurzzeitverträgen wurde sie endgültig als Ärztin angestellt. Als sie 1979 zu einer städtischen Krankenanstalt wechseln wollte, führte das Bekanntwerden der früheren Erkenntnis dazu, daß der in Aussicht genommene Abschluß eines Arbeitsvertrags zunächst nicht zustande kam. Ein Arbeitsplatz wurde ihr erst angeboten, nachdem sie vor dem Arbeitsgericht obsiegte und in der Berufungsinstanz einen für sie günstigen Vergleich erzielt hatte, bei dem die beklagte Stadt unter anderem erklärte, sie hätte aus heutiger Sicht keine Zweifel mehr an der Verfassungstreue der Klägerin. Da die Betroffene demnächst erneut ihren Arbeitsplatz wechseln möchte, befürchtete sie wiederum Schwierigkeiten. Sie wandte sich deshalb an mich. Sie brachte — wie sie dies von Anfang an getan hatte — vor, sie habe mit ihrer Unterschrift unter den Offenen Brief an den Bundesgerichtshof in keiner Weise das Komitee gegen Isolationsfolter oder die politischen Ansichten und das Vorgehen von Ulrike Meinhof unterstützen wollen. Sie habe allein dagegen protestieren wollen, daß eine Person gegen ihren Willen in Narkose untersucht werden sollte. Die Unterzeichnung des Briefs sei Ausdruck ihrer Überzeugung gewesen, daß niemand ohne seine Einwilligung körperlich-medizinischen Eingriffen unterzogen werden sollte. Daß sie auf dem Boden der Verfassung stehe, habe ihr bisheriges Verhalten im öffentlichen Dienst gezeigt. Das Landesamt für Verfassungsschutz sah dies anders:

Durch die Unterzeichnung des Offenen Briefs an den Bundesgerichtshof habe die Betroffene das „Komitee gegen Isolationsfolter“ unterstützt, das seine Funktion in erster Linie im offenen politischen Kampf für die Ziele der RAF gesehen habe. Es gehöre zum gesetzlichen Auftrag des Landesamts für Verfassungsschutz, solche Personen namentlich zu erfassen. Einer abschließenden Klärung der Frage, ob die Unterschriftsleistung eine Unterstützung des Komitees gegen Isolationsfolter darstellte oder allein Ausdruck der persönlichen Überzeugung war, bedurfte es jedoch nicht. Nach einem eingehenden Schriftwechsel war das Landesamt für Verfassungsschutz bereit, die Daten der Betroffenen zu löschen. Es nahm auch diesen Vorgang zum Anlaß zu prüfen, ob die Daten anderer Unterzeichner des Briefes weiter zu speichern sind oder gelöscht werden können.

2. Abschnitt: Polizei

Gelegentlich bekomme ich zu hören, ich sollte in meinen Tätigkeitsberichten auf Ausführungen über den Datenschutz im Bereich der Polizei verzichten. Als ich zu Beginn des letzten Jahres bei der Polizeichefbesprechung zu Gast war, verlangte man von mir, ich solle mich von den Presseberichten über meinen 2. Tätigkeitsbericht distanzieren und in Zukunft bei meiner Darstellung „mögliche Reaktionen der Presse“ bedenken. Diesen Forderungen kann ich nicht Rechnung tragen; sie widersprechen meinem Amtsverständnis. Ich habe den gesetzlichen Auftrag, dem Landtag einen Tätigkeitsbericht zu erstatten. Würde ich darin den Bereich der Polizei ausklammern, würde ich diesem Auftrag nicht gerecht. Gerade im Bereich der Polizei, der besonders empfindliche, weit in die Privatsphäre hineinreichende Daten weitgehend ohne Kontrollmöglichkeiten der Betroffenen verarbeitet, darf der Landtag, aber auch die Öffentlichkeit eine Darstellung der Situation erwarten. Nur so läßt sich eine — selbstverständlich begrenzte, weil Sicherheitsbelange wahrende — Transparenz herstellen. Ich wundere mich etwas über die Reaktion der Polizei auf meine Tätigkeitsberichte. Wer meine bisherigen Ausführungen zum Datenschutz im Bereich der Polizei gelesen hat, wird — so meine ich — feststellen, daß ich darin keine „Vorwürfe“ gegen die Polizei oder einzelne Personen erhob oder „Mißbräuche“ im Sinne einer absichtlichen Verletzung datenschutzrechtlicher Vorschriften schilderte. Ich erweckte auch nicht den Eindruck, als ob die Sicherheitsbehörden den Datenschutz fortlaufend und erheblich verletzten. Auch übte ich keine Kritik um der Kritik willen oder um das Ansehen der Polizei herabzumindern. Worum ich mich schon bisher bemühte und weiterhin bemühe, ist, in sachlicher und emotionsloser Weise darzustellen, inwieweit die Polizei den datenschutzrechtlichen Vorschriften Rechnung trägt und wo es Probleme im Verhältnis zwischen Polizei und Datenschutz gibt. Dabei zeigte und zeige ich nicht nur die Passiva, sondern selbstverständlich auch die Aktiva des Datenschutzes auf und mache deutlich, wo Sorgen von Bürgern unbegründet und das Handeln der Polizei rechtmäßig ist. Damit wird die Polizei ebenso behandelt wie andere Verwaltungszweige. Sie kann nicht erwarten, von mir nur gelobt zu werden. Akzeptiert die Polizei diesen Standpunkt, sollte es ihr möglich sein, meine Feststellungen und Schlußfolgerungen ohne Emotionen aufzunehmen. Im übrigen meine ich, daß eine verantwortungsbewußte Presse von sich aus in der Lage ist, über meine Ausführungen in angemessener Weise zu berichten.

1. Zur Situation

1.1 Neue Verwaltungsvorschriften

Das Jahr 1982 war anders als die beiden Jahre zuvor nicht so sehr vom Erlaß oder der Erarbeitung neuer datenschutzrechtlicher Vorschriften bestimmt. Sieht man einmal von der maßgeblich im Interesse der Polizei vorgenommenen 1. Änderung des Landesdatenschutzgesetzes ab, sind vor allem drei Verwaltungsvorschriften zu nennen:

- die Regelung über die Speicherung von Daten über Kontakte im Rahmen der Häftlingsüberwachung
- die Verwaltungsvorschrift des Innenministeriums über die Aussonderung und Behandlung archivwürdiger Akten bei der Polizei
- die erkennungsdienstlichen Richtlinien.

Bedeutsam ist vor allem die erste Regelung; von ihr soll später noch kurz die Rede sein. Bei der Verwaltungsvorschrift über archivwürdige polizeiliche Akten ist unter dem Aspekt des Datenschutzes nur die Bestimmung von Interesse, wonach die Staatsarchive die ihnen überlassenen kriminalpolizeilichen „Unterlagen“ nur noch zu wissenschaftlichen Zwecken nutzen dürfen. Meinen Intentionen wurde damit entsprochen. Die erkennungsdienstlichen Richtlinien verabschiedete inzwischen das zuständige Bund-Länder-Gremium, ihre Einführung im Lande steht kurz bevor. Die beschlossene Bundesfassung berücksichtigt meine zum Teil im 2. Tätigkeitsbericht wiedergegebenen Vorstellungen, die im Kern auf eine Zusammenstellung der gesetzlichen Regelungen über die erkennungsdienstliche Behandlung und die Einarbeitung der langjährigen Rechtsprechung und Literatur hierzu abzielten, stärker als der einstige Entwurf. Ich freue mich darüber umso mehr, als die Landesregierung in ihrer Stellungnahme zu meinem 2. Tätigkeitsbericht dies noch kategorisch ablehnte. Dem Vernehmen nach will das Innenministerium vor Inkraftsetzen der Richtlinien noch ein Gespräch mit mir über die Einfügung einiger zusätzlicher, in der Sache unstrittiger Punkte führen. Dies begrüße ich.

1.2 Neue Dateien

1.2.1 Allgemeines

Außer diesen Verwaltungsvorschriften wurden noch einige Errichtungsanordnungen für neue Bund-Länder-Dateien beim Bundeskriminalamt erlassen. Die Dateiend Richtlinien bestimmen nämlich, daß neue Dateien nur auf Grund einer besonderen Anordnung des Präsidenten des Bundeskriminalamts errichtet werden dürfen, die in bestimmten Fällen der Zustimmung des Bundes- und der Länderinnenminister bedarf. Eine solche Errichtungsanordnung muß unter anderem die Bezeichnung der Datei, den Zweck, ihre Rechtsgrundlage, den betroffenen Personenkreis, die Arten der zu speichernden personenbezogenen Daten, ihre Anlieferung, die Übermittlung, die Auskunftserteilung an Betroffene und die Speicherdauer angeben.

1.2.2 Datei „Landfriedensbruch und verwandte Straftaten“

Neu errichtet wurde im Jahr 1982 u. a. die Datei „Landfriedensbruch und verwandte Straftaten“. Deren Daten liefern die Länder im Rahmen eines Meldedienstes in herkömmlicher Weise an. In die neue Datei sollen Presseberichten zufolge alle Personen aufgenommen werden, gegen die in örtlichem, zeitlichem und sachlichem Zusammenhang mit einer politisch bestimmten öffentlichen Versammlung oder einem solchen Aufzug Ermittlungsverfahren wegen Landfriedensbruchs, schweren Hausfriedensbruchs, schwerer Gewalttätigkeiten, Plünderungen, bestimmter gemeingefährlicher Straftaten oder wegen Aufforderung zu solchen Straftaten eingeleitet wurden. Die Speicherung soll längstens zwei Jahre vom Datum der letzten Erfassung betragen. Bei einer Einstellung des Verfahrens, bei Freispruch oder bei einer Änderung des rechtlichen Gesichtspunkts dergestalt, daß eine Aufnahme in die Datei nicht mehr zulässig wäre, sind die Daten sofort zu löschen. Zugriff auf die Daten soll das Bundeskriminalamt haben, das auf Anfrage Auskunft an Dritte, insbesondere Polizeidienststellen, erteilt. Nur aus aktuellem Anlaß übernimmt das Bundeskriminalamt auf Antrag eines Landes für begrenzte Zeit die Daten über überörtlich und aggressiv agierende Tatverdächtige in den allen Polizeibeamten zugänglichen INPOL-Fahndungsbestand. Nach diesem Zeitraum löscht es die Daten im INPOL-Bestand.

Ich habe gegen die Einrichtung dieser Datei keine grundsätzlichen datenschutzrechtlichen Bedenken. In der Praxis muß die Polizei allerdings darauf achten, daß sie

- die Daten für eigene Präventivmaßnahmen sammelt und deshalb Dritten außerhalb der Polizei nur sehr begrenzt zur Verfügung stellen darf,
- die Daten dem Bundeskriminalamt nicht ungeprüft übermittelt, sondern nur dann, wenn der Betroffene wirklich der Tat verdächtig ist,
- stets vom Ausgang eines Ermittlungs- oder Strafverfahrens erfährt, um dann gegebenenfalls die Löschung der Daten veranlassen zu können. Dies zu gewährleisten, dürfte allerdings in der Praxis erhebliche Schwierigkeiten bereiten.

Ich habe aber Grund zur Klage, wie mangelhaft mich das Innenministerium am Verfahren beteiligte. Der Presse entnahm ich einst, eine Wiedereinführung des Meldedienstes „Gewalttätige Störer“ werde erwogen. Er war 1979 nach heftigen Diskussionen eingestellt worden. Auf meine erste Anfrage im August 1981 teilte mir das Innenministerium lediglich mit, in Bund-Länder-Gremien werde über die Einführung eines solchen Meldedienstes beraten. Als ich erfuhr, der Polizeiarbeitskreis habe bereits einen Beschlußvorschlag für die Innenministerkonferenz verabschiedet, bat ich um dessen Übersendung. Das Innenministerium weigerte sich jedoch, die Unterlage herauszugeben. Erst nachdem die Innenministerkonferenz Anfang 1982 über die Vorlage beraten, sie nicht akzeptiert und die Presse eingehend unterrichtet hatte, übersandte man mir die inzwischen überholte Vorlage. Auf eine weitere Intervention hin erhielt ich den Beschluß der Innenministerkonferenz vom 14. Jan. 1982, der der

Polizei weitere Erhebungen aufgab. Meiner Bitte, mich vor einer endgültigen Entscheidung der Innenminister zu hören, entsprach das Innenministerium nicht. Auch informierte es mich bis heute nicht über den endgültigen Beschluß der Innenministerkonferenz. Mein ganzes Wissen beruht also bislang lediglich auf den Berichten der Presse und öffentlichen Äußerungen meiner Kollegen, die ihre Innenministerien informiert haben.

Diese Verfahrensweise des Innenministeriums widerspricht dem Geist des Landesdatenschutzgesetzes. Zum Teil erklärt sie sich aus seinem Bestreben, einen weitergehenden Meldedienst einzuführen. Damit konnte es sich jedoch — auch ohne meine Intervention — in der Innenministerkonferenz nicht durchsetzen. Sein Verhalten mir gegenüber ist vor allem aus zwei Gründen bedenklich: Zum einen macht es mir unmöglich, meinem gesetzlichen Beratungsauftrag nachzukommen. Dies kann dazu führen, daß ich datenschutzrechtliche Bedenken erst nach Inkraftsetzen der Regelungen vorbringen kann und dadurch ein verhältnismäßig hoher Aufwand für Änderungen erforderlich wird. Zum andern trägt ein solches Vorgehen ganz sicherlich nicht zu einem guten Verhältnis zwischen Datenschutz und Polizei bei, an dem mir sehr gelegen ist. Es müßte selbstverständlich sein, daß die Polizei die Datenschutzbeauftragte über alle wichtigen Vorhaben mit datenschutzrechtlichem Bezug rechtzeitig und umfassend unterrichtet. Dies könnte oftmals zu einem für beide Seiten fruchtbaren Gedankenaustausch führen. Wer gute Argumente auf seiner Seite hat, braucht eine geistige Auseinandersetzung nicht zu fürchten.

1.3 Vollzug datenschutzrechtlicher Vorschriften

1.3.1 Bereinigung der Personenauskunftsdatei und anderer kriminalpolizeilicher Sammlungen

In meinem 2. Tätigkeitsbericht führte ich aus, daß die Polizei die Regelungen über Sperren und Löschen praktiziert, es aber noch längere Zeit beanspruchen wird, bis sie ihren Datenbestand bereinigt hat. Ein weiterer Schritt auf diesem Weg war die Mitte 1982 abgeschlossene Löschung von Daten, die nach geltendem Recht nicht mehr strafbare Verhaltensweisen betrafen. Hierbei ging es um folgendes:

Unser Strafrecht wurde in den siebziger Jahren wiederholt und grundlegend geändert. Nehmen wir an, die Polizei speicherte zulässigerweise eine damals strafbare Verhaltensweise in ihrer Personenauskunftsdatei. Bei einer später erfolgten Strafrechtsänderung wurde dann entweder die Strafbarkeit aufgehoben oder der Straftatbestand in eine Ordnungswidrigkeit umgewandelt oder seine Tatbestandsmerkmale geändert. Daraus zog die Polizei zunächst keine Konsequenzen für die Speicherung der Daten in der Personenauskunftsdatei. Erst nach Inkrafttreten der KpS-Richtlinien machte man sich daran, diese Fälle zu überprüfen. Verhältnismäßig einfach war dies bei den beiden erstgenannten Fallgruppen, weil hier die Polizei ohne weiteres die Daten löschen konnte. Schwieriger und arbeitsintensiver gestaltete sich die Prüfung der dritten Fallgruppe. Hier mußte die Polizei klären, ob die frühere Verhaltensweise eines Betroffenen

die Merkmale des neuen Straftatbestandes erfüllen. Nach Angaben des Innenministeriums wurden 13 119 Fälle überprüft. Ergebnis war: die Polizei löschte in 4250 Fällen die Daten der Betroffenen in der Personenauskunftsdatei und tilgte in weiteren 2738 Fällen gespeicherter Mehrfachtäter eine nicht mehr strafbare Verhaltensweise.

Bereits in meinem 1. Tätigkeitsbericht führte ich aus, wie wichtig es ist, daß die Justiz die Polizei in differenzierter Form über den Ausgang von Ermittlungs- und Strafverfahren unterrichtet. Nur dann kann die Polizei prüfen, ob in Dateien gespeicherte Daten zu löschen und kriminalpolizeiliche Unterlagen zu vernichten sind. Bereits Anfang 1981 verbesserte das Justizministerium die Mitteilungspraxis der Justiz. Weitere Fortschritte auf diesem Weg verspreche ich mir von einem neuen Mitteilungsvordruck, den die Polizei entwarf und der demnächst eingeführt wird. Er erleichtert der Justiz, der Polizei differenziert mitzuteilen,

- weswegen ein Angeklagter verurteilt,
- weshalb ein Verfahren eingestellt,
- ob der Angeklagte freigesprochen und ob dabei gegebenenfalls der Grundsatz „im Zweifel für den Angeklagten“ angewandt wurde.

Die Polizei kann dann daraus erforderlichenfalls datenschutzrechtliche Konsequenzen ziehen: Im ersten Fall wird sie die in der Personenauskunftsdatei gespeicherte Deliktsbezeichnung ändern, wenn sie wesentlich von ihrer Erstbeurteilung abweicht. Im Fall einer Einstellung wird sie prüfen, ob sie die Daten löschen kann. Im Falle eines Freispruchs wird die Polizei die Daten in der Regel löschen. Erfolgte der Freispruch nach dem Grundsatz „im Zweifel für den Angeklagten“, prüft sie auf Grund der Gesamtumstände und etwaigen eigenen Wissens vom Ergebnis der richterlichen Beweisaufnahme und der mündlichen, notfalls auch der schriftlichen Urteilsbegründung, ob sie die Daten löschen kann.

1.3.2 Abweichen von Regelfristen der KpS-Richtlinien

Die polizeiliche Praxis beschäftigte sich zu meiner Überraschung eingehend mit der Frage, ob sie je nach Sachlage von den Regelfristen der KpS-Richtlinien abweichen darf und erforderlichenfalls abweichen muß. Die KpS-Richtlinien sehen für die Speicherung von Daten und die Aufbewahrung kriminalpolizeilicher Sammlungen über Erwachsene in Bagatellfällen eine dreijährige, ansonsten eine zehnjährige Regelfrist vor. Hierzu argumentierte die Polizei zum Teil, eine Speicherungs- und Aufbewahrungsdauer zwischen drei und zehn Jahren könne es nicht geben. Ich widersprach dieser offensichtlich falschen Auffassung. Nach § 13 LDSG darf die Polizei Daten so lange speichern, wie dies zur rechtmäßigen Erfüllung ihrer Aufgaben erforderlich ist. Die KpS-Richtlinien konkretisieren diese Bestimmung, um der Polizei eine Orientierung zu geben und deren Arbeit zu erleichtern. Sie wollen jedoch, wie ihr Wortlaut und ihre Entstehungsgeschichte eindeutig belegen, nur „Regelfälle“ erfassen. Deshalb spricht man ja auch von Regelfristen. Unberührt bleibt das un-

mittelbar aus der Verfassung abgeleitete Abwägungsgebot zwischen dem öffentlichen Interesse, zu Zwecken der Strafverfolgung und der Gefahrenabwehr auf polizeiliche Erkenntnisse zurückgreifen zu können, und dem durch das Grundrecht auf freie Entfaltung der Persönlichkeit geschützten Interesse des einzelnen, solchen Einwirkungen der öffentlichen Gewalt nicht ausgesetzt zu sein. Das führt dazu, daß die Polizei in atypischen Fällen die Speicherdauer und Aufbewahrungsfrist abweichend festlegen darf und muß. Sie kann länger sein als die Regelfrist, aber auch kürzer. Um Mißverständnisse zu vermeiden, möchte ich jedoch hinzufügen: Ich verlange nicht, daß die Polizei alle vor Inkrafttreten der KpS-Richtlinien bereits gespeicherten Fälle daraufhin überprüft, ob sie atypisch gelagert sind. Ich meine jedoch, daß Polizeidienststellen bei einer Neueingabe oder bei einer erneuten Befassung mit einem Vorgang — beispielsweise auf Grund einer Überprüfung durch mich — dies mitbedenken und erforderlichenfalls handeln müssen.

1.3.3 Mißbräuchliche PAD-Abfrage

Im vergangenen Jahr wurde mir ein Fall echten Datenmißbrauchs bekannt. Das Justizministerium fragte bei mir offiziell an, ob ich wegen folgenden Vorgangs Strafantrag nach § 25 Abs. 3 LDSG stelle: Eine von zwei Freundinnen war mit einem Polizeibeamten, die andere mit einem Mann befreundet, der des Scheckbetrugs verdächtig war. Wegen dieses Verdachts fragte der Polizeibeamte den Polizeicomputer entweder selbst oder mit Hilfe eines gutgläubigen Terminalbedieners danach ab, ob in der Personenauskunftsdatei Daten über den Bekannten der Freundin seiner Freundin gespeichert sind. Dies war der Fall. Der Ausdruck über die gespeicherten Daten gelangte sodann über die beiden Freundinnen in die Hände dieses Bekannten.

Das Verhalten des Polizeibeamten führte zur Einleitung eines Ermittlungsverfahrens wegen Verrats von Dienstgeheimnissen und Verstoßes gegen das Landesdatenschutzgesetz. Es endete mit einer Einstellung nach § 153 a der Strafprozeßordnung gegen Zahlung einer Geldbuße in Höhe von 2500 DM. Ich hatte keinen Strafantrag gestellt, weil ich — abgesehen von einigen rechtlichen Erwägungen — das Verhältnis zur Polizei hierdurch nicht belasten wollte. Zu denken gibt mir freilich im nachhinein, daß die Staatsanwaltschaft die Einstellung des Verfahrens u. a. damit begründete, die absichtlich begangene Verletzung datenschutzrechtlicher Vorschriften habe damit an Gewicht verloren.

1.4 Verhältnis von Polizei und Datenschutz

Im abgelaufenen Jahr beherrschten Schlagworte wie „Überzogener Datenschutz“, „Sicherheit vor Datenschutz“, „Datenschutz ist Tatenschutz“ die Diskussion. Sie belasteten auch das Verhältnis zwischen der Polizei und den Datenschutzbeauftragten. Ich halte solche Aussagen für wenig hilfreich. Vernünftig diskutieren kann man nur auf der Basis konkreter Sachverhalte. Auch muß man die Materie genau kennen, die einschlägigen Rechts- und Verwaltungsvorschriften und ihre Hintergründe sowie die Rechtsprechung. Manchmal habe ich den

Eindruck, daß es hieran gerade bei denjenigen fehlt, denen die Leerformeln so leicht über die Lippen gehen. Natürlich beilegen sich die meisten hinzuzufügen, sie hätten selbstverständlich nichts gegen Datenschutz, nur „nicht so“. Sie vergessen allerdings zu sagen, was sie unter Datenschutz verstehen. Manch einer scheint den Datenschutz mit Datensicherung im Sinne organisatorischer oder technischer Schutzvorkehrungen gegen Datenmißbrauch gleichzusetzen. Bei vielen Kritikern des Datenschutzes vermisste ich auch, daß sie nicht deutlich zwischen den verschiedenen, zum Teil schon seit langer Zeit geltenden Vorschriften des Datenschutzes unterscheiden und außerdem den getroffenen Regelungen und ihrer Anwendung. Fehler einzelner Behörden bei der Gesetzesanwendung kommen in allen Bereichen vor. Sie rechtfertigen jedoch keine Aussage „gegen den Datenschutz“, sondern allenfalls die Forderung an ihre Aufsichtsinstanzen, mehr für die Aufklärung in Sachen Datenschutz zu tun. Falsch ist die Forderung, „Sicherheit müsse vor Datenschutz“ gehen. Sie ist ebenso falsch wie es die Umkehrung wäre, die bisher noch niemand gefordert hat. Die polizeiliche Aufgabe der Strafverfolgung und Gefahrenabwehr ist eine Aufgabe von hohem Rang. Selbstverständlich ist, daß die Polizei dabei Gesetz und Recht beachten muß und damit die Grundrechte der Bürger. Ihrer Sicherung dient auch der Datenschutz. Ich kann deshalb nur immer wieder sagen: Was nützt, ist nicht eine emotional angeheizte Auseinandersetzung mit Schlagworten, sondern eine im Ton moderate Sachdiskussion. Dazu bedarf es eines ständigen Dialogs und Informationsaustausches zwischen Polizei und Datenschutz. Dazu war und bin ich bereit.

Leider kam es zu solchen Kontakten im abgelaufenen Jahr nur selten. Nennen möchte ich zu allererst eine Veranstaltung der Schutzpolizeiinspektion Nord der Landespolizeidirektion Stuttgart II, bei der Fragen der Praxis eingehend behandelt wurden. Dankbar war ich, daß die Polizeidirektion Waiblingen bei ihrer Dienstversammlung einem meiner Mitarbeiter Gelegenheit gab, die Belange des Datenschutzes darzulegen. Mit dem Landeskriminalamt kam es zu einigen nützlichen Gesprächen über Einzelfragen. Selbstverständlich kann ich nicht alle Kontakte aufzählen. Sicher ist jedoch: der Dialog und Informationsaustausch muß vor allem auf höherer Ebene erheblich intensiviert werden. Es sollte nicht so sein, daß die Datenschutzbeauftragte über die Presse oder bei öffentlichen Veranstaltungen von angeblichen, ihr nicht bekannten Behinderungen durch den Datenschutz erfahren muß. Ich selbst trage meine Feststellungen und Überlegungen zu einem Problem zumeist lange, ehe ich darüber im Tätigkeitsbericht berichte, an das Innenministerium heran. Häufig biete ich noch ein Gespräch dazu an oder bitte hierum. Nur zum Teil erhielt ich hierauf überhaupt eine Reaktion. Der Informationsweg kann nicht einseitig sein. Ich erwarte, daß auch die Polizei ihre Karten auf den Tisch legt. Dazu gehört beispielsweise, daß sie mir

- von einzelnen Polizeidienststellen verfaßte Papiere über „Behinderungen“ durch den Datenschutz vorlegt oder über signifikante Fälle berichtet, die nach ihrer Auffassung gegen bestimmte Regelungen in Rechts- oder Verwaltungsvorschriften sprechen,
- sagt, weshalb Baden-Württemberg schon kurze Zeit nach Inkrafttreten der jahrelang beratenen KpS-Richtlinien und anscheinend im Gegensatz zu den übrigen Bundesländern meint, mit den in den KpS-Richtlinien festgelegten Aufbe-

wahrungs- bzw. Lösungsfristen nicht zurechtzukommen, und warum es sein „Wissen“ nicht vor der Entscheidung in die dafür vorgesehenen Bund-Länder-Gremien einbrachte und zur Diskussion stellte,

- ganz konkret schildert, welche Probleme es bei der Auskunftserteilung an Betroffene gibt. Schließlich ist doch bemerkenswert, daß es auch im Lager der Polizei sehr unterschiedliche Stimmen zur Auskunftserteilung gibt. Während ein führender Mitarbeiter der Polizeiführungsakademie auf einer Tagung des Bundeskriminalamts meinte, die Polizei könne „99,9 %“ ihres Datenbestandes offenlegen, spricht vor allem das Landeskriminalamt immer wieder von der Gefahr der Ausforschung. Diese unterschiedliche Beurteilung wird auch deutlich, wenn man die Zahl der Auskunftsverweigerungen beim Bundeskriminalamt oder in einigen Bundesländern mit denen in Baden-Württemberg vergleicht. Schließlich fiel mir bei der diesjährigen datenschutzrechtlichen Fachtagung des Bundeskriminalamts auf, daß dessen jetziger Vizepräsident im Zusammenhang mit der Auskunftserteilung nicht von Ausforschung sprach, sondern allein davon, daß sie mangels Interesse des Bürgers überflüssig sei. Ich will damit der Sachdiskussion nicht aus dem Wege gehen, meine jedoch, daß die Polizei zunächst einmal sorgfältig diese Fakten prüfen sollte.

Auch sollte mir die Polizei zum Beispiel

- sagen, aus welchen Gründen sie neue Dateien errichtet und wie sie diese ausgestalten will,
- bei der Erarbeitung neuer Verwaltungsvorschriften ihre Vorstellungen mitteilen und mir die Gründe dafür nennen, wenn sie Forderungen oder Vorschläge der Datenschutzbeauftragten nicht übernimmt,
- Unterlagen über Vorhaben, die die Datenverarbeitung betreffen, frühzeitig zur Verfügung stellen.

Nur so kann es zu einem besseren Verstehen der jeweils anderen Seite kommen. Das ist wichtig, denn die Datenschutzbeauftragte vertritt nicht nur — wie es gelegentlich, auch vom Herrn Innenminister öffentlich geäußert wurde — die Belange des Persönlichkeitsschutzes, sondern hat selbstverständlich auch die öffentliche Sicherheit im Auge. Ich gehe andererseits auch davon aus, daß sich die Polizei nicht nur um die Belange der öffentlichen Sicherheit kümmert, sondern auch den Bürger sieht. Natürlich wird es immer wieder zu Meinungsverschiedenheiten zwischen der Polizei und der Datenschutzkontrolle kommen. Man sollte sie jedoch in Kenntnis und Respekt vor der Meinung des anderen offen und fair austragen. Ansätze für einen besseren Dialog zwischen Innenministerium und mir glaube ich in jüngster Zeit erkennen zu können. Ich hoffe, daß sich dies im neuen Jahr bestätigt.

2. Eingeschränkte Kontrollmöglichkeit im Bereich der Polizei

Die Einschränkung meiner Kontrollbefugnis durch die Mitte Juli in Kraft getretene 1. Änderung des Landesdatenschutzgesetzes wirkt sich im Polizeibereich besonders stark aus, weil sie mit einer anderen „Maßnahme“ der Polizeidienststellen zusammentrifft: Die Polizeidienststellen erklären die meisten ihrer Karteien zu sogenannten internen Dateien. Darunter versteht man manuelle Karteien, aus denen die Behörde keine personenbezogene Daten an

Dritte übermittelt, die sie also ausschließlich selbst nutzt. Für solche Dateien gilt nur die Regelung des § 8 LDSG über die technische und organisatorische Datensicherung. Beide Maßnahmen zusammen führten dazu, daß nicht nur kriminalpolizeiliche Akten meiner Kontrolle entzogen sind, sofern die Daten nicht zugleich in einer „externen“ Datei gespeichert sind, sondern nach meinen Schätzungen auch mindestens die Hälfte bis zwei Drittel der existierenden Dateien. Ob diese zu Recht zu „internen Dateien“ erklärt wurden, d. h. ob in der Praxis tatsächlich keine Auskünfte aus ihnen erteilt werden, konnte ich noch nicht näher untersuchen, da es hierzu jeweils einer sorgfältigen Prüfung der Datei und der ihr zu Grunde liegenden Akten bedarf. Außerdem meinte das Landeskriminalamt, als ich in eine als intern erklärte Datei Einsicht nehmen wollte um festzustellen, ob dies tatsächlich so ist, dies liege außerhalb meiner Kontrollbefugnis. Nach dem Landesdatenschutzgesetz ist dies jedoch nicht so. Wie dem auch sei: ich gehe vom geschilderten Zustand aus und stelle die verbliebenen Kontrollmöglichkeiten im Sicherheitsbereich dar. Dabei verdeutliche ich anhand von Beispielen, zu welchen Einschränkungen die beschriebenen Maßnahmen bei generellen Kontrollen, aber auch bei Überprüfungen aus Anlaß einzelner Eingaben von Bürgern führen. Dem Herrn Innenminister schilderte ich die Situation bereits in einem Gespräch vor wenigen Wochen.

2.1 Generelle Kontrollen

2.1.1 Keine Kontrollen interner Dateien und Akten

Auf Grund der Gesetzesänderung ist es mir nicht mehr möglich, systematisch zu prüfen, ob

- die Polizeidienststellen kriminalpolizeiliche Unterlagen wie Ermittlungs- oder Kriminalakten, Listen usw. über bestimmte Vorgänge, Personengruppen usw. zu Recht anlegten,
- ob sie aus ihnen regelmäßig Daten an andere Behörden und Privatpersonen weitergeben, und wenn ja, ob dies zu Recht geschieht und
- ob Polizeidienststellen nicht nur ihre Dateien, sondern auch ihre kriminalpolizeilichen Unterlagen regelmäßig bereinigen.

Zwar gilt für solche Unterlagen nicht das Landesdatenschutzgesetz, wohl aber sind die bundesweit eingeführten Richtlinien für die Führung kriminalpolizeilicher Sammlungen (KpS-Richtlinien) anwendbar. Sie differenzieren ganz bewußt nicht zwischen Dateien, internen Dateien und Akten, sondern behandeln all diese Unterlagen im wesentlichen gleich. Sie wenden also die Vorschriften des Landesdatenschutzgesetzes über das Speichern und Weitergeben von Daten und die Pflicht zu ihrer Löschung praktisch entsprechend auf interne Dateien und kriminalpolizeiliche Akten an. All diese Vorschriften sind somit zwar von der Polizei zu beachten; ich kann jedoch ihre Einhaltung nicht mehr kontrollieren, soweit die Daten nicht in einer „externen“ Datei gespeichert sind.

2.1.2 Im Zweifel kein Prüfungseinstieg über Akten

Erschwert, teilweise fast unmöglich gemacht sind mir systematische Kontrollen aber auch, soweit eine Speiche-

rung von Daten in einer Datei denkbar oder wahrscheinlich ist, jedoch nicht feststeht. Ein „Einstieg“ in die Prüfung über die Akten ist nicht möglich. Ansatz für eine systematische Prüfung wären vor allem Datenübermittlungen zwischen Länderpolizeidienststellen und dem Bundeskriminalamt, zwischen Verwaltungsbehörden und Polizeidienststellen und umgekehrt. Dabei wären datenschutzrechtlich je nach dem, wie der Sachverhalt gelagert ist, die Zulässigkeit der Datenübermittlung oder Datenspeicherung, aber auch die Beachtung der Löschungsvorschriften von Interesse. Einige Beispiele sollen diese Aussage konkretisieren:

- Im Rahmen von Meldediensten, beispielsweise dem kriminalpolizeilichen Meldedienst in Staatsschutzsachen (KPMD-S) oder dem Meldedienst „Landfriedensbruch und verwandte Straftaten“ übermitteln die Polizeidienststellen der Länder auf herkömmlichem Weg personenbezogene Daten an das Bundeskriminalamt. Dieses speichert die erhaltenen Daten häufig, aber nicht immer in einer Datei, beispielsweise der Arbeitsdatei PIOS-Landesverrat oder der Datei „Landfriedensbruch und verwandte Straftaten“. Ob diese Datenspeicherung zu Recht geschieht oder ob die Daten gelöscht werden müssen, liegt nach den Verwaltungsvorschriften in der Verantwortung der die Daten anliefernden Polizeidienststellen. So muß beispielsweise die Polizeidienststelle A in Baden-Württemberg dafür Sorge tragen, daß im Rahmen des Meldedienstes „Landfriedensbruch und verwandte Straftaten“ zur gleichnamigen Datei gemeldete Daten eines Betroffenen gelöscht werden, wenn das Ermittlungs- oder Strafverfahren eingestellt wird oder Freispruch ergeht. Soweit baden-württembergische Stellen die Verantwortung für die Datenverarbeitung tragen, besteht an sich meine Kontrollkompetenz. Ich kann jedoch nicht ohne weiteres anhand der Mitteilungen an das Landeskriminalamt und der zu Grunde liegenden Akten prüfen, ob die Voraussetzungen für eine Dateispeicherung vorliegen oder die Löschung von Daten erforderlich ist. Solange ich nämlich nicht weiß, daß die Daten der Betroffenen tatsächlich in einer Datei gespeichert sind, ist mir dieser Einstieg verwehrt. Erfahren kann ich dies nur durch den Bundesbeauftragten für den Datenschutz.
- Nahezu unmöglich ist mir zu prüfen, was die Polizei mit personenbezogenen Daten macht, die ihr Verwaltungsbehörden aus Akten übermitteln. Nehmen wir einmal an, ich wollte — wie meine Kollegen — prüfen, wie Polizeidienststellen mit Demonstrationsanmeldungen verfahren, die ihnen Bürgermeister- und Landratsämter übermittelten. Beispielsweise wäre in diesem Zusammenhang von Interesse, ob und gegebenenfalls inwieweit die in der Demonstrationsanmeldung aufgeführten Versammlungsleiter dateimäßig erfaßt werden. Dies systematisch zu prüfen, ist mir jedoch praktisch nicht mehr möglich, weil zum einen die von den Bürgermeister- und Landratsämtern an die Polizeidienststellen übermittelten Daten in der Regel nicht aus Dateien, sondern aus Akten stammen und zum andern nicht feststeht, daß die Polizeidienststellen diese Daten dateimäßig verarbeiten.

- Ähnliche Schwierigkeiten bereitet schließlich eine systematische Prüfung, inwieweit Polizeidienststellen, z. B. im Rahmen von Personenüberprüfungsverfahren oder Verfahren auf Erteilung einer Erlaubnis (Fahrerlaubnis, Waffenbesitzkarte usw.), personenbezogene Daten an Verwaltungsbehörden übermitteln. Diese Daten können, müssen aber nicht aus Dateien stammen. Um prüfen zu können, müßte mir zunächst, z. B. auf Grund von Eingaben, eine Reihe von Personen bekannt sein, deren Daten Polizeidienststellen an Verwaltungsbehörden weitergeben. Sodann müßte ich feststellen, ob die Namen der Betroffenen in einer „externen“ Datei gespeichert sind und die Daten hieraus übermittelt worden sein könnten. Erst danach könnte ich mir den konkreten Vorgang ansehen. Es ist wohl ohne weiteres einsichtig, daß dies in einem weiten Bereich praktisch das Ende systematischer Kontrollen bedeutet.

2.2 Prüfung aus Anlaß von Eingaben

Die Gesetzesänderung schränkt nicht nur die Kontrollmöglichkeiten bei systematischen Prüfungen, sondern auch bei Einzelfallprüfungen auf Grund von Bürgereingaben erheblich ein. Wozu dies führt, möchte ich an drei Beispielen klarmachen, die sich an tatsächliche Begebenheiten anlehnen oder unmittelbar der Praxis entnommen sind:

- Ein Arbeitgeber kündigt einem Arbeitnehmer mit der Begründung, er habe Hinweise darauf, daß er Kommunist sei. Der Arbeitnehmer vermutet auf Grund bestimmter Äußerungen des Arbeitgebers, daß die Informationen von Sicherheitsbehörden stammen und wendet sich an mich. Ich überprüfe den Vorgang bei der in Betracht kommenden Polizeidienststelle und stelle fest, daß der Betroffene nicht in einer automatisierten Datei gespeichert ist. Nehmen wir einmal an, mir würde bekannt, daß der Betroffene jedoch in einer Datei gespeichert ist, die die Polizei als „intern“ bezeichnet, deren Einsichtnahme sie jedoch ebenso ablehnt wie die in die zu Grunde liegenden Akten. Was soll ich in einem solchen Fall dem Bürger als Ergebnis meiner Prüfung mitteilen? Soll ich ihm sagen, es war alles in Ordnung? Dies wäre eine Täuschung des Bürgers. Oder soll ich ihm sagen, er sei in seinen Rechten nach dem Landesdatenschutzgesetz nicht verletzt? Auch dies kann ich guten Gewissens nicht sagen, solange ich nicht eingehend prüfen konnte, ob es sich bei der angeblich internen Datei tatsächlich um eine solche handelt. Denn wäre dies nicht der Fall, würden also aus besagter Datei Daten übermittelt, müßte sich die Zulässigkeit der Speicherung und auch der etwaigen Übermittlung an den Vorschriften des Landesdatenschutzgesetzes messen lassen. Oder soll ich dem Bürger meine Feststellungen und die Begrenzung meiner Prüfungskompetenz darlegen? Dies wäre zwar ehrlich, würde aber zum einen möglicherweise Sicherheitsinteressen verletzen und zum andern bei den Betroffenen sicherlich Kopfschütteln auslösen. Ob er in einer „internen“ oder einer „externen“ Datei gespeichert ist, wird dem Betroffenen zumeist gleichgültig sein. Belastend ist beides für ihn. Er möchte eine klare Antwort darauf, ob die Polizei korrekt gehandelt hat. Deshalb möchte er von mir geprüft wissen, ob die Polizei — falls Unterlagen über ihn vorhanden sind — diese in Einklang mit dem

Landesdatenschutzgesetz und den KpS-Richtlinien führt und ob sie nicht unzulässigerweise Daten an Dritte übermittelte. Sicher — der Bürger kann sich auch an die speichernde Stelle oder das Innenministerium als Aufsichtsbehörde wenden, soweit mir eine Prüfung seines Falls nicht möglich ist. Ob dies bürgernah und ökonomisch ist und dem vielfach vorhandenen Wunsch des Bürgers nach einer Prüfung durch eine „unabhängige Instanz“ möglichst „vor Ort“ entspricht, mag jeder für sich selbst beantworten. Ich meine jedenfalls und habe dies auch in einem Schreiben an den Herrn Innenminister deutlich gemacht, daß weder dem Bürger noch der Polizei mit einer solch beschränkten Prüfung gedient ist. Der Bürger wird in solchen Fällen durch eine notwendigerweise relativierende Antwort meinerseits im Zweifel gelassen und die Behörden begeben sich der Chance, durch eine unabhängige Kontrollinstanz die Rechtmäßigkeit ihres Handelns bescheinigt zu bekommen.

— Ähnlich liegen die Dinge auch in zwei anderen Fällen:

- Im einen Fall hatten sich mehrere Bedienstete einer Behörde wegen eines in einer Illustrierten erschienenen Presseberichts an mich gewandt. Darin wird unter der Überschrift „Heroinabhängige am Steuer“ über die Teilnahme namentlich genannter und zum Teil abgebildeter Drogenabhängiger am Straßenverkehr berichtet. Die Behördenbediensteten wandten sich — wie sie betonten — nicht gegen den Artikel als solchen, sondern gegen die ohne Zustimmung der Betroffenen erfolgte Veröffentlichung mit Namen und Bild. Sie glaubten, konkrete Anhaltspunkte dafür zu haben, daß die Fotos, möglicherweise auch die in dem Artikel genannten personenbezogenen Angaben, von der Polizei stammten, und baten mich deshalb um Überprüfung. Auf eine entsprechende Anfrage bei der zuständigen Polizeidienststelle teilte mir das Innenministerium wenige Tage nach Verabschiedung der 1. Änderung des Landesdatenschutzgesetzes, aber vor deren Inkrafttreten folgendes mit:

„Die Prüfung des Sachverhalts ergab, daß Polizeidienststellen des Landes Baden-Württemberg keine personenbezogenen Daten aus Dateien der Illustrierten „...“ übermittelt haben.“ Mir blieb in diesem Fall nichts anderes übrig, als dies den anfragenden Bürgern mitzuteilen. Ob eine Kontrollinstanz damit ihrem Auftrag gerecht werden kann, möge jeder selbst beurteilen. Ich meine, daß der Landesbeauftragte für den Datenschutz in einem solchen Fall nur noch Briefträger oder Sprachrohr der zu kontrollierenden Behörde ist.

- In einem anderen Fall wandte sich eine Bürgerin an mich, weil ein Privatmann ihr gegenüber Äußerungen gemacht hatte, die ihrer Meinung nach nur auf Informationen von Sicherheitsbehörden beruhen konnten. Im Rahmen meiner angestellten Prüfung teilte mir das Landeskriminalamt folgendes mit: „Personenbezogene Daten, die zur Übermittlung an Dritte bestimmt sind oder in automatisierten Verfahren verarbeitet werden, sind bei der Polizei in Baden-Württemberg über Frau ... nicht gespeichert. Dementsprechend sind auch keine Daten an Dritte übermittelt worden.“ Nach dieser Formulierung ist es wahrscheinlich, daß die Polizei über die betroffene Frau personenbezogene Daten entweder in einer von ihr als

„intern“ angesehenen Datei oder in Akten erfaßt. Die Fakten teilt mir das Landeskriminalamt jedoch erst gar nicht mit, so daß ich noch nicht einmal der Frage nachgehen kann, ob nicht vielleicht doch das Landesdatenschutzgesetz eingreift. Ich kann so auch nicht prüfen, ob und gegebenenfalls aus welcher Art von Unterlage die Polizei Daten an Dritte übermittelt hat. Die Versicherung, dies sei nicht geschehen, kann nicht genügen.

All dies macht deutlich, daß auf Grund der 1. Änderung des Landesdatenschutzgesetzes, aber auch auf Grund der Erklärung vieler Karteien zu internen Dateien eine effektive Datenschutzkontrolle des Polizeibereichs nicht mehr gewährleistet ist. Baden-Württemberg nimmt damit im Bundesgebiet eine Sonderstellung ein. Alle meine Kollegen dürfen nach wie vor externe Dateien, interne Dateien, Akten, Listen usw. kontrollieren, obwohl sie doch — folgte man der These von der sog. „Klarstellung“ meiner Kompetenzen — zumindest ähnlichen Einschränkungen unterliegen müßten wie ich. Daß davon nicht die Rede sein kann, zeigte sich erst jüngst wieder bundesweit bei der von allen Datenschutzbeauftragten der Länder und des Bundes durchgeführten systematischen Prüfung im Bereich des Staatsschutzes. Erst recht können meine Kollegen auch Bürgereingaben uneingeschränkt nachgehen. In diesem Punkt hatte ich auf Grund einiger Äußerungen der Regierungsfraktion und des Herrn Innenministers bei der 3. Lesung des Gesetzentwurfs im Landtag zunächst noch die schwache Hoffnung, daß dies auch in Baden-Württemberg im Prinzip so sein würde und man wenigstens insoweit eine halbwegs funktionierende Datenschutzkontrolle erhalten wissen will. Vorübergehend gab es dafür auch Anhaltspunkte. Neuere Äußerungen von Behörden belegen leider das Gegenteil.

Mit dieser Entwicklung ist weder den Bürgern noch der Polizei gedient. Ich appelliere deshalb an den Landtag, vor allem die Regierungsfraktion, und die Landesregierung, auch in Baden-Württemberg im Sicherheitsbereich eine Datenschutzkontrolle zu ermöglichen, die diesen Namen verdient.

3. Prüfung der Abteilung Staatsschutz des Landeskriminalamts

3.1 Gegenstand der Prüfung

An 10 Tagen zwischen März und Juni dieses Jahres führte ich eine Prüfung der Abteilung Staatsschutz des Landeskriminalamts durch. Sie ist noch nicht abgeschlossen. Im Mittelpunkt meiner Betrachtung stand dabei die Datei „PIOS-Terrorismus“, die beim Bundeskriminalamt eingerichtet ist und die Bund und Länder gemeinsam betreiben. Diese Datei dient — kurz gesagt — der Bekämpfung der terroristischen Gewaltkriminalität. Zu diesem Zweck werden Daten über Personen (P), Institutionen (I), Objekte (O) und Sachen (S) im wesentlichen in Form eines Fundstellennachweises gespeichert. Die Daten fallen im Rahmen von Ermittlungsverfahren an, insbesondere wegen Bildung terroristischer Vereinigungen (§ 129 a des Strafgesetzbuchs), aber auch außerhalb von solchen, zum Beispiel im Rahmen der Häftlingsüberwachung oder bei Beobachtungen. Die Daten geben die Staatsschutzabteilungen der Landeskriminalämter bzw. das Bundeskriminalamt selbst ein. Nur sie sind auch abfrageberechtigt.

Mir ging es bei meinem Besuch nicht darum, „Verstöße“ gegen datenschutzrechtliche Vorschriften festzustellen. Ich wollte mir einen Eindruck über den Umfang und die Art der Datenverar-

beitung in diesem Bereich, über die Handhabung der KpS-Richtlinien und etwaige staatsschutzspezifische Probleme bei deren Umsetzung, über die Praxis der Speicherung von Daten, insbesondere im Rahmen der Häftlingsüberwachung, und über den Stand der Bereinigung der in dieser Abteilung geführten kriminalpolizeilichen Unterlagen verschaffen. Dabei lag und liegt mir daran, ganz besonders in diesem äußerst empfindlichen Bereich zu Lösungen zu kommen, die das Wissen und die Erfahrung der hier tätigen Beamten und damit die Sicherheitsinteressen berücksichtigen, andererseits aber auch den datenschutzrechtlichen Anforderungen Rechnung tragen. Ich glaube, guten Gewissens sagen zu können, daß sich meine Vorstellungen in diesem Rahmen halten und bei gutem Willen auch dort ein Konsens gefunden werden kann, wo dies bis jetzt noch nicht möglich war.

3.2 Feststellungen und Schlußfolgerung

Bei meinem Besuch stellte ich im einzelnen folgendes fest:

— Selbst Angehörige der Abteilung Staatsschutz tun sich zum Teil schwer zu sagen, wer weshalb in PIOS gespeichert ist. Das hat verschiedene Gründe:

- Zum einen vergaß man in der Vergangenheit häufig, in den Akten zu dokumentieren, daß eine bestimmte Person auf Grund eines bestimmten Sachverhalts in PIOS erfaßt wurde. Bereits die einschlägige Dienstanweisung schreibt vor, daß die Unterlagen an den ausgewerteten Stellen mit einem Erfassungsstempel zu versehen sind. Nur so läßt sich beispielsweise prüfen, ob der Sachverhalt die Speicherung der Daten in einer Datei rechtfertigt.
- Zum andern bereitet es mitunter erhebliche Mühe, auf Grund der in PIOS gespeicherten Fundstellen das Beweismittel für eine Datenspeicherung (z. B. das Anschriften- und Telefonverzeichnis in Notizbüchern) in den Akten zu finden; in einem Fall befand es sich gar bei der Staatsanwaltschaft. Nur mit Hilfe des Beweismittels kann man jedoch die Rechtmäßigkeit einer Datenspeicherung beurteilen, da die in PIOS gespeicherte Fundstellenangabe für sich allein nicht aussagekräftig ist.

Diese Mängel sind erklärlich, weil man beim Aufbau der Datei im Jahr 1975, aber auch danach in Anbetracht der Sicherheitslage solchen „Formalien“ nicht die nötige Aufmerksamkeit schenkte. Es liegt jedoch im Interesse der Polizei und des Datenschutzes, daß jede PIOS-Speicherung möglichst schnell anhand der Akten nachvollzogen werden kann. Ich schlug deshalb eine Reihe organisatorischer Maßnahmen vor, die das Landeskriminalamt zum Teil bereits akzeptierte und praktiziert.

— Das Landeskriminalamt speicherte bisher entsprechend einem Beschluß der Innenministerkonferenz von 1975 die Daten aller Personen, die inhaftierte terroristische Gewalttäter besuchten oder mit ihnen in Briefkontakt standen. Ausgenommen waren lediglich Kinder, Geistliche, Beamte, Sozialarbeiter und Gutachter, soweit sie beruflich mit den Häftlingen zu tun hatten. Diese pauschale Speicherung aller Kontaktpersonen ohne jede Prüfung im Einzelfall ist durch § 9 Abs. 1 LDSG nicht gedeckt. Zumindest in einem Teil der Fälle konnte durch hier nicht näher zu beschreibende Maß-

nahmen ausgeschlossen werden, daß es sich um einen „relevanten Kontakt“ handelte. Das Landeskriminalamt wies mich selbst auf einen Fall hin, in dem es über die Speicherung der Daten aller Besucher eines terroristischen Gewalttäters „nicht glücklich war“. Es hatte sich nämlich gezeigt, daß der Gefangene mit seinen Besuchern durchweg private Angelegenheiten besprach. Diese Daten hat das Landeskriminalamt inzwischen gelöscht. An einer generell differenzierenden Betrachtung sah es sich jedoch durch den Beschluß der Innenministerkonferenz gehindert. Inzwischen hat der Polizeiarbeitskreis der Innenministerkonferenz eine vorläufige Neuregelung der Häftlingsüberwachung beschlossen. Er trug damit den von vielen Seiten, nicht zuletzt auch von der Polizei selbst geäußerten Bedenken gegen die bisherige Praxis Rechnung.

Die Neuregelung ist im Lande inzwischen in Kraft. Sie sieht eine Relevanzprüfung des jeweiligen Kontakts mit dem inhaftierten Häftling vor. Bei Kontakten mit bestimmten Personengruppen unterbleibt grundsätzlich eine Speicherung. In zweifelhaften Fällen läßt sie eine kurzzeitige Speicherung zu, sieht jedoch als zusätzliche Sicherungsmaßnahme vor, daß über die Tatsache der Speicherung nur in beschränktem Umfang Auskunft erteilt werden darf. Die Speicherfristen sind insgesamt sehr differenziert ausgestaltet. Einzelheiten kann ich jedoch aus Gründen des Geheim-schutzes nicht mitteilen. Bedenkt man, wie schwierig es gerade in diesem Bereich ist, zu einem Ausgleich zwischen Sicherheitsaspekten und Datenschutz zu gelangen, kann man — glaube ich — mit der neuen Regelung zufrieden sein. Man muß nun sorgfältig beobachten, wie sie die Praxis anwendet.

- Das Landeskriminalamt speichert nach wie vor die Daten von Zeugen, Hinweisgebern und Anzeigeerstatern in PIOS, obwohl dem die gültigen Dateienrichtlinien entgegenstehen. Danach darf die Polizei die Daten dieses Personenkreises „nur im Rahmen zeitlich befristet geführter Spurendokumentationssysteme“ speichern. Sinn dieser Regelung ist, die Daten von Zeugen, Hinweisgebern und Anzeigeerstatern nur ausnahmsweise und unter engen Voraussetzungen zusammen mit Daten von Personen zu speichern, die Beschuldigte oder Tatverdächtige sind oder wie hier im weitesten Sinn in Verbindung mit terroristischen Aktivitäten gebracht werden. Es stellt nämlich eine besondere Gefährdung für die erstgenannte Personengruppe dar, mit Beschuldigten und Tatverdächtigen dieser Art in einen Topf geworfen zu werden. Nur wenn die Gefahren minimiert sind — wie dies bei einem zeitlich befristet geführten Spurendokumentationssystem der Fall ist, das in der Regel einem wesentlich enger begrenzten Zugriff als andere Dateien unterliegt —, soll die gemeinsame Speicherung dieser beiden Personengruppen zulässig sein. PIOS ist kein solches befristet geführtes Spurendokumentationssystem. Die Datei als solche wird nicht befristet geführt, sondern ist auf Dauer eingerichtet. Sie ist auch kein Spurendokumentationssystem im herkömmlichen Sinn. Darunter versteht man nämlich ein System, das der Dokumentation von Hinweisen und Spuren und damit Ermittlungs- und Aufklärungsarbeit in einem größeren, aber abgegrenzten Fallkomplex dient und in der Regel nur der ermittelnden Polizeidienststelle zur Verfügung steht. PIOS hat sich hingegen über seine ursprüngliche Konzeption hinaus, die vielleicht die einer

„SPUDOK“ war, zu einem Informationssystem (Fundstellennachweis) für den Bereich Terrorismus entwickelt, auf das alle Staatsschutzabteilungen der Landeskriminalämter und des Bundeskriminalamts Zugriff haben. Ist PIOS demnach kein zeitlich befristet geführtes Spurendokumentationssystem, so darf das Landeskriminalamt die Daten von Zeugen, Anzeigerstattern und Hinweisgebern darin nicht mehr speichern und muß früher eingegebene Daten löschen. Dies sieht auch der Bundesminister des Innern so, wie mir aus dessen Schreiben vom 11. Nov. 1982 an den Bundesbeauftragten für den Datenschutz bekannt ist. Das Bundeskriminalamt bereinigt bereits seit einiger Zeit die über Zeugen, Hinweisgeber und Anzeigerstatter gespeicherten Daten. Deshalb ist umso bedauerlicher, daß sich das Innenministerium mit der Begründung, PIOS sei ein befristet geführtes Spurendokumentationssystem, meiner Forderung bisher widersetzt. Ich hoffe jedoch, daß sich der Herr Innenminister doch noch der Auffassung des Bundesministers des Innern anschließt.

- Die Dateienrichtlinien erlauben, außer Beschuldigten, Tatverdächtigen und einigen anderen enumerativ aufgeführten Personengruppen auch „andere Personen“ in einer Datei zu speichern, „wenn zureichende tatsächliche Anhaltspunkte die Annahme rechtfertigen, daß dies zur Aufklärung oder vorbeugenden Bekämpfung schwerwiegender Straftaten, zur Ergreifung von zur Festnahme gesuchter Personen oder zur Abwehr einer im einzelnen Fall bestehenden erheblichen Gefahr erforderlich ist.“ Zum Ausgleich für diese ohne Zweifel sehr weitgehende Datenspeicherung sehen die Dateienrichtlinien vor, daß die Betroffenen über die Tatsache der Speicherung zu unterrichten sind, sobald die Dauer der Speicherung ein Jahr überschritten hat. Die Polizei kann die Unterrichtung nur zurückstellen, solange durch sie der mit der Speicherung verfolgte Zweck gefährdet würde. Bei meinem Kontrollbesuch stellte ich fest, daß das Landeskriminalamt den betroffenen Personenkreis von der Tatsache der Speicherung bisher nicht unterrichtet hat. Es prüft noch nicht einmal, ob eine Unterrichtung erfolgen muß oder ein Ausnahmefall vorliegt. Dies ist bisher wohl auch gar nicht möglich, weil die fraglichen Fälle bis jetzt nicht vor Ablauf der Jahresfrist in Wiedervorlage kamen. Diese Praxis entspricht nicht den Dateienrichtlinien. Dagegen läßt sich nicht einwenden — wie es das Innenministerium tut —, in den fraglichen Fällen komme eine Unterrichtung in der Regel nicht in Betracht. Wie ich aus dem Schreiben des Bundesministers des Innern an den Bundesbeauftragten für den Datenschutz weiß, beurteilt auch er dies anders. Das Bundeskriminalamt gibt in den fraglichen Fällen eine Wiedervorlagefrist von ca. 11 Monaten in PIOS ein. Nach Wiedervorlage prüft es dann, ob die Daten gelöscht werden können. Geschieht dies, ist eine Unterrichtung des Betroffenen überflüssig; andernfalls erfolgt sie. So sollte auch Baden-Württemberg verfahren.
- Bei der Datei PIOS-Terrorismus ist die Datenspeicherung aus verständlichen Gründen sehr weit ausgedehnt. Deshalb kommt selbstverständlich die Prüfung der Erforderlichkeit der Datenspeicherung nach nicht zu lang bemessenen Zeitabständen und gegebenenfalls der Löschung der Daten große Bedeutung zu. In diesem Punkt muß das Landeskriminalamt noch erhebliche Anstrengungen unternehmen. Dies gilt vor allem für die Daten, die es außerhalb von Ermittlungsver-

fahren, beispielsweise im Rahmen der Häftlingsüberwachung speichert. Selbstverständlich hat es auch hier schon Löschungen gegeben, vor allem auf Initiative des Bundeskriminalamts. Weiter sind die Bemühungen jedoch bei der Bereinigung der Daten gediehen, die es auf Grund von Ermittlungsverfahren speichert. Schon vor Beginn meines angekündigten Besuchs beim Landeskriminalamt hat der Datenstationsleiter aus Eigeninitiative und ohne Kenntnis der dafür Verantwortlichen einige Ermittlungsverfahren PIOS-bereinigt. Während meines Besuchs machte dann die Bereinigung rasche Fortschritte. Nur ein besonders markantes Beispiel zur Verdeutlichung: Als ich dem Landeskriminalamt eines Tages in der Frühe mitteilte, ich wolle ein bestimmtes Verfahren prüfen, waren nach seiner Unterlage vom selben Tag 28 Personen in PIOS gespeichert. Am Nachmittag waren bereits die Daten von 26 Personen gelöscht.

Wichtig ist mir bei der Bereinigung vor allem eines: Es darf nicht mit der Löschung von Daten in PIOS sein Bewenden haben. In der Abteilung Staatsschutz gibt es neben dieser automatisierten Datei u. a. noch eine in vollem Umfang dem Landesdatenschutzgesetz unterliegende Lichtbildkartei sowie mehrere Dateien, die das Landeskriminalamt als „intern“ bezeichnet. Dazu gehört beispielsweise die Indexkartei, in der alle beim Staatsschutz erfaßten Personen samt Aktenfundstellen verzeichnet sind. Daneben gibt es dann selbstverständlich noch jede Menge kriminalpolizeilicher Unterlagen. Nach dem Landesdatenschutzgesetz, den Dateien- und KpS-Richtlinien müssen auch diese Unterlagen bereinigt werden. Mir kommt es darauf an, daß diese Bereinigung der verschiedenen kriminalpolizeilichen Sammlungen Hand in Hand geht. Es sollte also nicht so sein, daß die Daten zunächst in PIOS und erst später einmal in der Lichtbildkartei usw. gelöscht werden. Ich empfahl deshalb dem Landeskriminalamt schon vor Monaten, für die Durchführung der Bereinigung ein Konzept zu erarbeiten. Dieses soll auch zeitliche Vorstellungen über den Ablauf der Bereinigungsaktion enthalten. Das Innenministerium teilte mir daraufhin mit, das Landeskriminalamt arbeite zur Zeit an einer neuen Dienstanweisung für die Anlage von Akten, die Erfassung von Daten in PIOS, deren Löschung und Bereinigung. Nach deren Fertigstellung könnte man Aussagen über Ablauf und zeitliche Dauer der Bereinigung machen. Ich begrüße dies und hoffe, daß man mir die Dienstanweisung und die daran anknüpfenden Überlegungen bald zur Kenntnis gibt. Ich möchte zum Abschluß noch eines betonen: Es geht mir nicht darum, daß die Prüfung und Bereinigung der Staatsschutzunterlagen von heute auf morgen durchgeführt wird. Ich weiß, daß dies unmöglich ist, weil einerseits der Aufwand erheblich und andererseits die Staatsschutzabteilung mit den „normalen“ Aufgaben stark belastet ist. Dennoch sollte sich das Landeskriminalamt auch dieser Aufgabe kontinuierlich und im Rahmen des Möglichen widmen. Aus polizeilicher wie aus datenschutzrechtlicher Sicht sollte die Bereinigung des Datenbestandes nicht an letzter Stelle der Prioritätenliste stehen.

4. Eingaben

Im Polizeibereich gab es wiederum eine Fülle von Anfragen und Eingaben; sie nahmen gegen Jahresende deutlich zu. Die Bürger wollen vor allem wissen, ob und unter welchen Voraussetzungen

die Polizei Auskunft über gespeicherte Daten erteilt und welche Stelle für die Auskunftserteilung zuständig ist. Zum Teil erkundigen sie sich auch nach den Voraussetzungen für die Löschung von Daten. Viele Bürger bewegt die Frage, ob eine Datenspeicherung der Polizei zulässig ist. Andere sorgen sich, ob die Polizei ihre Daten an Behörden oder Private weitergab, und bringen dazu Anhaltspunkte vor. In diesen Fällen stehe ich bei der Nachprüfung vor erheblichen praktischen Schwierigkeiten, wenn die Anfrage der Behörde und die Antwort der Polizei nicht schriftlich erfolgte. Dann ist es oft schon schwierig festzustellen, welche Polizeidienststelle Daten weitergegeben haben könnte. Gibt es dieses Hindernis nicht oder hat man es überwunden, gibt es weitere Probleme: Zum einen protokollieren Polizeidienststellen solche Auskünfte an Dritte selten; zum anderen ist die Datenweitergabe allenfalls in einer Akte dokumentiert, auf die mir seit der Beschränkung meiner Kontrollbefugnis der Zugriff verwehrt ist. Deshalb gehen solche Überprüfungen leider immer wieder einmal aus wie das Hornberger Schießen. Was bleibt, ist ein ungutes Gefühl. Exemplarisch dafür ist die Eingabe eines 18jährigen Mädchens. Sie wandte sich an mich, weil ihr Arbeitgeber — die amerikanischen Streitkräfte — ihr mit der Begründung gekündigt hatte, er habe von der deutschen Polizei über ihre Kontakte zur Rauschgiftszene erfahren. Meine Nachfrage bei der Landespolizeidirektion erbrachte — wie erwartet — nichts. Ihr Rauschgiftdezernat versicherte mir glaubhaft, es hätte die Daten nicht weitergegeben. Hierzu habe kein Anlaß bestanden, da außer einem Ermittlungsverfahren und vereinzelten Kontakten in der Rauschgiftszene nichts Negatives über das Mädchen bekanntgeworden sei. Man habe deshalb im Einverständnis mit ihr versucht, den Arbeitgeber zur Rücknahme der Entlassung zu bewegen. Dies sei jedoch vergeblich gewesen. Eine weitere Sachaufklärung war mir leider nicht möglich. Deshalb konnte ich auch keinen Verstoß gegen Datenschutzvorschriften feststellen. Aber unbefriedigend ist dies — gerade auch angesichts der Folgen für die Betroffene — allemal. Schon deshalb wäre ich der Sache gerne auf den Grund gegangen, auch wenn dies nicht zu einer Rücknahme der Entlassung durch den Arbeitgeber geführt hätte.

Aus der Fülle der Eingaben greife ich einige heraus, die unter tatsächlichen oder rechtlichen Aspekten bedeutsam sind:

- Wozu eine Datenspeicherung bei der Polizei führen kann, zeigt folgender Fall: Die Polizei lud eines Tages einen bisher nicht vorbestraften Mann vor und eröffnete ihm, sie führe Ermittlungen gegen einen Unbekannten, der andere am Telefon mit obszönen Beleidigungen terrorisiert. Auf die Frage des Mannes, wie man auf ihn komme, erklärte die Polizeibeamtin, er sei der Polizei kein Unbekannter. Was war geschehen? Die Polizei hatte im Zuge der Ermittlungen gegen Unbekannt eine sogenannte PAD-Recherche durchgeführt. Zu diesem Zweck ließ sie die Namen der Personen ausdrucken, die in der Personenauskunftsdatei wegen einschlägiger Ermittlungs- oder Strafverfahren erfaßt sind. Dabei stieß man auf den Mann. Gegen ihn hatte die Polizei im Jahre 1976 wegen sexueller Beleidigung ermittelt. Dem lag folgender Sachverhalt zu Grunde: Ein ausländisches Ehepaar hatte Anzeige erstattet, weil es eine zunächst unbekannte Person angeblich ständig angerufen und wiederholt beleidigt hatte. Dabei sollen auch obszöne Ausdrücke gebraucht worden sein. Das Ehepaar ließ deshalb eine Fangschaltung einrichten. Auf diese Weise stellte sich heraus, daß drei der fraglichen Gespräche vom Telefonanschluß einer Krankenkasse aus geführt wurden. Das Ehepaar führte daraufhin bei der Krankenkasse Nachforschungen durch. Dabei ergab sich, daß unser Mann der Anrufer war. Die Anrufe begründete er

damit, daß Inhaber des Telefonanschlusses ausweislich der Unterlagen der Krankenkasse eines ihrer Mitglieder war, mit dem er aus dienstlichen Gründen telefonieren mußte. Die Ermittlungen der Kriminalpolizei beschränkten sich darauf, mit dem Geschäftsstellenleiter der Krankenkasse ein Gespräch zu führen. Eine Vernehmung erfolgte jedoch nicht. Auch hörte die Polizei den verdächtigen Mann nicht. Angeblich hat sie ihn mehrfach vorgeladen; er soll jedoch nicht erschienen sein. Exakte Unterlagen darüber finden sich nicht in den Akten. Eine Vernehmung des Krankenkassenmitglieds, das der Mann angeblich anrufen wollte, erfolgte ebenfalls nicht. Ob die Polizei das von dem ausländischen Ehepaar über die Gespräche aufgenommene Tonband auf strafbare Handlungen hin abhörte, ist unklar. In ihrer Strafanzeige an die Staatsanwaltschaft heißt es hierzu lediglich, „die Tonbandkassette weist keine tatrelevanten Merkmale auf.“ Die Staatsanwaltschaft stellte das Ermittlungsverfahren mit der zweifelhaften Begründung ein, die Geschädigten — das ausländische Ehepaar — hätten keinen Strafantrag gestellt. Der Mann bestritt mir gegenüber entschieden die ihm zur Last gelegte Tat. Er brachte vor, er habe im Rahmen seiner Sachbearbeitertätigkeit mit einem Mitglied der Krankenkasse Verbindung aufnehmen müssen und deshalb die auf der Leistungskarte vermerkte Telefonnummer angerufen. Daraufhin habe sich eine ausländisch sprechende Frau gemeldet und danach ein Mann, der ihn mit einem wahren Schwall von Beleidigungen überzogen habe. Weil er geglaubt habe, sich verwählt zu haben, habe er die fragliche Telefonnummer mehrmals angerufen, sei jedoch stets beleidigt worden. Eine förmliche Ladung zu einer Vernehmung habe er nicht erhalten. Er sei deshalb davon ausgegangen, daß die Ermittlungen seinerzeit im Sande verlaufen seien. Die jetzt angestellten Nachforschungen ergaben, daß das Krankenkassenmitglied früher die in der Leistungskarte vermerkte Telefonnummer besaß.

Ich beanstandete die Speicherung der Daten dieses Mannes durch die Polizei nach § 18 LDStG. Sie war zur rechtmäßigen Erfüllung der Aufgaben der Polizei nicht erforderlich. Das Interesse des Mannes, künftig bei ähnlichen Ermittlungen nicht stets in die polizeiliche Überprüfung einbezogen zu sein oder gar als Tatverdächtiger zu gelten, überwog das öffentliche Interesse, zu Zwecken der Strafverfolgung oder Gefahrenabwehr auf polizeiliche Erkenntnisse zurückgreifen zu können. Bei der Würdigung der Gesamtumstände des Falles, die ich hier nicht im einzelnen nachvollziehen kann, sprach für die Löschung der Daten, daß der 50jährige Mann der Polizei ansonsten unbekannt war, die Tat bestritt, das Ermittlungsverfahren eingestellt worden war, die Tonbandkassette entweder keine Anhaltspunkte für eine Straftat bot oder gar nicht abgehört wurde und die Polizei — und das scheint das letztlich Ausschlaggebende zu sein — nahezu alle weiteren Ermittlungen unterließ. Dies kann nicht zum Nachteil des Mannes gereichen. Sollen Daten über einen Tatverdächtigen/Beschuldigten auf längere Dauer in einer Datei der Polizei gespeichert werden, ist es ein rechtsstaatliches Gebot, die vorhandenen Beweismittel auszuschöpfen. Dies sah wohl auch das Innenministerium so. Es entsprach meiner Beanstandung im Ergebnis und veranlaßte die Löschung der Daten.

- Ein ausländischer Staatsangehöriger wandte sich mit der Behauptung an mich, er sei zu Unrecht erkennungsdienstlich behandelt worden. Deshalb sei die Speicherung seiner Daten und die Aufbewahrung der angefallenen Unterlagen unzulässig. Ich stellte fest, daß die Polizei gegen diesen Mann wegen Ver-

dachts der Trunkenheit, des Diebstahls, eines Verstoßes gegen das Ausländergesetz und das Betäubungsmittelgesetz ermittelt. Die erkennungsdienstliche Behandlung war daher durch § 81 b der Strafprozeßordnung gedeckt und die Speicherung von Daten bzw. Aufbewahrung von Unterlagen zumindest bis zum Abschluß des Verfahrens zulässig.

- Mehrere Eingaben sind bei mir zur Zeit zu der Frage anhängig, ob die Polizei zu Recht Daten an Verwaltungsbehörden übermittelt hat. Im Rahmen verschiedener Verwaltungsverfahren — beispielsweise der Erteilung einer Fahrerlaubnis, einer Waffenbesitzkarte, bestimmter gewerberechtlicher Erlaubnisse, eines Jagdscheins — muß die Zuverlässigkeit der Antragsteller geprüft werden. Die gesetzlichen Regelungen sind allerdings sehr unterschiedlich ausgestaltet. In der Praxis schalten die Verwaltungsbehörden die Polizei zum Teil in die Prüfung ein, zum Teil ist dies sogar ausdrücklich in Verwaltungsvorschriften vorgesehen. Man kann die einzelnen Verfahren sicher nicht über einen Kamm scheren. Was mich jedoch insgesamt stört und was wohl auch nicht mit § 10 Abs. 1 LDSG und den KpS-Richtlinien zu vereinbaren ist, ist folgender Umstand: Die Polizeidienststellen teilen ohne weitere Prüfung alles mit, was sie über den Betroffenen in ihren Unterlagen finden. Dabei sind sie sich oftmals nicht bewußt, daß jede Mitteilung für den Betroffenen nachteilige Folgen haben kann. Er kann zum Beispiel „nur“ in seinem Ansehen herabgemindert werden, wie dies vor allem in kleineren Gemeinden leicht möglich ist, oder aber ein Gutachten beibringen müssen. Mitunter erfahren Bürger in diesem Zusammenhang erstmals, daß die Polizei gegen sie irgendwann einmal ein Ermittlungsverfahren führte, das mit der Einstellung endete. Wer meint, der Polizei sei aus Gründen der Arbeitsbelastung weder möglich noch zumutbar, die „Erforderlichkeit“ der Datenweitergabe zu prüfen, und letztlich entscheide ja ohnehin die Verwaltungsbehörde, verkennt, daß schon die Weitergabe von Daten an eine andere Behörde in die Position des Bürgers eingreift. Die Polizei muß deshalb vor einer Weitergabe ihrer — in Akten erfaßten oder Dateien gespeicherten — Daten prüfen, ob sie diese überhaupt nach Landesdatenschutzgesetz und KpS-Richtlinien aufbewahren und speichern darf. Ist dies nicht der Fall, ist auch die Übermittlung unzulässig. Deshalb muß die Polizei beispielsweise den Ausgang von Ermittlungs- oder Strafverfahren in ihre Überlegungen einbeziehen. Und noch ein Weiteres: Die Unterlagen der Polizei sind im Grundsatz vertraulich und zunächst einmal nur zur Erfüllung ihrer Aufgaben bestimmt. Sie können deshalb nicht schrankenlos anderen Behörden geöffnet werden. Das würde praktisch zu einer Umgehung des Bundeszentralregistergesetzes führen nach dem Motto, was die Verwaltungsbehörde nicht aus dem Register erfährt, erfährt sie von der Polizei. Dies kann und darf nicht sein.
- Mehrere Bürger wandten sich gegen das Erfassen und Kennzeichnen der sogenannten Zigeunernamen mit der Abkürzung „ZN“. Als Beispiele nannten sie das von der Polizei verwendete Formular „Strafanzeige“, den Vordruck „Anzeige über den Verlust eines Personalausweises/Passes“ sowie ein Erhebungsbogen der Landeswohlfahrtsbehörden. Sie wandten sich nicht gegen die Erhebung dieses Namens, sondern dagegen, daß ihm jeweils die Abkürzung „ZN“ vorangestellt wird. Dies sei eine Diskriminierung der Sinti und ein Rückfall in die Vergangenheit. Auch gäbe es Anhaltspunkte, daß das Polizeipräsidium Karlsruhe besondere Unterlagen über Sinti führe. Schließlich sei wichtig zu wissen, was mit der in Baden-Würt-

temberg früher bestanden Landfahrerkartei geschah. Ergebnis meiner Nachforschungen war:

- Die Polizei stellt in ihrem Formular „Strafanzeige“ den sogenannten Zigeurnamen zur Kennung der Namensart die Abkürzung „ZN“ voran. Dies ist datenschutzrechtlich ebenso wenig zu beanstanden wie der Umstand, daß die Polizei solche Namen in der Personenauskunftsdatei speichert — vorausgesetzt allerdings, daß dies zur Strafverfolgung und Gefahrenabwehr erforderlich ist. Dann darf die Polizei alle Namen erfassen, unter denen die Betroffenen bekannt sind, da sie bei etwaigen Ermittlungen weiterhelfen können. Eine ganz andere Frage ist, ob das Voranstellen der Abkürzung „ZN“ vor solche Namen aus polizeilicher Sicht geboten ist. Dies kann diskriminierend wirken. Ich bat deshalb das Innenministerium zu prüfen, ob man nicht statt dessen die Abkürzung „GN“ für Genanntname verwenden könne. Das Innenministerium verneinte dies wie einige Innenressorts anderer Länder. Es meint, die Speicherung des Zigeurnamens sei „im Interesse einer effektiven Kriminalitätsbekämpfung erforderlich“. Dieses Argument geht an der Sache vorbei, da es mir nicht um die Speicherung des Zigeurnamens sondern nur um dessen Kennzeichnung geht. Ich hoffe, daß man bei der Beratung dieser Frage im zuständigen Bund-Länder-Gremium sorgfältiger differenziert.
 - Das Formular „Anzeige über den Verlust eines Personalausweises/Passes“ war früher ebenso ausgestaltet wie das Anzeigeformular der Polizei. Inzwischen findet sich darin jedoch kein Hinweis mehr auf den sogenannten Zigeurnamen.
 - Auch die Landeswohlfahrtsverbände verwenden keinen Erhebungsbogen mehr, in dem der Zigeurname vorgesehen ist. Ein Landeswohlfahrtsverband räumte allerdings ein, daß in der Vergangenheit in Einzelfällen ein überholter Erhebungsbogen benutzt wurde. Er will dafür sorgen, daß dies künftig nicht mehr geschieht.
 - Bei einem vorher nicht angekündigten Kontrollbesuch des Polizeipräsidiums Karlsruhe fand ich keine Anhaltspunkte dafür, daß es besondere Karteien oder kriminalpolizeiliche Unterlagen über Sinti führt. Ich stieß weder auf eine Landfahrerkartei noch auf „Zigeuner-Akten“, die während der Zeit des Nationalsozialismus aus rassistischen Gründen angelegt wurden. In der Aktenhaltung befanden sich lediglich Akten über Sinti, gegen die strafrechtliche Ermittlungsverfahren geführt werden oder wurden. Die Aufbewahrung dieser Unterlagen ist im Rahmen der KpS-Richtlinien zulässig. Darüber hinaus prüfte ich, ob die Landespolizeidirektion Karlsruhe besondere Unterlagen über Sinti führt. Auch dies ist nicht der Fall. Zwar gab es bei der ehemaligen Kriminalhauptstelle Karlsruhe Vorgänge über solche Sinti, die polizeilich in Erscheinung getreten waren. Diese Akten, die einst Bestandteil der allgemeinen Aktenhaltung waren, wurden jedoch nach 1970 bereinigt. Ebenso wenig habe ich Anhaltspunkte, daß andere Polizeidienststellen besondere Unterlagen über Sinti führten. Die mit Erlaß vom 23. Juli 1953 beim Landeskriminalamt eingerichtete Zentralkartei zur Bekämpfung von Zigeunerdelikten wurde am 1. Okt. 1971 wieder aufgelöst. Die angefallenen Akten und die Kartei wurden, wie man mir glaubhaft versicherte, vernichtet.
- Im Rahmen einer Eingabe stellte ich fest, daß die Polizei über einen Bürger Daten wegen Nötigung speichert. Das Verfahren hatte jedoch nur zu einem Bußgeldbescheid der Verkehrsbe-

hörde wegen einer Verkehrsordnungswidrigkeit geführt. Die Polizei mußte daher die Daten löschen.

- In Norddeutschland fand die Polizei eines Tages Zahlkarten einer Bibelgesellschaft, auf die rechtsradikale Parolen geschmiert waren. Die Polizei wollte deshalb von der Bibelgesellschaft die Namen und Anschriften aller Spender aus diesem Gebiet wissen. Es handelte sich dabei um ca. 30—40 Adressen. Ich sagte der anfragenden Bibelgesellschaft, die Datenübermittlung an die Polizei beurteile sich nicht nach dem Landesdatenschutzgesetz, sondern nach dem weitgehend identischen kirchlichen Datenschutzrecht. Wäre sie eine Frage des staatlichen Datenschutzrechts, würde ich folgende Überlegungen anstellen: Die von der Polizei gewünschten Daten sind relativ sensibel. Denn aus ihnen ergibt sich, welche Person der Bibelgesellschaft Spenden zukommen läßt. Damit wird die religiöse Einstellung dieser Personen kundgetan. Man müsse deshalb an die Erforderlichkeit der Herausgabe dieser Daten nach dem Grundsatz der Verhältnismäßigkeit strenge Anforderungen stellen. Dabei falle besonders ins Gewicht, daß es erhebliche Zweifel gäbe, ob der Täter tatsächlich unter dem Spenderkreis zu finden sei. Denn die Zahlkarten besäßen nicht nur die bereits bekannten Spender, sondern seien auch Zeitschriften beigelegt und an verschiedenen Stellen ausgelegt. Bei dieser Sachlage käme eine Bekanntgabe der erbetenen Adreßdaten nicht in Betracht.

3. Abschnitt: Strafrechtspflege

1. Registrieren von Prozeßbesuchern

Durch mehrere Eingaben erfuhr ich, daß Besucher beim Betreten des Stuttgarter Landgerichts-, des Oberlandesgerichts- und des Prozeßgebäudes in Stuttgart-Stammheim registriert werden. Dies löste bei manchen Besuchern erhebliche Sorge aus. So befürchtete ein Bürger, er werde wegen seiner zeitweiligen Teilnahme an einem Prozeß gegen Rechtsterroristen künftig bei den Sicherheitsbehörden als „potentieller Sympathisant der Terroristen“ gelten. Ein Journalist, der als Prozeßberichterstatter in Stuttgart-Stammheim tätig ist, vermutete, seine erfaßten Daten seien an die Polizei weitergegangen. Zur Begründung berichtete er, die Polizei habe ihn bei der Besichtigung des Festnahmeorts zweier in Stuttgart-Stammheim angeklagter Personen überprüft, durchsucht und danach gefragt, „ob er sich öfter in Stuttgart aufhalte“ und „für bestimmte Prozesse interessiere“. Meine Nachforschungen bestätigten diese Befürchtungen und Vermutungen nicht. Ich stellte folgendes fest:

- Die Pforte am Landgerichts- und Oberlandesgerichtsgebäude Stuttgart notiert jeden Tag aus Sicherheitsgründen in einer Liste die Prozeßbesucher mit Name, Vorname, Geburtsdatum, Geburtsort und Wohnort und den von ihnen aufgesuchten Sitzungssaal. In diese Liste dürfen keine anderen Personen als der Justizwachtmeister an der Empfangspforte Einsicht nehmen. Die beiden Gerichte bewahren die Listen etwa eine Woche auf und vernichten sie danach. Dieses Verfahren beruht auf einer gemeinsamen Verfügung der beiden Gerichtspräsidenten und stützt sich auf das Hausrecht. Gegen diese Art des Registrierens gibt es aus der Sicht des Datenschutzes keine Bedenken. Das Landesdatenschutzgesetz ist hier überhaupt nicht anwendbar, weil die Daten in einer Liste und nicht in einer Datei er-

faßt werden. Verletzt ist aber auch nicht das allgemeine Persönlichkeitsrecht der Prozeßbesucher. Denn zum einen ist das Registrieren aus Sicherheitsgründen angezeigt. Zum andern erleidet der Prozeßbesucher dadurch keine nennenswerten Nachteile: Die Listen nützen nur die Justizwachtmeister zu Identifizierungszwecken. Sie geben die darin enthaltenen Personalien nicht an die Sicherheitsbehörden weiter, geschweige denn, daß diese sie gar in ihren Computern speichern. Auch werden die Unterlagen innerhalb kurzer Zeit vernichtet. Diese Vorgehensweise trägt den schutzwürdigen Belangen der Gerichtsbesucher Rechnung und wahrt den Grundsatz der Verhältnismäßigkeit.

- Ähnlich ist die Situation in Stuttgart-Stammheim. Dort notieren Polizeibeamte im Wege der Amtshilfe für die Justiz die Personalien der Zuhörer und lichten ihre Ausweise ab. Diese Unterlagen dienen nur dem Überprüfen der Personalien der Prozeßbesucher. Die eingesetzten Polizeibeamten liefern die Ablichtungen und Namenslisten am Ende jedes Sitzungstages dem Gericht ab. Das Gericht vernichtet sie anschließend. Geregelt ist dies in einer sitzungspolizeilichen Anordnung des jeweiligen Gerichtsvorsitzenden. Diese Anordnung habe ich kraft Amtes nicht zu beurteilen, da sie die Gerichtsvorsitzenden in Ausübung ihrer richterlichen Tätigkeit erlassen. Anhaltspunkte, daß die Praxis abweichend von diesen Anordnungen verfährt und beispielsweise erfaßte Daten an die Polizei weitergibt, habe ich nicht.

Das Registrieren von Prozeßbesuchern hat, wie die beunruhigten Bürger richtig sehen, freilich nicht nur datenschutzrechtliche Aspekte. Es stellt sich auch die Frage, ob das Vorgehen mit den Vorschriften des Gerichtsverfassungsgesetzes über die Öffentlichkeit von Gerichtsverhandlungen vereinbar ist. Hierüber hat die Justiz selbst zu befinden. Meines Wissens bejaht die Rechtsprechung diese Frage.

2. Mitteilungen von Staatsanwaltschaften oder Gerichten an Empfänger von Geldauflagen

Nach § 153 a der Strafprozeßordnung kann die Staatsanwaltschaft mit Zustimmung des Gerichts und des Beschuldigten vorläufig von der Erhebung der öffentlichen Klage absehen und zugleich dem Beschuldigten die Zahlung eines Geldbetrages auferlegen. Ist die Klage bereits erhoben, kann das Gericht mit Zustimmung der Staatsanwaltschaft und des Angeschuldigten das Verfahren gegen Zahlung einer Geldbuße vorläufig einstellen. In beiden Fällen kann die Tat nicht mehr als Vergehen verfolgt werden, wenn der Beschuldigte die Auflage erfüllt hat. Wie ich bereits in meinem 2. Tätigkeitsbericht darstellte, gibt es bei der Durchführung dieses Verfahrens Probleme wegen des Persönlichkeitsschutzes des Beschuldigten. So war es bisher Praxis der Staatsanwaltschaften, den Beschuldigten lediglich über die beabsichtigte Verfahrenseinstellung zu unterrichten, ohne seine ausdrückliche Zustimmung hierzu einzuholen. Gleichzeitig setzten die Staatsanwaltschaften — und das war das eigentlich Bedenkliche — die potentiellen Empfänger der Geldauflage, also zum Beispiel das Rote Kreuz, von der zu erwartenden Zahlung des Beschuldigten in Kenntnis. Erfreulicherweise stellte das Justizministerium inzwischen sicher, daß die Empfänger der Geldbuße erst nach Zustimmung des Beschuldigten hiervon erfahren. Auf ein weiteres Problem machte mich eine im sozialen Bereich tätige Bürgerin aufmerksam. Manche Staatsanwaltschaften und Gerichte teilten den Empfängern von Geldbußen nicht nur den Namen des Zahlungspflichtigen, das Verfahrensaktenzeichen und die Höhe des Geldbetrages mit, sondern auch den

Tatvorwurf. Das Rote Kreuz erfuhr dadurch beispielsweise, ob gegen den Beschuldigten ein Ermittlungsverfahren wegen „fahrlässiger Körperverletzung“, „Beleidigung“ oder wegen „Diebstahl“ lief. Diese Angaben benötigt der Empfänger der Geldbuße nicht; auch hat er kein berechtigtes Interesse hieran. Ich bat deshalb das Justizministerium, diese Praxis abzustellen. Es entsprach umgehend diesem Wunsch.

3. Nennung des Beschuldigten in der Einstellungsverfügung der Staatsanwaltschaft

Gibt die Staatsanwaltschaft einem Antrag auf Erhebung der öffentlichen Klage nicht statt oder verfügt sie nach dem Abschluß der Ermittlungen die Einstellung des Ermittlungsverfahrens, so hat sie den Antragsteller, den sog. „Anzeigeersteller“ unter Angabe der Gründe zu bescheiden. Dies schreibt § 171 der Strafprozeßordnung vor. Ein solcher Bescheid kann unter dem Gesichtspunkt des Persönlichkeitsschutzes Probleme aufwerfen; hierauf wies mich eine besonders wachsame Bürgerin hin. Sie hatte bei der Polizei Anzeige gegen Unbekannt erstattet, weil ihr jemand Benzin aus dem Fahrzeug gestohlen hatte. Der Polizeibeamte sagte ihr bei der Aufnahme der Anzeige, die Polizei habe einen anonymen Hinweis auf eine Person erhalten, die der Dieb sein könne, aber noch überprüft werde. Einige Zeit später erhielt unsere Bürgerin die Einstellungsverfügung der Staatsanwaltschaft. Diese nannte den Beschuldigten mit vollem Namen, obwohl — so unsere wackere Bürgerin — „sich aus den Einstellungsgründen ergab, daß gegen den Beschuldigten von vornherein nur ein vager Verdacht bestand, der im Laufe des Ermittlungsverfahrens durch nichts erhärtet wurde“. Die Bürgerin hält es für eine unnötige Bloßstellung des Beschuldigten, daß ihr dessen Name bekanntgegeben wurde, obwohl sie Anzeige gegen Unbekannt erstattet hatte. Sie sieht darin einen Verstoß gegen die Unschuldsvermutung und eine Verletzung des allgemeinen Persönlichkeitsrechts des zu Unrecht Verdächtigten. Damit griff sie ein Problem auf, das bislang niemand sah und deshalb auch die juristische Literatur nicht behandelt. Es ist aber von großer praktischer Bedeutung. Man stelle sich bloß einmal vor, was los ist, wenn ein Bewohner eines kleinen Dorfes Anzeige wegen Brandstiftung gegen Unbekannt erstattet und dann aus der Einstellungsverfügung der Staatsanwaltschaft erfährt, sie habe gegen seinen Nachbarn ermittelt. Die Strafprozeßordnung schreibt nicht im einzelnen vor, welchen Inhalt der Bescheid an den Anzeigeersteller haben muß. Den Anforderungen der Strafprozeßordnung ist Genüge getan, wenn sie dem Anzeigeersteller eine Abschrift ihrer Einstellungsverfügung zusendet. Sie muß dies jedoch nicht. Verpflichtet ist sie lediglich, ihm die wahren Gründe der Einstellung des Verfahrens in einer für ihn verständlichen Form mitzuteilen. Die Staatsanwaltschaft sollte in Zukunft bei der Art und Weise, wie sie den Anzeigeersteller unterrichtet, nicht nur dessen strafprozessuale Rechte im Auge haben, sondern auch bedenken, daß hierbei das allgemeine Persönlichkeitsrecht des Beschuldigten auf dem Spiel steht. Sine qua non muß die Staatsanwaltschaft bei Anzeigen gegen Unbekannt sehr sorgfältig abwägen, ob sie dem Anzeigeersteller den Namen des Beschuldigten mitteilen soll. Dies gilt vor allem dann, wenn sie nur sehr vage Anhaltspunkte für die Täterschaft eines Beschuldigten hat oder nach Abschluß des Verfahrens überhaupt kein Tatverdacht mehr besteht. In diesen Fällen sollte sich der Staatsanwalt vergegenwärtigen, welche Auswirkung seine Mitteilung an den Anzeigeersteller für den Beschuldigten haben kann, vor allem dann, wenn dieser die Information nicht für sich behält. Auf diese Weise kann in den Augen der Öffent-

lichkeit am Beschuldigten „etwas hängen bleiben“. Das aber muß verhindert werden.

Das Justizministerium sieht die Problematik ähnlich. Es unterrichtete die Generalstaatsanwälte hierüber. Da sie jedoch stärkere Beachtung verdient, schlage ich vor, bei sich bietender Gelegenheit eine entsprechende Regelung in die Richtlinien für das Straf- und Bußgeldverfahren aufzunehmen.

4. Versendung sensibler Unterlagen durch die Justiz an die Arbeitgeber eines Scheidungswilligen

„Kleine Ursachen, große Wirkung“ könnte man bei folgendem Problem sagen, auf das mich der betriebliche Datenschutzbeauftragte einer großen Firma aufmerksam machte. Die baden-württembergischen Familiengerichte holen zur Durchführung des Versorgungsausgleichs im Rahmen eines Ehescheidungsverfahrens per Vordruck beim Arbeitgeber Auskünfte über die in der Ehezeit erworbenen Anwartschaften auf Leistungen der betrieblichen Altersversorgung ein. Der Vordruck enthält zwar den Hinweis „Personalsache: vertraulich!“. Auch heißt es im weiteren Text noch einmal „dieses Ersuchen und seine Anlagen enthalten vertrauliche personenbezogene Angaben über Ihren Arbeitnehmer“. Doch übersah man beim Gestalten des Vordrucks eines: Der Hinweis auf die Vertraulichkeit der Unterlagen ist von außen nicht erkennbar; denn er erscheint nicht im Brieffenster des Kuverts. Das führte im konkreten Fall dazu, daß nicht die Personalabteilung, sondern eine andere Stelle der Firma von der beabsichtigten Ehescheidung eines Mitarbeiters erfuhr. Die Vertraulichkeit über diese sehr persönliche Angelegenheit war damit nicht mehr gewahrt. Ich bat deshalb das Justizministerium, den Vordruck so zu ändern, daß der Hinweis „Personalsache: vertraulich“ im Brieffenster erscheint. Das Justizministerium sagte mir sehr rasch zu, bei der Neuauflage des Vordrucks meinem Wunsch zu entsprechen.

5. Offenbarung von Sozialdaten für Zwecke der Strafverfolgung

Seit dem Inkrafttreten des Zehnten Buchs des Sozialgesetzbuchs (SGB X) am 1. Jan. 1981 sind die Möglichkeiten, Sozialdaten für Zwecke der Strafverfolgung zu offenbaren, wesentlich genauer als bisher eingegrenzt. Sozialleistungsträger dürfen den Strafverfolgungsorganen wie allen übrigen Behörden auch

- nach § 68 SGB X bestimmte, weniger sensible Daten offenbaren, soweit kein Grund zur Annahme besteht, daß sie dadurch schutzwürdige Belange beeinträchtigen,
- nach § 69 Abs. 1 Nr. 1 SGB X alle Sozialdaten offenbaren, die diese für die Durchführung eines Strafverfahrens benötigen, das mit der Erfüllung einer gesetzlichen Aufgabe durch die Sozialleistungsträger in Zusammenhang steht,
- nach § 73 SGB X auch Sozialdaten offenbaren, soweit dies auf richterliche Anordnung zur Aufklärung eines Verbrechens oder zur Aufklärung eines Vergehens erforderlich ist. Bei Vergehen ist allerdings nur eine Offenbarung der in § 73 Nr. 2 SGB X genau bezeichneten, weniger sensiblen Angaben möglich.

Vor allem die Regelung des § 73 SGB X stößt bei den Strafverfolgungsorganen immer wieder auf Kritik. Sie berücksichtigt viel zu wenig das vom Gesetzgeber mit der Neuregelung des Sozialgeheimnisses verfolgte Anliegen, den Schutz der Sozialdaten aufzuwerten und sicherzustellen, daß niemand bloß deshalb der Preisgabe seiner personenbezogenen Daten mehr als andere Bürger

ausgesetzt ist, weil er der Sozialversicherung angehört oder sonst Ansprüche auf Sozialleistungen hat. Hinzu kam noch der Gedanke, Sozialdaten sollten mindestens genauso geschützt sein wie Angaben, die unter das Steuergeheimnis fallen. Ich verweise dazu auf die in § 30 Abs. 4 Nr. 5 der Abgabenordnung getroffene Regelung. Besonders kritisiert wird, daß es zur Offenbarung einer richterlichen Anordnung bedarf. Viele dieser Kritiker wissen nicht, wie und aus welchen Gründen es zu dieser Regelung kam: Der Sozialausschuß des Deutschen Bundestags hatte die Frage eingehend erörtert und letztlich auf Antrag der CDU/CSU-Fraktion mit Mehrheit abgelehnt, daß auch der Staatsanwalt anordnungsbefugt ist. Grund war vor allem seine Weisungsgebundenheit. Darauf hinzuweisen besteht besonderer Anlaß, weil die Landesregierung in ihrer Stellungnahme zu meinem 2. Tätigkeitsbericht diese Regelung kritisiert hatte. Nur wenig Verständnis für die Bedeutung des Sozialdatenschutzes zeigt ihr Hinweis, eine Eilzuständigkeit der Staatsanwaltschaft sei in der Strafprozeßordnung „sogar“ für Maßnahmen wie Beschlagnahme, Durchsuchung und vorläufige Festnahme vorgesehen. Offenbar meint die Landesregierung, solche Maßnahmen würden den Betroffenen stets stärker belasten als die Offenbarung von Sozialdaten. Diese Betrachtungsweise hat zwar eine lange Tradition, ist aber nicht allein schon deshalb richtig. Vor allem läßt sie die Rechtsprechung des Bundesverfassungsgerichts darüber völlig außer acht, wie sich die Weitergabe persönlicher Daten auf das durch Artikel 1 und 2 Abs. 1 GG geschützte Persönlichkeitsrecht auswirken kann. Die Weitergabe etwa von Sozialhilfeakten, die zahlreiche Angaben über die persönlichen, wirtschaftlichen, sozialen und gesundheitlichen Verhältnisse eines Sozialhilfeempfängers und seiner Angehörigen enthalten, kann sehr viel schwerer in die Rechtsstellung des Betroffenen einwirken als beispielsweise eine Beschlagnahme bestimmter Gegenstände, eine Durchsuchung oder sogar eine vorläufige Festnahme. In keinem Fall kann hier, wie das die Stellungnahme der Landesregierung suggeriert, von einem in jedem Fall geringeren Eingriff gesprochen werden. Ich verstehe, daß sich die Praxis mit solchen neuen, mit dem bisherigen Rechtsverständnis nicht ohne weiteres in Einklang zu bringenden Regelungen zunächst einmal schwertut. Dies sollte jedoch nicht dazu führen, sofort eine Änderung zu verlangen. Allein schon der Respekt vor der Entscheidung des Gesetzgebers sollte vielmehr gebieten, der Praxis den rechtspolitischen Hintergrund der Regelung deutlicher zu machen und dafür um Verständnis zu werben.

6. Strafvollzugsstatistik

Wie stark die Macht der Gewohnheit in der öffentlichen Verwaltung ist, beweist dieser Vorgang einmal mehr: Die Justizvollzugsanstalten des Landes übersenden dem Statistischen Landesamt zum Erstellen der jährlichen Strafvollzugsstatistik Zählkarten über jeden Strafgefangenen, der am 31. März einsitzt oder zu diesem Zeitpunkt vorübergehend aus der Vollzugsanstalt abwesend ist. Auf diese Weise geben sie mehr als 40 Informationen über jeden Strafgefangenen weiter: Ich nenne nur Name, Vorname, Bekenntnis, Staatsangehörigkeit, Familienstand, Kinderzahl, Wohnung, Geburtstag und erlernter Beruf, ausgeübte Tätigkeit, Vorstrafen sowie Name und Wohnung der nächsten Angehörigen. Einen Teil dieser Angaben wertet das Statistische Landesamt überhaupt nicht aus. So ist es zum Beispiel mit dem Geburtsort, dem erlernten Beruf, der ausgeübten Tätigkeit und Kinderzahl des Strafgefangenen und den Namen und der Wohnung seiner nächsten Angehörigen. Andere Angaben benötigt das Statistische Landesamt nicht in der detaillierten Weise, wie es sie erhält. Es

erfährt zum Beispiel die genaue Anschrift des Strafgefangenen, obwohl es nur wissen muß, ob der Strafgefangene einen Wohnsitz im Inland oder Ausland hat oder ob er „ohne Wohnsitz“ ist. Die Weitergabe dieser Daten ist völlig überflüssig und verstößt damit gegen § 10 LDSG. Ich forderte das Justizministerium auf sicherzustellen, daß die Justizvollzugsanstalten in Zukunft dem Statistischen Landesamt nur noch die wirklich erforderlichen Daten übermitteln. Das Justizministerium will dies tun. Es bemüht sich zur Zeit, gemeinsam mit den Justizressorts der anderen Länder und des Bundes, den bundeseinheitlichen Vordruck der Zählkarten zu ändern.

4. Teil: Personalwesen

1. Personalbogen

Wer sich um einen Arbeitsplatz oder Dienstposten in der öffentlichen Verwaltung bemüht, muß zunächst einmal einen Fragebogen ausfüllen. Darin werden eine Reihe von Fragen zur Person des Bewerbers, seinem Familienstand, den Personalien seiner Kinder und Eltern, seiner Ausbildung, seinen abgelegten Prüfungen und nach etwa anhängigen Straf- und Disziplinarverfahren gestellt. Dieser sogenannte Personalbogen ist Grundlage für die Entscheidung über die Einstellung. Kommt es zur Einstellung, wird er zu den Personalakten genommen und dort weitergeführt. Häufig muß auch ein Landesbediensteter einen Personalbogen ausfüllen, wenn er die Dienststelle wechselt. So ist es immer dann, wenn die neue Dienststelle nicht die Hauptpersonalakten führt. Dies ist beispielsweise bei Lehrern der Fall, die an eine andere Schule versetzt werden.

Verschiedene Eingaben waren für mich Anlaß, einer Reihe von Fragen nachzugehen, die die Verwendung dieser Personalbogen aufwirft:

1.1 Inhalt der Personalbogen

Der Arbeitgeber „Öffentliche Verwaltung“ darf ebenso wie jeder private Arbeitgeber vom Bewerber oder Bediensteten nur nach den Grundsätzen Daten erheben, welche die arbeitsrechtliche Rechtsprechung zum Fragerecht des Arbeitgebers entwickelte. Danach entscheidet im Einzelfall eine Interessenabwägung zwischen den Interessen des Arbeitnehmers und dem berechtigten Auskunftsbedürfnis des Arbeitgebers über die Umstände, die für die konkrete Tätigkeit von Bedeutung sind. Daraus ergeben sich für den Inhalt von Personalbogen folgende Forderungen:

- Daten, die weder für die Entscheidung über die Einstellung noch für die Durchführung des Dienst- oder Arbeitsverhältnisses von Bedeutung sind, dürfen in keinem Falle in den Personalbogen aufgenommen werden. Aus diesem Grunde halte ich Fragen nach Name, Beruf und Wohnort der Eltern, wie sie derzeit noch der in der Landesverwaltung verwendete Personalbogen enthält, nicht für zulässig. Bei Minderjährigen reicht aus, wenn nach Name und Anschrift des gesetzlichen Vertreters gefragt wird.
- Der Personalbogen sollte grundsätzlich zwischen den Angaben unterscheiden, die für die Entscheidung über eine Bewerbung erforderlich sind, und solchen, die die öffent-

liche Verwaltung erst nach der Entscheidung über die Einstellung zur Begründung und Durchführung des Dienst- oder Arbeitsverhältnisses benötigt. Es gibt beispielsweise keinen Grund, warum ein Bewerber schon im Bewerbungsverfahren Angaben über Vorname und Geburtstag seiner Kinder machen und seine Bankverbindung nennen soll. Ebenso wenig benötigt man zu diesem Zeitpunkt Angaben über den Zeitpunkt seiner Eheschließung, Scheidung oder des Todes des Ehegatten.

- Führen Beschäftigungsstellen nicht selbst die Hauptpersonalakten, sollten sie mit dem Personalbogen nur die Daten erheben und bei sich aufbewahren, die sie für die Erfüllung ihrer konkreten Aufgaben benötigen. Würden sie alle Angaben abfragen, die im Personalbogen enthalten sind, der sich bei den Hauptpersonalakten befindet, handeln sie dem Grundsatz der Konzentration der Personalakten zuwider. Sie würden Angaben, die durch das Personalaktegeheimnis geschützt sind, bei sich aufbewahren, ohne daß dazu eine sachliche Notwendigkeit besteht. In der Regel wird es ausreichen, wenn die Beschäftigungsstelle Name und Vorname, Geburtsname, Wohnort, Straße und Hausnummer, Amts- und Berufsbezeichnung, Familienstand, ausgeübte Nebentätigkeit und den privaten Telefonanschluß kennt.

Das Innenministerium, mit dem ich wegen des in der Landesverwaltung verwendeten Personalbogens verhandelte, teilte mir mit, es wolle bei der beabsichtigten Überarbeitung dieses Bogens meinen Empfehlungen zum Inhalt weitgehend Rechnung tragen. Es will allerdings an einem einheitlichen Personalbogen festhalten. Dagegen ist dann nichts einzuwenden, wenn im Personalbogen deutlich gemacht wird, welche Angaben der Betroffene im Bewerbungsverfahren, welche er nach der Einstellung und welche er bei Versetzungen und Abordnungen gegenüber der neuen Dienststelle machen muß.

1.2 Rückgabe der Personalbogen

In dem Personalbogen muß der Bewerber um einen Dienstposten oder Arbeitsplatz im öffentlichen Dienst eine ganze Reihe von Angaben machen, die seine persönlichen Lebensumstände betreffen. Hat die Bewerbung keinen Erfolg, stellt sich die Frage, ob dieser Personalbogen nicht im Interesse des Bewerbers wieder zurückzugeben ist. Eine solche Rückgabepflicht sah zwar der vom Bundesminister für Arbeit und Sozialordnung im Jahr 1977 herausgegebene Entwurf eines Arbeitsgesetzbuches — allgemeines Arbeitsvertragsrecht — ausdrücklich vor. Geltendes Recht wurde diese Regelung aber bis jetzt noch nicht. Diese unbefriedigende Rechtslage sollte die öffentlichen Arbeitgeber jedoch nicht davon abhalten, schon jetzt den Personalbogen und auch die übrigen Bewerbungsunterlagen zurückzugeben. Dafür spricht vor allem die Wertentscheidung, die der Gesetzgeber in den Regelungen über die Speicherung von Bewerberdaten in Dateien getroffen hat. Werden nämlich Personaldaten von Bewerbern in Dateien gespeichert, so sind diese Daten nach § 2 Abs. 3 LDStG i.V. mit § 27 Abs. 3 Satz 2 BDSG auf Verlangen des Bewerbers zu löschen, wenn ihre Kenntnis für den Zweck der Speicherung, also für die rechtmäßige Aufgabenerfüllung des potentiellen Arbeitgebers nicht mehr erforderlich ist. Dies ist bei einer Bewerbung der Fall, sobald feststeht, daß sie erfolglos blieb und die Stelle anderweitig besetzt ist.

2. Vertraulichkeit der Personalakten

Während der Dauer eines Dienst- oder Arbeitsverhältnisses entsteht eine große Zahl von Vorgängen, die mit ihm in einem inneren Zusammenhang stehen. Alle diese Vorgänge sind Teile der Personalakten. Sie enthalten folglich im Regelfall zahlreiche sehr sensible Angaben über den Bediensteten und vermitteln ein umfassendes Bild über seinen beruflichen und persönlichen Werdegang. Die Rechtsprechung zog schon vor langem die Konsequenz aus der sich hieraus für den Bediensteten ergebenden Gefährdung und entwickelte den Grundsatz der Vertraulichkeit der Personalakten. Danach sind Personalakten geheimzuhalten. Sie dürfen Dritten grundsätzlich nicht überlassen werden.

Diese Geheimhaltungsverpflichtung ist schon beim Führen von Personalakten zu beachten. Aus diesem Grunde darf man beispielsweise nicht, wie dies bei einer Universität geschah, komplette EDV-Listen, die zur Überprüfung der Versicherungspflicht der Angestellten erstellt wurden und Angaben über zahlreiche Bedienstete enthielten, der Einfachheit halber zu den Personalakten der einzelnen, auf den Listen aufgeführten Bediensteten nehmen. Auf diese Weise erhält nämlich jeder dieser Bediensteten, der in seine Personalakten Einsicht nimmt, Kenntnis von den Daten seiner Kollegen, die dem Personalaktegeheimnis unterliegen.

Der Grundsatz der Vertraulichkeit der Personalakten wirkt sich aber auch im Verkehr mit anderen Behörden aus. Personalaktenführende Behörden dürfen deshalb anderen Behörden stets nur diejenigen Teile der Personalakten überlassen, die diese zur Erfüllung ihrer Aufgabe unbedingt benötigen. Nicht in Einklang mit diesen Grundsätzen steht nach meiner Auffassung eine vom Landesamt für Besoldung und Versorgung geübte Praxis. Diese Behörde fordert beim Ausscheiden eines angestellten Mitarbeiters einer Behörde dessen vollständige Hauptpersonalakte zur Einsicht an. Sie tut dies, um über die Zuerkennung eines Übergangsgeldes nach dem Bundesangestelltentarifvertrag zu entscheiden oder den beruflichen Werdegang des ausgeschiedenen Angestellten während der letzten 15 Jahre für eine etwaige Versorgungsrente zu bescheinigen. Die Personalakten enthalten jedoch in der Regel Unterlagen, zum Beispiel Bewerbungsunterlagen mit Schul- und Ausbildungszeugnissen, Bescheinigungen über die Teilnahme an Fortbildungsveranstaltungen, Auszüge aus Scheidungsurteilen u. ä., die für die Zuerkennung eines Übergangsgeldes und über die Bescheinigung des beruflichen Werdegangs ohne Bedeutung sind. Sie dürfen deshalb auch nicht dem Landesamt für Besoldung und Versorgung überlassen werden. Ich empfahl aus diesem Grund dem Finanzministerium, das Landesamt für Besoldung und Versorgung zu einer Änderung seiner Praxis anzuhalten. Seine Antwort steht noch aus.

3. Bekanntgabe von Personaldaten für Organisationsuntersuchungen

Verschiedentlich wurde ich gefragt, ob und unter welchen Voraussetzungen es zulässig ist, einem mit der Durchführung von Organisationsuntersuchungen beauftragten privaten Unternehmen Personaldaten aus Personaldateien zur Verfügung zu stellen. So wollte beispielsweise eine Stadt den wirtschaftlichen Betrieb ihres Bauhofs überprüfen lassen. In dieser Frage vertrete ich folgende Auffassung:

Personaldaten dürfen nach § 2 Abs. 3 LDSG unter den Voraussetzungen des § 24 Abs. 1 BDSG an Dritte übermittelt werden. Den sich daraus ergebenden Anforderungen wird entsprochen, wenn

- nur die für die Untersuchung unbedingt notwendigen Daten übermittelt werden;
- das Organisationsunternehmen vertraglich verpflichtet wird, die übermittelten und die darüber hinaus bei der Untersuchung erhobenen personenbezogenen Daten nur für die Durchführung der Organisationsuntersuchung zu verwenden, die Daten nicht weiterzugeben und sie zu löschen, sobald sie nicht mehr für die Untersuchung benötigt werden;
- das Organisationsunternehmen sorgfältig ausgewählt wird,
- Kontroll- und Auskunftsrechte vereinbart werden, die es ermöglichen, die Einhaltung der Vereinbarung zu überwachen.

4. Unterrichtung über Nebentätigkeiten

Wegen der aktuellen Situation auf dem Arbeitsmarkt schenkt man der Nebentätigkeit von Angehörigen des öffentlichen Dienstes verstärkt Aufmerksamkeit. In einigen Fällen wollten Gemeinderäte von der Verwaltung Auskunft über Art und Umfang der Nebentätigkeit der Gemeindebediensteten. Aus der Sicht des Datenschutzes ist dazu zu sagen: Ob und welche Informationen der Bürgermeister dem Gemeinderat mitteilen darf und muß, richtet sich nicht nach den Bestimmungen des Landesdatenschutzgesetzes, sondern nach den dafür in § 24 Abs. 3 und 4 der Gemeindeordnung getroffenen Regelungen. Danach kann jeder Gemeinderat an den Bürgermeister schriftlich oder mündlich Anfragen über einzelne Angelegenheiten der Gemeinde und ihrer Verwaltung richten. Der Bürgermeister muß in seiner Antwort dem Gemeinderat das an Informationen über Vorgänge in der Gemeindeverwaltung zugänglich machen, was dieser für die Ausübung seines Mandats wissen muß. Ob und in welchen Fällen danach der Bürgermeister personenbezogene Auskunft über solche Nebentätigkeiten der Gemeindebediensteten geben kann, läßt sich nur aufgrund der Umstände des Einzelfalls entscheiden. Dabei kommt es sicher ebenso auf die Größe der Verwaltung wie auch darauf an, welche Bediensteten von der Anfrage betroffen sind. Im Regelfall dürfte eine personenbezogene Auskunft nicht erforderlich sein. Wird die Auskunft in einer Sitzung des Gemeinderats gegeben, ist zu beachten, daß nach § 35 Abs. 1 der Gemeindeordnung nicht öffentlich verhandelt werden darf und muß, wenn es das öffentliche Wohl oder berechnete Interessen einzelner erfordern. Dies wird in der Regel dann der Fall sein, wenn der Bürgermeister tatsächlich personenbezogene Auskünfte über Art und Umfang der genehmigten Nebentätigkeiten gibt.

5. Bekanntgabe von Personaldaten an Personalräte

Der Personalrat ist bei der Ausübung seiner bedeutungsvollen Aufgabe in starkem Maße darauf angewiesen, daß ihn die Dienststelle über alle wichtigen Angelegenheiten informiert. Insbesondere kann er seine Aufgabe zu überwachen, daß die zu Gunsten der Beschäftigten geltenden Gesetze, Verordnungen, Tarifverträge, Dienstvereinbarungen und Verwaltungsanordnungen eingehalten werden, nur sachgerecht wahrnehmen, wenn er im Besitz der dazu notwendigen Informationen ist. Um dies sicherzustellen, verpflichtet § 68 Abs. 2 des Landespersonalvertretungsgesetzes die Dienststelle ausdrücklich, den Personalrat zur Durchführung seiner Aufgaben rechtzeitig und umfassend zu unterrichten und ihm die dazu erforderlichen Unterlagen vorzulegen. Wie mir eine Reihe von Anfragen zeigen, führte erstaunlicherweise auch hier der Erlaß des Landesdatenschutzgesetzes zu gewissen Unsicher-

heiten. Obwohl dieses Gesetz von vornherein als Auffanggesetz angelegt und in § 30 LDSG ausdrücklich zum Ausdruck gebracht ist, daß besondere Rechtsvorschriften des Bundes oder des Landes den Vorschriften des Landesdatenschutzgesetzes vorgehen, trug man immer wieder an mich die Frage heran, ob eine Weitergabe bestimmter, für die Arbeit des Personalrats notwendigen Informationen nicht gegen das Landesdatenschutzgesetz verstoße. Ich kann dazu nur sagen, daß sich die Frage, welche Information der Personalrat von der Dienststelle erhalten kann, allein nach den Bestimmungen des Landespersonalvertretungsgesetzes beantwortet und daß deshalb das Landesdatenschutzgesetz zu keiner Änderung der Rechtslage führte.

6. Automatisiertes Verfahren zur Unterstützung der Personalverwaltung

Bereits in meinem 1. Tätigkeitsbericht befaßte ich mich mit den „Automatisierten Verfahren zur Unterstützung der personalverwaltenden Stellen der Oberfinanzdirektion (UPS)“. Die Oberfinanzdirektion Freiburg setzt es derzeit im Probetrieb ein. Um mich über den aktuellen Stand und die dabei auftretenden datenschutzrechtlichen Probleme zu unterrichten, unterzog ich dieses Verfahren einer weiteren Prüfung. Dabei zeigte sich eine Reihe von Mängeln, die ich beanstanden mußte und die vor einem endgültigen Einsatz dieses Verfahrens unbedingt behoben werden müssen:

6.1 Keine Gewähr für die Vollständigkeit von Auswertungen

Eine der Aufgaben von UPS soll sein, Personalentscheidungen vorzubereiten. Insbesondere soll damit jeweils der Kreis der Bediensteten, die für bestimmte Personalentscheidungen in Betracht kommen, schnell und zuverlässig ermittelt werden. Die Überprüfung ergab, daß UPS in seinem derzeitigen Stand diese Aufgabe nicht zuverlässig erfüllen kann:

- Das Verfahren prüft derzeit nicht, ob alle Grunddaten eines Bediensteten vollständig eingegeben sind. Zwingend vorgeschrieben ist lediglich die Eingabe der Personalnummer. Weitere Daten des Bediensteten brauchen nicht gespeichert werden. Dies kann zur Folge haben, daß ein Bediensteter allein deshalb nicht in die engere Auswahl für eine Personalentscheidung gelangt, weil über ihn nicht alle die Daten, die für die Auswahl maßgebend sind, gespeichert sind. Um dies zu vermeiden, muß festgelegt werden, welche Daten jeweils unbedingt eingegeben werden müssen (Muß-Datenfelder) und welche nur eingegeben werden können (Kann-Datenfelder). Durch automatisierte Vollständigkeitsprüfungen muß UPS verhindern, daß nur in einem Teil der Muß-Felder Daten eingegeben werden können.
- Es fehlen Festlegungen darüber, welche einzelnen Merkmale in welcher Form zu einer Datenart eingegeben, gespeichert und abgefragt werden können. So ist es z. B. dem einzelnen Sachbearbeiter überlassen, ob er die Besoldungsgruppe A 12 mit oder ohne Zwischenraum zwischen „A“ und „12“ eingeben will. Das Resultat ist, daß bei einer Abfrage, die nur in einer der beiden geschilderten Eingabeweisen erfolgt, die Beamten, deren Besoldungsgruppe A 12 auf die andere Weise eingegeben wurde, im Ausdruck nicht aufgeführt werden. Sie werden damit aus dem Kreis der für die Personalentscheidung in Frage kommenden Bediensteten ausgeschieden. Nicht festgelegt sind auch die

Abkürzungen einzugebender Daten. Möglich ist zum Beispiel, den Familienstand „verheiratet“ mit „verh“, „vrh“, „vhei“ usw. anzugeben. Im Rahmen der vorgesehenen Feldlänge können sogar völlig beliebige Inhalte eingegeben werden. Je nach der bei der Abfrage verwendeten Abkürzung werden auch hier nur die Daten der Bediensteten ausgedruckt, bei denen die entsprechende Abkürzung eingegeben wurde.

- Schließlich ist die Gewähr für eine zuverlässige Erfüllung der Aufgaben von UPS auch deshalb nicht gegeben, weil die Richtigkeit der eingegebenen Daten nicht im erforderlichen Maß überprüft wird. Die bis jetzt durchgeführte automatisierte Prüfung reicht bei weitem nicht aus.

6.2 Sperrung und Löschung

UPS kann gespeicherte Daten zur Zeit nicht sperren. Auch bestehen keine konkreten Vorstellungen, ob und wann Daten zu löschen sind. Es werden zwar 124 von 141 gespeicherten Daten in eine sogenannte Historie überführt. Auf die darin enthaltenen Daten kann aber nach wie vor wie auf die aktuell gespeicherten Daten zurückgegriffen werden. Von einer Löschung kann deshalb keine Rede sein. Dies aber verlangt § 27 Abs. 3 BDSG, sofern die dort näher festgelegten Voraussetzungen vorliegen.

7. Eingaben

Weil im Personalwesen viele persönliche Daten verarbeitet werden, nimmt nicht wunder, daß manch ein Bediensteter Grund zur Klage hat.

- Welcher glücklich verheiratete Familienvater wäre nicht überrascht, wenn ihm ein Brief seiner Besoldungsbehörde mit der Mitteilung ins Haus flattert, er sei geschieden und erhalte deshalb ab nächsten Monat vorläufig einen geringeren Ortszuschlag. Genau dies aber war bei einem Beamten geschehen. Das Landesamt für Besoldung und Versorgung hatte versehentlich das Scheidungsurteil eines namensgleichen Kollegen zu seinem Besoldungsakt genommen. Das Resultat war das erwähnte Schreiben. Gleichzeitig speicherte das Amt über den Beamten in der automatisierten Besoldungsdatei die unrichtigen Merkmale „geschieden“ und „ohne Kind“. Außerdem wurde der Ortszuschlag tatsächlich gekürzt. Erst nach zweimaligem Anlauf erreichte der Beamte, daß das Landesamt für Besoldung und Versorgung die unrichtigen Daten berichtigte und ihm sein Gehalt wieder in der früheren Höhe ausbezahlte. Es entschuldigte sich für seinen Fehler bei dem Beamten. Das Finanzministerium, dem gegenüber ich den Vorgang beanstandete, bat das Landesamt für Besoldung und Versorgung, darum besorgt zu sein, daß die für das Berechnungsverfahren maßgebende Arbeitsanleitung künftig beachtet wird.
- Ein Erfassungsfehler lag folgendem zunächst sehr undurchsichtigen Fall einer Universitätsangestellten zugrunde: Die Universitätskasse hatte schon bei Aufnahme ihres Arbeitsverhältnisses neben dem richtigen Geburtstag ihres schon über 27 Jahre alten Sohnes fälschlicherweise eine Kennziffer in den Computer eingegeben, nach der ein Kind unter 27 Jahren bei der Berechnung des Ortszuschlags zu berücksichtigen war. Da der Sohn schon über 27 Jahre alt, aber noch ausnahmsweise im Ortszuschlag zu berücksichtigen war, erkannte die Universität die unrichtige Speicherung erst längere Zeit später. Finanzielle

Nachteile entstanden dadurch glücklicherweise nicht. Wenig bürgerfreundlich war freilich das Verhalten der Universität der Angestellten gegenüber. Anstatt sie umfassend über den Sachverhalt zu informieren, schickte ihr die Universität ohne weitere Erklärungen mehrmals Berichtigungen der Meldungen zur Sozialversicherung und teilte auf Anfrage lediglich mit, es handle sich um einen Programmierfehler. Daß eine solche Vorgehensweise zu einer erheblichen Verunsicherung bei den Betroffenen führen kann, kam der Universität offenbar nicht in den Sinn.

- Nicht gerade begeistert war ein Lehrer, als ihm von privater Seite ohne Absenderangabe durch die Post ein Brief zugeschickt wurde mit seiner Lohnsteuerbescheinigung für das Kalenderjahr 1980. Solche Lohnsteuerbescheinigungen stellt das Landesamt für Besoldung und Versorgung aus; sie enthalten dieselben Daten wie die Lohnsteuerkarte. Der anonyme Zusender konnte also aus ihr neben Name, Vorname, Geburtsdatum und Adresse des Lehrers Angaben zum Beispiel über dessen Steuerklasse, Bekenntnis, Bruttoarbeitslohn usw. ersehen. Bei der Überprüfung konnte ich feststellen, daß es sich bei der übersandten Lohnsteuerbescheinigung um eine Ausfertigung handelte, die für die vom Landesamt für Besoldung und Versorgung geführten Besoldungsakten bestimmt ist. Nicht aufzuklären war, auf welche Weise die Bescheinigung in den allgemeinen Postverkehr gelangte, an wen sie ging und wer sie schließlich dem Lehrer zuleitete. Hierauf kam es letztlich für die datenschutzrechtliche Würdigung auch nicht an. Entscheidend ist, daß die Lohnsteuerbescheinigung aus dem Verfügungsbereich des Landesamtes für Besoldung und Versorgung in die Hände Dritter gelangte, die davon keine Kenntnis nehmen dürfen. Darin lag ein Verstoß gegen den Grundsatz der Vertraulichkeit der Personalakten, gegen § 11 LDSG sowie die Geheimhaltungspflicht des Arbeitgebers nach dem Einkommenssteuergesetz. Ich beanstandete deshalb diesen Vorfall beim Finanzministerium.

5. Teil: Statistik

1. Allgemeines zum Datenschutz beim Statistischen Landesamt

Staat und Gesellschaft benötigen in großem Umfang Informationen als Grundlage für Entscheidungen und Planungen. Diese Informationen gewinnen sie zu einem wesentlichen Teil aus amtlichen Statistiken. In Baden-Württemberg ist es in erster Linie Aufgabe des Statistischen Landesamts, die dazu erforderlichen Erhebungen durchzuführen und das gewonnene Datenmaterial auszuwerten. Da dabei in großem Umfang personenbezogene Daten verarbeitet werden müssen, kommt dem Datenschutz bei der Arbeit dieser Behörde ganz entscheidende Bedeutung zu. Bei einer an Ort und Stelle vorgenommenen Überprüfung einzelner Bereiche wurde deutlich, daß sich das Statistische Landesamt dieser Tatsache durchaus bewußt ist und dem Datenschutz einen wichtigen Stellenwert beimißt. Weniger erfreulich war allerdings, daß das Amt glaubte, bei dem angemeldeten Kontrollbesuch Datensicherungsmaßnahmen vorspiegeln zu müssen, die es so in der Alltagspraxis nicht anwendet. Es hatte die Bediensteten der Registratur nämlich angewiesen, während des Kontrollbesuchs die Akten-schränke, in denen die Erhebungsunterlagen aufbewahrt werden,

abzuschließen. Diese Maßnahme ist sonst nicht üblich. Ich meine, das Statistische Landesamt sollte eigentlich solche Methoden nicht nötig haben.

Neben einigen Mängeln bei einzelnen statistischen Erhebungen zeigten sich folgende Probleme allgemeiner Art, die noch nicht befriedigend gelöst sind:

- Nach § 11 Abs. 7 des Bundesstatistikgesetzes sollen Name und Anschriften der Auskunftspflichtigen von den übrigen Angaben getrennt und unter besonderem Verschuß gehalten werden. Dieser Forderung trägt das Statistische Landesamt bisher nur in vollem Umfang bei der automatisierten Datenverarbeitung Rechnung, nicht aber bei der Aufbewahrung von Erhebungsbogen. Bei zahlreichen statistischen Erhebungen sind neben sonstigen Angaben auch Namen und Anschrift auf dem Erhebungsbogen einzutragen. So werden z. B. bei der Mikrozensus-Erhebung umfangreiche Angaben über die beruflichen, wirtschaftlichen und sozialen Verhältnisse des Auskunftspflichtigen zusammen mit dessen Namen und Anschrift erhoben. Diese Erhebungsbogen bewahrt das Statistische Landesamt nach der Auswertung gesammelt auf, ohne daß es eine Trennung des Namens und der Anschrift von den sonstigen Angaben vornimmt. Das Statistische Landesamt erkannte die Berechtigung meiner Forderung im Grundsatz an. Es sagte mir zu, sich in Abstimmung mit den Statistischen Ämtern des Bundes und der übrigen Länder um eine Lösung des Problems zu bemühen.
- Auch eine weitere Forderung des Bundesstatistikgesetzes wird noch nicht ausreichend beachtet. § 11 Abs. 7 dieses Gesetzes verlangt, daß die zur Identifizierung des Auskunftspflichtigen sowie sonstiger Betroffener dienenden Daten, insbesondere Namen und Anschriften zu löschen sind, wenn sie für die statistische Arbeit nicht mehr benötigt werden. Bisher orientiert sich das Statistische Landesamt bei der Vernichtung von mit Name und Anschrift versehenen Erhebungsbogen zum Teil an bundeseinheitlichen „Mindestaufbewahrungsfristen“, zum Teil beseitigt es Unterlagen erst dann, wenn die vorhandene Lagerkapazität nicht mehr ausreicht. Dies widerspricht § 11 Abs. 7 des Bundesstatistikgesetzes. Ich forderte das Amt deshalb auf, einen Katalog zu erstellen, in dem für jede einzelne Statistik festgelegt wird, wann Unterlagen auszusondern und zu vernichten sind. Das Statistische Landesamt machte dazu geltend, hierzu sei ein bundeseinheitliches Vorgehen unbedingt notwendig; es werde sich bemühen, eine solche Regelung herbeizuführen.

2. Statistikgeheimnis

Niemand läßt sich gern zur Erstellung einer amtlichen Statistik ausfragen. Wird man dazu durch Gesetz verpflichtet, will man wenigstens Gewißheit haben, daß die Angaben nur zu dem bei der Befragung angegebenen Zweck verwendet werden. Nur dann kann man auch erwarten, daß die Angaben richtig und damit auch aussagekräftig sind. Um dies sicherzustellen, wurde das Statistikgeheimnis geschaffen. Die sich daraus ergebende Geheimhaltungspflicht entfällt nur, wenn ein Gesetz dies vorsieht oder der Betroffene ausdrücklich in die Weitergabe oder Veröffentlichung seiner Angaben einwilligt. Übermittelt werden dürfen selbstverständlich auch zusammengefaßte Angaben, bei denen sich die darin enthaltenen Angaben nicht mehr bestimmten Personen zuordnen lassen, und Einzelangaben, die so anonymisiert sind, daß die Person, auf die sie sich beziehen, nicht identifiziert werden kann. Wann dies

der Fall ist, ist nicht immer einfach zu beurteilen. So bat zum Beispiel jüngst ein privates Forschungsinstitut das Statistische Landesamt um Mitteilung, wieviel Kinder jährlich in einem Zeitraum von 15 Jahren in den einzelnen Gemeinden zweier Landkreise tot oder mit Mißbildungen geboren wurden und wieviel Personen an Leukämie verstorben sind. Das Institut wollte u. a. auf Grund dieser Zahlen zu Aussagen darüber gelangen, ob zwischen dem Betrieb von Kernkraftwerken und solchen gesundheitlichen Schäden ein Zusammenhang besteht. Das Statistische Landesamt entsprach dieser Bitte zu Recht nicht. Es erhält zwar auf Grund des Gesetzes über die Statistik der Bevölkerungsbewegung und Fortschreibung des Bevölkerungsstandes über jede Lebens- oder Totgeburt sowie über jeden Sterbefall bestimmte Angaben zur Erstellung einer Bundesstatistik. Bei Geburten erfährt es zum Beispiel auch von erkennbaren Fehlbildungen und der Wohngemeinde der Eltern. Das Statistikgeheimnis stand jedoch der Weitergabe der Zahlen an das Institut entgegen, weil es bei der gewünschten gemeindebezogenen Auswertung nur ein oder zwei Fälle pro Jahr und Gemeinde gab. Hätte man sie genannt, wäre die Anonymität der betroffenen Personen nicht mehr gewahrt geblieben.

3. Einzelne Statistiken

3.1 Volkszählung 1983

In der Bundesrepublik findet im April 1983 erstmals seit 1970 erneut eine Volks- und Berufszählung statt. Sie ist verbunden mit gebäude- und wohnungsstatistischen Fragen und einer Arbeitsstättenzählung. Bei der Volkszählung wird eine Vielzahl detaillierter personenbezogener Angaben erfragt, u. a. Name, Anschrift, Geschlecht, Geburtstag, Familienstand, Zugehörigkeit oder Nichtzugehörigkeit zu einer Religionsgesellschaft, Staatsangehörigkeit, erlernter Beruf und Schulabschluß. Die gesetzgeberischen und praktischen Vorarbeiten für diese Zählung laufen seit Jahren. Das Finanzministerium und das Statistische Landesamt weisen ihr eine so überragende Bedeutung zu, daß sie glaubten, mir Ratschläge darüber geben zu müssen, wie ich bei einer öffentlichen Darstellung von Fragen des Datenschutzes bei der Volkszählung zu verfahren hätte. Im einzelnen stellten sich mir bisher folgende Probleme:

- Fast alle Stadtkreise in Baden-Württemberg versandten Ende Februar/Anfang März 1982 auf Veranlassung des Statistischen Landesamts Erhebungsbogen für eine Testbefragung für die Volks- und Berufszählung 1983. Die Volkszählung 1983 will man u. a. auch dazu benutzen, die Melderegister entsprechend den Anforderungen des neuen Melderechts zu berichtigen. Hierzu sind Fragen nach der Hauptwohnung und Nebenwohnung erforderlich. Die Testbefragung diente dazu, die zweckmäßigste Formulierung der Fragen zu erproben. Das Statistische Landesamt hatte zu diesem Zweck schon Anfang Februar 1982 mit den Städten verschiedene Schulungsveranstaltungen durchgeführt. Dabei übergab es den Städten auch ein Musteranschreiben an die zu befragenden Haushalte. Die Städte versandten diese Anschreiben im Vertrauen auf die Ordnungsgemäßheit des Verfahrens zusammen mit den Erhebungsbogen unter ihrem Namen. Die ausgefüllten Erhebungsbogen leiteten sie an das Statistische Landesamt weiter, das sie auswertete und später vernichtete. Weder das Anschreiben an die Haushalte noch die Erhebungsbogen enthielten, wie ich zu meiner Überraschung feststellte, einen Hinweis darauf, daß die

Angaben auf freiwilliger Grundlage erfolgen. Ein solcher Hinweis hätte aber nach § 6 Abs. 3 Nr. 2 des Bundesstatistikgesetzes sowie nach § 9 Abs. 2 des Landesdatenschutzgesetzes gemacht werden müssen, um auch dem über die Rechtslage nicht unterrichteten Bürger die Möglichkeit zu geben, frei darüber zu entscheiden, ob er den Erhebungsbogen ausfüllen will. Dieses Vorgehen wurde von mir beanstandet. Das Finanzministerium gab mir zwar in der Sache recht und wies das Statistische Landesamt an, bei ähnlichen Erhebungen einen ausdrücklichen Hinweis auf die Freiwilligkeit der Beantwortung aufzunehmen. Im gleichen Atemzug fühlte es sich aber wieder einmal bemüht, mir die Zuständigkeit zur Erteilung der Beanstandung zu bestreiten.

- Im Oktober 1982 begann die Erhebung der gebäude- und wohnungsstatistischen Fragen bei solchen Eigentümern, die nicht selbst in ihren Gebäuden wohnen. Das Volkszählungsgesetz läßt diese Gebäudevorerhebungen zu, da die Zähler bei der „eigentlichen“ Zählung im April 1983 die Eigentümer in diesen Fällen in ihren Gebäuden nicht antreffen. Die Angaben sämtlicher Gebäudeeigentümer sollen aber zu diesem Zeitpunkt vorliegen. Für diese Gebäudevorerhebung übermittelten die Gebäudebrandversicherungsanstalten aus ihren Dateien die Objekt- und Eigentümeranschriften. Diese Übermittlung war nach § 10 LDSG zulässig. Das Statistische Landesamt benötigte die Anschriften, um die Erhebung für die Gebäudevorerhebung mit Namen und Anschrift der Eigentümer versehen zu können. § 8 des Volkszählungsgesetzes verpflichtet zwar die für die Grundsteuer zuständigen Stellen der Gemeinden, den Erhebungsstellen auf Anforderung diese Angaben zu nennen. Die Entstehungsgeschichte und der Wortlaut des Volkszählungsgesetzes lassen jedoch den Schluß zu, daß man dadurch nicht die Übermittlung der erforderlichen Daten durch andere Stellen ausschließen wollte.

3.2 Hochschulstatistik

Die auf Grund des Hochschulstatistikgesetzes geführten Statistiken werfen immer wieder Fragen und Probleme auf.

- Das Statistische Landesamt befragt jährlich auf Grund des Hochschulstatistikgesetzes die Schüler der Gymnasien, die die Schule nach erfolgreichem Besuch der 12. oder 13. Jahrgangsstufe verlassen, nach ihren Studien- und Berufswünschen für Zwecke einer Hochschulzugangsstatistik. Diese Statistiken sollen neben einer Übersicht über die Zahl der Studienanfänger in den nächsten Semestern auch detaillierte Angaben über die Studienwünsche nach Studienfächern und Hochschulen erbringen. Obwohl mir das Statistische Landesamt im Jahr 1980 schriftlich angekündigt hatte, daß es ab 1981 auf den Erhebungsbogen nicht nach Name und Vorname der Schüler fragt, sahen auch die Erhebungsbogen für die Befragung 1982 diese Fragen noch vor. Im Begleitschreiben an die Schulen und Schüler teilte das Statistische Landesamt dazu noch mit, die Angabe des Namens auf den Bogen sei nicht erforderlich, sie erleichtere aber den Lehrern die Rücklaufkontrolle. Trotz dieses Hinweises wurden in großem Umfang die Namen auf den Erhebungsbogen eingetragen, die die Schulen dem Statistischen Landesamt wieder zuleiteten.

Diese Erhebungspraxis verstößt gegen § 7 Nr. 1 des Hochschulstatistikgesetzes. Diese Vorschrift sieht die Erhebung von „Angaben zur Person“ vor. Hierunter fallen zwar im allgemeinen auch der Name und Vorname. Diese Angaben sind aber für die konkrete Statistik nicht erforderlich. Weder ist eine Verknüpfung der mit ihr gewonnenen Daten mit anderen Erhebungseinheiten vorgesehen, noch wird der Name zu Vollzähligkeitskontrollen benötigt. Diese können auch mit Hilfe von Namenslisten durchgeführt werden, die die Schulen selbst führen. Es wäre mit dem Grundsatz der Verhältnismäßigkeit nicht zu vereinbaren, wenn die Schulen gleichwohl dem Statistischen Landesamt die Namen der Schüler übermitteln. Genau dieser Erfolg trat aber dadurch ein, daß die vom Statistischen Landesamt ausgegebenen Erhebungs- und Mantelbogen an die Schulen den Eintrag von Name und Vorname der Schüler vorsahen. Auf meine Beanstandung nach § 18 Abs. 1 LDSG vertrat das Finanzministerium demgegenüber die Auffassung, die Erhebung von Name und Vorname der Schüler sei durch das Hochschulstatistikgesetz gedeckt. Auch sah es in dem beanstandeten Vorgehen keinen Widerspruch zu der vom Statistischen Landesamt gemachten Zusage. Diese habe eine Erhebung von Name und Vorname auf freiwilliger Grundlage nicht ausgeschlossen. Durch den Hinweis an Schulen und Schüler sei die Freiwilligkeit für alle Beteiligten klar gewesen. Dieser Beurteilung kann ich mich nicht anschließen. Erhebungsbogen, Mantelbogen und Rundschreiben an die Schüler erwecken den gegenteiligen Eindruck. In dem Rundschreiben ist ausgeführt, der Erhebungsbogen enthalte nur solche Fragen, die für die Gewinnung der benötigten Unterlagen unbedingt erforderlich seien. Darüber hinaus weist es darauf hin, daß der Schüler zur Beantwortung der Fragen im Erhebungsbogen verpflichtet sei. Der Erhebungsbogen selbst enthält ebenfalls den Hinweis auf die Auskunftspflicht. Wenn es dennoch am Ende des Rundschreibens an die Schüler heißt, daß der Bogen auch ohne Namensangabe abgegeben werden könne, entsteht für die betroffenen Schüler ein widersprüchlicher Eindruck. Eine derartig mißverständliche Information ist kein Hinweis auf die Freiwilligkeit nach § 9 Abs. 2 LDSG. Trotz seiner gegenteiligen Auffassung beauftragte das Finanzministerium aber das Statistische Landesamt, nochmals mit den Statistischen Ämtern der Länder und des Bundes die Frage zu erörtern, ob auch Name und Vorname des Schülers erhoben werden sollen.

- Ein Beispiel dafür, wie Behörden bei statistischen Erhebungen nicht vorgehen sollten, erfuhr ich aus der Eingabe eines Studenten. Dieser hatte sich geweigert, für die Hochschulstatistik eine Reihe von Angaben zu machen, weil er bei diesen Fragen keinen unmittelbaren Zusammenhang mit dem Hochschulbesuch sah und deshalb der Auffassung war, damit würde unangemessen in seine Persönlichkeitssphäre eingegriffen. Anstatt ihn über Sinn und Zweck der Hochschulstatistiken zu unterrichten und um Verständnis für die im Hochschulstatistikgesetz getroffenen Regelungen zu werben, wies ihn das Statistische Landesamt daraufhin nur auf seine bestehende Auskunftspflicht hin. Zugleich drohte es ihm an, bei nicht fristgemäßer Beantwortung ein Bußgeldverfahren einzuleiten. In diesem Fall werde es auch seinen Dienstvorgesetzten informieren, daß er entweder nicht in der Lage sei, die Bestimmungen eines Gesetzes zu beurteilen oder nicht willens, sie einzuhalten. Mit einer solchen Vorgehensweise wird ein unzulässiger Druck auf

den Auskunftspflichtigen ausgeübt. Das Bundesstatistikgesetz sieht in Fällen der Auskunftsverweigerung lediglich die Durchführung eines Bußgeldverfahrens vor. Daraus folgt, daß andere Mittel oder Sanktionen ausgeschlossen sind. Ich teilte dies dem Statistischen Landesamt mit und gehe davon aus, daß es sich in solchen Fällen künftig darauf beschränkt, auf die mögliche Durchführung eines Bußgeldverfahrens hinzuweisen.

6. Teil: Kommunalwesen

Die Kommunalverwaltung arbeitet wegen ihrer umfassenden Aufgaben mit einer Fülle von Rechtsvorschriften unterschiedlichster Art. Darunter befindet sich auch eine ganze Reihe von Einzelbestimmungen, die Regelungen über den Umgang mit personenbezogenen Daten enthalten. Ihre Anwendung wirft ebenso wie das Landesdatenschutzgesetz Probleme auf.

1. Kommunalwahlrecht

Diese Aussage gilt in besonderem Maße für § 15 a der Kommunalwahlordnung (KomWO). Wiederholt sprachen mich Bürger darauf an; auch die Presse befaßte sich mehrfach damit. § 15 a KomWO regelt zum einen das Anfertigen von Auszügen oder Abschriften der Wählerverzeichnisse zu Wahlzwecken. Es ist während der Auslegungsfrist erlaubt, soweit dadurch die Wahlvorbereitungen nicht behindert werden. Auch dürfen die Auszüge und Abschriften nur für Zwecke der Wahl verwendet und Dritten nicht zugänglich gemacht werden. Zum andern regelt § 15 a KomWO das Erteilen von Auskünften über Einträge in den Wählerverzeichnissen und über Unterschriften für Wahlvorschläge. Solche Auskünfte können nur Behörden, Gerichte und sonstige amtlichen Stellen im Zusammenhang mit der Wahl erhalten.

Die erheblichen Schwierigkeiten der Praxis bei der Auslegung und Anwendung dieser Vorschrift sind vor allem darauf zurückzuführen, daß ihr Wortlaut viele Fragen offenläßt. Besonders deutlich wird dies in folgenden Fällen:

- Da ist zunächst die Frage des Anwendungsbereichs des § 15 a KomWO. Unklar ist, ob Unterschriften für Bürgerbegehren ebenso geschützt sind wie Unterschriften für einen Wahlvorschlag. Dagegen spricht rein formal, daß § 15 a KomWO im Abschnitt „Vorbereitung der Wahl und Wahlorgane“ steht und Bürgerbegehren und Bürgerentscheid keine „Wahlen“ sind. Auch fehlt im Abschnitt „Anhörung der Bürger, Bürgerentscheid und Bürgerbegehren“ ein Verweis auf § 15 a KomWO. Es heißt dort lediglich: „Auf die Durchführung des Bürgerentscheids finden die Bestimmungen für die Wahl des Bürgermeisters entsprechende Anwendung“. § 15 a KomWO ist damit jedoch nicht — zumindest nicht in vollem Umfang — einbezogen, weil bei Bürgermeisterwahlen keine Unterschriften für Wahlvorschläge beizubringen sind. Für eine Anwendung des § 15 a KomWO auch auf Unterschriftslisten für ein Bürgerbegehren spricht jedoch, daß die Vorschrift den Schutz des Wahlgeheimnisses bezweckt. Dieses erstreckt sich nach ständiger höchsterichterlicher Rechtsprechung auch auf die Wahlvorbereitung und die Behandlung von Unterschriftslisten. Sieht man diesen Zusammenhang, so kann man Unterschriftslisten für ein Bür-

gerbegehren nicht anders behandeln als Unterschriftslisten für einen Wahlvorschlag. Eine Klarstellung des § 15 a KomWO in diesem Sinne wäre jedoch zu begrüßen.

- Eine weitere Frage ist, ob § 15 a KomWO über seinen Wortlaut hinaus nicht nur das Weitergeben von Daten der Unterschriftslisten an Dritte verbietet, sondern auch jede über die Nachprüfung der Unterschriftsliste hinausgehende Nutzung der Daten durch die Behörde, bei der die Unterschriftsliste eingereicht werden muß. Ein Beispiel aus der Praxis soll zeigen, worum es geht: Nach der Abstimmung über einen Bürgerentscheid wird der Verdacht laut, das Bürgermeisteramt habe nahezu ausschließlich Unterzeichner des Bürgerbegehrens zum Wahldienst herangezogen und deren Namen den Unterschriftslisten für das Bürgerbegehren entnommen. Hier stellt sich die Frage, ob das Bürgermeisteramt die Unterschriftslisten in dieser Weise auswerten durfte. Gegen die Einbeziehung solcher Fälle spricht der bereits oben erwähnte Sinn und Zweck dieser Vorschrift und der Zusammenhang mit dem Wahlgeheimnis, das sich auch auf die Behandlung von Unterschriftslisten erstreckt. Allerdings ist das Wahlgeheimnis hier notwendigerweise eingeschränkt: Der Unterzeichner eines Bürgerbegehrens muß sich gegenüber der Gemeinde offenbaren. Zweifelsfrei ist jedoch das Wahlgeheimnis auch hier im Rahmen des nach der Natur der Sache Möglichen zu wahren. So geht die Literatur überwiegend davon aus, daß Unterschriftslisten nicht für andere Zwecke als solche der Überprüfung der Wahlvorschläge verwendet werden dürfen. Für den geschilderten Fall folgt daraus, daß das Bürgermeisteramt die Unterschriftslisten nur heranziehen dürfte, um festzustellen, ob das in der Gemeindeordnung festgelegte Quorum für die Durchführung des Bürgerentscheids erreicht ist. Jede weitere Nutzung ist untersagt. Für die Praxis wäre jedoch gut, wenn die Kommunalwahlordnung hierüber eine ausdrückliche Regelung enthielte.
- Ferner stellt sich die Frage, inwieweit man nach einer Wahl in das Wählerverzeichnis einsehen kann. Auch hierfür ein praktisches Beispiel. Der wiedergewählte Bürgermeister einer kleineren Gemeinde nahm wenige Tage nach der Wahl Einsicht in das Wählerverzeichnis, um sich über das Wahlverhalten zu unterrichten. War dies zulässig? Vorfrage ist auch hier, ob § 15 a KomWO überhaupt anwendbar ist. Denn er steht — wie bereits erwähnt — im Abschnitt „Vorbereitung der Wahl“. Dafür sprechen allerdings der Wortlaut der Bestimmung sowie Sinn und Zweck der Regelung. Auch gilt die entsprechende Regelung in der Bundeswahlordnung ebenso für die Zeit nach der Wahl. Geht man hiervon aus, steht man wiederum vor dem Problem, ob § 15 a KomWO die verwaltungsinterne Nutzung des Wählerverzeichnisses verbietet oder jedenfalls nur bestimmten Personen für bestimmte, im engeren Sinn im Zusammenhang mit der Wahl stehende Zwecke, zum Beispiel zur Wahlprüfung, gestattet. Für eine solch enge Auslegung läßt sich wiederum der Grundsatz der geheimen Wahl ins Feld führen, der sich nach Meinung der Literatur auch auf Vermerke über die Teilnahme an einer Wahl in den Wählerverzeichnissen bezieht. Doch selbst wenn man dies bejaht, stellt sich immer noch die Frage, ob ein wiedergewählter Bürgermeister, der als Bewerber kraft Gesetzes nicht dem Gemeindewahlausschuß angehören darf, in seiner Eigenschaft als Leiter der Gemeindeverwaltung in das Wählerverzeichnis Einsicht nehmen und damit Kenntnis über die Teilnahme einzelner Bürger an der Wahl erhalten darf. Ich will diese Frage hier nicht beantworten. Mir geht es nur darum aufzuzeigen, wo in der Praxis

Probleme liegen. Ihre Klärung in der Kommunalwahlordnung wäre sicher hilfreich.

Schon aus diesen Gründen sollte § 15 a KomWO geändert werden. Erforderlich ist dies aber auch, weil er zum Teil von datenschutzrechtlichen Vorschriften des Melderechts abweicht, ohne daß es dafür einen überzeugenden Grund gibt:

- So ist es nach § 15 a KomWO zulässig, daß Auszüge und Abschriften der Wählerverzeichnisse die Geburtstage der Wahlberechtigten enthalten. Demgegenüber bestimmt § 22 des Melderechtsrahmengesetzes, der Eingang in das neue Landesmeldegesetz finden wird, daß die Meldebehörden den Parteien und Wählergruppen im Zusammenhang mit Wahlen die Geburtstage der Wahlberechtigten nicht mitteilen dürfen. Man sollte § 15 a KomWO an die datenschutzfreundlichere Regelung anpassen.
- Gewisse Friktionen zwischen Kommunalwahlrecht und Melde-recht gibt es noch in einem anderen Punkt. Nach § 15 a KomWO darf während der Auflegungsfrist jedermann Auszüge und Abschriften des Wählerverzeichnisses zu Wahlzwecken fertigen. Demgegenüber dürfen die Meldebehörden nach § 22 des Melderechtsrahmengesetzes und der entsprechenden Vorschrift des künftigen Landesmeldegesetzes nur Parteien und Wählergruppen im Zusammenhang mit Wahlen Auskunft aus dem Melderegister erteilen. Der Empfängerkreis ist also unterschiedlich weit gezogen: im einen Fall jedermann, im anderen Fall nur Parteien und Wählergruppen. Auch für diese Differenzierung sehe ich heute keine überzeugende Begründung mehr. Natürlich verkenne ich nicht, daß sich die eine Regelung auf das Melderegister bezieht, die andere auf das Wählerverzeichnis, das lediglich auf der Grundlage des Melderegisters erstellt wird. Auch weiß ich wohl, daß der Zweck beider Vorschriften nicht identisch ist. Im Wahlrecht steht die öffentliche Kontrolle der Wahl im Vordergrund, während die Regelung im Melderecht den Interessen der Parteien und Wählergruppen an Stimmenwerbung dient. Darüber sollte man eines nicht übersehen: Ein gewitzter Auskunftssuchender kann während der Auflegungsfrist des Wählerverzeichnisses die Schranken, die das Melde-recht setzt, ohne weiteres umgehen. Er kann in dieser Zeit zu vollständigen Listen aller Wahlberechtigten kommen, ohne daß eine wirkliche Kontrolle des Verwendungszwecks gewährleistet wäre. Dies läßt sich mit dem Erfordernis einer demokratischen Kontrolle der Wahlvorbereitungen nicht ausreichend rechtfertigen. Sie ist auch möglich, wenn nicht mehr jedermann Abschriften der Wählerverzeichnisse verlangen kann. Das Einsichtsrecht der Wahlberechtigten in die öffentlich ausgelegten Wählerverzeichnisse genügt für diesen Zweck völlig. Auch sollte man nicht außer acht lassen, daß sogar am Sinn der öffentlichen Auslegung von Wählerverzeichnissen zunehmend, und keineswegs nur von Seiten des Datenschutzes, Zweifel ge-äußert werden. Diese Kritik muß jedoch erst recht der weit-gefaßten Regelung über das Ausfertigen von Abschriften der Wählerverzeichnisse gelten. Würde man einmal untersuchen, weshalb solche Abschriften verlangt werden, würde man sicher häufig feststellen, daß es dem Antragsteller nicht um die Kon-trolle der Wahlvorbereitungen, sondern um die Wahlwerbung oder um ganz andere Zwecke geht. Hierfür setzen die Daten-schutzvorschriften außerhalb des Kommunalwahlrechts die richtigen Grenzen.

Ich teilte meine Änderungsvorschläge zu § 15 a KomWO dem In-nenministerium mit. Es sagte zu, sie bei der beabsichtigten Über-

arbeitung der Kommunalwahlordnung zu berücksichtigen oder — wie im letzten Punkt — zumindest zu bedenken.

2. Meldewesen

Eine Stadtverwaltung holte meinen Rat ein, weil sich bei ihr ein Bürger wegen folgenden Sachverhalts beschwert hatte: Bei der Anmeldung eines Adoptivkindes trug das Einwohnermeldeamt auf Wunsch des Adoptivvaters eine Auskunftssperre im Melderegister ein. Das Regionale Rechenzentrum, bei dem die Gemeinde ihre Daten verarbeiten läßt, übermittelte dann — wie üblich — die Daten des Kindes an die öffentlich-rechtliche Religionsgesellschaft, der das Kind angehört. Es wies dabei auf die bestehende Auskunftssperre hin. Auf Grund unglücklicher Umstände blieb dies jedoch unbeachtet und eine kirchliche Mitarbeiterin fragte beim Adoptivvater unter Verwendung des Geburtsnamens nach dem Kind. Dieser Fall macht deutlich, daß die Meldebehörden nicht recht wissen, wie sie in Adoptionsfällen verfahren sollen. Sollen sie eine Auskunftssperre im Melderegister eintragen und welche Bedeutung hat eine solche? Im „Normalfall“ entfaltet eine Auskunftssperre nur Wirkung im Verhältnis zwischen der Meldebehörde und einem privaten Auskunftssuchenden, nicht jedoch im Verhältnis zwischen Meldebehörde und anderen Behörden und öffentlich-rechtlichen Religionsgesellschaften. Deshalb dürfen sie trotz Auskunftssperre Daten zum Beispiel an Kirchen übermitteln. Anders verhält es sich jedoch in Adoptionsfällen. § 1758 des Bürgerlichen Gesetzbuchs sieht hierfür ein Offenbarungs- und Ausforschungsverbot vor. Danach darf man „Tatsachen, die geeignet sind, die Annahme eines Kindes und ihre Umstände aufzudecken“, ohne Zustimmung des Annehmenden und des Kindes nicht offenbaren oder ausforschen — es sei denn, besondere Gründe des öffentlichen Interesses erfordern dies. Dieses Offenbarungsverbot unterscheidet sich in einem sehr wesentlichen Punkt von der Auskunftssperre. Es gilt nämlich auch im Verhältnis der Meldebehörde zu anderen Behörden bzw. zu einer öffentlich-rechtlichen Religionsgesellschaft. Welche konkreten Auswirkungen es hat, läßt sich nur im Einzelfall sagen. Auf jeden Fall ist jedoch dafür Sorge zu tragen, daß das Offenbarungs- und Ausforschungsverbot nach § 1758 BGB nicht mit der Auskunftssperre gleichgesetzt und routinemäßig Daten an Dritte übermittelt werden. Das bedingt eine besondere Kennzeichnung im Melderegister und eine Einzelfallprüfung vor einer Datenübermittlung. Das Innenministerium sagte mir zu, eine entsprechende Regelung in die Verwaltungsvorschrift zum neuen Landesmeldegesetz aufzunehmen.

Allein diese Beispiele belegen, wie notwendig es ist, bei der Schaffung und Auslegung von Rechtsvorschriften das Zusammenspiel der verschiedenen Rechtsnormen generell und des allgemeinen und bereichsspezifischen Datenschutzes im besonderen zu sehen und daraus die notwendigen Konsequenzen zu ziehen.

7. Teil: Sorgen der Bürger

1. Zur Situation

Das Landesdatenschutzgesetz und die zahlreichen anderen Vorschriften des Datenschutzes haben letztlich das Ziel, den Bürger davor zu schützen, daß die öffentliche Hand seine Persönlichkeits-sphäre durch den Umgang mit seinen Daten ungerechtfertigt be-

einträchtigt. Da leider der Erlass von Rechtsvorschriften noch keine Garantie für ihre Beachtung ist, schuf der Landtag zur Kontrolle der Einhaltung datenschutzrechtlicher Vorschriften das Amt des Landesbeauftragten für den Datenschutz. Seine Arbeit ist unmittelbar auf den Bürger ausgerichtet. Er steht im Mittelpunkt. Seinen Anliegen und Sorgen habe ich mich zu stellen. Aus diesem Grund messe ich gerade dem Bearbeiten von Bürgereingaben, in denen sich die Sorgen der Bürger am unmittelbarsten artikulieren, ganz besondere Bedeutung zu. Die folgende Darstellung ist keine erschöpfende Aufzählung und Schilderung aller an mich herangetragenen Bürgerfragen und -nöte. Sie gibt nur beispielhaft eine Reihe von Problemen wieder, wegen der sich im letzten Jahr Bürger an mich wandten.

2. Einzelne Sorgen

2.1 Gesundheitswesen

Kranke Bürger sind besonders schutzbedürftig, weil sie viele sensitive Daten angeben müssen, um die notwendige medizinische Betreuung zu erhalten. Viele von ihnen sorgen sich über den Umgang medizinischer Stellen mit ihren Daten.

- Einer verheirateten berufstätigen Frau fiel auf, daß eine Universitätsklinik von ihr und anderen ambulanten Patientinnen Daten erhob, die sie weder für die Behandlung noch für die Abrechnung benötigte. Die Klinik wollte von der Patientin zum Beispiel Religion und Staatsangehörigkeit wissen, und auch Anschrift, Beruf, Arbeitgeber und Krankenkasse ihres Ehemannes, obwohl sie selbst krankenversichert war.

Bei meiner Überprüfung stellte sich heraus, daß die Universitätsklinik der Einfachheit halber bei ihren ambulanten Patienten dieselben Daten erhob und speicherte, die sie bei den stationären Patienten für die Behandlung und Abrechnung mit der Krankenkasse braucht. Ich beanstandete dieses Übermaß gespeicherter Daten. Die Universitätsklinik sicherte mir eine Änderung ihrer Praxis zu.

Dank der Aufmerksamkeit der Bürgerin, die mir diesen Fall schilderte, konnte ich auch folgende rechtswidrige Praxis der Universitätsklinik abstellen: Um Schreibarbeiten zu sparen, stempelte die Klinik alle Daten der ambulanten Patientinnen, die sie in der geschilderten Weise erhoben hatte, auf die Rezepte der Patientinnen. Sie bedachte nicht, daß auf diese Weise der Apotheker Konfession und Staatsangehörigkeit seiner Kundin und Name und Arbeitgeber ihres Ehemanns erfuhr. Auch diese Praxis stellte die Universitätsklinik nach meiner Beanstandung ab.

- Wiederholt suchten Krankenhausärzte und ihre Mitarbeiter meinen Rat, weil es Meinungsverschiedenheiten gab, in welchem Umfang die ärztliche Schweigepflicht im internen Krankenhausbetrieb gilt. Dazu ist zu sagen: Das Arztgeheimnis gilt grundsätzlich auch gegenüber der Krankenhausverwaltung. Behandelnde Ärzte und ihre Mitarbeiter dürfen deshalb der Verwaltung nur die Angaben offenbaren, die sie zum Zweck der Abrechnung und zur Erledigung anderer ihr obliegender Aufgaben bei der Erfüllung des Krankenhausvertrags benötigt. Ein Krankenhausleiter kann deshalb nicht verlangen, daß ihm die Sekretärinnen der Ärzte eine Zeitlang Durchschriften der Arztbriefe über-

lassen, damit die Verwaltung ihre Schreibleistungen kontrollieren kann. Sollte die Verwaltung wider Erwarten nicht in der Lage sein, diese Kontrolle auf andere Weise durchzuführen, müßten die Arztsekretärinnen zunächst in den Durchschlägen die Namen, Anschriften und alle anderen Hinweise unkenntlich machen, welche auf die Identität der Patienten schließen lassen. Ebenso wenig können Krankenhausärzte mit privatem Liquidationsrecht der Verwaltung einfach Durchschriften ihrer Honorarrechnungen übergeben, damit sie überprüfen kann, ob der Arzt seinen Ablieferungsbetrag an das Krankenhaus richtig berechnet hat. Wenn eine Kontrolle nicht anders möglich ist, muß man die Durchschriften so gestalten, daß auf ihnen nicht die Diagnose steht. Merkwürdig berührte mich das Ansinnen einer Krankenhausverwaltung, der Chirurg möge ihr seine Operationsbücher zur Einsicht überlassen, damit sie für die Pflegesatzverhandlungen mit den Krankenkassen eine Statistik erstellen könne. Der richtige und ohne Schwierigkeiten gangbare Weg ist, daß die Chirurgische Abteilung die gewünschten statistischen Zahlen für die Verwaltung zusammenstellt.

- Ein Problem ganz anderer Art aus dem Krankenhausalltag schilderte mir eine große Industriefirma. Bei ihr ist es seit eh und je Brauch, daß ihre Sozialarbeiterin oder ein anderer Mitarbeiter erkrankte Kollegen und Pensionäre der Firma im Krankenhaus besucht. Um zu erfahren, wer gerade im Krankenhaus liegt, ging die Sozialarbeiterin früher zur Pforte des Krankenhauses, sah die Patientenkartei durch und schrieb sich alle Patienten heraus, deren Karte einen Hinweis auf die Betriebskrankenkasse ihrer Firma enthielt. Diese Praxis konnte die Firma selbstverständlich nicht beibehalten. Sie war mit § 11 Abs. 1 LDSG allein schon deshalb nicht vereinbar, weil die Firma kein berechtigtes Interesse an der Kenntnis aller in der Patientenkartei enthaltenen Daten glaubhaft machen konnte. Das Krankenhaus konnte der Firma auch nicht ihren Wunsch erfüllen, ihr statt dessen in Zukunft in regelmäßigen Abständen die Namen aller jetzigen und ehemaligen Mitarbeiter mitzuteilen, die gerade im Krankenhaus liegen. Diese Vorgehensweise würde nicht ausschließen, daß sie schutzwürdige Belange des einen oder anderen betroffenen Mitarbeiters beeinträchtigt. Das heißt freilich nicht, daß die Firma ihr sicherlich begrüßenswertes soziales Engagement nicht fortsetzen kann. Der Datenschutz steht ihm nicht entgegen, wenn die Einwilligung der Patienten eingeholt wird. Vorschläge, wie dies geschehen kann, machten die Krankenhausleitung und ich der Firma. Ich hoffe deshalb, daß sie eine praktikable Lösung findet.
- Ein ehemaliger Patient der Neurologischen Abteilung einer Universitätsklinik schilderte mir, wie er völlig unerwartet auf nicht gerade taktvolle Weise an eine jahrelang zurückliegende Behandlung in dieser Klinik erinnert wurde. Eines Tages läutete ein junger Mann an seiner Haustür und wollte ihn sprechen. Auf die Frage seiner Ehefrau nach dem Grund des Besuchs klärte der junge Mann die Frau über den früheren Krankenhausaufenthalt ihres Mannes auf und sagte, er wolle deshalb ihren Mann für eine wissenschaftliche Arbeit befragen. Darüber war die Frau so schockiert, daß sie den jungen Mann abwies. Diese mehr als verständliche Reaktion zeigt, daß Universitätskliniken schon in eigenem Interesse mit mehr Einfühlungsvermögen und

Rücksichtnahme vorgehen sollten. Denn anderenfalls bringen sie sich um die Chance, daß ein ehemaliger Patient zur Mitarbeit an ihrem Forschungsvorhaben bereit ist.

2.2 Sozialwesen

— Datenerhebung in der Sozialhilfe

Das Bundessozialhilfegesetz gewährt ebenso wie die übrigen Sozialleistungsgesetze Leistungen an einzelne Bürger nur unter ganz bestimmten Voraussetzungen. Im Regelfall kommt es dabei ganz entscheidend auf die persönlichen und wirtschaftlichen Verhältnisse der Hilfesuchenden und ihrer Angehörigen an. Das Vorliegen dieser Umstände hat jeweils der Sozialhilfeträger zu prüfen. Dazu muß er sich die erforderlichen Kenntnisse verschaffen. Dies aber ist wiederum vielfach nur möglich, wenn der Hilfesuchende mitwirkt. In welchem Umfang er dazu verpflichtet ist, ergibt sich im einzelnen aus den §§ 60 bis 67 des Allgemeinen Teils des Sozialgesetzbuchs (SGB I). Danach muß der Hilfesuchende unter anderem

- alle für die Leistung erheblichen Tatsachen angeben,
- zustimmen, daß Dritte die erforderlichen Auskünfte über ihn geben, wenn der Sozialleistungsträger dies verlangt,
- alle Änderungen in den für die Leistung entscheidenden Verhältnissen unverzüglich mitteilen und
- erforderlichenfalls Beweismittel angeben und Beweisurkunden vorlegen.

Die Praxis verwendet zum Erheben der benötigten Angaben und zum Einholen der erforderlichen Zustimmungserklärungen im Regelfall Vordrucke. Eine Reihe von Bürgern und Verbänden beschwerte sich bei mir über den Umfang der darin geforderten Angaben und über die gleichzeitig verlangten umfassenden Einwilligungserklärungen. In der Tat werfen die verwendeten Vordrucke eine Reihe datenschutzrechtlicher Probleme auf:

- Da sich die Vordrucke für eine Vielzahl von Fallgestaltungen eignen sollen, birgt dies die Gefahr in sich, daß in manchen Fällen durchaus notwendige Angaben auch in solchen Fällen erhoben werden, wo dies nicht der Fall ist. Dies sollte man durch eine entsprechende Gestaltung der Vordrucke vor allem in den Fällen unterbinden, in denen der Hilfesuchende eine ganz bestimmte Einzelleistung beantragt und nicht nur pauschal alle möglichen Arten von Sozialhilfeleistungen.
- Fast kein Antragsvordruck trägt der Verpflichtung aus § 79 SGB X in Verbindung mit § 9 Abs. 2 BDSG Rechnung und weist darauf hin, welche Angaben freiwillig sind und welche Angaben angegeben werden müssen, damit der Sozialhilfeträger über den Antrag sachgerecht entscheiden kann.
- Vordrucke für Einwilligungserklärungen, die von der Einhaltung des Bankgeheimnisses, der ärztlichen Schweigepflicht oder des Sozialgeheimnisses entbinden, sind noch immer vielfach zu pauschal und inhaltlich und zeitlich zu unbestimmt.
- Die Sozialhilfeträger fordern solche Einwilligungserklärungen oft noch automatisch bei jeder Antragstellung und

prüfen zunächst nicht, ob dafür im konkreten Fall ein Bedürfnis besteht. Diese Automatik besteht vor allem dann, wenn der Antragsvordruck selbst die Einwilligungserklärung enthält. § 60 Abs. 1 Nr. 1 SGB I stellt das Einholen solcher Einwilligungen in das Ermessen des Sozialleistungsträgers. Er übt dieses Ermessen nur sachgerecht aus, wenn er konkret überlegt, in welchen Fällen das Einholen einer Einwilligungserklärung erforderlich ist. Dies ist beispielsweise nicht der Fall, wenn der Hilfesuchende die erforderlichen Bescheinigungen beibringen kann und will.

Ich schilderte diese Probleme den Kommunalen Landesverbänden und Landeswohlfahrtsverbänden und stieß dabei auf großes Verständnis. Dies gibt mir Grund zu hoffen, daß sich Fortschritte erzielen lassen. Das Erheben von Daten im Sozialleistungsbereich berührt die betroffenen Bürger existentiell und sollte deshalb auf das unumgängliche Maß beschränkt werden.

— Gewährung von Sozialhilfe in Form von Sachleistungen

Ein Sozialhilfeempfänger sprach ein Problem des Datenschutzes an, das in der gegenwärtigen Situation leider recht aktuell ist. Er beklagte sich, das Sozialamt gebe ihm zum Beschaffen von Kleidern nicht das notwendige Geld, sondern lediglich Berechtigungsscheine, gegen deren Vorlage er bei einer vom Sozialamt bestimmten Organisation Kleider beziehen könne. Durch dieses Verfahren erfahre die Organisation, daß er Sozialhilfeempfänger sei. Dies verstoße gegen das Datenschutzgesetz. Er werde damit zum Menschen zweiter Klasse gestempelt. Obwohl ich das Unbehagen im Prinzip verstehe, konnte ich dem Bürger in eigener Sache nicht rechtgeben. Das Sozialamt muß nach pflichtgemäßem Ermessen entscheiden, in welcher Weise es Hilfe leistet. Dieses Ermessen ist begrenzt durch die allgemeinen Grundsätze der Sozialhilfe, insbesondere durch § 1 Abs. 2 des Bundessozialhilfegesetzes. Danach ist mit dem Ziel der Sozialhilfe, dem Empfänger ein menschenwürdiges Leben zu ermöglichen, nicht vertretbar, einmalige Leistungen generell in Form von Berechtigungsscheinen zu gewähren. Damit werde, so betont das sozialrechtliche Schrifttum, dem Hilfeempfänger nämlich die Teilnahme am wirtschaftlichen Leben verbaut. Ihm werde der Anreiz und die Möglichkeit genommen, bei der Bedarfsdeckung Einsparungen zu seinen Gunsten zu erzielen. Außerdem würde er gegenüber Dritten durch den Berechtigungsschein von vornherein als Empfänger öffentlicher Hilfeleistungen abgestempelt. Gerade der letzte Gesichtspunkt ist, seit die Sozialdaten durch die Neuregelung des Sozialgeheimnisses stärker als früher geschützt sind, von besonderer Bedeutung. Das alles heißt im Ergebnis, daß Sozialämter nur in begründeten Einzelfällen Berechtigungsscheine ausgeben dürfen. Ein solcher Ausnahmefall lag hier vor, weil zu befürchten war, daß der Hilfeempfänger das Geld des Sozialamts nicht zweckentsprechend verwendet. Das Verhalten des Sozialamts war folglich nicht zu beanstanden. Es durfte die Tatsache, daß der Inhaber des Berechtigungsscheins Sozialhilfeempfänger ist, der Kleiderstelle offenbaren. In solchen wohl kaum zu vermeidenden Fällen erscheint mir besonders wichtig, daß das Sozialamt die Stelle, bei der Sozialhilfeempfänger Berechtigungsscheine einlösen können, darauf hinweist, daß auch sie dem Sozialgeheimnis unterliegt und ihr Wissen

nur zum Zweck der Abrechnung mit dem Sozialamt verwenden darf.

— Verletzung des Sozialgeheimnisses

In einen Kirchturm wollte mich der Oberbürgermeister einer Großstadt unseres Landes versetzen, weil ich es gewagt hatte, eine von seiner Verwaltung begangene Verletzung des Sozialgeheimnisses zu beanstanden. Der Anlaß dafür war folgender: Die Stadt und der Trägerverein einer Kindertagesstätte führten einen Prozeß wegen der Leistung von Personalkostenzuschüssen. Zur Begründung ihrer ablehnenden Haltung erwähnte die Stadt in einem ihrer Schriftsätze an das Gericht u. a. Einzelheiten aus einem Scheidungsverfahren eines namentlich genannten Vereinsmitglieds. Die Stadt hatte diese Einzelheiten durch eine Anfrage des Scheidungsgerichts bei ihrem Sozial- und Jugendamt erfahren. Da die strittige Frage der Gewährung von Personalkostenzuschüssen auch Gegenstand einer öffentlich ausgetragenen Kontroverse mit dem Trägerverein war, leitete die Stadt der Einfachheit halber gleich den kompletten Schriftsatz einer Tageszeitung zu, den diese auszugsweise veröffentlichte. Mit der Weitergabe des Schriftsatzes an die Zeitung hatte die Stadt Angaben offenbart, die dem Sozialgeheimnis unterliegen. Eine Offenbarungsbefugnis war nicht gegeben. Die Weitergabe war insbesondere nicht zur Erfüllung der Aufgaben der Stadt als Träger der Jugendhilfe erforderlich. Eine sachgerechte Information der Presse wäre sehr wohl auch ohne Namensnennung und Aushändigung des gesamten Schriftsatzes möglich gewesen.

Besonders bemerkenswert war die Reaktion des Regierungspräsidiums, das ich in seiner Eigenschaft als Rechtsaufsichtsbehörde der Stadt einschaltete. Es konnte sich gerade noch dazu durchringen, mir zu bestätigen, daß die Information der Presse auch ohne Namensnennung möglich gewesen wäre. Gegenüber dem Oberbürgermeister selbst wollte es diese Feststellung offenbar nicht unmittelbar treffen. Ihm leitete das Regierungspräsidium lediglich eine Abschrift des an mich gerichteten Schreibens zur Kenntnis zu. Eine solche „diplomatische“ Reaktion ist von besonderer Bedeutung, weil ich seit der durch das 1. Gesetz zur Änderung des Landesdatenschutzgesetzes vom 24. Juni 1982 (GBl. S. 265) erfolgten Einschränkung meiner Kontrollbefugnis Fälle dieser Art nicht mehr überprüfen kann. Bekanntlich begründeten die Befürworter der Novelle diese Einschränkung im wesentlichen damit, die Einhaltung der datenschutzrechtlichen Bestimmungen sei bereits durch die herkömmlichen Aufsichtsinstanzen in ausreichendem Maße gewährleistet. Was von diesem Argument zu halten ist, zeigt dieser Vorgang einmal mehr.

— Parkausweis für Schwerbehinderte

Viele Schwerbehinderte sind außergewöhnlich gehbehindert. Sie können von der Straßenverkehrsbehörde einen besonderen Parkausweis erhalten. Dieser berechtigt sie u. a. zum gebührenfreien Parken an Parkuhren oder zum Parken an besonders gekennzeichneten Stellen in Straßen, in denen das Parken und Halten sonst allgemein verboten ist. Der Parkausweis muß gut sichtbar im Innern des Fahrzeugs angebracht sein. Wiederholt erkundigten sich bei mir vor den

Kopf gestoßene Bürger, wo denn hier der Datenschutz bleibe. Da auf der Vorderseite des bundeseinheitlich festgelegten Parkausweises der Name der Schwerbehinderten einzutragen sei, könne jeder Passant den Schwerbehinderten identifizieren, ohne daß dazu die geringste sachliche Notwendigkeit bestünde. Leider kennen offenbar nicht alle Verkehrsbehörden die Möglichkeit, diese unerwünschte Nebenwirkung des Parkausweises zu vermeiden. Ein Blick in eine herausgegebene Verwaltungsvorschrift des Innenministeriums hilft hier weiter. Auf Antrag des Berechtigten kann das Namensfeld auf dem Parkausweis freibleiben und statt dessen der Name auf der Rückseite eingetragen werden. Einen einzigen Nachteil hat dieses Verfahren: das Ausland anerkennt einen so gestalteten Ausweis nicht.

2.3 Schulen und Hochschulen

— Weitergabe von Schülerdaten an Sparkassen und Banken

Wer den lobenswerten Vorsatz faßt, einen Blick in das Schulgesetz unseres Landes zu werfen und dabei nachsehen will, welche Aufgaben dieses Gesetz unseren Schulen zuweist, erfährt einiges über die Erziehungs- und Bildungsaufgaben der Schule. Vergeblich sucht er jedoch danach, daß es auch Aufgabe der Schule ist, Wirtschaftsunternehmen Adressenmaterial zu Werbezwecken zu liefern. Genau diese Rolle muten aber insbesondere Banken und Sparkassen immer wieder unseren Schulen zu. Nun läßt sich kaum etwas dagegen sagen, wenn sie die Schule in aller Bescheidenheit um solches Adressenmaterial bitten. Die Schule hat es dann ja in der Hand, frei darüber zu entscheiden und kann, wenn sie der Bitte Rechnung tragen will, die Einwilligung der Schüler bzw. ihrer Eltern einholen. Wesentlich bedenklicher ist allerdings, wenn eine Bank, deren Ansinnen die Schule ablehnte, einzelne Schüler unter Aussetzung einer Belohnung dazu veranlaßt, die Schüleradressen aus dem Klassentagebuch abzuschreiben. Handelte es sich dabei nur um Einzelfälle, sieht die Sache wesentlich anders aus bei folgender konzertierten Vorgehensweise zahlreicher Sparkassen unseres Landes einschließlich der Landesgirokasse: Sie geben sich großzügig und gewähren Zuwendungen zu Schulandaufenthalten, Studienreisen und ähnlichen Veranstaltungen. Dieses an sich sehr begrüßenswerte Verhalten hat allerdings einen Pferdefuß. Die Zuwendung wird nur gewährt, wenn die Schule der Sparkasse Name, Anschrift und Geburtstag aller teilnehmenden Schüler als Gegenleistung zur Verfügung stellt. Diese Daten sollen gezielte Werbeaktionen bei den Schülern ermöglichen. Da diese Art der Gewinnung von Adressen zu Werbezwecken auf eine Empfehlung des Württ. Sparkassen- und Giroverbandes beruht, wandte ich mich an ihn und bat, er möge doch seine Mitglieder bitten, die Gewährung von Zuwendungen nicht mehr von der Überlassung der Schülerdaten abhängig zu machen. In seiner Antwort zeigte der Verband zwar viel Verständnis für den Datenschutz im allgemeinen, lehnte es aber ab, meiner Bitte zu entsprechen und war lediglich bereit, seine Mitglieder von meiner Auffassung zu unterrichten. Ich bedauere diese Haltung außerordentlich. Zwar ist das Verhalten der Sparkassen sicherlich nicht rechtswidrig, da es ihnen freisteht, die Bedingungen festzulegen, unter denen sie Zuwendungen an Schulen geben möchten. Eine ganz andere Frage ist jedoch, ob angemessen ist, wenn

dem Gemeinwohl verpflichtete Anstalten des öffentlichen Rechts — und das sind die Sparkassen — auf die geschilderte Art Adressen zu Werbezwecken kaufen. Sie üben dabei nämlich einen ganz erheblichen Druck auf die Schule und die Eltern aus. Die Schule, d. h. im Regelfall der Klassenlehrer, wird sich, um die Zuwendung zu erhalten, bemühen, der Forderung der Sparkassen nachzukommen. Tut sie dies, ohne zuvor die Einwilligung der Eltern einzuholen, verstößt sie damit gegen die Übermittlungsregelung des § 11 LDSG. Widersteht der Klassenlehrer der Versuchung zu einem gesetzeswidrigen Verhalten und versucht er, die Einwilligung der Eltern zu bekommen, sehen diese sich ebenfalls unter Druck gesetzt, da ja der Zuschuß nur gewährt wird, wenn die Daten aller teilnehmenden Schüler geliefert werden. Die einzelnen Eltern müssen also nicht nur berücksichtigen, welche Auswirkungen eine Weigerung auf ihr Kind hätte, sondern müssen auch die Folgen für die Klassenkameraden in Rechnung stellen.

Wenn demgegenüber der Württ. Sparkassen- und Giroverband geltend macht, die gewünschte Übermittlung würde in keinem Fall schutzwürdige Belange beeinträchtigen, kann ich mich dem nicht anschließen. Eine Beeinträchtigung schutzwürdiger Belange sehe ich allein schon darin, daß größtenteils minderjährige Schüler und ihre Eltern einer gezielten Werbung teilweise sogar in Form von Hausbesuchen ausgesetzt werden. Das dagegen vorgetragene Argument, der junge Mensch sei zuvor in der Schule durch verbrauchererzieherischen Unterricht auf solche Werbeaktionen vorbereitet worden, scheint mir bei weitem zu optimistisch. Aber auch unabhängig von diesen generellen Überlegungen kann die Schule nicht ausschließen, daß durch eine Übermittlung schutzwürdige Belange zumindest einzelner Schüler nicht doch beeinträchtigt sind. Immerhin wird der Sparkasse bei der gewünschten Datenübermittlung nicht nur der Name und die Anschrift, sondern auch der Geburtstag, die Schulart, die Klasse und die beabsichtigte Teilnahme an der Schulveranstaltung mitgeteilt. Es kann sehr wohl bei einzelnen Schülern der Schule unbekannte beachtenswerte Gründe geben, die dagegen sprechen, daß die Sparkasse diese Daten erfährt. Schließlich dürfen nicht einmal die Einwohnermeldeämter den Sparkassen solche Daten von Personengruppen ohne deren Einwilligung geben. Auch eine ganze Reihe anderer öffentlichen Stellen, zum Beispiel Deutsche Bundespost, Kraftfahrt-Bundesamt, stellen solche Daten nur noch dann für Werbezwecke zur Verfügung, wenn dazu die Einwilligung der Betroffenen vorliegt. Ich meine, auch die Sparkassen und Banken sollten dies respektieren und davon ablassen, die Schulen und die Eltern in der geschilderten Weise unter Druck zu setzen.

— Erhebung von Studentendaten

Die Einführung eines neuen automatisierten Studenten-Verwaltungssystems an einer Universität des Landes löste bei ihren Studenten erhebliche Aufregung aus. Im Zuge dieser Maßnahme war es notwendig, daß die Universität alle für Zwecke der Verwaltung und der Hochschulstatistik benötigten Daten von allen Studenten neu erhebt. Die Erhebungsaktion betraf also auch Studenten, die bereits eingeschrieben waren und sich lediglich für das Wintersemester 1982/1983 zurückmelden wollten. Der sehr umfangreiche Erhebungsbogen erweckte Argwohn bei einer ganzen Reihe

von Studenten. Am meisten kritisierten sie die Fragen nach dem Schulabschluß, der beruflichen Ausbildung und der sozialen Stellung ihrer Eltern. Sie machten zu Recht geltend, daß die Universität diese Angaben nicht für die Erfüllung ihrer Aufgaben benötigt. Gleichwohl mußte ich den Studenten sagen, daß die Universität diese Fragen zu Recht stellt. Sie erhob nämlich gleichzeitig mit den Daten für ihre Verwaltungszwecke auch die Angaben, die zur Durchführung der amtlichen Hochschulstatistik benötigt werden. § 4 Nr. 2 des Hochschulstatistikgesetzes sieht aber vor, daß gerade auch solche Angaben über die Eltern erhoben werden. Im übrigen machten die Eingaben einmal mehr deutlich, daß die sich aus dem Nebeneinander von Datenerhebung und -speicherung für Zwecke der Hochschulen und für Zwecke der Hochschulstatistik ergebenden Probleme leider noch immer nicht befriedigend gelöst sind. Meine Bemühungen, gemeinsam mit dem Wissenschaftsministerium zu einer landeseinheitlichen Klärung zu gelangen, hatten leider noch keinen Erfolg.

— Auskunft über gespeicherte Daten

Ein Beispiel dafür, wie selbst klar gefaßte Bestimmungen des Landesdatenschutzgesetzes der Fehldeutung durch die Verwaltung unterliegen, zeigt der Fall eines ehemaligen Bewohners eines Wohnheims eines Studentenwerks. Er bat das Studentenwerk um Auskunft, welche Daten es über ihn speichert. Das Studentenwerk teilte ihm daraufhin lediglich die in der Datei gespeicherten Datenarten und nicht die einzelnen über ihn konkret gespeicherten Daten mit. Letzteres verlangt aber § 12 Abs. 1 LDSG. Nur so ist der Betroffene in der Lage, die Zulässigkeit der Datenspeicherung zu überprüfen und gegebenenfalls sein Recht auf Berichtigung, Sperren und Löschen auszuüben.

2.4 Verkehrswesen

— Kontrolle von Fahrlehrern

Fahrschulen und Fahrlehrer unterliegen nach dem Fahrlehrergesetz einer Überwachung durch die Erlaubnisbehörden. Diese müssen sich dabei des Treuhandvereins für Verkehrserziehung und Verkehrssicherheit e. V. bedienen. Seine Prüfer werden dann jeweils im Auftrag der Erlaubnisbehörden tätig. Gegen die Vorgehensweise einer dieser Prüfer wandte sich ein nebenberuflich als Fahrlehrer tätiger Beamter. Der Prüfer hatte in seinem Prüfbericht über die Fahrschule, die den Fahrlehrer beschäftigte, seine gesamten Einkünfte als Fahrlehrer aufgelistet und der zuständigen Erlaubnisbehörde mitgeteilt. Außerdem bemängelte er im Prüfbericht, es liege keine Bescheinigung über die — in Wirklichkeit erteilte — Nebentätigkeitsgenehmigung vor. Dieser Fall ist unter zwei Aspekten erwähnenswert. Datenschutzrechtlich von Bedeutung ist, daß es nicht zu den Aufgaben der Erlaubnisbehörden und damit auch nicht zu den Aufgaben des Treuhandvereins und seiner Prüfer gehört zu kontrollieren, ob für die Beschäftigung eines Beamten als Fahrlehrer eine Nebentätigkeitsgenehmigung erforderlich ist und ob diese vorliegt. Eine Übermittlung dieser Daten an die Erlaubnisbehörde ist deshalb nach § 10 LDSG unzulässig. Erwähnenswert ist aber auch, wie sich das von mir in dieser Frage eingeschaltete Innenministerium verhielt.

Obwohl ich ihm den hier geschilderten Sachverhalt vorge-
tragen hatte, beschränkte es sich im wesentlichen darauf,
meine Zuständigkeit in dieser Angelegenheit zu bestreiten
und mich um Abgabe der Eingabe zu „ersuchen“. Meine Zu-
ständigkeit hielt es deshalb nicht für gegeben, weil es im
Gegensatz zu mir der Auffassung ist, daß weder der Treu-
handverein noch seine Prüfer bei der Überwachung der
Fahrschulen eine hoheitliche Tätigkeit ausüben. Erst nach-
dem ich nach ca. 7 Monaten, um die Angelegenheit zum Ab-
schluß zu bringen, dem Innenministerium meine abschlie-
ßende rechtliche Beurteilung des Falles mitteilte, bequeme
es sich zu der Aussage, es habe bereits 9 Monate zuvor dem
Treuhandverein mitgeteilt, daß die Prüfer keinen Nachweis
über die Nebentätigkeitsgenehmigung verlangen und daß
sie deshalb auch nicht von der Fahrschule eine Auflistung
der Einkünfte aus der Nebentätigkeit des Fahrlehrers for-
dern können. Hätte das Innenministerium mir diese Hal-
tung sofort mitgeteilt, dann hätte ich dies dem Fahrlehrer
gleich schreiben können und die Angelegenheit wäre erle-
digt gewesen. Anstatt diesen einfachen Weg zu wählen, der
dem Bürgeranliegen am schnellsten Rechnung trägt,
glaubte das Innenministerium, einen völlig unnötigen und
unfruchtbaren Kompetenzstreit vom Zaun brechen zu müs-
sen.

— **Formulare für die Erteilung der Fahrerlaubnis**

Wie schwer sich Behörden mit der Hinweispflicht nach § 9
Abs. 2 LDSG tun, wenn sie auf Antrag eines Bürgers tätig
werden, zeigte eine Führerscheinstelle besonders deutlich.
Sie schrieb in ihrem Formular für die Erteilung der Fahr-
erlaubnis einfach: „Die Erfassung und Verarbeitung der
personenbezogenen Daten Nr. 01 bis Nr. 07 sind gemäß
§ 10 Abs. 2 der Straßenverkehrszulassungsordnung erfor-
derlich“. Dieser Hinweis war für den Bürger nicht nur ver-
wirrend, sondern schlicht falsch. § 10 Abs. 2 StVZO erlaubt
nicht, bestimmte Daten zu erheben, sondern lediglich eine
Kartei über Führerscheininhaber zu führen. Ich riet der
Führerscheinbehörde deshalb, auf ihrem Formular die Bür-
ger darauf hinzuweisen, daß ihr eine günstige Entscheidung
nur möglich ist, wenn sie die im Formular bezeichneten An-
gaben machen.

— **Werbung mit Daten von Autofahrern**

Immer wieder beklagten sich Bürger, ihnen gingen nach Zu-
lassung ihres Fahrzeugs Werbeprospekte oder Fragebogen
von Meinungsforschungsinstituten zu, obwohl sie damit
nicht einverstanden seien. Die Zulassungsstellen hatten je-
weils versehentlich diese Tatsache dem Kraftfahrt-Bundes-
amt nicht mitgeteilt. Um diese Fehlerquelle auszuschalten,
schlug ich dem Wirtschaftsministerium vor, seine Vor-
drucke für die Meldungen an das Kraftfahrt-Bundesamt zu
ändern. Dies ist inzwischen geschehen.

— **Meldedienst „Inhaber von Luftbilderlaubnissen“**

Von 1973 bis Herbst 1982 meldeten die Regierungspräsi-
dien dem Bundesminister für Verkehr alle Personen, denen
sie eine Erlaubnis zum gewerblichen Herstellen von Luft-
bildaufnahmen erteilten. Im Rahmen des Meldedienstes
gaben sie jeweils Name und Anschrift des Erlaubnisinha-
bers, Tag der Ausstellung der Erlaubnis, ihre Geltungs-
dauer und etwaige Auflagen, zum Beispiel Gebietsbeschrän-

kungen für die Flüge weiter. Diese Praxis ging auf eine Initiative des Bundesministers für Verkehr zurück. Er meinte, die Daten für statistische Zwecke und zur Gefahrenabwehr zu benötigen. Beide Argumente überzeugen nicht. Für statistische Zwecke reichen Zahlen; die Person des Inhabers der Flugerlaubnisse ist hier ohne Interesse. Zur Gefahrenabwehr ist nicht der Bund, sondern allein das Land zuständig. Ich meldete deshalb beim Wirtschaftsministerium Bedenken gegen diese Praxis an, das sich mit dem Bundesminister für Verkehr in Verbindung setzte. Dieser trug meinen Bedenken Rechnung und hob seinen Erlaß von 1973 über den Meldedienst auf.

2.5 Bauwesen

— Baulückenkataster

Bürger, Gemeinderäte und Gemeinden fragen mich immer wieder, ob die Gemeinden sogenannte Baulückenkataster aufstellen dürfen. In ihnen sollen in etwa folgende Daten erfaßt werden: Gemarkung, Flurstücknummer, Grundstücksgröße, Grundbuchstelle, Katasterkarte, Erhebungsdatum, Eigentümer mit Anschrift, Eigentumsverhältnis, derzeitige Nutzung, Art und Maß der baulichen Nutzung, realisierbare Wohneinheiten, Maßnahmenstand (Bauanfrage, Baugesuch, mit Bau begonnen usw.). Ein solches Kataster soll hauptsächlich dazu dienen, Maßnahmen zur Schließung von Baulücken einzuleiten. Das Bundesbaugesetz räumt den Gemeinden die Möglichkeit ein, im Geltungsbereich eines qualifizierten Bebauungsplans den Grundstückseigentümer durch Bescheid zu verpflichten, innerhalb angemessener Frist sein Grundstück entsprechend den Festsetzungen des Bebauungsplans zu bebauen. Voraussetzung dafür ist, daß städtebauliche Gründe die alsbaldige Durchführung der Maßnahmen erfordern. Vor Erlaß eines solchen Baugeschäfts soll die Gemeinde mit den Eigentümern erörtern, wie die Maßnahmen durchgeführt werden können und welche Finanzierungsmöglichkeiten aus öffentlichen Kassen bestehen. Um diese Aufgaben bewältigen zu können, bedarf es — jedenfalls in größeren Städten — der Aufstellung eines Baulückenkatasters. Es begegnet keinen datenschutzrechtlichen Bedenken. Dabei kann dahingestellt bleiben, ob das Landesdatenschutzgesetz in vollem Umfang anwendbar ist. Voraussetzung dafür wäre, daß die Gemeinde das Baulückenkataster als Datei führt und daraus Daten an außerhalb der Gemeindeverwaltung und des Gemeinderats stehende Personen und andere Behörden übermittelt. Dies wird häufig nicht der Fall sein. Selbst wenn das Landesdatenschutzgesetz eingreift, darf die Gemeinde die eingangs genannten Daten speichern — vorausgesetzt, sie will die erwähnten Maßnahmen nach dem Bundesbaugesetz treffen. Erhebt sie dabei Daten bei den Grundstückseigentümern, muß sie die Hinweispflicht des § 9 Abs. 2 LDSG beachten. Häufig werde ich in diesem Zusammenhang noch gefragt, ob der Bürgermeister die Namen der Eigentümer unbebauter Grundstücke in öffentlicher Gemeinderatssitzung bekanntgeben darf. Die Frage beurteilt sich nicht nach dem Landesdatenschutzgesetz, sondern nach § 35 Abs. 1 der Gemeindeordnung. Diese Vorschrift schreibt, soweit es „berechtigten Interessen einzelner“ erfordern, eine nichtöffentliche Sitzung vor.

— Eintrag im „Roten Punkt“

Erstaunt war ich, von einem Architekten zu hören, daß eine Baurechtsbehörde in den an der Baustelle anzubringenden Freigabebeschein („Roter Punkt“) stets die Baukosten einträgt. Der Architekt hatte hiergegen Bedenken, die ich aus folgenden Gründen teilte: Nach der Landesbauordnung muß der Baufreigabebeschein lediglich die Bezeichnung des Bauvorhabens und die Namen und Anschriften des Bauherrn und des Bauleiters enthalten. Sie verpflichtet den Bauherrn weiter, spätestens bei Baubeginn in dem Baufreigabebeschein Namen, Anschrift und Rufnummer der Bauunternehmer für die Rohbauarbeiten einzutragen — es sei denn, daß an der Baustelle ein besonderes Schild mit diesen Angaben angebracht ist. Damit hat der Gesetzgeber den notwendigen Inhalt des „Roten Punkts“ festgelegt. Die genannten Vorschriften verbieten zwar nicht, weitere Angaben in den Baufreigabebeschein aufzunehmen. Jedoch steht § 11 LDSC der öffentlichen Bekanntgabe der Baukostensumme entgegen. Ein berechtigtes Interesse der Allgemeinheit an der Kenntnis dieser Angabe besteht nicht. Sie ist vielmehr allein für die Baurechtsbehörde zur Berechnung der Gebühren von Bedeutung.

— Verkabelung

Ein Bürger, der bei der Deutschen Bundespost beschäftigt ist, meldete während der Auslegung Bedenken gegen den Entwurf einer Satzung an, durch die die Gemeinde die Errichtung von Außenantennen für Fernseh- und UKW-Tonrundfunk verbieten wollte. Die Stadtverwaltung gab diese mit seinem Namen und seiner Anschrift an die Deutsche Bundespost zur Stellungnahme weiter. Deshalb befürchtete der Bürger berufliche Nachteile. Die von mir gehörte Stadtverwaltung berief sich darauf, sie hätte eine Stellungnahme der Deutschen Bundespost einholen müssen, weil nur die Post in der Lage sei, sachkundig auf die fernmelde- und funktechnischen Fragen des Bürgers zu antworten. Hinzu komme, daß die Satzung in einem engen Zusammenhang mit dem Vorhaben der Post stehe, in Neubaugebieten Breitbandkabelanlagen zu erstellen. Die namentliche Nennung des Bürgers gegenüber der Post sei erfolgt, weil ein Interesse an der vertraulichen Behandlung der Angelegenheit nicht erkennbar gewesen sei. Ich teilte dem Bürger mit, daß die Stadtverwaltung mit der Weitergabe seiner Daten an die Deutsche Bundespost nicht gegen das Landesdatenschutzgesetz verstieß, weil die übermittelten Daten nicht aus einer Datei (Kartei) stammten. Andere datenschutzrechtliche Vorschriften seien ebenfalls nicht verletzt. Gleichwohl stimmte ich dem Bürger darin zu, daß die Weitergabe seiner Daten nicht erforderlich gewesen wäre. Ich regte deshalb bei der Stadtverwaltung an, künftig in ähnlichen Fällen Bedenken eines Bürgers ohne Namensnennung an Dritte weiterzugeben.

2.6 Steuerwesen

- Offenbar als Sakrileg empfand es der Vorsteher eines Finanzamts, daß sich ein Bürger in einer Steuersache an mich wandte und um Überprüfung eines bestimmten Sachverhalts bat. Zunächst einmal weigerte er sich unter Hinweis auf das Steuergeheimnis, mir zur näheren Aufklärung erbetene Auskünfte zu erteilen. Er tat dies, obwohl selbst das

um die Einhaltung meiner Befugnisse stets sehr besorgte Finanzministerium in einem der gesamten Steuerverwaltung zugegangenen Erlaß zum Ausdruck gebracht hatte, daß eine Auskunftserteilung in solchen Fällen nicht das Steuergeheimnis verletzt. Darüber hinaus aber — und dies ist weitaus gravierender — hielt er es für erforderlich, dem Bürger in einem Schriftsatz an das Finanzgericht vorzuwerfen, dieser habe ihn bei mir „angeschwärzt“. Ich halte ein solches Vorgehen für indiskutabel. Es ist das gute Recht eines jeden Bürgers, behördliches Vorgehen von den Stellen überprüfen zu lassen, die in unserem Rechtssystem dafür vorgesehen sind. Dazu gehört auch die Anrufung der Landesbeauftragten für den Datenschutz. Tut er dies, muß dies die Behörde auch dann respektieren, wenn sie sich in der Sache selbst im Recht fühlt.

- Wenig bürgerfreundlich erwies sich ein anderes Finanzamt. Ein Bürger bat diese Behörde um Auskunft über seine bei ihm gespeicherten Daten. Sie übersandte ihm daraufhin einen Computerausdruck, der von den persönlichen Angaben wie Name, Vorname, Geburtstag und Anschrift abgesehen fast nur Abkürzungen oder Schlüsselzahlen enthielt. Ein solches Vorgehen mag zwar aus der Sicht der Verwaltung rationell sein. Es stellt jedoch keine Auskunft nach dem Landesdatenschutzgesetz dar. Erteilt eine Behörde einem Bürger Auskunft, muß sie verständlich sein. Die Bedeutung von Schlüsselzahlen und Abkürzungen ist ihm im Regelfall nicht bekannt. Die Behörde muß sie deshalb in geeigneter Weise erläutern. Nur so kann sich der Bürger ein Bild von den über ihn gespeicherten Daten machen und ihre Richtigkeit überprüfen.
- Ein Finanzamt hatte über Jahre hinweg erfolglos gegen einen Handelsvertreter wegen rückständiger Steuerschulden Vollstreckungsmaßnahmen ergriffen. Eines Tages sah ein Mitarbeiter der Vollstreckungsstelle dieses Finanzamts, daß vor dem Haus des Handelsvertreters der Geschäftswagen einer Computerfirma parkte. Er schloß daraus, der Handelsvertreter habe zu dieser Firma Geschäftsbeziehungen. Die Vollstreckungsstelle pfändete daraufhin mögliche Forderungen des Handelsvertreters gegen die Computerfirma. Aus der Pfändungs- und Einziehungsverfügung erfuhr die Computerfirma, daß der Handelsvertreter Steuerschulden hatte. Die Pfändung ging ins Leere, da der Handelsvertreter keine Forderungen gegenüber der Computerfirma besaß. Gleichwohl verstieß die Vollstreckungsstelle nicht gegen den Datenschutz. Das Finanzamt darf immer dann pfänden, wenn es auf Grund bestimmter Tatsachen vom Vorhandensein von Forderungen ausgehen kann. Dabei nimmt die Abgabenordnung in Kauf, daß im Einzelfall keine Forderungen bestehen und deshalb Dritte durch die erfolglose Pfändung dem Steuergeheimnis unterliegende Angaben erfahren. Ein Steuerschuldner, gegen den über Jahre hinweg Vollstreckungsmaßnahmen erfolglos blieben, muß hinnehmen, daß eine Vollstreckungsstelle allein auf Grund der Tatsache handelte, daß ein Geschäftsfahrzeug vor seinem Haus geparkt war.

2.7 Kommunalabgaben

— Feuerwehrabgabe

Um die Feuerwehrabgabe festzusetzen, lassen sich manche Gemeinden von den Finanzämtern das Jahreseinkommen

ihrer abgabepflichtigen Bürger mitteilen. Etliche von ihnen sahen darin eine Verletzung des Steuergeheimnisses. Dem vermochte ich mich nicht anzuschließen. Nach § 31 der Abgabenordnung sind die Finanzämter berechtigt, den Gemeinden Besteuerungsgrundlagen mitzuteilen, die diese zur Festsetzung ihrer Abgaben benötigen. Dies ist der Fall, wenn eine Gemeinde in ihrer Feuerwehrabgabesatzung festlegt, daß sich die Höhe der Abgabe nach dem Jahreseinkommen des Pflichtigen richtet. Zu einer solchen Regelung in der Satzung ermächtigt das Feuerwehrgesetz die Gemeinde. Dort heißt es nämlich wörtlich: „Bei der Veranlagung können die persönlichen und wirtschaftlichen Verhältnisse der Abgabepflichtigen berücksichtigt werden.“ Daraus folgt: Die Gemeinde kann in ihrer Satzung bestimmen, daß das Jahreseinkommen bei der Festsetzung der Abgaben berücksichtigt wird, sie muß es aber nicht. Sie könnte statt dessen in verfassungsrechtlich unbedenklicher Weise auch einen einheitlichen Abgabesatz vorsehen, den sie in bestimmten Fällen, zum Beispiel bei bestimmten Jahreseinkommen, auf Antrag des Abgabepflichtigen ermäßigen kann. Dies hätte aus der Sicht des Datenschutzes den Vorteil, daß es dem Abgabepflichtigen überlassen bliebe, ob er sein Einkommen offenbaren will. Damit entfielen die Mitteilung der Einkommen aller Abgabepflichtigen an die Gemeinde, die sicher häufig ohne deren Kenntnis erfolgt. Aber wie gesagt: Dies liegt in der Entscheidung des Satzungsgebers, also der Gemeinde. Differenziert man von vornherein nach dem Jahreseinkommen, so dürfen die Finanzämter auch dessen Höhe an die Gemeinden mitteilen. Das Steuergeheimnis ist insoweit durch eine ausdrückliche gesetzliche Vorschrift durchbrochen. Es ist jedoch nicht aufgehoben. Deshalb sind die mit der Festsetzung und Erhebung der Feuerwehrabgabe betrauten Bediensteten der Gemeinde zur Wahrung des Steuergeheimnisses verpflichtet.

— Fremdenverkehrsabgabe

Eine Bürgerin fragte mich, ob Gemeinden eine Fremdenverkehrsabgabe und Gewerbesteuer erheben dürften. Sie meinte, dies sei ausschließlich Sache des Finanzamtes. Nur ihm gegenüber sei sie zur Offenbarung verpflichtet. Bedenken habe sie vor allem dagegen, der Gemeinde die Höhe des Gesamtumsatzes in ihrem Fremdenverkehrsbetrieb mitzuteilen. Ich klärte die Bürgerin darüber auf, daß Fremdenverkehrsabgabe und Gewerbesteuer als Kommunalabgaben nach den einschlägigen Rechtsvorschriften unmittelbar von der Gemeinde und nicht vom Finanzamt festgesetzt und erhoben werden. Das Kommunalabgabengesetz und die Abgabenordnung verpflichten den Bürger, gegenüber der Gemeinde die für die Festsetzung der Abgabe erforderlichen Angaben zu machen und Vordrucke auszufüllen. Welche Angaben erforderlich sind, läßt sich nur im Einzelfall beurteilen. Gegen die Aufforderung einer Fremdenverkehrsgemeinde, ihr zur Festsetzung der Fremdenverkehrsabgabe die Höhe des Gesamtumsatzes mitzuteilen, bestehen jedoch keine Bedenken. Denn die Höhe der Fremdenverkehrsabgabe muß sich — wie es im Gesetz heißt — nach dem „Maß der dem Abgabepflichtigen erwachsenden wirtschaftlichen Vorteile richten“.

— Grundsteuer

Eine Bürgerin erhielt einen Grundsteuerbescheid für ein Grundstück, das ihr nicht gehörte. Nachdem ihre Beschwer-

de nichts gefruchtet hatte, wandte sie sich an mich. Meine Nachprüfung ergab, daß die Stadt zwei Personen miteinander verwechselte und deshalb die Bürgerin zu Unrecht mit ihren Daten in der Grundsteuerdatei gespeichert war. Die Stadtverwaltung berichtigte daraufhin ihre Daten.

2.8 Justizverwaltung

— Datenschutz bei den Gerichtskassen

Ein Bürger wandte sich an mich, weil ihm eine Gerichtskasse eine vorgedruckte Postkarte mit Antwortkarte zusandte. Auf der Postkarte heißt es unter anderem: „Ihre Zahlung kann leider nicht verbucht werden, weil das Kasenzeichen/die zuständige Behörde bzw. deren Geschäftszeichen nicht angegeben ist. Wir bitten deshalb, die anhängende Antwortkarte ... mit den notwendigen Angaben zurückzusenden.“ Im Falle unseres Bürgers hatte die Gerichtskasse auf der Antwortkarte durch einen handschriftlichen Zusatz um Zusendung einer Fotokopie des Urteils gebeten, weil der Bürger beim Einzahlen des Bußgeldes das Aktenzeichen falsch angegeben hatte und sie deshalb den Betrag nicht verbuchen konnte. Der Bürger meinte, solche Rückfragen sollten in verschlossenen Kuverts erfolgen, da es sich hier um sehr persönliche Angelegenheiten handle. Ich unterstützte dieses Anliegen gegenüber dem Justizministerium, weil aus der Rückfrage in der Tat jeder andere — etwa der Briefträger oder Nachbarn, in deren Briefkasten die Postkarte versehentlich gelangt — ersehen können, daß der Bürger einen Geldbetrag bei der Gerichtskasse eingezahlt hat. Dies ist zwar objektiv unverfänglich, da die Zahlung vielerlei Gründe haben kann. Gleichwohl legen nicht nur besonders sensible Bürger Wert darauf, daß andere solche Vorgänge nicht erfahren. Leider entsprach das Justizministerium meiner Bitte nur zum Teil und wies die Gerichtskassen lediglich an, mit der vorgedruckten Karte keine weiteren als die dort vorgedruckten Angaben zu erbitten.

— Grundbuchwesen

Immer wieder mußte ich mich mit Grundbuchangelegenheiten befassen. Einige Bürger bezweifelten, ob andere Einsicht in das Grundbuch erhielten. Andere klagten, das Grundbuchamt habe ihnen die Einsicht verweigert. In allen Fällen war mir die Nachprüfung des konkreten Sachverhalts verwehrt, da die Führung des Grundbuchs zur freiwilligen Gerichtsbarkeit und damit zur Rechtspflege gehört und sich hierauf meine Kontrollbefugnis nicht erstreckt. Ich konnte deshalb den Bürgern nur die Voraussetzungen für die Grundbucheinsicht nennen, wie sie § 12 der Grundbuchordnung festlegt.

8. Teil: Elektronische Datenverarbeitung

1. Abschnitt: Möglichkeiten und Grenzen der Datenschutzkontrolle

Immer wieder fragen mich Bürger, ob ich die Beachtung des Datenschutzes bei der elektronischen Datenverarbeitung wirklich prüfen kann. Diese Zweifel äußern nicht nur Personen, denen die elektronische Datenverarbeitung ein Buch mit sieben Siegeln ist, sondern auch

Fachleute, die sehr viel von elektronischer Datenverarbeitung verstehen. Sie greifen damit ein Grundsatzproblem auf, das mich seit Beginn meiner Tätigkeit beschäftigt. Einerseits habe ich durch das Landesdatenschutzgesetz weitreichende Möglichkeiten, mir ein Bild vom Stand der elektronischen Datenverarbeitung in den verschiedenen Zweigen der öffentlichen Verwaltung zu machen. Andererseits schränken in der Natur der Sache liegende Umstände diesen Spielraum empfindlich ein. Der Computer kann wohl Enormes leisten; doch muß ihm selbst der kleinste Schritt vorgegeben werden. Der Aufwand für Planung, Programmierung und Pflege all dieser Schritte ist extrem hoch. Es ist ausgeschlossen, jeden einzelnen Schritt nachzuvollziehen und seine Richtigkeit zu beurteilen. Deshalb stößt die Datenschutzkontrolle auch bei vorbildlich geführten Rechenzentren auf Grenzen.

1. Programmkontrolle

Welche Programme mit personenbezogenen Daten arbeiten, ergibt sich aus der Programmübersicht. Das Statistische Landesamt verwaltet zum Beispiel 3 639 Programme. Da die Programmübersicht nur eine Kurzinformation über jetzt und früher eingesetzte Programme enthält, kann man aus ihr nicht sicher und schnell ersehen, ob die einzelnen Programme die personenbezogenen Daten einwandfrei im Sinne des Datenschutzes verarbeiten. Feststellen ließe sich dies nur durch eine exakte Prüfung jedes einzelnen Programms. Dies ist aber wegen der Vielzahl und Komplexität der dabei nachzuvollziehenden Programmschritte nur begrenzt möglich. Eine lückenlose Nachprüfung könnte mit den Programmänderungen und Neuentwicklungen nie Schritt halten. Deshalb bleibt nichts anderes übrig, als einige Programme einzelner Sachgebiete der Verwaltung herauszugreifen. Selbst dann läßt sich nicht jeder einzelne Programmschritt der ausgewählten Programme in vertretbarer Zeit nachvollziehen. Die Zahl der auf einem einzelnen Sachgebiet eingesetzten Programme ist dafür viel zu hoch. Zum Beispiel gibt es zur Erledigung der Finanzaufgaben der Gemeinden gegenwärtig 980 Programme, die zusammen das Verfahren „Kommunales Finanzwesen“ bilden. Diese Programme müssen alle richtig zusammenwirken, so daß es nicht weiterhilft, nur einige seiner Programme zu prüfen.

Die Kontrolle der Programme eines Verfahrens ist grundsätzlich auf drei Arten möglich, von denen jede ihre eigenen Grenzen hat:

— Kontrolle anhand der Programm- und Verfahrensdokumentation

Die Dokumentation vermittelt ein Bild, wie die Programme eines Verfahrens Daten verarbeiten sollen und welche Verarbeitungsergebnisse zu erwarten sind. Sie offenbart Verfahrensmängel, zum Beispiel, daß kein Schutz der Daten vor unbefugtem Zugriff besteht. Die Methode hilft vor allem bei größeren Verfahren nicht weiter, weil die Programmdokumentation zu umfangreich ist, als daß man sie in vertretbarer Zeit vollständig lesen und prüfen kann. Auch versagt die Methode, wenn die Dokumentation unvollständig ist oder mit dem tatsächlichen Programm nicht übereinstimmt. Die zweite Arbeitsweise der Fallgestaltung ist sehr häufig, unter anderem weil die Informatik keinen Weg kennt, Probleme der Praxis in Programme umzusetzen, die in allen Einzelheiten richtig sind.

— Kontrolle durch Testen

Praktische Tests bieten sich an, wenn man eine unvollständige, unklare oder falsche Dokumentation vermutet. Auf diese Weise

lassen sich einzelne Aspekte des Datenschutzes, zum Beispiel Speicherung einzelner Personen oder unbefugter Zugriff auf den Datenbestand, bei solchen Verfahren klären, bei denen die Daten am Bildschirm eingegeben, sofort verarbeitet und die Ergebnisse am Bildschirm angezeigt werden. Bei Verfahren, die ohne Bildschirm arbeiten, eignet sich der Test nur in Ausnahmefällen: zum einen wären in der Regel hierfür langwierige Vorbereitungen am Computer notwendig. Zum anderen kann man bei der Anwendung dieser Verfahren nicht mehr mit Testdaten, sondern nur noch mit echten Daten arbeiten, weil sonst die Testdaten automatisch an andere Stellen abgegeben, zum Beispiel Gehälter an fiktive Personen überwiesen würden. Schließlich wäre ein Test nur dann absolut zuverlässig, wenn man alle Kombinationen aller möglichen — und zwar zulässigen und unzulässigen — Eingabedaten eingibt, verarbeitet und die Ergebnisse kontrolliert. Der Aufwand dafür übersteigt jedes vernünftige Maß.

— Kontrolle mit Programmlisten

Jedes Programm, das in einem Computer abläuft, kann man ausdrucken. Mit der dabei entstehenden Programmliste kann man die Datenschutzaspekte eines Programms prüfen. Diese Prüfmethode eignet sich nur, um das Ausmaß eines bereits bekannten Verstoßes gegen den Datenschutz festzustellen. Denn ihr Aufwand ist außerordentlich hoch, weil — wie beim Programmieren selbst — jeder einzelne Programmschritt nachvollzogen wird. Ein Programm besteht in der Regel aus mehreren hundert bis tausend Programmschritten. Ein guter Programmierer kann täglich ca. 20 Schritte programmieren. Die Prüfung der Programmlisten eines Verfahrens, das aus mehreren hundert Programmen bestehen kann, würde also Monate oder gar Jahre dauern.

2. Kontrolle des Programmeinsatzes

Wer bei einem eingesetzten Verfahren welche personenbezogenen Daten von welcher Stelle aus verarbeiten kann, läßt sich vollständig nur anhand der sogenannten Generierungsprogramme feststellen. Diese Generierungsprogramme erstellt das Rechenzentrum, um die Forderungen der Anwender, die technischen Einrichtungen und die erforderlichen Datensicherungsmaßnahmen aneinander anzupassen. Sie sind außerordentlich umfangreich, weil sie eine Vielzahl der technischen Eigenschaften der arbeitenden Computer und ihrer Eingabe- und Ausgabegeräte festlegen, beschreiben und steuern. Auch hat jedes Generierungsprogramm seine eigene Programmiersprache. Die Kontrolle dieser Generierungsprogramme ist deshalb im Ergebnis ebenso schwierig wie die Kontrolle der Programme eines Verfahrens; sie stößt auf dieselben Grenzen.

3. Kontrolle flexibler Verfahren

Besonders schwer ist, bei den Anwendern flexibler Verfahren die Aspekte des Datenschutzes zu kontrollieren. Insbesondere gilt dies für Verfahren, die beliebige Texte über eine große Zahl von Personen speichern und sie auf vielfältige Weise, zum Beispiel über eine bestimmte Person, miteinander verknüpfen können. Diese Flexibilität macht die Verfahren weniger transparent. Während es bei herkömmlichen Verfahren ohne weiteres möglich ist, Zahl und Namen der gespeicherten Personen aufzulisten, geht dies hier nicht in gleicher Weise. Zwar kann man Personen, über deren Namen Textverknüpfungen erfolgen, abrufen, nicht aber Personen, deren

Name nur an einer Textstelle auftritt, über die nicht verknüpft wird. Diese Personen bleiben im Verborgenen — es sei denn, man druckt die gesamte Datenbank aus. Die Auswertung der hierbei in der Regel anfallenden Papierberge ist faktisch nicht möglich.

Es gab bislang keine Bürgereingabe, die ich wegen dieser Grenzen nicht hätte aufklären können. Sie zeigen jedoch, wie wichtig es ist, daß sich die datenverarbeitenden Stellen nicht mit der Existenz einer unabhängigen Datenschutzkontrolle beruhigen, sondern sich im Rahmen ihrer Eigenverantwortung laufend um eine Verbesserung des Datenschutzes bei der elektronischen Datenverarbeitung bemühen.

2. Abschnitt: Erfahrungen aus der Praxis

Ein Schwerpunkt meiner Arbeit im vergangenen Jahr war, die Probleme des Datenschutzes beim Einsatz der elektronischen Datenverarbeitung zu vertiefen. Um zu sehen, ob und wie der Datenschutz von der ersten Phase der Entwicklung eines Verfahrens bis hin zu dessen Anwendung in der täglichen Routine beachtet wird, führte ich Kontrollbesuche bei der Datenzentrale Baden-Württemberg, den Regionalen Rechenzentren Heidelberg und Südlicher Oberrhein in Freiburg, dem Landesamt für Besoldung und Versorgung, der Oberfinanzdirektion Freiburg, den Rechenzentren des Statistischen Landesamts, der Universitäten Karlsruhe und Konstanz und der von den Industrie- und Handelskammern des Landes getragenen Göppinger Arbeitsgemeinschaft für Datenverarbeitung GmbH durch. Informationsbesuche beim Gemeinsamen Rechenzentrum des Sozial-, Justiz- und Wirtschaftsministeriums, dem Regionalen Rechenzentrum Mittlerer Neckar in Stuttgart und den Städten Emmendingen, Leonberg und Weinheim rundeten das Bild ab. Gezielte Kontrollen wegen einzelner automatisierter Datenverarbeitungsvorgänge führte ich beim Landeskriminalamt und zwei Universitäten des Landes durch.

1. Verfahrensentwicklung

Wer automatisierte Verfahren plant und entwickelt, ohne an den Datenschutz zu denken, läuft Gefahr, dies unter Umständen später teuer bezahlen zu müssen. Der Aufwand für nachträgliche Verfahrensänderungen ist ungleich größer. Deshalb steht die Verwaltung ihnen meist kritisch bis ablehnend gegenüber. Schon Kostengründe gebieten, die Aspekte des Datenschutzes bereits zu Beginn der Verfahrensentwicklung zu bedenken. Leider ist dies noch nicht immer der Fall. Vielfach stehen ausschließlich technische Probleme im Vordergrund. So nutzt beispielsweise die Praxis die neuesten technischen Möglichkeiten, zum Beispiel die Direktabfrage über Bildschirm, beschreibt aber nicht eindeutig genug die dabei zu beachtenden Sicherheitsmaßnahmen. Von besonderem Nachteil ist dies für die Verfahrensanwender, weil sie gerade auf solche Informationen angewiesen sind.

1.1 Verfahrensdokumentation

Die Verfahrensdokumentation soll dem Anwender ermöglichen, das Verfahren richtig einzusetzen. Aus ihr muß er zum Beispiel ersehen, wie er personenbezogene Daten sperren und löschen und Kennworte beim Einsatz von Bildschirmen sinnvoll nutzen kann. Sie muß auch beschreiben, welche Datensicherheitsmaßnahmen je nach Sensitivität der Daten zu treffen sind. Nicht alle überprüften Verfahrensdokumentationen erfüllten diese Anforderungen. Nicht wenige Dokumentationen sind so formelhaft und technisch knapp gefaßt, daß sie den Anwender

schlechterdings überfordern. So erwähnt zwar die Datenzentrale in ihrer Verfahrensdokumentation des Verfahrens „Finanzwesen“ und „Einwohnerwesen“ den Einsatz von Kennworten, beschreibt aber ihre Wirkungsweise nicht so eindeutig, daß die Anwender ihre Möglichkeiten voll nutzen können. Sie sagt zum Beispiel nicht, daß man Kennworte häufig ändern kann. Dies aber ist notwendig, um den Zugriff Unbefugter zu verhindern. Sie sagt auch nicht, daß sich die Kennworte eignen, den Zugriff auf bestimmte Mitarbeiter und ausgewählte Daten zu beschränken.

1.2 Programmtests

Trotz meiner wiederholten Hinweise testen viele Stellen ihre Programme immer noch grundsätzlich mit Originaldaten und nicht mit anonymisierten Daten. So verwenden die Regionalen Rechenzentren zum Test der Verfahren der Datenzentrale Kopien von Originaldaten aus Produktionsdateien. Dies ist aus mehreren Gründen problematisch:

- Nach dem Zufallsprinzip ausgewählte Testdaten erfassen in der Regel nicht alle zu prüfenden Fälle.
- Programmierer erhalten ohne Notwendigkeit Zugang zu personenbezogenen Daten.
- Nicht immer ist den beim Test erstellten Listen anzusehen, daß es sich um Testergebnisse handelt. Deshalb besteht die Gefahr, daß sie das Rechenzentrum oder eine andere Stelle als normale Arbeitsergebnisse behandelt.

Programmtests sollen nachweisen, daß alle im Programm vorgesehenen Funktionen richtig ablaufen. Sie sollen also nicht nur die Bedürfnisse des Programmierers abdecken, sondern auch der Stelle, die das Programm in Auftrag gab, eine Kontrolle der richtigen und vollständigen Problemlösung ermöglichen. Deshalb muß der Test alle wesentlichen Variationen eines Verfahrens erproben. Nur so läßt sich prüfen, ob das Verfahren personenbezogene Daten korrekt verarbeitet und eine unkorrekte Verarbeitung abweist.

Um das Testen von Programmen zu erleichtern, schlug ich der Datenzentrale vor, ein landeseinheitliches Verfahren zu entwickeln, das für alle zu testenden Verfahren anonyme Testdaten zur Verfügung stellt. Es soll so ausgestaltet sein, daß die testenden Stellen auch selbst konstruierte Testfälle einspielen können.

2. Verfahrensanwendung

Während die Verfahrensdokumentation beschreibt, was das Verfahren kann und was bei seinem Einsatz zu beachten ist, geht es bei der Verfahrensanwendung um die Umsetzung seiner Regelungen in die Praxis. Beim Einsatz eines automatisierten Verfahrens sind häufig während der einzelnen Phasen der Datenverarbeitung verschiedene Stellen einbezogen. Jede dieser Stellen muß sich bemühen, den Anforderungen des Datenschutzes gerecht zu werden. Dies gilt unabhängig davon, ob sie Daten erhebt, erfaßt, in einem Rechenzentrum oder über Bildschirm vor Ort verarbeitet oder die Arbeitsergebnisse auswertet. Die erfaßten Daten müssen richtig und vollständig sein. Das Rechenzentrum darf nur die Daten verarbeiten, die ihm die autorisierte Stelle überließ. Arbeitsergebnisse muß es an die richtige Stelle geben. Nur Berechtigte dürfen

über Bildschirm auf die Daten zugreifen. Nicht mehr benötigte Daten sind zu löschen. Diesen Anforderungen des Datenschutzes trägt die Praxis noch nicht in ausreichendem Maße Rechnung:

2.1 Datenerfassung

Bei den meisten eingesetzten Verfahren sind die Daten in normierter Form einzugeben. Deshalb muß die datenerfassende Stelle sie entsprechend aufbereiten. Dabei kann sie sich unterschiedlicher Methoden bedienen. Entweder setzt sie auf herkömmliche Weise die Daten in maschinell lesbare Datenträger um oder nutzt sie die moderne Form der Direkteingabe über Bildschirm. Unabhängig hiervon erfordert der Datenschutz, die erfaßten Daten auf ihre Richtigkeit und Vollständigkeit hin zu überprüfen. Daran muß auch die datenverarbeitende Stelle selbst ein Interesse haben. Im Rahmen dieser Kontrolle muß sie feststellen können, wer welche personenbezogenen Daten zu welcher Zeit erfaßt oder direkt über Bildschirm eingegeben hat. Hierfür bieten sich zwei Wege an: Der eine ist die programmgesteuerte Protokollierung aller Eingaben. Diese Methode ist sehr kostenaufwendig, weil bei jeder gespeicherten Person zusätzlich im Computer festgehalten werden muß, wer wann welches ihrer gespeicherten Daten eingab bzw. änderte. Der andere Weg ist, die Erfassungsbelege entsprechend zu kennzeichnen. Er ist wesentlich billiger und erfüllt in der Regel auch den angestrebten Zweck.

Noch nicht alle Stellen sind sich ihrer Verantwortung für die Richtigkeit und Vollständigkeit der erfaßten Daten bewußt. Insbesondere unterstellen viele Behörden, daß die Programme Plausibilitätskontrollen enthalten und damit das Verarbeiten falsch erfaßter Daten weitgehend verhindern. Wie sich dieses mangelnde Bewußtsein der eigenen Verantwortung bei der Datenerfassung auswirkt, sollen folgende Beispiele belegen:

- Eine Industrie- und Handelskammer vernichtete die Erfassungsbelege bereits vor der Verarbeitung der erfaßten Daten im Rechenzentrum. Deshalb war nicht mehr möglich, durch einen Vergleich der Verarbeitungsergebnisse mit den Erfassungsbelegen festzustellen, ob hierbei unrichtige Daten verarbeitet wurden.
- Ein Erfassungsprogramm des von der Datenzentrale entwickelten Verfahrens „Krankenhauswesen“ vergibt zum Zweck der Eingabekontrolle automatisch für alle Gerätebediener das Kennzeichen „01“ und für alle Bildschirme die Nummer „001“. Diese Methode verdient nicht, Eingabekontrolle genannt zu werden. Sie läßt nicht erkennen, wer von wo Daten eingegeben hat. Dies muß aber bis zur Verarbeitung der Daten im Rechenzentrum möglich sein. Die Datenzentrale wird ihr Erfassungsprogramm in diesem Sinne ändern.
- Hält man bei der Datenerfassung für das von der Datenzentrale entwickelte Verfahren „Finanzwesen“ bestimmte Reihenfolgen nicht ein, können falsche Kontrollsummen und damit der Eindruck entstehen, als ob Daten nicht richtig erfaßt worden seien. Ein weiterer Mangel des Verfahrens ist, daß ein absichtlicher oder versehentlicher Druck auf eine bestimmte Funktionstaste am Erfassungsgerät dazu führt, daß keine Prüfung der gerade erfaßten Daten stattfindet. Diese Mängel sind auf Schwächen im Betriebssystem der Datenerfassungsgeräte zurückzuführen. Deshalb ist es Sache des Herstellers, hier umgehend Abhilfe zu schaffen.

- Mangelhaft ist auch ein Datenerfassungsprogramm des von der Datenzentrale entwickelten Verfahrens „Personalwesen“. Durch schlichten Druck auf eine Taste ist es möglich, alle erfaßten Daten zu zerstören. Die ganze Datenerfassung muß wiederholt werden. Mein Hinweis auf diesen Fehler führte zu einer Änderung des Datenerfassungsprogramms.

2.2 Kennworte

Mit Hilfe von Kennworten läßt sich die Gefahr verringern, daß Unbefugte auf personenbezogene Daten zugreifen. Kennworte kann man für einzelne Geräte (z. B. Bildschirm, Datenstation), für einzelne Organisationseinheiten von Behörden (zum Beispiel für die Personalstelle), für einzelne Verfahren (zum Beispiel das Verfahren „Kommunales Finanzwesen“), für einzelne Funktionen (z. B. nur Datenabfrage oder Datenabfrage und -änderung) und für einzelne Personen vergeben. Am schwächsten ist die Schutzfunktion gerätebezogener Kennworte. Hier kann jeder, der das Kennwort kennt, auf die personenbezogenen Daten zugreifen, die dem Gerät zugeordnet sind. Den besten Schutz bieten personenbezogene Kennworte. Hier hat grundsätzlich nur sein Inhaber Zugriff. Damit Kennworte ihre volle Wirkung entfalten können, müssen folgende Grundvoraussetzungen erfüllt sein:

- Das Kennwort darf bei seiner Eingabe auf dem Bildschirm nicht sichtbar sein. Leider ist dies längst nicht immer der Fall.
- Bildschirmverfahren müssen die mit der Eingabe des Kennworts eröffnete Zugriffsberechtigung automatisch zurücknehmen, wenn über den Bildschirm eine bestimmte Zeit lang keine Datenverarbeitung erfolgte. Auf diese Weise läßt sich verhindern, daß Unbefugte den Bildschirm nutzen, wenn der Kennwortinhaber vorübergehend mit ihm nicht arbeitet, es aber versäumt hat, seine Berechtigung zurückzunehmen.
- Kennworte sind häufig zu wechseln, um zu verhindern, daß Unbefugte sie ausforschen und mißbräuchlich nutzen. Wie häufig diese Änderung geschieht, sollte grundsätzlich Sache seines Inhabers sein. Unabhängig hiervon sollte eine automatisierte Kontrolle vorsehen, daß die Gültigkeit des Kennworts nach einer bestimmten Zeit oder einer bestimmten Zahl von Zugriffen erlischt.

Wie man das Kennwort ausgestaltet, hängt von den einzelnen eingesetzten Verfahren ab. Kennworte können numerisch oder alphabetisch sein oder aus einer Kombination von Ziffern und Buchstaben bestehen. Auch ihre Länge ist variabel. Ein kurzes Kennwort erleichtert zwar die Eingabe, erhöht aber auch die Gefahr des Ausforschens.

2.2.1 Einsatz von Kennworten

Die Verwaltungspraxis setzt Kennworte in unterschiedlicher Weise ein:

- Die Informationssysteme der Polizei und der Steuerverwaltung kennen keinen Kennwortschutz. Deshalb kann nach Einschalten des Bildschirms jeder auf die Daten zugreifen, die dem Gerät zugeordnet sind.

Zwischen beiden Informationssystemen besteht jedoch ein wesentlicher Unterschied: Während jedes der 80

Finanzämter des Landes nur auf die von ihm selbst eingegebenen Daten Zugriff hat, haben die 22 000 Polizeibeamten im Lande über die Datenstationen die Möglichkeit, alle in der Personenauskunftsdatei gespeicherten ca. 700 000 Straftäter mit ca. 1,5 Millionen Straftaten abzurufen.

- Auf das Personalinformationssystem der Oberfinanzdirektion Freiburg kann nur ihre Personalstelle mit dem ihr zugeordneten Kennwort zugreifen.
- Das von der Datenzentrale entwickelte Verfahren „Kommunales Finanzwesen“ kennt die personenbezogene Vergabe von Kennworten. Damit stellt es sicher, daß zum Beispiel nur ein bestimmter Kassenbeamter über einen bestimmten Bildschirm einer bestimmten Dienststelle auf bestimmte ausgewählte Daten zugreifen kann. Diese Art von Kennwortvergabe ist vorbildlich.

2.2.2 Kennworte bei polizeilichen Landesinformationssystemen

Weil die Polizei in ihren Informationssystemen höchst sensible Daten verarbeitet, ist ein Kennwortschutz unerläßlich. Ich schlug dem Innenministerium deshalb vor, personenbezogene Kennworte oder Ausweisleser einzuführen. Hierbei bedachte ich sehr wohl die wirtschaftlichen, organisatorischen und polizeilichen Aspekte dieses Vorschlags. Nach dem derzeitigen Stand will das Innenministerium meinen Vorschlägen nur zum Teil folgen:

- Das Innenministerium erwägt, halbjährlich wechselnde datenstationsbezogene Kennworte einzuführen. Dies ist nicht ausreichend. Es liegt auf der Hand, daß ein so gestaltetes Kennwort innerhalb kurzer Zeit einem verhältnismäßig großen Personenkreis bekannt wird und damit seine Schutzfunktion verliert. Andererseits verstehe ich gut, daß sich das Innenministerium aus Kostengründen nicht in der Lage sieht, Ausweisleser einzuführen, wie es bereits bei den polizeilichen Informationssystemen von Berlin und Niedersachsen üblich ist. Dann aber bleibt wegen der Sensitivität der gespeicherten Daten kein anderer Weg als der des personenbezogenen Kennworts. Diese personenbezogenen Kennworte müßten zusätzlich bestimmten Datenstationen und bestimmten Verfahren zugeordnet werden. Der Kennwortinhaber muß sie jederzeit ändern können. Der Ablauf ihrer Gültigkeit ist automatisiert zu überwachen. Ein nicht fristgerecht geändertes Kennwort ist außer Kraft zu setzen.
- Das Innenministerium erwägt, einen Bildschirm, der durch Eingabe eines Kennworts einsatzbereit ist, automatisch abzuschalten, wenn über ihn eine Stunde lang keine Datenverarbeitung erfolgte. Dies ist aus zwei Gründen ungenügend. Zum einen ist nicht notwendig — wie das Innenministerium meint —, das Datensichtgerät ganz abzuschalten. Es genügt, die Zugriffsberechtigung zurückzunehmen. Zum anderen ist die Rücknahme frühestens nach einer Stunde erheblich zu spät. Sie sollte ungefähr nach 15 Minuten erfolgen. Die Zeit für die Wiederaufnahme des Dialogs durch neue Eingabe des Kennworts beträgt maximal drei Sekun-

den. Dadurch leidet die Auskunftsbereitschaft des polizeilichen Informationssystems nicht.

- Das Innenministerium ist bereit, Eindringversuche in das polizeiliche Informationssystem im Rechenzentrum des Landeskriminalamts zu protokollieren. Dies allein reicht jedoch nicht aus. Notwendig ist vor allem, die betroffene Polizeidienststelle unverzüglich über den Eindringversuch zu informieren, damit sie weitere Schritte einleiten kann.

2.3 Löschen und Auslagern

Das fristgerechte Löschen von personenbezogenen Daten ist ein zentrales Anliegen des Datenschutzes. Die meisten der mir bekannten Verfahren sehen zwar generell eine Löschung vor. Unklar ist jedoch vielfach, wann sie zu erfolgen hat. Insbesondere enthalten einige Verfahrensdokumentationen der von der Datenzentrale entwickelten Verfahren keine klare Aussage, wie lange die Daten zu speichern sind. Wegen dieses Mangels verfahren die einzelnen Rechenzentren unterschiedlich. Die meisten löschen Daten in aktuellen Dateien nur, wenn sie Kapazitätsgründe dazu zwingen. Je größer ihre Speicherkapazität ist, desto geringer ist damit die Notwendigkeit zur Löschung. Zwingen sie Kapazitätsprobleme schließlich zum Handeln, löschen sie die Daten nicht endgültig, sondern löschen sie nur in der aktuellen Datei, speichern sie aber erneut — zum Teil in vollem Umfang — auf „Archivbänder“. Folge dieser sogenannten Auslagerung ist, daß für einzelne Verfahren umfangreiche „Datenfriedhöfe“ entstehen. Dies ist um so gefährlicher, als die Daten auf den Archivbändern nicht einmal gesperrt, also nicht dem allgemeinen Zugriff entzogen sind. Es ist ohne weiteres möglich, die Daten nach wie vor uneingeschränkt zu verarbeiten. Zwei Beispiele sollen dies verdeutlichen:

- Jedes Krankenhaus, das das von der Datenzentrale entwickelte Verfahren „Krankenhauswesen“ einsetzt, löscht zwar nach Abschluß der Behandlung und Abrechnung der Leistungen mit dem Kostenträger die Daten des Patienten in der aktuellen Datei. Es bewahrt sie jedoch auf einem in diesem Zusammenhang erstellten Archivband noch 30 Jahre auf. Die Datenzentrale meint, dies sei notwendig, um bei rückwirkenden Pflegesatzänderungen die erbrachten Leistungen neu berechnen zu können. Ich halte eine so lange Speicherung nicht für erforderlich. Auch ist mir keine Rechtsvorschrift bekannt, die dies rechtfertigen könnte. Ich forderte deshalb von der Datenzentrale, die Aufbewahrungsfrist erheblich abzukürzen. Außerdem verlangte ich von den Regionalen Rechenzentren, daß sie ihre Archivbänder mit solchen Patientendaten sperren.
- Zahlreiche Bußgeldstellen, z. B. der Bürgermeisterämter Stuttgart, Ulm, Heidelberg, Konstanz und Waiblingen, der Landratsämter Böblingen, Rems-Murr-Kreis und Heilbronn und des Regierungspräsidiums Karlsruhe, wickeln die Verfahren wegen Verkehrsordnungswidrigkeiten automatisiert ab. Sie speichern jeden Verkehrsteilnehmer wegen jeden Verstoßes, der zu einem Verwarnungsgeld oder einer Geldbuße führt, in ihrer „Ordnungswidrigkeiten-Datei“. Bei Kontrollbesuchen eines Regionalen Rechenzentrums und einer Bußgeldstelle stellte ich fest, daß diese „Ordnungswidrigkeiten-Datei“ nicht nur Daten über laufende Bußgeldverfahren, sondern auch über seit langem abgeschlos-

sene oder ruhende Verfahren enthält, und man diese Daten im Direktzugriff über Bildschirm abrufen kann. Ich halte diesen Zustand für bedenklich, weil durch die längerfristige Datenspeicherung eine Art von örtlicher Verkehrsünderdatei entsteht. Das Führen besonderer Unterlagen auf örtlicher Ebene, die ausschließlich zur Erkennung von Mehrfachtätern dienen, ist jedoch unzulässig. Dies sagt auch das Innenministerium in einem Erlaß. Ich forderte das Regionale Rechenzentrum auf, alle abgeschlossenen Ordnungswidrigkeitenfälle umgehend zu sperren und in Absprache mit den Bußgeldstellen die Aufbewahrungszeit für diese Daten entscheidend zu verkürzen. Die Datenzentrale ist außerdem bereit, ihre Verfahrensdokumentation durch eindeutige Anweisungen zu ergänzen.

3. Archivverwaltung

Jeder, der elektronische Datenverarbeitung betreibt, unterhält im allgemeinen ein Archiv, in dem er alle Datenträger aufbewahrt, die gerade nicht im Einsatz sind. Maßnahmen des Datenschutzes müssen verhindern, daß Unbefugte Datenträger mit personenbezogenen Daten aus den Archiven entfernen und diese nutzen. Außerdem muß jederzeit feststellbar sein, auf welchem Archivband sich welche Daten befinden, wie lange diese aufzubewahren sind und wo das Archivband konkret lagert. Die Regionalen Rechenzentren setzen wegen der großen Zahl von Archivbändern — in einem waren es ca. 4800 — häufig automatisierte Verwaltungssysteme ein. Sie ermöglichen, Bestandsverzeichnisse zu erstellen, und erleichtern Bestandskontrollen.

Auch bei der Archivverwaltung mangelt es öfter noch an den erforderlichen Datenschutzmaßnahmen. In einem Regionalen Rechenzentrum, das ich kontrollierte, waren häufig weder die Archivräume noch die Magnetbandschränke abgeschlossen. Nicht einmal geregelt war, wer wann zu welchem Zweck welche Archivbänder entnehmen durfte. Alle Mitarbeiter des Rechenzentrums und manchmal sogar Kunden und Besucher konnten das Archiv betreten. Während des Kontrollbesuchs entnehmen nicht nur Mitarbeiter, sondern auch ein Kunde Archivbänder, ohne nachweisen zu müssen, daß sie sie zur Erfüllung ihrer Aufgaben benötigen. Selbst die Liste der archivierten Bänder war nicht unter Verschuß, so daß es nicht besonders schwer war, sich über den Datenbestand des Rechenzentrums zu informieren. Niemand kontrollierte, ob der Archivbestand mit dem Inhalt dieser Liste übereinstimmt. Auch diese Mängel will das Rechenzentrum beheben. Vor allem wird es festlegen, wer für den Ablauf des gesamten Betriebs im Archiv verantwortlich ist und wer Zutritt zum Archiv hat. Ebenso will es in Zukunft in unregelmäßigen Abständen den ganzen Archivbestand auf seine Vollständigkeit hin überprüfen.

4. Auftragsdatenverarbeitung

Nur wenige Behörden können ihre automatisierte Datenverarbeitung völlig in eigener Regie betreiben. Die meisten sind darauf angewiesen, daß ihnen andere Stellen die benötigten Verfahren entwickeln und sie bei deren Anwendung unterstützen. Im allgemeinen weiß, wer einen Auftrag übernimmt, daß er sich an die Vorstellungen seines Auftraggebers halten muß. So sieht es auch das Landesdatenschutzgesetz: auftragnehmende Stellen dürfen personenbezogene Daten nur im Rahmen der Weisungen der auftraggebenden Stelle verarbeiten. Dieser Tatsache sind sich aber leider längst nicht alle öffentlichen Stellen bewußt. Weil sie oft

andere Stellen einschalten, um deren Spezialwissen und technische Einrichtungen zu nutzen, tun sie alles, was diese ihnen raten. Überspitzt gesagt: manche Auftraggeber werden im Rahmen der Weisungen ihrer Auftragnehmer tätig. Diese Einstellung hat für den Bürger negative Auswirkungen. Auf seine Frage, warum die Gemeinde über ihn bestimmte Daten erhebt und speichert, bekommt er lediglich zur Antwort, dies sei Folge des Einsatzes der automatisierten Datenverarbeitung. Hinter dieser nichtssagenden Auskunft verbirgt manche Gemeinde ihre Unkenntnis über die Arbeitsweise des von ihr eingesetzten Verfahrens und die dabei verarbeiteten personenbezogenen Daten. Ähnliches läßt sich auch auf anderer Ebene beobachten. Die Finanzämter des Landes und des Landesamts für Besoldung und Versorgung bedienen sich zur Erledigung ihrer Aufgaben der Rechenzentren der Oberfinanzdirektionen. Ihnen ist meist nicht bewußt, daß sie damit Auftraggeber der Oberfinanzdirektion sind, nach deren Weisungen sie sich beim üblichen Verwaltungsvollzug zu richten haben. Wiederholt trug ich dieses Problem an das Finanzministerium heran. Meine konkreten Vorschläge liegen ihm seit einem Jahr auf dem Tisch. Sein Schweigen kann ich mir nur noch mit seinen Schwierigkeiten erklären zu realisieren, daß es im Bereich der Verarbeitung personenbezogener Daten neben dem hierarchischen Weisungsrecht von oben nach unten auch Weisungen von unten nach oben gibt.

5. Dienstprogramme

Jedes Rechenzentrum braucht eine „Feuerwehr“, um in Notfällen funktionsfähig zu bleiben. Diesem Ziel dient der Einsatz sogenannter Dienstprogramme (Utilities). Mit ihnen ist es möglich, spontan Daten aller Art auch dann zu verarbeiten, wenn es kein spezielles Programm für die plötzlich notwendig werdende Datenverarbeitung gibt. Solche Dienstprogramme stellen den Datenschutz vor erhebliche Probleme. Mit ihnen kann man nämlich z. B. Magnetbänder kopieren, den Inhalt einer Datei verändern oder ausdrucken, ohne daß dies jemand merkt. Wie leicht es dazu kommen kann, erlebte ich auf drastische Weise: eines Tages landete auf meinem Schreibtisch ein Paket mit EDV-Ausdrucken eines staatlichen Rechenzentrums, die ein Bürger auf dem Müll gefunden haben will. Bei den Listen handelte es sich um das Telefonverzeichnis, eine Ausbildungsübersicht und die Haushaltsüberwachungsliste eines Rechenzentrums. Dies hatte den Ausdruck und Verlust der Listen überhaupt nicht bemerkt. Der Vorfall gab auch dem Rechenzentrum zu denken. Aus Gründen des Datenschutzes ist notwendig, den Einsatz von Dienstprogrammen auf das unbedingt notwendige Maß zu beschränken, ihn in die automatisierte Protokollierung einzubeziehen und die Notwendigkeit ihres Einsatzes mindestens stichprobenweise zu prüfen.

3. Abschnitt: Entwicklungstrends

Die Abhängigkeit der öffentlichen Verwaltung von der elektronischen Datenverarbeitung wird zusehends zum Risiko für den Datenschutz. Die technischen Schwachstellen nehmen an Zahl und Bedeutung zu, weil

- der Trend weg von der Akte hin zur ausschließlichen Speicherung personenbezogener Daten im Computer geht,
- immer weniger Verfahren isoliert und immer mehr in gegenseitiger Abhängigkeit ablaufen und damit die Fehler eines Verfahrens in den anderen Verfahren weitere Fehler verursachen,

- die Anpassung der Verfahren wegen ihrer zunehmenden Komplexität an tatsächliche und rechtliche Änderungen fehleranfälliger ist,
- über Bildschirm immer mehr Personen Daten der Datenbanken abrufen und teilweise auch ändern können,
- die Fehlersuche bei komplexen Systemen schwieriger und zeitaufwendiger ist.

Je weiter diese Entwicklung voranschreitet, um so größer ist auch die Gefahr, daß die Verarbeitung personenbezogener Daten nicht den Erfordernissen des Datenschutzes Rechnung trägt. Ziel muß sein, solche Risiken möglichst mit Hilfe der Technik zu reduzieren.

1. Pflege von Programmen

Jedes eingesetzte Programm steht nicht ein für allemal fest, sondern ist laufend den neuen Gegebenheiten anzupassen. Die heute übliche Programmpflege weist vor allem folgende Sicherheitslücken auf:

- Wird ein Programm mehrfach geändert, weiß man nicht mehr, wer welche Änderung zu welcher Zeit und aus welchem Anlaß vorgenommen hat.
- Es ist nur sehr schwer möglich, frühere Programmversionen herzustellen und ablaufen zu lassen. Dies ist aber unverzichtbar, wenn zum Beispiel beim Ablauf eines neu geänderten Programms plötzlich Fehler auftreten.
- Da die Programmübersicht häufig nicht vollständig ist, läßt sich nur unter großem Aufwand ermitteln, welche Programme tatsächlich im Einsatz sind.

Ein Regionales Rechenzentrum analysierte das Risiko dieser Schwachstellen. Es entwickelte eine neue Konzeption der Programmpflege mit dem Ziel, nicht nur diese zu beheben, sondern zugleich auch die Arbeit der Programmierer generell zu erleichtern und Kosten zu sparen. Dieses Ziel ließ sich realisieren, weil das Rechenzentrum ein dafür besonders geeignetes Betriebssystem einsetzt. Es protokolliert jede einzelne Änderung jedes Programms und den Zeitpunkt dieser Änderung. Dadurch ist möglich, auf frühere Programmversionen zurückzugehen und eine vollständige Programmübersicht zu erstellen. Das Rechenzentrum glaubt aufgrund seiner bisherigen Erfahrungen, daß sein neues System zur Programmpflege die Sicherheit seiner Datenverarbeitung entscheidend erhöhte.

2. Fernwartung

Programm- oder Maschinenfehler können den Ablauf der Datenverarbeitung empfindlich stören. Wenn der Hersteller derartige Fehler beheben muß, geschieht dies herkömmlicherweise auf zwei Wegen:

- Der Hersteller sucht im Rechenzentrum den Fehler und erhält dabei Einblick in alle Datenverarbeitungsvorgänge, die mit dem Fehler zusammenhängen können.
- Das Rechenzentrum übergibt dem Hersteller Ausdrucke über alle Vorgänge, in denen der Fehler sein kann.

Bei beiden Wegen sieht der Hersteller weitaus mehr Verarbeitungsvorgänge mit personenbezogenen Daten, als er an sich zur Fehlersuche und -behebung sehen muß.

Die Hersteller entwickelten vor einigen Jahren ein Fernwartungskonzept, das ihnen zwar die Fehlersuche erheblich erleichtert, aber den Datenschutz vor neue Probleme stellt: Sobald ein Fehler auftritt, stellen Rechenzentrum und Hersteller eine Verbindung zwischen einem Bildschirm des Herstellers und dem Computer im Rechenzentrum her. Der Hersteller sucht über seinen Bildschirm im Dialog mit dem Computer des Rechenzentrums den Fehler. Ohne besondere Sicherheitsvorkehrungen kann er dabei beliebige personenbezogene Daten eingeben und die im Computer des Rechenzentrums befindlichen Daten abrufen und ändern. Das Rechenzentrum bemerkt dies längst nicht in jedem Fall. Unter dem Aspekt des Datenschutzes ist dies völlig unannehmbar. In Betracht kommt deshalb nur ein Fernwartungskonzept, das zumindest folgende Datensicherungsmaßnahmen bietet:

- Der Hersteller muß sich beim Rechenzentrum anmelden und ein Kennwort eingeben, bevor er den Dialog mit dem Computer beginnt.
- Jedes Rechenzentrum muß festlegen können, in welchem Umfang der Hersteller Einblick in die Datenverarbeitungsvorgänge erhält. Dies kann auf folgende Weise geschehen:
 - Der Hersteller darf nur die Daten kontrollieren, die Auskunft über die Arbeitsweise der Maschine und ihrer angeschlossenen Ein-/Ausgabegeräte geben. In diesem Fall ist ausgeschlossen, daß er personenbezogene Daten abrufen und selbst ändert.
 - Der Hersteller darf zusätzlich Fehler im Betriebssystem suchen. In diesem Fall kann es sein, daß er personenbezogene Daten und Kennworte in Einzelfällen sieht. Deshalb muß das Rechenzentrum vor Beginn der Fernwartung zumindest sensitive personenbezogene Daten vorsorglich von der Maschine nehmen. Außerdem muß es alle Kennworte, die der Hersteller erfährt, durch andere ersetzen.
- Das Rechenzentrum protokolliert für seine Kontrolle alle Daten, die der Hersteller im Rahmen der Fernwartung an seinem Bildschirm eingibt und abrufen.
- Das Rechenzentrum muß die Verbindung zwischen seinem Computer und dem Bildschirm des Herstellers jederzeit trennen können.

3. Reduzierung der Akten

Das herkömmliche Arbeitsmittel der öffentlichen Verwaltung ist die Akte. Hieran hat der Einsatz der elektronischen Datenverarbeitung im Prinzip nichts geändert. Aus der Akte ist nach wie vor das ganze Verwaltungshandeln zu ersehen, auch wenn es teilweise automatisiert erfolgte. Insbesondere gibt die Akte Auskunft, welche Daten die Verwaltung sich über einen Bürger beschaffte, wie sie sie verarbeitete und in welchem Umfang sie diese noch vorrätig hält.

Neuerdings versucht man, Arbeitsvorgänge möglichst nur noch im Computer durchzuführen. Schriftliche Unterlagen hierüber sollen nur im Ausnahmefall, zum Beispiel bei Prozessen, in die Akten kommen. Erste Ansätze dieser Entwicklung finden sich bei der begonnenen Automatisierung des Führerscheinwesens. Die kommunale Datenverarbeitung Mittlerer Neckar erwägt, in Zukunft zum Beispiel folgende Vorgänge ausschließlich automatisiert abzuwickeln:

- Die Gemeinde gibt die Personalien des Führerscheinbewerbers und ihre Stellungnahme zu seiner Eignung an ihrem Bildschirm

ein. Die Führerscheinbehörde läßt sich diese Äußerungen an ihrem Bildschirm anzeigen, ehe sie über den Antrag auf Erteilung der Fahrerlaubnis entscheidet. Damit entfällt die bislang übliche schriftliche Stellungnahme der Gemeinde, welche die Führerscheinbehörde in ihre Akten nahm.

- Die Führerscheinbehörde holt die Auskünfte beim Kraftfahrt-Bundesamt über etwaige Eintragungen des Führerscheinbewerbers durch Austausch von Magnetbändern ein und läßt sie am Bildschirm anzeigen. Damit entfällt der bislang übliche Schriftverkehr zwischen Führerscheinbehörde und Kraftfahrt-Bundesamt.

Jede papierlose Speicherung bedeutet zusätzliche Gefahren für den Umgang mit personenbezogenen Daten. Es ist nicht mehr möglich, sie mit der Akte zu vergleichen und festzustellen, wer Daten eingegeben hat, ob dabei Fehler passierten und ob jemand die Daten unzulässig verarbeitete. Um diese Vorgänge auch bei solchen Verarbeitungsmethoden feststellen zu können, ist notwendig, besondere Datensicherungsmaßnahmen zu treffen. Zumindest folgendes ist erforderlich:

- Die Eingabekontrolle muß automatisiert erfolgen. Dazu protokolliert man entweder in einer eigenen Protokolldatei, wann welche Daten eingab, oder man speichert zusätzlich zu den Daten den Zeitpunkt ihrer Eingabe und den Sachbearbeiter. Je nach Art des Verfahrens reicht es aus, jeweils nur die Information über die letzte Änderung vorzuhalten.
- Am Bildschirm darf nur arbeiten, wer sich mit einem persönlichen Kennwort ausweisen kann. Dies muß das Verfahren laufend oder zumindest bei bestimmten Anlässen weiter prüfen.
- Um Verarbeitungsfehler feststellen und beheben zu können, sind die einzelnen Datenverarbeitungsvorgänge zu protokollieren.

4. Abschnitt: Bildschirmtext

Zusätzliche Möglichkeiten, die elektronische Datenverarbeitung zu nutzen, bieten die neuen Medien. Dazu zählen insbesondere Videotext, Bildschirmtext und Kabelfernsehen. Im Vordergrund des Interesses steht Bildschirmtext. Die Deutsche Bundespost beabsichtigt, dieses neue Informations- und Kommunikationssystem ab September 1983 stufenweise bundesweit einzuführen.

1. Beschreibung von Bildschirmtext

Bildschirmtext soll grundsätzlich jeder nutzen können. Mit diesem System kann man über die öffentlichen Fernmeldenetze textorientierte Informationen und andere Dienste abrufen oder Mitteilungen an bestimmte andere Teilnehmer übermitteln. Der Teilnehmer ruft sie in der Regel über einen Fernsprechananschluß mit einem Sichtgerät ab. Ein Modem transformiert dabei die zu übertragenden Informationen an die Anforderungen des Fernsprechnetzes. Ein „Bildschirmtext-Decoder“ speichert jeweils die Information und wandelt sie in stehende Texte und Grafiken, die sogenannten Bildschirmtextseiten um. Zum Abruf und zur Eingabe der Informationen benutzt der Teilnehmer in der Regel die Eingabetastatur des Sichtgeräts oder die entsprechend eingerichtete Fernbedienung des Fernsehempfängers.

2. Vorhaben der Deutschen Bundespost

Das Bildschirmtextsystem der Deutschen Bundespost besteht aus einer Bildschirmtextzentrale in Ulm, mit ihr verbundenen Bildschirmtextvermittlungsstellen (Ortsnetzen), die der Teilnehmer über Telefon anwählt, und an das System angeschlossenen externen Rechnern. In der Bildschirmtextzentrale können die Anbieter Informationen zum kostenlosen oder entgeltlichen Abruf durch alle Teilnehmer speichern. Sie können ihre Informationen auch auf einem externen Rechner führen. Er bietet den Anbietern darüber hinaus zwei weitere Möglichkeiten:

- Die Anbieter können den Abruf der Information auf bestimmte Teilnehmergruppen oder einzelne Teilnehmer, zum Beispiel die Kunden eines Versandhauses, beschränken.
- Sie können bestimmten Teilnehmergruppen oder einzelnen Teilnehmern den Dialog mit dem externen Rechner ermöglichen, zum Beispiel den Bankkunden zur Abwicklung ihrer Bankgeschäfte.

Die Deutsche Bundespost will den Teilnehmern ferner ermöglichen, Mitteilungen als „elektronische Postkarten“ an andere Teilnehmer zu senden.

3. Datenschutzprobleme

Die Einführung von Bildschirmtext bringt eine Reihe von datenschutzrechtlichen Gefahren mit sich. Ihr Ausmaß läßt sich abschließend erst nach längerem Einsatz des Systems beurteilen. Sicher ist jedoch schon jetzt, daß es zur Anlegung umfangreicher Sammlungen personenbezogener Daten in der Bildschirmtextzentrale und in den externen Rechnern kommt:

- In der Bildschirmtextzentrale speichert die Deutsche Bundespost alle zum Betrieb von Bildschirmtext notwendigen Daten. Für jeden Bildschirmtextteilnehmer sind dies zumindest
 - die Grunddaten
zum Beispiel Name, Anschrift und Telefonnummer
 - die Abrechnungsdaten
sie setzen sich zusammen aus den Grundgebühren, den Entgelten für die aus der Bildschirmtextzentrale oder den externen Rechnern abgerufenen kostenpflichtigen Informationen und den Gebühren für Mitteilungen;
 - der Inhalt der zugesandten und verschickten Mitteilungen.
- Im externen Rechner können über alle Teilnehmer, die im Rahmen eines Vertrags- oder vertragsähnlichen Verhältnisses mit ihm kommunizieren, personenbezogene Daten anfallen.

Aus den so entstehenden Datensammlungen läßt sich nicht nur eine Vielzahl von für sich genommen harmlosen Einzeldaten gewinnen. Vielmehr können die Einzeldaten ohne Schwierigkeiten zusammengefaßt werden mit der Folge, daß umfassende Interessen- oder gar Persönlichkeitsprofile über den Benutzer entstehen. Dies ist vor allem möglich, wenn man die Abrechnungsdaten entsprechend auswertet. Dabei läßt sich feststellen,

- von welchen Anbietern der Teilnehmer Informationen abrief,
- an welcher Art von Information er interessiert war,
- wie häufig er die einzelnen Informationen abrief und
- zu welcher Zeit dies geschah.

Schon dieses Wissen genügt, seine Interessen und Sehgewohnheiten zuverlässig zu beurteilen. Mit keinem konventionellen Medium kann man eine vergleichbar sichere Aussage darüber treffen.

Eine weitere Gefahr für den Persönlichkeitsschutz ist, daß diese Datensammlungen über ihren ursprünglichen Zweck hinaus für eine Vielzahl anderer Zwecke verwendet werden können.

4. Zielvorstellungen des Datenschutzes

Meine Zielvorstellungen hierzu stellte ich bereits in meinem 1. Tätigkeitsbericht dar. Die Konferenz der Datenschutzbeauftragten der Länder und des Bundes beschloß entsprechende Grundsätze für den Datenschutz bei den Neuen Medien. Die Kernpunkte sind:

- Die Deutsche Bundespost darf als Betreiber von Bildschirmtext personenbezogene Daten über die Inanspruchnahme von Bildschirmtext nur erheben und speichern, soweit und solange dies erforderlich ist, um den Dialog mit Bildschirmtext und den externen Rechnern zu ermöglichen und die erbrachten Leistungen abzurechnen.
- Aus den Abrechnungsdaten darf nicht hervorgehen, wann, wie lange und wie oft welcher Teilnehmer auf welche Weise Bildschirmtext in Anspruch nahm.
- Personenbezogene Daten des Teilnehmers dürfen nur an Anbieter und nur dann übermittelt werden, wenn dies wegen der Art der vom Teilnehmer geforderten Leistung erforderlich ist. Dies gilt insbesondere für die Abrechnungsdaten. Sie dürfen demnach nicht an Anbieter oder an andere Dritte weitergegeben werden.
- Abrechnungsdaten sind zu löschen, sobald sie zur Abrechnung nicht mehr erforderlich sind.
- Der Schutz der bei Bildschirmtext anfallenden Daten darf nicht auf die Verarbeitung in Dateien beschränkt werden.
- Der Anbieter darf vom Teilnehmer personenbezogene Daten nur erheben und diese speichern, wenn das Erbringen der Leistung oder die Abwicklung des Vertragsverhältnisses andernfalls unmöglich wäre. Diese Daten dürfen nur im Rahmen der Zweckbestimmung der vereinbarten Leistungen verarbeitet werden — es sei denn, der Betroffene willigt in eine weitergehende Verarbeitung ein.
- Personenbezogene Daten, die zur Steuerung des Dialogs zwischen Teilnehmer und Bildschirmtextzentrale bzw. externem Rechner vorübergehend gespeichert werden müssen, sind unmittelbar nach Beendigung des Dialogs zu löschen.
- Es sind technische und organisatorische Maßnahmen zu treffen, die die Einhaltung dieser Anforderungen sicherstellen.

5. Entwurf eines Staatsvertrags über Bildschirmtext

Diese Zielvorstellungen trug ich an das Staatsministerium heran, das zur Zeit zusammen mit den anderen Ländern einen Staatsvertrag über Bildschirmtext vorbereitet. Dieser Staatsvertrag soll in der Bundesrepublik einheitliche Rahmenbedingungen für die Nutzung von Bildschirmtext schaffen.

Der erste Entwurf eines Staatsvertrags, der Vorschriften zum Datenschutz enthielt, entsprach zu einem Gutteil meinen Zielvorstel-

lungen. In der zentralen Frage der Abrechnung wich er hiervon jedoch ab. Er sah nämlich vor:

- Die Deutsche Bundespost darf über jeden Teilnehmer zu Abrechnungszwecken speichern, wann, wie lange und wie oft er auf welche Weise Bildschirmtext in Anspruch nahm. Die Speicherung soll allerdings so erfolgen, daß dies „nicht erkennbar“ ist.
- Sie darf Abrechnungsdaten an Anbieter übermitteln, soweit dies „zur Beitreibung von Forderungen erforderlich ist.“ Die Datenschutzbeauftragten der Länder und des Bundes hielten diese Regelungen für bedenklich. Sie bekräftigten deshalb erneut ihre Auffassung, daß keine aufgeschlüsselten Abrechnungsdaten gespeichert werden dürfen und eine Übermittlung an Anbieter unterbleiben muß. In diesem Sinne wandte ich mich an den Herrn Ministerpräsidenten. Er hatte in einem Zeitungsinterview die Bedeutung des Datenschutzes bei Bildschirmtext „angesichts der nahezu grenzenlosen technischen Möglichkeiten und des sehr sensiblen Bereichs des Persönlichkeitsschutzes“ betont und in diesem Zusammenhang erklärt, die Speicherung von Abrechnungsdaten dürfe „nur in anonymisierter Form“ erfolgen. Inzwischen wurde der Entwurf des Staatsvertrags teilweise abgeändert. Während sich in bezug auf die Speicherung der Abrechnungsdaten keine Änderung ergab, sollen sie nunmehr nur noch dann an Anbieter übermittelt werden, wenn eine Forderung auch nach Mahnung nicht beglichen wird. Dies stellt zweifellos eine Verbesserung dar. Sie reicht jedoch immer noch nicht aus. Das eigentliche Abrechnungsproblem besteht darin, bei einer Vielzahl von Anbietern die von den Teilnehmern an sie zu entrichtenden Entgelte richtig zu verbuchen. Eine zweckmäßige Lösung könnte sein, für jeden Anbieter und jeden Teilnehmer einen Gebührenzähler in der Bildschirmtextzentrale zu führen. Sobald ein Teilnehmer eine entgeltpflichtige Information abrufen, wäre der Gebührenzähler des jeweiligen Teilnehmers und des jeweiligen Anbieters um dieselbe Anzahl von Gebühreneinheiten zu erhöhen. Das Verfahren ist dem Abrechnungsverfahren der Fernmeldegebühren nachempfunden. Eine Einschränkung von Bildschirmtext wäre damit in keiner Weise verbunden. Ich hoffe immer noch, daß diese datenschutzfreundlichere Regelung Eingang in den Staatsvertrag findet und von der Deutschen Bundespost im Bildschirmtextprojekt berücksichtigt wird.

Schlußbemerkung

Das Jahr 1982 war ein schwieriges Jahr für den Datenschutz in Baden-Württemberg. Es stand ganz im Zeichen der Bestrebungen, den Datenschutz zurückzudrängen und so zurechtzubiegen, daß die Verwaltung altgewohnte Vorgehensweisen fortsetzen und sogar ausbauen kann. Diese „Gegenreformation“ auf dem Gebiet des Datenschutzes hatte selbstverständlich ganz erhebliche Auswirkungen auf meine Arbeit. Ich mußte mich nicht nur mit ihr auseinandersetzen, sondern laufend falsche Informationen richtig stellen und den Versuch unternehmen, mich dieser abträglichen Entwicklung so gut es geht entgegenzustellen. Darüber durfte ich die eigentliche Tagesarbeit nicht vernachlässigen. Denn die Bürger erwarten zu Recht, daß sie so intensiv und effektiv wie irgend möglich getan wird. All dies beanspruchte auch die Arbeits-

kraft meiner 11 Mitarbeiter aufs äußerste. Ohne ihre große Sachkenntnis, Tatkraft und Loyalität wäre es nicht möglich gewesen, den vielfältigen Aufgaben gerecht zu werden. Ich danke ihnen sehr herzlich für ihren unermüdlichen Einsatz und nenne für sie alle meinen Stellvertreter, Herrn Ministerialrat Werner Schneider. Mein Dank gilt auch den vielen Bürgern, die mich durch die verschiedensten Beweise der Anteilnahme in meiner Arbeit ermutigten.

Anlage

**Gesetzentwurf der Landesregierung zur Änderung des
Landesdatenschutzgesetzes**

(Stand: 26. Oktober 1982)

Vorblatt

A. Zielsetzung

Durch die Änderung des Landesdatenschutzgesetzes soll der Konflikt zwischen den Belangen des Datenschutzes und der wissenschaftlichen Forschung beseitigt werden, insbesondere soll die Einrichtung von Krankheitsdatenregistern ermöglicht werden.

B. Wesentlicher Inhalt

Die wissenschaftliche Forschung unter Verwendung personenbezogener Daten ist auch ohne die Einwilligung des Betroffenen zulässig, wenn das öffentliche Interesse an der Durchführung eines bestimmten Forschungsvorhabens das Geheimhaltungsinteresse des Betroffenen erheblich überwiegt und die Einwilligung des Betroffenen nicht eingeholt werden kann oder deren Einholung unzumutbar ist.

Personenbezogene Daten, die einem Berufs- oder besonderen Amtsgeheimnis unterliegen, dürfen den wissenschaftlichen Einrichtungen oder einer zur Führung eines Krankheitsdatenregisters befugten öffentlichen Stelle übermittelt werden, ohne daß der Übermittelnde hierdurch seine ihm obliegenden Berufs- oder Standespflichten verletzt.

Eine besondere Gewährleistung des Datenschutzes wird dadurch erzielt, daß bei der Verarbeitung personenbezogener Daten ohne die Einwilligung des Betroffenen diejenigen Merkmale, die sich auf eine bestimmte Person beziehen oder eine solche erkennen lassen, gesondert zu speichern und zu sichern sind.

Die fachlich zuständige oberste Landesbehörde wird ermächtigt, durch Rechtsverordnung die Einrichtung von Krankheitsdatenregistern (z. B. Krebsregister) zu erlauben, wenn dies im öffentlichen Interesse liegt.

C. Alternativen

Keine.

D. Kosten

Bei der Anwendung der im Entwurf vorgesehenen Verfahrensweisen im Umgang mit personenbezogenen Daten werden zusätzliche Kosten entstehen. Eine Schätzung dieser Kosten ist nicht möglich.

Gesetzentwurf

Artikel 1

Anderung des Landesdatenschutzgesetzes

Das Gesetz zum Schutz vor Mißbrauch personenbezogener Daten bei der Datenverarbeitung vom 4. Dezember 1979 (GBl. S. 534), geändert durch Gesetz vom 30. Juni 1982 (GBl. S. 265), wird wie folgt geändert:

1. In § 13 Abs. 3 Satz 1 werden nach dem Wort „entgegenstehen“ die Worte „sowie das zuständige öffentliche Archiv ein Interesse an der Übernahme verneint hat“ eingefügt.
2. § 20 erhält folgende Fassung:

„§ 20

Datenverarbeitung für bestimmte Forschungsvorhaben

(1) Hochschulen und andere öffentliche Einrichtungen mit der Aufgabe unabhängiger Forschung (wissenschaftliche Einrichtungen) können ohne Einwilligung des Betroffenen die für bestimmte Forschungsvorhaben erforderlichen personenbezogenen Daten speichern oder verändern, wenn

1. schutzwürdige Belange des Betroffenen wegen der Art der Daten, wegen ihrer Offenkundigkeit oder wegen der Art ihrer Verwendung nicht beeinträchtigt werden oder
2. a) das öffentliche Interesse an der Durchführung des bestimmten Forschungsvorhabens das Geheimhaltungsinteresse des Betroffenen erheblich überwiegt und
b) die Einholung der Einwilligung des Betroffenen, insbesondere wegen der Gefährdung des Forschungszwecks oder des Betroffenen oder wegen Art und Umfang des mit der Einholung der Einwilligung verbundenen Aufwandes nicht zumutbar oder möglich ist.

(2) Das öffentliche Interesse im Sinne von Absatz 1 Nr. 2 Buchst. a) überwiegt in der Regel erheblich, wenn

1. das Forschungsvorhaben nach Fragestellung, Methodik und Art der Durchführung einen wesentlichen Nutzen für die Allgemeinheit erwarten läßt,
2. der Zweck der Forschung nicht auf andere Weise zu erreichen ist und
3. keine unverhältnismäßigen Nachteile für den Betroffenen zu erwarten sind.

(3) Unter den in Absatz 1 genannten Voraussetzungen sind öffentliche und private Stellen berechtigt, personenbezogene Daten, auch soweit sie einem Berufs- oder besonderen Amtsgeheimnis unterliegen, ohne Einwilligung des Betroffenen an wissenschaftliche Einrichtungen zu übermitteln. Die wissenschaftliche Einrichtung trägt die Verantwortung dafür, daß bei der Übermittlung die Voraussetzungen des Absatzes 2 Nr. 1 und 2, die übermittelnde Stelle dafür, daß die Voraussetzungen des Absatzes 2 Nr. 3 vorliegen. Satz 1 gilt für die Übermittlung von öffentlichen Stellen an andere öffentliche oder private Einrichtungen mit der Aufgabe unabhängiger Forschung entsprechend.

(4) Absatz 3 gilt auch für personenbezogene Daten, die nicht aus Dateien übermittelt werden.

(5) Bei der Verarbeitung personenbezogener Daten nach Absatz 1 Nr. 2 sind die Merkmale, die sich auf eine bestimmte Person beziehen oder eine solche erkennen lassen, gesondert zu speichern und zu sichern. Sie dürfen mit den übrigen Daten nur zusammengeführt werden, wenn dies zur Erreichung des Forschungszwecks erforderlich ist. Die Merkmale, die sich auf eine bestimmte Person beziehen oder eine solche erkennen lassen, sind zu löschen, wenn sie zur Erreichung des Forschungszwecks nicht mehr erforderlich sind.

(6) Die nach Absatz 5 verarbeiteten personenbezogenen Daten unterliegen nicht der Auskunftspflicht nach § 12.

(7) Wissenschaftliche Einrichtungen dürfen auf Grund von nach Absatz 1 gespeicherten personenbezogenen Daten, die sie nicht unmittelbar vom Betroffenen erhoben haben, den Betroffenen über weitere für die Durchführung des Forschungsvorhabens erforderliche Daten nur befragen, wenn der Betroffene in die Befragung gegenüber der Person oder Stelle eingewilligt hat, die die Daten unmittelbar von dem Betroffenen erhoben hat oder wenn durch die Befragung Nachteile für den Betroffenen nicht zu erwarten sind.

(8) Personenbezogene Daten dürfen veröffentlicht werden, soweit hierdurch schutzwürdige Belange des Betroffenen wegen der Art der Daten oder ihrer Offenkundigkeit nicht beeinträchtigt werden; als offenkundig gelten auch Daten, die aus allgemein zugänglichen Quellen entnommen sind.

(9) Bei der Mitteilung nach § 17 Abs. 2 darf die Beschreibung der Aufgaben, zu deren Erfüllung die Kenntnis der personenbezogenen Daten erforderlich ist, auf die Angabe „Forschungsvorhaben“ beschränkt werden.“

3. Nach § 20 wird folgender § 20 a eingefügt:

„§ 20 a

Krankheitsdatenregister

(1) Zur Erfassung, Beobachtung und Erforschung des Entstehens, der Verbreitung und des Verlaufs von Krankheiten kann die zuständige oberste Landesbehörde wissenschaftlichen Einrichtungen und anderen öffentlichen Stellen durch Rechtsverordnung erlauben, ohne Einwilligung der Betroffenen die erforderlichen personenbezogenen Daten in zentralen Registern zu speichern, zu verändern und für Zwecke der wissenschaftlichen Forschung bereitzustellen, wenn dies im öffentlichen Interesse erforderlich ist.

(2) Die Rechtsverordnung muß insbesondere bezeichnen

1. die zur Führung des Registers befugte wissenschaftliche Einrichtung oder öffentliche Stelle (Registerstelle),
2. die Art und den Umfang der personenbezogenen Daten und den Kreis der Betroffenen,
3. den Forschungsbereich, für welchen die Daten verwendet werden dürfen und
4. den Zeitraum, für den die Daten erhoben und verarbeitet werden dürfen.

(3) Einer Erlaubnis durch Rechtsverordnung bedarf es nicht, wenn die Registerstelle in dem Krankheitsdatenregister nur solche per-

sonenbezogenen Daten verarbeitet, die sie unmittelbar vom Betroffenen erhoben hat. In diesem Falle gelten für die Registerstelle die Vorschriften des § 20 Abs. 5, 8 und 9 entsprechend.

(4) Personenbezogene Daten können von öffentlichen und privaten Stellen, auch soweit sie einem Berufs- oder besonderen Amtsgeheimnis unterliegen, an die Registerstelle übermittelt werden, wenn die Voraussetzungen des § 20 Abs. 1 Nr. 1 oder 2 Buchst. b) und Abs. 2 Nr. 3 vorliegen. § 20 Abs. 4 und 5 gilt entsprechend.

(5) Die Registerstelle ist berechtigt, unter den Voraussetzungen des § 20 Abs. 1 Nr. 1 und 2 Buchst. a) und nach Maßgabe der Rechtsverordnung nach den Absätzen 1 und 2 die für bestimmte Forschungsvorhaben erforderlichen personenbezogenen Daten ohne Einwilligung des Betroffenen an wissenschaftliche Einrichtungen zu übermitteln. § 20 Abs. 3 Satz 2 gilt entsprechend. Eine weitere Übermittlung durch die wissenschaftliche Einrichtung an Dritte ist unzulässig.

(6) § 20 Abs. 6 und 9 gilt entsprechend.“

Artikel 2

Änderung des Bestattungsgesetzes

Das Gesetz über das Friedhofs- und Leichenwesen vom 21. Juli 1970 (GBl. S. 395), zuletzt geändert durch das Zweite Gesetz zur Änderung von Zuständigkeiten der Ministerien vom 25. Juli 1972 (GBl. S. 400), wird wie folgt geändert:

In § 22 Abs. 2 werden nach dem Wort „Todesursachenstatistik“ die Worte „und für die wissenschaftliche Forschung“ eingefügt.

Artikel 3

Änderung des Gesetzes über die Gliederung der Archivverwaltung

Das Gesetz über die Gliederung der Archivverwaltung vom 19. November 1974 (GBl. S. 497) wird wie folgt geändert:

§ 2 Abs. 2 erhält folgende Fassung:

„(2) Die Staatsarchive nehmen alle übrigen Aufgaben des Archivwesens einschließlich der Landes- und Kreisbeschreibung wahr. Insbesondere verwahren sie historisches und das bei den Staatsbehörden ausgeschiedene Schriftgut sowie andere Unterlagen, welche die Staatsbehörden nicht mehr benötigen (Archivgut). Sie machen das Archivgut allgemein nutzbar.“

Artikel 4

Inkrafttreten

Dieses Gesetz tritt am in Kraft.