LANDTAG VON BADEN-WÜRTTEMBERG

Drucksache 9 / **2540**

9. Wahlperiode

31. 12. 85

Mitteilung

der Landesbeauftragten für den Datenschutz

Sechster Tätigkeitsbericht
der Landesbeauftragten für den Datenschutz

Schreiben der Landesbeauftragten für den Datenschutz vom 30. Dezember 1985 Nr. C 2310:

Anbei übersende ich Ihnen meinen 6. Tätigkeitsbericht, den ich nach § 16 Abs. 2 des Landesdatenschutzgesetzes dem Landtag von Baden-Württemberg zum 31. Dezember 1985 zu erstatten habe.

Dr. Ruth Leuze

Eingegangen: 31. 12. 85 / Ausgegeben: 14. 01. 86

Sechster Tätigkeitsbericht der Landesbeauftragten für den Datenschutz in Baden-Württemberg

INHALTSVERZEICHNIS

Seite

1. Teil: Zur Situation 10

1. Die Großwetterlage 10

2. Der Datenschutzalltag 12

3. Die Zukunft 13

2. Teil: Neue Herausforderungen für den Datenschutz 13

1. Abschnitt: Landessystemkonzept 14

1. Was sind seine Ziele? 14

2. Welche Schranken setzt die Verfassung? 16

2.1 Verfassungsgemäßes Datenschutzrecht 16

2.2 Absicherung durch Organisation und Verfahren 17

3. Die „Szenarien" des Landessystemkonzepts 18

3.1 Die Herausforderungen der Bürokommunikation 19

3.1.1 Was Bürokommunikationssysteme leisten 19

3.1.2 Welche Folgen hat es für den Bürger? 21

3.1.2.1 Führungsorientierung des Informationswesens im Staatsministerium 21

3.1.2.2 Büroautomation bei den Regierungspräsidien 21

3.1.3 Was ändert sich für die Mitarbeiter? 23

3.1.4 Ungelöste technische und organisatorische Probleme 24

3.1.4.1 Geschäftsgang auf Elektronik umstellen 24

3.1.4.2 Fälschungen verhindern 25

3.1.4.3 Berechtigungen abgestuft vergeben 25

3.2 Die hohen Risiken eines landeseinheitlichen Kommunikationsnetzes 26

3.2.1 Der Weg zum landeseinheitlichen Netz 26

3.2.2 Welche Folgen hat dies für den Datenschutz? 28

3.2.2.1 Trend zum freien Datenfluß 28

3.2.2.2 Faktische Unkontrollierbarkeit 29

3.2.2.3 Komplexität führt zu Fehlern 29

3.2.2.4 Verschlüsselung ist kein Allheilmittel 30

3.3 Sicherheitsprobleme bei Personal Computern 31

3.3.1 Was der Personal Computer Neues bringt 31

3.3.2 Seine speziellen Risiken für den Datenschutz in der öffentlichen Verwaltung 32

3.3.2.1 Richtig programmieren will gelernt sein 32

Seite

3.3.2.2 Unzählige Datensammlungen können entstehen 33
3.3.2.3 Sicherheitssoftware fehlt 33

2. Abschnitt: Bericht der Kommission „Neue Führungsstruktur" Baden-Württemberg 35

1. Ausgangslage 35

2. Die datenschutzrelevanten Vorschläge 36

2.1 Ministerium für Kommunikation und Kunst 36

2.2 Zusammenlegung von Justiz- und Innenministerium 38

2.3 Die Landesdatenschutzkommission 38

3. Abschnitt: Der Gesetzgeber und der Datenschutz 41

1. Ausgangslage 41

2. Datenschutzgesetze 42

3. Archivgesetze 43

3.1 Was kommt ins Archiv? 44

3.2 Kritik 44

4. Statistikgesetze 44

4. Abschnitt: Auswirkungen auf die Datenschutzkontrolle 45

1. Verlagerung der Schwerpunkte 45

1.1 Stellungnahme und Anhörungen 45

1.2 Bürgereingaben 45

1.3 Kontrollen 46

2. Ausstattung der Dienststelle 46

3. Teil: Sorglosigkeit und Datenmißbrauch nehmen nicht ab 47

1. Aktuelle Mißbrauchsfälle 47

1.1 Der raffinierte Kreisamtmann 47

1.2 Datenmißbrauch bei der Polizei 49

1.2.1 Polizeidaten im Wirtshaus 49

1.2.2 Der gläserne Geschäftsführer 49

1.2.3 Hilfe für den Geschäftsfreund 51

1.2.4 Der vorgetäuschte Verkehrsunfall 51

Seite

2. Wozu Gleichgültigkeit und Gedankenlosigkeit führen können 51

2.1 Die überflüssigen EDV-Listen 52

2.2 Wozu Adreßaufkleber mit Patientendaten herhalten müssen 52

2.3 Vom Umgang der Polizei mit Lichtbildern 54

2.4 Die Nachteile der Photokopie 54

3. Wie hilflos ist die Technik gegenüber Datenmißbrauch? 55

4. Teil: Sicherheitsbereich 57

1. Abschnitt: Polizei 57

1. Umgang mit Daten von Nachrüstungsgegnern 57

1.1 Mutlangen 57

1.1.1 Kritik des Präsidenten des Bundeskriminalamts 57

1.1.2 Reaktionen der Bürger 58

1.1.3 Bilanz 60

1.2 Waldheide 61

1.2.1 Wie die Polizei zunächst verfuhr 62

1.2.2 Was dazu zu sagen war 64

1.2.2.1 Personenfeststellungen 64

1.2.2.2 Fertigen einer Anhaltemeldung 65

1.2.2.3 Sammlung der Anhaltemeldungen 66

1.2.2.4 Weitergabe von Daten 68

1.2.3 Konsequenzen 68

1.2.4 Die Folgen von Nötigungen durch Sitzblockade 69

1.3 EUCOM 69

2. Direktzugriff der Fachhochschule für Polizei und der Landespolizeischule auf ZEVIS, INPOL und PAD 70

3. Die freiwillige ed-Behandlung Prostituierter 72

4. Max-Planck-Institut untersucht KpS-Fristen 73

2. Abschnitt: Zentrale Namenskarteien der Staatsanwaltschaften 76

1. Ausgangslage 76

2. Zentrale Namensdatei (ZENDA) der Staatsanwaltschaft Stuttgart 77

2.1 Die bisherige Vorgehensweise 77

Seite

2.2 Meine Einwände 78
2.2.1 Tatvorwurf 78
2.2.2 Verfahrenserledigung 78
2.2.3 Sperren und Löschen 78
2.2.4 Auskünfte an Rechtsanwälte 79

3. Abschnitt: Gesetzgebung 80

1. Zur Situation 80

2. Polizeigesetz 82
2.1 Gefahrenvorsorge 82
2.2 Vorbeugende Bekämpfung von Straftaten 83
2.3 Nichtstörer und „andere Personen" 83
2.4 Öffentliche Veranstaltungen und Versammlungen 84
2.5 Speicherung von Daten aus Ermittlungsverfahren für Zwecke der vorbeugenden Bekämpfung von Straftaten in Dateien 84
2.6 Weitergabe von Daten aus Unterlagen der Polizei 85
2.7 Löschen von Daten in Dateien 86
2.8 Auskunft 87
2.9 Zusätzlicher Regelungsbedarf 87

3. Verfassungsschutzgesetz 89

5. Teil: Hochschulen und Forschung 91

1. Forschungsvorhaben 91
1.1 „Öffentlichkeitsbeteiligung bei der Genehmigung von umweltrelevanten Großvorhaben" 92
1.2 Wählerverhalten im Bundestagswahlkreis Tübingen 93
1.3 Unternehmerbefragung 93
1.4 Abhören von Notrufen zur Spracherforschung 94
1.5 Patientenfragebogen der Europäischen Dialyse- und Transplantationsgesellschaft 94
1.6 Perinatalerhebung 95

2. Blutspendedienst 96
2.1 Was der Spender offenbaren muß 96
2.2 Weitergabe von Blutspenderdaten 97
2.3 Aufbewahrung von Blutspenderdaten 99

3. Studentenwerke 100
3.1 Kontrolle mit Hindernissen 100
3.2 Wie kommt der Student an einen Wohnheimplatz? 101

Seite

3.3 Auskünfte des Amts für Ausbildungsförderung 101

3.4 Mängel in der Datensicherheit 102

4. Was im ärztlichen Attest über einen erkrankten Kandidaten stehen darf 103

5. Gerangel um Studenten 104

6. Teil: Gesundheit und Soziales 106

1. Krebsregister 106

2. Das Gesundheitsamt 107

2.1 Die schulärztliche Untersuchung 107

2.2 Die amtsärztliche Untersuchung 108

2.3 Ein sinnloser Meldedienst 109

2.4 Die Liste der Medizinalpersonen 110

3. Sonderregister über psychiatrisch Kranke beim Einwohnermeldeamt 111

3.1 Bisheriges Verfahren 111

3.2 Meine Bewertung 111

4. Gesetzliche Krankenversicherung 112

4.1 Der Online-Anschluß 112

4.2 Der Mutterpaß 114

4.3 Offenbarung von Sozialdaten an Gerichte 115

4.4 Verhindert der Sozialdatenschutz das Aufdecken von Manipulationen? 116

7. Teil: Der Mitarbeiter im öffentlichen Dienst 118

1. Personaldatensysteme 118

1.1 Lehrerdatenbank 118

1.1.1 Direktzugriff der Oberschulämter 118

1.1.2 Berichtigung der gespeicherten Lehrerdaten 119

1.1.3 Automatisierte Protokolle 119

1.2 PAISY (Personal-Abrechnungs- und administratives Informationssystem) 120

1.2.1 Fehlzeiten 120

1.2.2 Sperren von Personaldaten 121

1.2.3 Automatisierte Prüfungen unerläßlich 121

1.3 PSA (Personal- und Stellenverwaltungssystem am Arbeitsplatz) 122

Seite

1.3.1 Umgang mit Bewerberdaten 122
1.3.2 Fehler beim Einsatz vermeiden 122

2. Änderungsmitteilung über persönliche Verhältnisse 123

3. Registrieren von Telefondaten 123
3.1 Privatgespräche 124
3.2 Dienstgespräche 124
3.3 Sonderfälle 124

4. Die Trennung von Beihilfestelle und Personalstelle 124

5. Ärztliche Unterlagen über Polizeibeamte 125

8. Teil: Andere Schwerpunkte 126

1. Abschnitt: Die Gemeinde 126

1. Was Kreditschutzorganisationen von Gemeinden über Bürger wissen wollen 127

2. Information des Gemeinderats und der Öffentlichkeit über datenschutzrelevante Vorgänge 129

3. Zweitwohnungssteuer 130

4. Kurtaxe 131

2. Abschnitt: Die Gebäudebrandversicherungsanstalten 131

1. Die Pflichtversicherung 131

2. Die Zweckentfremdung 132
2.1 Die umfangreiche Amtshilfe 132
2.1.1 Mitteilungen an die Finanzämter 133
2.1.2 Mitteilungen an die Vermessungsbehörde 133
2.2 Die Nutzung durch die Gemeinden 134

3. Datensicherung 135

3. Abschnitt: Handels- und Gaststättenzählung 1985 135

1. Die mangelhafte Rechtsgrundlage 135

2. Die unrechtmäßige Verarbeitung von Steuerdaten 136

9. Teil: Sorgen der Bürger 136

1. Vorsicht Forellenzucht 137

2. Terroristenfahndung 139

Seite

3. Razzia 139
4. Wer eine Kaserne photographiert 140
5. Beschlagnahme einer Adreßkartei 140
6. Die Bewerbung beim Konsulat 141
7. Schweigepflicht und Suizidversuch 142
8. Werbung über alles 142
9. Der mißtrauische Patient 142
10. Was Schwerbehinderte hinnehmen müssen 143
11. Die unterbliebene Adoption 143
12. Was Väter nichtehelicher Kinder erleben 144
13. Weitergabe von Elternlisten 144
14. Beurteilung von Schulanfängern durch die Hintertür 145
15. Von Häsle, Fröschle und Herrn Specht 145
16. Reisekostenabrechnungen von Beratungslehrern 146
17. Wenn Ehrungen peinlich werden 146
18. Der kopierte Personalausweis 147
19. Was im Grundbuchauszug alles stehen kann 147
20. Besuch in der Strafanstalt 148
21. Der benachteiligte Gläubiger 149
22. Vertrauliches auf Farbbändern 150

Schlußbemerkung 150

1. Teil: Zur Situation

Was wird aus dem Datenschutz? Bleibt er bei dem Wettlauf zwischen Technik und Recht auf der Strecke oder gelingt bei den Veränderungen unserer Zeit, ihm den Platz zu verschaffen, der ihm zukommt? Dies waren die wichtigsten Fragen des Jahres 1985. Um sie wird zur Zeit noch gerungen.

Zunächst schienen in dieser Auseinandersetzung die Aussichten für den Datenschutz gar nicht so ungünstig zu sein. Immerhin gab und gibt es das Volkszählungsurteil 1983 mit seinen deutlichen Vorgaben, welche Richtung im Datenschutz einzuschlagen ist. Diese Vorgaben und die Unwägbarkeiten und Risiken durch den ständig wachsenden Einsatz der modernen Informations- und Kommunikationstechniken hätten eigentlich — sollte man meinen — genügend Schubkraft entwickeln müssen, um tatsächlich zu einer entscheidenden Verbesserung des Datenschutzes zu gelangen. Dem ist jedoch leider nicht so.

Gewiß, eines bewirkte das Volkszählungsurteil: Die Gesetzgebungsmaschinerie lief an. Gesetzesformulierer waren gefragt. Jedenfalls auf Bundesebene schmiedete man allenthalben Gesetzgebungspläne. Zieht man jedoch Bilanz nach all diesen Aktivitäten und Anstrengungen, dann muß das Ergebnis ernüchtern. Bisher blieb es überwiegend bei Entwürfen. Vor allem haben wir noch keine neuen allgemeinen Datenschutzgesetze. Auch stehen die notwendigen gesetzlichen Regelungen im Sicherheitsbereich nach wie vor aus. Zwar sollen sich die Koalitionsfraktionen des Deutschen Bundestags inzwischen nach langen Verhandlungen über einige wichtige Komplexe aus diesem Bereich geeinigt haben. Unklar ist jedoch noch, wie diese Einigung aussieht. Der Öffentlichkeit liegen bislang keine ausformulierten Gesetzentwürfe vor. Es gibt allein Kommentierungen allgemeiner Art. Sie lassen befürchten, daß von dem angekündigten großen Durchbruch zu mehr Datenschutz keine Rede sein kann.

1. Die Großwetterlage

Wegen des politischen Klimas, das derzeit den Datenschutz umgibt, kann dies den Kenner der Situation kaum verwundern. Wenn je im unmittelbaren Anschluß an das Volkszählungsurteil ein Hauch von Datenschutzfrühling zu spüren war, dann ist er längst hinweggeweht. Das Klima ist merklich frostiger geworden. Der Widerstand gegen den Datenschutz in Politik, Wirtschaft und Verwaltung ist spürbar gewachsen. Die in meinem letzten Bericht geschilderte Strategie der Schadensbegrenzung trug Früchte. Schon sind wir wieder in einer Zeit, in der manche Politiker — ähnlich dem ceterum censeo des alten Cato in Richtung Karthago — Stellungnahmen zu Sicherheitsfragen nicht glauben abgeben zu können, ohne gleichzeitig den „überzogenen Datenschutz" zu kritisieren. Wie in der Zeit vor dem Volkszählungsurteil feiern Schlagworte wie Datenschutz = Tatenschutz wieder fröhliche Urstände. Wann immer irgendwo eine Panne passiert, eine Spionageaffäre aufgedeckt, ein Verbrechen begangen und nicht sofort aufgeklärt wird, sofort findet sich der passende Sündenbock: der überzogene Datenschutz. In geradezu klassischer Manier zeigte sich dieser Automatismus nach der Flucht eines leitenden Mitarbeiters des Bundesamts für Verfassungsschutz in die DDR. Sofort stimmten einige Politiker und

Publizisten wieder einmal das Lied vom überzogenen Datenschutz an. Dabei konnte man doch wahrlich nicht behaupten, im Falle Tiedge hätten dessen Vorgesetze wegen des Datenschutzes zu wenig gewußt. Nicht immer liegt die Unsinnigkeit des Vorwurfs gegen den Datenschutz allerdings so klar auf der Hand. Oft genug machen sich die Apologeten von Sicherheit und Ordnung die weit verbreitete Unwissenheit über den Datenschutz, was er erlaubt und was er verbietet, zunutze und malen ein Zerrbild an die Wand, das in keiner Weise mit der Realität übereinstimmt. Da die Fragen der inneren und äußeren Sicherheit selbstverständlich jeden zu Recht berühren, bedarf es keiner großen Phantasie, um sich auszumalen, welche Wirkung ein solches Vorgehen auf die Öffentlichkeit und das politische Klima hat.

Diese Tendenz trifft mit einer ganz anderen Entwicklung zusammen: dem wachsenden Einsatz der modernen Informations- und Kommunikationstechniken und des damit einhergehenden Ausrufes der Informationsgesellschaft. Die Euphorie, die ob dieser herrlichen Zukunftsaussichten allenthalben ausgebrochen ist, läßt die Frage schon gar nicht mehr ernsthaft aufkommen, welche Auswirkungen dies alles auf die Freiheit des Menschen hat, welche Risiken bestehen und wie man ihnen begegnen kann. Wer dies gleichwohl tut, läuft Gefahr, in die Ecke der Kulturpessimisten, Nörgler und ewig Gestrigen gestellt zu werden, die den Anschluß an die Zukunft verpaßt haben. In einem solchen Klima besteht mehr Interesse für die Frage, wie sich Informationen nutzen lassen, als für die Frage, welche Kommunikation unterbleiben muß. Am treffendsten findet sich diese Haltung in der Aussage eines Politikers aus Hessen wieder, das Zeitalter der Kommunikation lebe schließlich davon, daß Daten fließen. Bei einer solchen Denkweise kommt dem Datenschutz im wesentlichen bloß noch die Rolle zu, offenkundigen Mißbrauch zu verhindern. Allzu leicht fällt dabei unter den Tisch, daß man aber Mißbrauch erst feststellen kann, wenn zuvor festgelegt wird, wer wann welche Informationen wie lange und wozu erheben, speichern und nutzen darf und daß es dabei das Selbstbestimmungsrecht und damit die Freiheit des anderen soweit wie irgend möglich zu wahren gilt. Ohne diesen Hintergrund fallen dann schnell so bezeichnende Aussagen wie: Der Datenschutz soll nur den Mißbrauch, nicht aber den Gebrauch von Daten verhindern. Wohl wahr, nur ist mit einem solchen Satz überhaupt nichts zur entscheidenden Frage gesagt, wo der Gebrauch endet und der Mißbrauch anfängt. Genau diese Frage aber ist die Gretchenfrage des Datenschutzes.

Bei diesen Bemühungen um die Schaffung eines modernen Datenschutzrechts begnügte sich Baden-Württemberg weitgehend mit der Rolle eines Souffleurs im Hintergrund. Auf offener Bühne wollte man nicht mitspielen; hatte man Angst vor Kritik? Auch wollte man keine eigene Inszenierung aufführen. Statt dessen setzte man ein Stück auf den Spielplan, das schon im Jahr zuvor nicht gerade ein Renner war: Warten auf Bonn. Da sich dieses Stück nicht gerade durch viel Handlung auszeichnet, stand die Datenschutzgesetzgebung — jedenfalls im Lande — nicht im Mittelpunkt der Diskussion. Daran änderte sich auch nichts durch den von der SPD-Landtagsfraktion eingebrachten Entwurf eines neuen Landesdatenschutzgesetzes. Auch dieser erfreuliche Vorstoß konnte die Landesregierung nicht aus ihrer Reserve locken. Alles in allem: die Szene beherrschten im wesentlichen einzelne Probleme, die sich aus der praktischen Anwendung des Datenschutzes ergaben.

2. Der Datenschutzalltag

Nicht möglich ist, über diesen Datenschutzalltag ein einheitliches Urteil abzugeben. Dazu waren die Verhältnisse zu unterschiedlich. Weder wäre es gerechtfertigt, Regierung und Verwaltung vorzuwerfen, sie würden dem Datenschutz von vornherein nicht die Bedeutung zumessen, die er verdient, noch besteht Anlaß dazu, in großes Lob auszubrechen. Nicht zu bestreiten ist freilich: allein schon die geschilderte datenschutzpolitische Großwetterlage trug ihr Schärflein dazu bei, daß das Innenministerium im Sicherheitsbereich keine Neigung zeigte, von seinem schon seit Jahren festliegenden harten Kurs abzugehen. Auch fehlte es nicht an Bemühungen, den Datenschutz zu diskretitieren, indem man ihn für alle möglichen tatsächlichen oder vermeintlichen Mängel und Mißtöne verantwortlich machte. Selbst der Leistungssport hatte — glaubt man den Worten des Vorsitzenden des Landtagsausschusses für Schule, Jugend und Sport — unter dem Datenschutz zu leiden, weil er angeblich die Talentsicherung ungebührlich erschwert. Schließlich kann ganz sicher auch niemand sagen, alle Mitarbeiter der Verwaltung würden die Notwendigkeit eines effektiven Datenschutzes uneingeschränkt bejahen und sich demgemäß verhalten. Bis es soweit ist, ist noch viel Überzeugungsarbeit und Aufklärung zu leisten und sind noch mehr als genug gewohnte Verhaltensweisen zu überdenken. Auch gilt es bis dahin, noch viele Nachlässig- und Sorglosigkeiten auszumerzen. Auf der anderen Seite will ich gerne anerkennen, daß eine wachsende Zahl von Mitarbeitern um die Bedeutung des Datenschutzes weiß und auch bereit ist, ihn zu praktizieren. Oft genug bedurfte es im Rahmen meiner Kontrollpraxis nur eines kleinen Anstoßes, um ein datenschutzfreundlicheres Vorgehen selbst dann zu erreichen, wenn dazu keine rechtliche Verpflichtung bestand. Diese Lagebeurteilung gilt für alle Verwaltungszweige. Es wäre nicht gerechtfertigt, die Ministerien in „gute" und „schlechte" aufzuteilen. Dafür sind die Verhältnisse zu unterschiedlich. Immer wieder zeigt sich: Nicht so sehr die Aufgabe oder eine bestimmte Gruppenzugehörigkeit entscheiden über die Berücksichtigung des Datenschutzes, sondern viel eher die Einstellung der einzelnen Mitarbeiter. Diese wiederum prägen selbstverständlich in starkem Maße die Vorstellungen der Vorgesetzten — haben sie doch letztendlich das Sagen. Bei all dem darf jedoch eines nicht außer acht bleiben: Die beste Motivation der Mitarbeiter nützt wenig, wenn sie sich nicht auf ein Datenschutzrecht abstützen kann, das tatsächlich die Bezeichnung Datenschutz verdient. Davon sind wir noch um einiges entfernt.

Keine Pauschalurteile sind auch über die Einstellung zur unabhängigen Datenschutzkontrolle möglich. Hier wie dort wechseln Licht und Schatten. Positiv zu bemerken ist vor allem, daß mich die Ministerien wesentlich besser als früher über ihre Pläne und Vorhaben unterrichten und am Erlaß von Rechtsvorschriften beteiligen. Auch das Bemühen des Herrn Innenministers, ein freundliches Klima zu schaffen und mit mir immer wieder das Gespräch zu suchen, ist viel wert. Auf der anderen Seite ereignen sich aber auch nicht ganz selten Dinge, für die ich keinerlei Verständnis habe. Zwei Beispiele seien dazu angeführt:

— Voll Verwunderung mußte ich der Presse entnehmen, daß der Landrat des Landkreises Biberach sich über einen überzogenen Datenschutz beklagte, der angeblich die Arbeit der Krankenhausseelsorge erschwert. Er werde dafür sorgen, daß in den Krankenhäusern des Landkreises Biberach die

Geistlichen weiterhin die für die Betreuung der Patienten notwendigen Informationen erhalten — Datenschutz hin oder her. Außerdem kündigte er an, er werde „die Auseinandersetzung mit der Datenschutzbeauftragten nicht scheuen". Vor dieser Kampfansage Kontakt mit mir aufzunehmen, kam ihm gar nicht in den Sinn. Für ihn war es offensichtlich eine ausgemachte Sache, daß ich mich für überzogenen Datenschutz einsetze und damit die Arbeit der Krankenhausseelsorge erschweren will.

— Nicht akzeptieren kann ich die Art und Weise, wie mir das Innenministerium vorzuschreiben versucht, wie ich Eingaben von Bürgern, die den Datenschutz im privaten Bereich betreffen, zu behandeln habe. Das Ministerium weiß genau, wie selbstverständlich es für mich ist, in solchen Fällen die Bürger auf die gesetzliche Zuständigkeitsregelung hinzuweisen. Es sollte nun aber auch endlich zur Kenntnis nehmen, daß es dem einzelnen Bürger überlassen bleiben muß, darüber zu entscheiden, ob er Beschwerde bei der Aufsichtsbehörde für den nichtöffentlichen Datenschutz — sprich dem Innenministerium — einlegen will oder nicht. Anstatt von mir wie von einer nachgeordneten Behörde die „Vorlage" von Anfragen und Eingaben zu verlangen, sollte es sich lieber darüber Gedanken machen, weshalb sich die Bürger auch in solchen Angelegenheiten an mich wenden und trotz meines Hinweises auf die gesetzliche Zuständigkeitsregelung von seiner Einschaltung absehen.

Gewiß ist ein solches Denken in Feindbildern und sind solche Gängelungsversuche nicht alltäglich. Allein aber, daß es sie gibt, ist ein bedenkliches Zeichen. Sie sind zudem unnötig und nur geeignet, die gebotene sachliche Zusammenarbeit zwischen allen Beteiligten zu beeinträchtigen.

3. Die Zukunft

Am Ende meiner Situationsbeschreibung steht eine Bitte: Bald sind vermutlich auf Jahre hinaus die Weichen im Datenschutz gestellt. Bislang deutet alles darauf hin, daß die Verantwortlichen dabei nur die Gegenwart und „nur" das sehen, was sich heute im Informationsbereich abspielt. Wer aber die Weichen nicht von vornherein falsch stellen will, muß den Blick zugleich viel stärker auf die rapide ansteigenden Möglichkeiten der Einflußnahme und Manipulation durch die neuen Informationstechniken richten. Manche Datenerhebung und manche Datenweitergabe, die heute noch tragbar und hinnehmbar erscheint, kann sich in ihrer Kumulation mit neuen Vorgehensweisen verhängnisvoll auswirken. Vor solchen Entwicklungen sollten wir uns jetzt schon wappnen. Ein Versäumnis käme teuer zu stehen; denn nachträgliche Abhilfe ist nach aller Erfahrung nur sehr schwer möglich.

2. Teil: Neue Herausforderungen für den Datenschutz

Die intensive Beschäftigung der Landesregierung mit den neuen Techniken und ihr engagiertes Eintreten für neue Verwaltungsstrukturen zwangen mein Amt, sich mit diesen Bestrebungen auseinanderzusetzen. Bei der neuen Informationstechnik wundert dies kaum — weiß doch inzwischen fast jeder, daß mit ihrer rasanten

Entwicklung immer neue Gefährdungen für den Datenschutz einhergehen. Weniger auf der Hand liegt, daß auch eine Umorganisation im Behördengefüge und eine Änderung der Arbeitsmethoden der Verwaltung den Datenschutz zurückwerfen oder vorantreiben können. Dazu muß man wissen: für den Datenschutz ist nicht bloß entscheidend, wie die rechtlichen Regelungen über den Umgang mit Informationen aussehen, sondern auch, wer diese anzuwenden hat, nach welchen Maximen dabei gearbeitet wird, welche weiteren Aufgaben zu erledigen sind und welche Interessenkonflikte es dabei zu lösen gibt. Die Themen „Neue Technik" und „Neue Verwaltungsstruktur" gestalten sich außerordentlich schwierig, weil hier Vorhaben der Regierung zur Debatte stehen,

— deren Ziele noch sehr unbestimmt sind,
— die mit einer Technik arbeiten sollen, die teils unerprobt, teils noch nicht einmal entwickelt ist, und
— deren organisatorisches Umfeld im Dunkeln liegt.

Wenn dann noch das Datenschutzrecht — also der Beurteilungsmaßstab — im Wandel begriffen ist, wird die Sache vollends kompliziert. Gerade aber so ist derzeit die Lage. Wer es mit dem Datenschutz ernst meint, muß sich gleichwohl schon jetzt bemühen, die geplanten Veränderungen zu analysieren und die damit einhergehenden Probleme herauszuarbeiten, und versuchen aufzuzeigen, wie man ihnen rechtzeitig begegnen kann.

1. Abschnitt: Landessystemkonzept

1. Was sind seine Ziele?

Die Landesregierung will den Weg in die Informationsgesellschaft nicht nur nicht verpassen, sondern weitaus mehr: sie will mit High Tech in der Landesverwaltung dabei sogar eine Schrittmacherrolle übernehmen. Ihr Ziel ist, durch den Einsatz modernster Informations- und Kommunikationstechniken

— ihren Führungskräften schneller als bisher ganz gezielte Informationen an die Hand zu geben und damit bessere Entscheidungsgrundlagen zu schaffen,

— die Leistungen der öffentlichen Verwaltung durchweg qualitativ und quantitativ zu verbessern,

— der Wirtschaft Anstöße zur Entwicklung neuer elektronischer Produkte zu geben und auf diese Weise ihre ohnehin mit Verve betriebene Förderung der neuen Technologien weiter zu intensivieren,

— Rationalisierungsreserven wo auch immer zu erschließen.

Den Fahrplan für diese Reise in die Zukunft soll das Landessystemkonzept bilden. Entgegen dem Eindruck, den dieses Wort hervorruft, handelt es sich hierbei nicht um einen fertigen, ausgereiften und bis ins Detail ausgearbeiteten Plan, nach dem die Züge bloß noch fahren oder anders gesagt, die Behörden bloß noch handeln müssen. Das Wort „Landessystemkonzept" steht vielmehr ganz allgemein für eine Vielzahl noch unbekannter, denkbarer, möglicher und bereits feststehender Schritte, die die Behörden Zug um Zug machen sollen, damit die Verwaltung möglichst rasch ein supermodernes Informations- und Kommunikationssystem erhält. Das Landessystemkonzept soll also der

Orientierungsrahmen für die künftige Gestaltung der Informationslandschaft in Baden-Württemberg sein. Bislang ist er nur in ersten Umrissen zu erkennen. Was gegenwärtig unter dem Schlagwort „Landessystemkonzept" in vieler Munde ist, ist nichts anderes als ein etwa 60 Seiten umfassendes Grundsatzpapier, in dem die Landesregierung ihre bisherigen, nicht immer koordinierten Ideen, Überlegungen und konkreten Aktivitäten zur weiteren Automatisierung der öffentlichen Verwaltung darlegt. Dieses Grundsatzpapier basiert auf dem „Gutachten über die Erstellung eines Landessystemkonzepts für einen rationellen und wirtschaftlichen Einsatz der Informations- und Kommunikationstechniken in der öffentlichen Verwaltung des Landes Baden-Württemberg", das die zu einer Arbeitsgemeinschaft zusammengeschlossenen Firmen Diebold, Dornier und IKOSS im Auftrag der Landesregierung erarbeitet und im Dezember 1984 vorgelegt haben. Dieses Gutachten präsentiert als Modell eines Landessystemkonzepts ein „Gesamtszenario", das die Richtung für die Entwicklung der Informationsverarbeitung des Landes aufzeigt und den dafür zu schaffenden organisatorischen und technischen Rahmen angibt. Zum anderen beschreibt es vor dem Hintergrund des Gesamtszenarios in zehn „Einzelszenarien" mögliche Projekte für den Einsatz neuer Techniken. Dabei geht es, um noch einmal in die Sprache der Gutachter zu verfallen, um folgende Anwendungen:

— Netzkonzeption für die Landesverwaltung
— Haushaltsmanagement-System
— Büroautomation in einem Regierungspräsidium
— Büroautomation bei einem Familiengericht
— Dokumentation und Schriftgutverwaltung
— Führungsorientierung des Informationswesens
— Btx-Kommunikation zwischen Bürger und Steuerverwaltung
— Umweltinformationssystem
— Personalverwaltungssystem
— Regierungsmanagementsystem.

Die Landesregierung ließ sich von diesem Gutachten so beeindrucken, daß sie bereits Mitte Januar 1985 grünes Licht für die sofortige Realisierung von vier Einzelszenarien gab: der Führungsorientierung des Informationswesens, des Haushaltsmanagement-Systems, der Büroautomation in den Regierungspräsidien und der Büroautomation bei einem Familiengericht. Die dazu flugs erarbeiteten Realisierungsvorschläge der Ministerien billigte sie am 15. Juli 1985. Von mindestens ebenso, wenn nicht weitreichenderer Bedeutung ist freilich ihr gleichzeitig gefaßter Beschluß, wesentliche Elemente des Gesamtszenarios zu übernehmen. So

— übertrug die Landesregierung inzwischen dem Amtschef des Staatsministeriums die Aufgabe des Landessystembeauftragten,

— rief den Landessystemausschuß ins Leben, dem hochrangige Vertreter aller Ressorts angehören und dessen Aufgabe ist, die Automatisierungsvorhaben der einzelnen Ministerien nach einheitlichen Kriterien zu bewerten und nach landespolitischen Zielen zu gewichten,

— richtete beim Staatministerium das von den Gutachtern empfohlene Informationstechnische Zentrum ein, das nun als Stabsstelle für Information und Kommunikation firmiert und dessen Aufgabe ist, Konzeptionen und Rahmenrichtlinien zu entwickeln, landeseinheitliche Standards und Schnittstellen für die Informations- und Kommunikationstechniken festzu-

legen, um damit eine möglichst reibungslose und ungehinderte Kommunikation innerhalb der einzelnen Behörden zu ermöglichen, den Einsatz der neuen Techniken zu koordinieren und für eine Abstimmung wichtiger Einzelprojekte mit dem Gesamtplan zu sorgen.

Damit ja auch alles zügig vorangeht, bewilligte der Landtag jüngst dem Staatsministerium 17 neue Stellen, den vier Regierungspräsidien zur Einführung eines Bürokommunikationssystems je 3 Stellen zusätzlich und stellte zudem erhebliche Mittel zur Anschaffung neuer Technologien zur Verfügung.

2. Welche Schranken setzt die Verfassung?

Es ist keine Frage: Das Landessystemkonzept fordert den Datenschutz aufs äußerste heraus. Denn es sieht die Verwaltung als Informationseinheit. Der Datenschutz dagegen verlangt vom Staat, sein Wissen auf zahlreiche kleine Informationseinheiten aufzuteilen. Das Landessystemkonzept will eine von Hindernissen weitgehend freie Kommunikation zwischen den Behörden; der Datenschutz dagegen, daß jeder Bürger grundsätzlich selbst darüber entscheidet, welcher Behörde er welche Informationen für welche Zwecke zukommen lassen will. Wegen dieser extremen Gegensätzlichkeit hätte die Landesregierung eigentlich gleich zu Anfang sagen müssen, wie sie sich eine Lösung dieses Zielkonflikts vorstellt und wie sie ihrer Pflicht, die Grundrechte der Bürger zu achten, nachkommen will. Leider begnügt sie sich in ihrem über 60seitigen Grundsatzpapier mit der trivialen Aussage, der Datenschutz sei zu beachten. Auch ihr weiterer Hinweis, es ginge nicht darum, „den gläsernen Menschen zu realisieren, sondern bei aller Komplexität und Kompliziertheit der künftig automationsgestützt arbeitenden öffentlichen Verwaltung ein möglichst hohes Maß an Transparenz in dieser Verwaltung zu gewährleisten", vermittelt nicht gerade den Eindruck, die Landesregierung sei sich der Grenzen voll bewußt, die das informationelle Selbstbestimmungsrecht jedes Bürgers ihrem Landessystemkonzept setzt. Gewiß ist es nicht leicht, diese Grenzen aufzuzeigen — bewegt man sich doch hier auf juristischem und technischem Neuland. Dies entbindet freilich nicht, Positionen zu beziehen und die unverrückbaren verfassungsrechtlichen Rahmenbedingungen zu verdeutlichen:

2.1 Verfassungsgemäßes Datenschutzrecht

Gerade die „heutigen und künftigen Bedingungen der automatischen Datenverarbeitung" und die sich daraus ergebenden Möglichkeiten der Einflußnahme waren für das Bundesverfassungsgericht Anlaß, in seinem Volkszählungsurteil das Grundrecht des Bürgers, grundsätzlich selbst über Preisgabe und Verwendung seiner Daten zu entscheiden, zu betonen und wirksame Regelungen zu seinem Schutz zu fordern. Dies gilt erst recht, wenn sich die Datentechnik, wie es das Landessystemkonzept will, zur Informations- und Kommunikationstechnik entwickelt, die außer Daten auch Sprache, Bilder, Texte und Graphiken verarbeitet und dadurch mehr Wissen über jeden Bürger schneller, gezielter, leichter und vielfältiger nutzen kann. Deswegen sind beim Aufbau solcher integrierter Informationssysteme die Möglichkeiten weitaus größer, den Bürger zu beeinflussen, zu manipulieren, zu steuern, zu durchschauen oder durch Mißbrauch ganz neuer Art zu schädigen. Will man die totale

Verkabelung aller Amtsstuben, ist folglich vordringlicher denn je, daß wir ein Datenschutzrecht erhalten, das den strengen verfassungsrechtlichen Anforderungen so, wie sie das Bundesverfassungsgericht beschreibt, gerecht wird. Der Gesetzgeber muß klar definieren, welche Behörden zu welchem Zweck welche Daten wie verwenden dürfen und wer auf welche Weise auf sie zugreifen darf. Kurzum: er muß exakte Spielregeln festlegen, die die Behörden beim geplanten Einsatz der modernen Informations- und Kommunikationstechniken zu beachten haben. Erst wenn es diese gibt, kann die Regierung daran gehen, innerhalb dieses Rahmens die modernen Informations- und Kommunikationstechniken in allen Amtsstuben umfassend einzusetzen und Informationen über Bürger en masse zu verarbeiten. Weil die Landesregierung das Landessystemkonzept will, müßte sie schon deshalb mit demselben Elan, den sie hier an den Tag legt, auch die Gesetzgebung im Datenschutz vorantreiben.

2.2 Absicherung durch Organisation und Verfahren

Die besten Rechtsvorschriften, was die Verwaltung mit Informationen über Bürger machen darf, nutzen freilich wenig, wenn sie leicht zu umgehen sind, dies zudem nicht auffällt und daher ohne Konsequenzen bleibt. So wäre es beispielsweise, wenn ein Gesetz einen Datenabgleich zwischen zwei Datenbanken verbietet, die in der Landesverwaltung eingesetzte Informations- und Kommunikationstechnik diese beiden Datenbanken aber so integriert, daß sich gleichwohl die in ihnen gespeicherten Informationen über Bürger im Handumdrehen verknüpfen ließen. Deshalb fordert das Grundgesetz zwingend, das Recht des Bürgers auf Selbstbestimmung über seine Daten durch entsprechende Technik, Organisation und Verfahren zusätzlich abzusichern. Nach der ständigen Rechtsprechung des Bundesverfassungsgerichts ist die öffentliche Gewalt nämlich nicht bloß verpflichtet, Eingriffe in die Grundrechte zu unterlassen, sondern hat auch die Pflicht, durch eine entsprechende Ausgestaltung ihrer Organisation und ihres Verfahrens wirksame Vorkehrungen zu deren Schutz zu treffen. Konkret bedeutet dies: Im Rahmen des Landessystemkonzepts müssen Technik, Organisation und Verfahren so beschaffen sein, daß die Rechtsvorschriften zum Schutz des informationellen Selbstbestimmungsrechts auch tatsächlich eingehalten werden. Welche Maßnahmen im einzelnen dazu nötig sind, beurteilt sich nach dem Grad der möglichen Gefährdung des Grundrechts auf Datenschutz. Diese Gefährdung ist um so höher, je sensibler die verarbeiteten Informationen über Bürger sind und je leichter sich mit der eingesetzten Technik die Regeln des Datenschutzes unterlaufen lassen. Diese Gefahr kann bei der Realisierung des Landessystemkonzepts sehr hoch sein, weil eines seiner Ziele die technisch unbegrenzte Informationsverarbeitung und Kommunikation ist. Um solche Gefährdungen zurückzudrängen, wenn nicht auszuschließen, ist es beispielsweise unerläßlich, Datenströme gegeneinander abzuschotten. Dafür werden die bislang eingesetzten Techniken — etwa der Paßwortschutz — sicher nicht immer ausreichen. Neue Abschottungsmethoden müssen zur Anwendung kommen. Solange und soweit sich gebotene Abschottungen wegen des Stands der Technik oder zu hoher Kosten nicht erreichen lassen, darf die Landesregierung insoweit neue Kommuni-

kationstechniken selbst dann nicht einsetzen, wenn dies zu Lasten der Effektivität der Verwaltung geht und zugleich einen Verzicht auf Rationalisierung bedeutet. Ebensowenig wäre vertretbar, wenn die Landesregierung aus Gründen der Technologieförderung Informationstechniken einsetzen würde, die noch gar nicht ausgereift und deren Risiken deshalb überhaupt noch nicht abzusehen sind. Ein solches Vorgehen mag vielleicht im Bereich der Privatwirtschaft noch akzeptabel sein; gewiß aber nicht in der Verwaltung, die zur Wahrung der Grundrechte verpflichtet ist. Ihr ist verwehrt, auf dem Rücken der Bürger Experimente vorzunehmen.

Bei all dem, was von Verfassungs wegen zu geschehen hat, muß klar sein: der Staat darf moderne Informations- und Kommunikationstechniken nur einsetzen, soweit dies ohne eine Gefährdung des informationellen Selbstbestimmungsrechts möglich ist. Dieses Grundrecht ist der alleinige Maßstab. Das bedeutet zugleich: Nicht der Mensch hat sich nach der Technik zu richten, sondern die Technik ihm unterzuordnen.

3. Die „Szenarien" des Landessystemkonzepts

Dieser verfassungsrechtliche Hintergrund sollte für die Landesregierung eigentlich Anlaß sein, ihre Pläne gründlich zu bedenken und sorgfältig deren Auswirkungen auf den Datenschutz zu untersuchen, ehe sie an eine Realisierung geht. Davon ist bisher leider nicht viel zu spüren. In ihrem Bestreben, möglichst bald vorzeigbare Ergebnisse zu erzielen, begnügt sie sich mit einem Lippenbekenntnis zum Datenschutz und verzichtet darüber hinaus auch auf die sonst in der Technik übliche Gründlichkeit. So glaubt sie, ohne generelle systematische Analyse des Ist-Zustands der staatlichen Datenverarbeitung auskommen zu können. Auch entschied sie sich, Einzelprojekte in Angriff zu nehmen, ohne die selbst vom Diebold-Dornier-IKOSS-Gutachten für notwendig gehaltene detaillierte Untersuchung durchzuführen. Ein solches Vorgehen mag vielleicht noch für Projekte angehen, die — wie etwa das Haushaltsmanagementsystem — voraussichtlich nur einen geringen Bezug zum Datenschutz haben. Es ist jedoch keinesfalls bei Vorhaben akzeptabel, die sich unmittelbar auf die Verarbeitung von Bürgerdaten auswirken. Zu ihnen zählen das unbekümmerte Streben nach landeseinheitlichen Standards für die Informationsverarbeitung und Kommunikation ebenso wie die Einzelprojekte zur Automation der Büros und zum Aufbau eines landeseinheitlichen Netzes.

Weil detaillierte Analysen und Untersuchungen bisher fehlen, ist es enorm schwierig zu sagen, was die Landesregierung letztendlich im Rahmen des Landessystemkonzepts in die Tat umsetzen will und wie dies aus der Sicht des Datenschutzes zu bewerten ist. Wer sich jedoch die Arbeitsweise und die Aufgaben der Verwaltung vor Augen hält, den Stand der Technik kennt und dies in Relation zu den bisherigen Aussagen der Landesregierung zum Landessystemkonzept setzt, dem wird schon eher deutlich, vor welcher Herausforderung der Datenschutz steht. Dafür Problembewußtsein zu schaffen, sehe ich als meine Aufgabe an. Ich wies deshalb gleich, nachdem mir das Staatsministerium das Diebold-Dornier-IKOSS-Gutachten zur Kenntnis gab, die Ministerien auf die schwerwiegenden datenschutzrechtlichen Probleme hin, die eine Realisierung des darin vorgeschlagenen Landessystemkonzepts mit sich bringt. Leider

mußte ich dann im Sommer den Kabinettsbeschlüssen zum Landessystemkonzept entnehmen, daß diese Bedenken dort keinen Eingang gefunden haben. Dies war mir Anlaß, dem Staatsministerium — voran dem Landessystembeauftragten — die Problematik nochmals in einem ausführlichen Gespräch vorzutragen.

3.1 Die Herausforderungen der Bürokommunikation

Nachdem die öffentliche Verwaltung Anfang der 70er Jahre ihre Massengeschäfte auf breiter Ebene automatisierte, stehen die Amtsstuben jetzt — geht es nach dem Landessystemkonzept — vor einer neuen Automatisierungswelle. Die Landesregierung will nämlich die besonderen Fähigkeiten der neuen Computer und Programme dazu nützen, auch alle Einzelfälle unterschiedlichster Ausgestaltung automatisiert zu bearbeiten. Ihr längerfristiges Ziel ist, mit solchen Bürokommunikationssystemen das vollautomatisierte, „papierlose" Büro zu schaffen.

3.1.1 Was Bürokommunikationssysteme leisten

Wer ein vollautomatisiertes Büro betritt, findet anstelle der bisherigen Aktenstöße, Notizzettel, Kalender und Schreibutensilien als wichtigstes Inventar einen Bildschirm mit Telefon. Je nach Arbeitsplatz ist noch ein Drucker, ein Fernkopierer und ein Datenspeicher, z. B. eine Diskette, angeschlossen. Diese Geräte sind über Kabel mit dem Bürokommunikationssystem verbunden. Dabei handelt es sich um viele, über das Telefonnetz miteinander verbundene Computer, die irgendwo in der Behörde oder ganz woanders stehen können. In ihnen sind alle Informationen gespeichert, die sich bislang in Registraturen und Akten, Notizzetteln und Handakten finden. Will ein Mitarbeiter seine Unterlagen, braucht er nicht mehr den Registrator und Amtsboten bemühen oder im Schreibtisch kramen, sondern bloß auf ein paar Knöpfe drücken und schon steht ihm alles zur Verfügung.

— Wie erfährt man, was zu tun ist?

Kommt der Mitarbeiter morgens ins Büro und schaltet den Bildschirm an, leuchten ihm gleich alle Termine entgegen, die er wahrzunehmen hat. Auch zeigt der Bildschirm ihm gleich an, ob ihm sein Chef abends zuvor eine wichtige Nachricht hinterließ und wer ihm während seiner Abwesenheit wann eine Mitteilung fernmündlich durchgab. Sobald der Mitarbeiter die Nachricht erstmals erfährt, kann das Bürokommunikationssystem den Zeitpunkt genau registrieren und dem Absender in Sekundenschnelle mitteilen, daß und wann seine Nachricht angekommen ist. Weiter informiert das Bürokommunikationssystem den Mitarbeiter am Bildschirm in Übersichten, was sonst alles zu tun ist. Wählt der Mitarbeiter beispielsweise das Symbol „Posteingangskorb", sieht er sofort, wer wann elektronische Post an ihn absandte und wann sie eintraf. Auch welche Vorgänge zur Wiedervorlage kamen, welche Schreiben von Bürgern oder Behörden eingingen und welche Akten sonst zu bearbeiten sind, erfährt er auf diese Weise.

— Wie arbeitet man damit?

Will der Mitarbeiter an einem bereits am Vortag begonnenen Vorgang weiterarbeiten, kramt er nicht mehr wie bisher nach seinen Konzeptzetteln, sondern öffnet einfach per Knopfdruck die Datei dieses Vorgangs. Braucht er zusätzliche Informationen — etwa aus juristischen Informationssystemen, Wirtschaftsdatenbanken oder Bildschirmtext-Angeboten —, kann er diese, ohne sich aus seinem Sessel zu erheben, über Bildschirm abrufen. Die dafür anfallenden Kosten registriert das Bürokommunikationssystem — so wie heute bei den Telefonaten — mit Uhrzeit und Datum des Abrufs und Kennzeichen des jeweils benutzten Informationsdienstes. Will der Mitarbeiter die Hilfe eines Kollegen — sei er nah oder fern — in Anspruch nehmen, kann er ihm ohne weiteres die ganze Akte elektronisch zusenden und ihm gleichzeitig sein Anliegen in einer mündlichen oder schriftlichen Begleitnachricht mitteilen. Wählt er für den Versand Teletex und Fernkopierer, kann er seine Nachricht per Knopfdruck grundsätzlich an jeden Ort der Welt senden. Ihr Empfänger kann bereits Sekunden später diese Nachricht an seinem Bildschirm abrufen und seine Antwort unverzüglich als eigenes elektronisches Dokument auf dem gleichen Weg zurückschicken. Weiter kann der Mitarbeiter jederzeit mit seinem Bildschirm auf das elektronische Archiv seiner Behörde zugreifen — etwa, weil er vergleichbare Fälle sucht oder mehr über einen Bürger wissen will, der in seiner elektronischen Akte genannt ist. Hat er schließlich auf diese Weise alles abgeklärt, tippt er seine Entscheidung am Bildschirm ein.

— Wie erfolgen Postversand und Registratur?

Der Mitarbeiter kann seine Entscheidung — sei es Brief, Aktenvermerk, Rede oder Gutachten — an wen auch immer als elektronische Post, ausgedruckten Brief oder Teletex versenden. Zudem erhält das elektronische Archiv den Vorgang zur Ablage. Dort kann man ihn jederzeit wieder mit einer Vielzahl von Suchkriterien abrufen. Geeignete Kriterien sind beispielsweise die Namen aller in irgendeiner elektronischen Akte genannten Bürger, die Namen der Bearbeiter, das Eingangs- oder Versanddatum eines Briefes, Aktenvermerkes oder anderen Dokumentes sowie Stichworte aus Dokumenten oder Synonyme.

— Wie überblickt man alles?

Zwar verbannt das Bürokommunikationssystem durch seine bloße Existenz nicht das manchmal schon chaotische Aktendurcheinander aus den Amtsstuben. Es verschafft aber auf jeden Fall den Chefs allemal mehr Überblick über den Stand der Arbeiten und mehr Möglichkeiten zur Kontrolle ihrer Mitarbeiter. Denn die Systeme geben jederzeit Auskunft, was bei dem einzelnen Mitarbeiter gerade zur Bearbeitung ansteht, wie viele Rück-

stände er hat, wer in welchem Umfang an der Bearbeitung eines Falles mitwirkte und wieviel Zeit dies in Anspruch nahm.

3.1.2 Welche Folgen hat es für den Bürger?

Die Landesregierung will solche Bürokommunikationssysteme vorerst für die Vorhaben „Führungsorientierung des Informationswesens" beim Staatsministerium und „Büroautomatisierung bei den Regierungspräsidien" beschaffen. Beide Projekte betreffen den Bürger — allerdings in unterschiedlichem Maß:

3.1.2.1 Führungsorientierung des Informationswesens im Staatsministerium

Das neue System soll dem Staatsministerium für jedes seiner Probleme schnell viele und gezielte Informationen liefern, damit sie in eine Rede einfließen, bei einer Pressemitteilung auftauchen und in die Fülle seiner Entscheidungen eingehen. Seine Referenten sollen auch aus Kabinettsvorlagen und anderen Beiträgen der Ministerien, aus juristischen und parlamentarischen Informationsdiensten, dem Landesinformationssystem und anderen nationalen und internationalen Datenbanken Informationen abrufen und gleich am Bildschirm mit eigenen Beiträgen zu einem neuen Text zusammenstellen. Im Laufe der Zeit soll auch ein elektronisches Archiv etwa mit den Reden des Ministerpräsidenten und den Kabinettsbeschlüssen entstehen. Das alles ist gedacht, die Effizienz des Staatsministeriums zu steigern. Beim derzeitigen Stand der Planung braucht ein Bürger kaum damit zu rechnen, in dieses System zu kommen. Deshalb betrifft dieses Projekt ihn und damit den Datenschutz nur am Rande. Gleichwohl kann aber niemand gleichgültig sein zu sehen, wie die Regierung mit diesem System ihre Effizienz und Schlagkraft in einem enormen Maße steigert und dem auf seiten des Parlaments nichts Gleichwertiges entgegensteht.

3.1.2.2 Büroautomation bei den Regierungspräsidien

Mit diesem Projekt will man die papierlose Bürokommunikation bei den Regierungspräsidien Stuttgart und Freiburg erproben. Schwerpunkte des Stuttgarter Projekts soll die Erprobung der abteilungs- und referatsübergreifenden Koordinierung beim Umweltschutz sein. Das Freiburger System soll eingehende Schreiben — sei es von Bürgern, Behörden oder Unternehmen — mit Blattlesern und Scannern gleich beim Posteingang automatisiert lesen, speichern, mit bereits vorliegenden Informationen verknüpfen, zur anschließenden Bearbeitung verteilen und schließlich im elektronischen Archiv registrieren.

Zwei spezifische Gefahren für den Datenschutz sehe ich hier:

— Die erste Gefahr resultiert aus den enormen Verknüpfungs- und Auswertungsmöglichkeiten eines solchen Systems bei den Regierungspräsidien. Dort laufen nämlich wegen ihrer vielfältigen Aufgaben — nicht umsonst spricht man von der Bündelungsfunktion — eine Fülle von Informationen aus den unterschiedlichsten Lebensbereichen zusammen. Technisch wäre es dann ohne weiteres möglich, alles, was immer Bürger zu den Themen Wohnungswesen, Baulandumlegung, Lastenausgleich, Gewerbeförderung, Preisüberwachung, Verkehrswesen, Veterinärwesen, Straßenbau, Sozialwesen, Wasserversorgung und Landschaftsentwicklung, einzelnen Bußgeldverfahren und Genehmigungsverfahren von Flughäfen vorbringen, per Knopfdruck abzurufen und miteinander zu verknüpfen. Diese Situation könnten einzelne Mitarbeiter ausnutzen, indem sie bei ihren Entscheidungen über Anliegen von Bürgern Informationen heranziehen, die da nicht einfließen dürften. Sachfremde Erwägungen könnten die Entscheidung beeinflussen, ja sogar den Ausschlag geben.

— Die andere Gefahr geht von der enormen Kommunikationsmöglichkeit dieses Systems aus. Neue, unnötige Datenströme sind zu befürchten, weil es ein Leichtes ist, Akten in Sekunden elektronisch zu kopieren und zu versenden. Um wieviel bequemer ist es doch, einem Kollegen, den man um Rat fragt, gleich eine Kopie der gesamten Akten zuzuleiten, als erst noch mühsam Auszüge anzufertigen und den Sachverhalt anonym zu schildern. Das System erleichtert aber auch den bewußten Mißbrauch: Hinterläßt es doch keine Spuren, wenn jemand per Knopfdruck Daten über Bürger unbefugt weitergab. Sein Risiko, entdeckt zu werden, ist dabei gleich null.

Auf lange Sicht wird wohl dem Bürger die Bürokommunikation auch anderswo begegnen. Denn das Diebold-Dornier-IKOSS-Gutachten schlägt vor, für die ganze Landesverwaltung ein umfassendes Kommunikationssystem mit elektronischer Post aufzubauen. Es soll alle im Lande entstehenden Einzelsysteme — sei es bei den Familiengerichten, Schulen oder Ministerien — nach und nach miteinander verbinden. Da die Gutachter zudem empfehlen, alle automatisierten Registraturen und Archive nach demselben Schema — einem landeseinheitlichen Aktenplan — aufzubauen, steht einer landesweiten Datenabfrage und -verknüpfung praktisch nichts mehr im Weg. Zwar gibt es dazu noch keinen Beschluß der Landesregierung. Allerdings

kommt es auf einen solchen kaum an, weil die wesentlichen Voraussetzungen nicht die Landesregierung, sondern die Post mit ihrem ISDN-Netz schafft. Wenn Baden-Württemberg dieses Netz nutzt, ohne in seine Bürokommunikationssysteme ausreichende Sicherungen einzubauen, kann dies zu heute noch gar nicht übersehbaren Möglichkeiten führen, Bürger zu überwachen oder deren Verhalten zu beeinflussen.

3.1.3 Was ändert sich für die Mitarbeiter?

Bürokommunikationssysteme bringen für den Mitarbeiter mehr Kontrollen mit sich. Dafür gibt es drei Gründe:

— Von der Verwaltungskontrolle zur Mitarbeiterkontrolle

In einem Rechtsstaat ist die Kontrolle des Verwaltungshandelns unerläßlich. Um dem Parlament, den Gerichten, Rechnungshöfen, anderen Kontrollinstanzen und auch der Verwaltung selbst diese Kontrolle zu ermöglichen und damit zugleich die Rechte der Bürger zu garantieren, zeichnet die Verwaltung seit jeher detailliert auf, welcher Mitarbeiter wann welche Akten in welcher Weise und in welchem Umfang bearbeitet. Diese Aufzeichnungen lassen sich nur für die Kontrolle eines Mitarbeiters im Einzelfall nutzen. Praktisch unmöglich ist dagegen, damit umfassende Verhaltens- und Leistungskontrollen der Mitarbeiter durchzuführen. Denn keine Behörde wird sich die Mühe machen, ihre Unmengen von Akten daraufhin systematisch durchzusehen und auszuwerten. Das wäre auch zu mühsam. Mit der Einführung der Bürokommunikation ändert sich dies schlagartig. Ein Ziel jedes Bürokommunikationssystems ist nämlich, den Zugriff auf das elektronische Archiv zu erleichtern. Das heute noch so weitverbreitete mühsame Suchen in Registraturen und Archiven, Vorakten, vergleichbaren Fällen, früheren Stellungnahmen und anderen Schriftsätzen soll ein Ende haben. Ein probates Mittel dazu ist, das elektronische Archiv nach den Namen von Mitarbeitern zu durchsuchen. Das tut man etwa, wenn man weiß, daß der Mitarbeiter X schon einen Präzedenzfall bearbeitet hat, Y den X vertreten soll und deshalb wissen muß, welche Vorgänge zur Zeit bei X laufen, oder ein Bürger sich auf ein Gespräch mit Mitarbeiter Z beruft, der gerade nicht erreichbar ist. Der Schritt von diesen kleinen unproblematischen Anfragen zu einer umfassenden Leistungs- und Verhaltenskontrolle ist klein und die Versuchung sicher groß.

— Mitarbeiterkontrolle auch über Abrechnungsdaten

Beim Bürokommunikationssystem fallen aller Voraussicht nach eine Fülle von Informationen über Mitarbeiter an, die es bislang noch gar nicht gibt. Während die Behörden heute registrieren, wer

wann welche Telefonnummer anrief und wieviel dies kostet, zeichnet das Bürokommunikationssystem auch auf, wer wann in welchem Maße neben dem Telefon auch Telex, Bildschirmtext, Fernkopieren, juristische und andere kostenpflichtige Informationssysteme nutzt. Aus diesen Abrechnungsdaten kann man ableiten, wie sehr ein Mitarbeiter auf solche Hilfsmittel angewiesen ist, wie lange er sich täglich ungefähr im Büro aufhielt, wer seine Kommunikationspartner sind, welchen persönlichen Arbeitsstil er pflegt, wie groß sein Wissen und seine Arbeitsleistung ist.

— Weitere Kontrolldaten können anfallen

Ob und inwieweit das Bürokommunikationssystem darüber hinaus Verhalten und Leistung der Mitarbeiter registriert, hängt von seiner technischen Ausgestaltung ab. Möglich ist beispielsweise, auch die Einzelheiten der Bearbeitung — etwa die Tages- oder Anschaltzeit und damit Dauer der täglichen Arbeitszeit — festzuhalten. Außerdem wäre es ein Leichtes, dem Chef heimlich anzuzeigen, welcher seiner Mitarbeiter gerade was macht, welche Kommunikationsdienste er dabei benutzt und welche Nachrichten — auch private — er austauscht.

Diese bislang ungeahnten Möglichkeiten einer Kontrolle der Leistung und des Verhaltens von Mitarbeitern machen es dringlicher denn je, ein Personaldatenrecht zu schaffen, das präzise festlegt, ob, wann und unter welchen Voraussetzungen Behörden welche Informationen über die einzelnen Mitarbeiter nutzen dürfen. Dies allein bewirkt jedoch noch keinen ausreichenden Schutz der Mitarbeiter. Hinzu kommen muß eine abgestimmte Konzeption von technischen und organisatorischen Schutzvorkehrungen. Darüber hinaus sind weitere Kontrollmechanismen, beispielsweise ein ausreichendes Mitwirkungsrecht der Personalvertretungen, zu schaffen.

3.1.4 Ungelöste technische und organisatorische Probleme

Die modernen Bürokommunikationssysteme sind erst seit wenigen Monaten auf dem Markt. Deshalb kann nicht verwundern, daß sie sich für die speziellen Anforderungen der öffentlichen Verwaltung noch keineswegs eignen.

3.1.4.1 Geschäftsgang auf Elektronik umstellen

Wie die Geschäfte innerhalb jeder Behörde laufen müssen, ist in der Dienstordnung für die Landesbehörden in Baden-Württemberg so genau festgelegt, daß sicher mancher darüber staunt. Da muß der Abteilungsleiter die von ihm täglich durchgesehene Post mit einem Sichtvermerk versehen; je nach Stellung hat man mit Grün-, Rot- oder Blaustift zu schreiben, damit Verantwortlichkeiten nicht verwischt werden. Sind mehrere Beamte an einer Entscheidung beteiligt, darf der eine die Texte des

anderen nicht ohne weiteres abändern. Wer letztlich nach vielem Hin und Her die Verantwortung nach außen trägt — also „schlußzeichnet" —, legt den endgültigen Text fest. Das alles führt häufig zu Änderungen, Umschreiben und Korrekturen des Entwurfs: Schwarz-, Rot-, Blau- und Grüngeschriebenes mengt sich mitunter zum bunten Allerlei und trotzdem muß eindeutig klar und jederzeit nachprüfbar sein, wer was gemacht hat. Soll dies alles ein Bürokommunikationssystem leisten, ist es nicht damit getan, den Mitarbeitern lediglich einen Farbbildschirm hinzustellen, damit sie je nach Stellung ihren Text in grün, rot oder blau eintippen. Wichtig ist vielmehr, die hinter diesen Formalien stehende Sicht eines korrekten Verwaltungshandelns auf die völlig neuen Verhältnisse der Bürokommunikationssysteme zu übertragen. Diese wichtige Aufgabe hat meines Wissens noch niemand angepackt.

3.1.4.2 Fälschungen verhindern

Wer weiß, welche heiklen Entscheidungen täglich Behörden treffen, versteht, daß manchmal Mitarbeiter im nachhinein gern anders entschieden hätten oder ihre Verantwortung für eine Fehlentscheidung nicht mehr wahrhaben wollen. Kein Mitarbeiter und kein Chef kann sich — geht es korrekt zu — beim heutigen System seiner Verantwortung später entziehen. Seine Mitwirkung ist in der Akte durch Unterschrift dokumentiert. Wer dies nachträglich vertuschen will, müßte Urkunden unterdrücken, fälschen oder ganze Akten vernichten. So hohe Hindernisse gibt es beim Bürokommunikationssystem nicht zu überwinden: Elektronisch gespeicherte Informationen kann man nämlich in der Regel, ohne Spuren zu hinterlassen, ändern. Zwar suchen die Entwicklungslabors der Universitäten und EDV-Hersteller nach Methoden, die der Sicherheit einer Unterschrift nahekommen. Außer vielen Ideen gibt es jedoch noch nichts: keine verwendbaren Serienprodukte, kein Organisationskonzept für den Einsatz sicherer automationsgestützter Methoden und schon gar keine Analyse der bei jedem Einsatz technischer Produkte vorhandenen Schwachstellen.

3.1.4.3 Berechtigungen abgestuft vergeben

Wer für was zuständig und wer wozu berechtigt ist, spielt im Behördenalltag eine große Rolle; ein komplexes Gefüge von Zuständigkeiten und Berechtigungen ist die Folge: Was ein Oberregierungsrat darf, darf der ihm zuarbeitende Amtsrat noch lange nicht. Akten, die ein Regierungsrat aus der Registratur holen darf, sind dem Ministerialrat aus einer anderen Abteilung nicht zugänglich. Diktate eines Regierungsdirektors darf die selbstbewußte Sekretärin nicht ändern. Dies sind nur wenige Beispiele. Der Geschäftsverteilungsplan, die Dienst-

ordnung und besondere Geheimhaltungsverpflichtungen spielen hier eine Rolle. Wohl noch niemand hat die schwierige Aufgabe übernommen, dieses Geflecht von Befugnissen so formelhaft darzustellen, daß ein Programmierer es in ein EDV-Programm umsetzen könnte. Selbst wenn das einmal getan ist, bleibt immer noch die Aufgabe, dieses Programm in ein sicheres Bürokommunikationssystem zu integrieren.

3.2 Die hohen Risiken eines landeseinheitlichen Kommunikationsnetzes

Datennetze entstehen, wenn man mehrere Computer, Bildschirme, Drucker und andere Datenterminals für Zwecke des Datenaustauschs über Fernmeldeleitungen miteinander verbindet. Die Informatik will ebenso wie die EDV-Hersteller und die Post die Datenübertragung in Netzen künftig so einfach gestalten, wie das Telefonieren im weltumspannenden Fernsprechnetz mit seinen 600 Mill. Fernsprechteilnehmern schon lange ist. Dasselbe Ziel verfolgt — grob gesagt — auch das Landessystemkonzept. Nach dem Willen der Landesregierung soll schon bis April 1986 eine einheitliche landesweite Netzkonzeption auf dem Tisch liegen.

3.2.1 Der Weg zum landeseinheitlichen Netz

Um zu verstehen, was es mit einem solchen landeseinheitlichen Netz auf sich hat, muß man die heutige und die künftige Technik kennen.

— Die heutigen Datennetze

Bislang gibt es kein Einheitsnetz, sondern verschiedene, voneinander unabhängige Datennetze. Die Finanzverwaltung wickelt ihr Integriertes Automatisiertes Besteuerungsverfahren über die drei Datennetze der Oberfinanzdirektionen Stuttgart, Karlsruhe und Freiburg ab, an die 81 Finanzämter und Teile der Hochbauverwaltung angeschlossen sind. Die Polizei betreibt für ihre verschiedenen Informationssysteme — ich nenne bloß INPOL, PAD, MOD, PIOS und die SPUDOK's —, für ihren Datenabruf beim Kraftfahrt-Bundesamt in Flensburg und für die Zoll- und Grenzschutzstellen an den Grenzen ein landesweites Datennetz; 273 Datenterminals sind daran angeschlossen. Die 67 staatlichen Vermessungsämter können mit ihren 108 Kleincomputern über Fernmeldeleitungen den Großrechner des Rechenzentrums der Innenverwaltung im Landeskriminalamt anwählen und dort das zentrale automatisierte Liegenschaftsbuch lesen und fortschreiben. Im Mittelpunkt eines anderen umfangreichen Datennetzes steht der Großrechner des Gemeinsamen Rechenzentrums des Sozial-, Justiz-, Wirtschafts-, Finanz- und Innenministeriums (RSJW); angeschlossen sind: Landesversorgungsamt, Finanzministerium, Oberfinanzdirektionen Stuttgart und Freiburg, Hochbauämter, Universitätsbauämter, Autobahnamt, Regierungspräsidien Stuttgart, Freiburg, Karlsruhe und Tübingen, Straßenbauamt Heidel-

berg, Amtsgericht Stuttgart, Wirtschaftsministerium, Ernährungsministerium, Geologisches Landesamt und Landesbergamt. Das eigene Datennetz des Ernährungsministeriums nutzen u. a. vier Forstämter, die Landesanstalt für Umweltschutz und die staatlichen Tierschutzstellen. Die vier Oberschulämter Stuttgart, Karlsruhe, Tübingen und Freiburg betreiben im Verbund Rechner, an die kleinere lokale Datennetze angeschlossen sind. Im Mittelpunkt eines weiteren Datennetzes stehen die Rechner des Statistischen Landesamts; einer davon ist mit dem Bildschirmtextnetz verbunden.

— Kommunikationsmöglichkeiten der heutigen Netze

Zwischen diesen einzelnen Netzen bestehen derzeit nur ein paar Verbindungen, die man an den Fingern abzählen kann. Deshalb kann beispielsweise der Kriminalist beim Landeskriminalamt nicht über das Polizeinetz die neuestens Zahlen der Kriminalstatistik direkt in den Computer des Statistischen Landesamts eingeben. Ebensowenig kann er von dort die Angaben der Bürger zur Handels- und Gaststättenzählung 1985 abrufen. Wären die Netze von Polizei und Statistischem Landesamt miteinander verbunden oder gar einheitlich, dann wäre dies kein großes technisches Problem. Wer mit anderen zusammen im Netz ist, dem kann nämlich der Netzverwalter leicht — oft sogar bloß durch Knopfdruck — den Zugriff auf die Daten der anderen ermöglichen. Weil dies so einfach ist, verspricht sich die Landesregierung von einem einheitlichen landesweiten Netz neben einer Kostenminderung eine enorme Erleichterung des Informationsaustauschs — gewiß nicht zu Unrecht.

— Wie das Universalnetz aussehen könnte

Schon innerhalb weniger Monate könnte man die Netze der Finanzverwaltung, des Statistischen Landesamts, des RSJW und des Ernährungsministeriums zu einem einzigen Netz zusammenlegen. Das geht so einfach, weil deren Computer und Datenterminals schon heute weitgehend nach den Normen des gleichen EDV-Herstellers arbeiten. Man müßte deshalb diese Normen bloß noch — wie auch das Diebold-Dornier-IKOSS-Gutachten empfiehlt — konsequent anwenden — etwa im Rahmen des SNA-Konzepts (Systems Network Architecture). Dadurch entstünde ein riesiges Verwaltungsnetz, an das man auch die Netze der Polizei, Vermessungs- und Oberschulämter anschließen könnte. Dreierlei Möglichkeiten gäbe es dafür: Zum einen könnte man diese Behörden nach und nach mit SNA kompatiblen Computern und Datenterminals ausstatten. Zum zweiten könnte man diese Netze mit Hilfe besonderer Computer und/oder Programme mit dem SNA-Netz zusammenlegen. Dies ginge rasch, wäre aber sehr teuer. Die dritte Variante ist, die Zusammenlegung dieser Netze mit der Einführung des vollautomatisierten Büros zu verbinden. Dies wäre der eleganteste Weg — entsteht doch so nicht nur ein einheitliches Datennetz, son-

dern zugleich Zug um Zug ein Universalnetz, das sich nicht nur für den Austausch von Daten, sondern auch für die Übertragung von Bildern, Texten und Ferngesprächen eignet.

— Die Kommunikationsmöglichkeiten eines Universalnetzes

Heute kann man sich noch gar nicht so ganz vorstellen, was ein solches Netz alles leistet: Mit seiner Hilfe könnten der Personalsachbearbeiter einer Oberfinanzdirektion, der Referent im Innenministerium, der Kriminalbeamte einer Polizeidirektion, der Baurat eines Hochbauamts, der Programmierer des Landesversorgungsamts, der Vermessungsingenieur eines Vermessungsamts mit jedem Mitarbeiter irgendeiner Behörde in Baden-Württemberg elektronische Akten austauschen, telefonieren, elektronische Post und Fernkopien, Btx-Mitteilungen und Fernschreiben im Rahmen der Bürokommunikation versenden und empfangen. Außerdem könnten sie mit Hilfe dieser Technik von allen Computern aller Behörden des Landes Daten abrufen und diese an andere Behörden oder Privatpersonen beliebig versenden.

Freilich könnte man auch in solch einem Universalnetz die Kommunikationsmöglichkeiten der einzelnen Mitarbeiter beschränken. Dafür müßte man die Bürokommunikation und den Datenabruf begrenzen. Dies freilich würde den erklärten Zielen der Bürokommunikation, einen freien Datenaustausch zu ermöglichen, zuwiderlaufen und den Nutzen der teuren Geräte und Computer erheblich mindern. Es wäre somit unrealistisch, das zu erwarten. Ebenso ist eine Einschränkung des Datenabrufs nicht ohne Probleme: Die durch das Universalnetz transportierten Personendaten würden trotzdem unterwegs in einer Vielzahl von Computern unterschiedlicher Behörden landen und können dort in falsche Hände gelangen.

3.2.2 Welche Folgen hat dies für den Datenschutz?

In Umrissen zeichnen sich schon jetzt folgende Probleme ab:

3.2.2.1 Trend zum freien Datenfluß

Nach den Datenschutzgesetzen dürfen Behörden Informationen über Bürger nicht austauschen — es sei denn, eine Rechtsvorschrift erlaubt dies. In krassem Gegensatz dazu steht die technische Konzeption eines landeseinheitlichen Kommunikationsnetzes: nach ihr können grundsätzlich alle Behörden nach Belieben Informationen über Bürger austauschen — es sei denn, ein besonderer Computerbefehl oder Schutzcode verhindert dies im Einzelfall. So wäre es selbst bei Behörden, zwischen denen es praktisch keinen Austausch von Personendaten geben darf.

3.2.2.2 Faktische Unkontrollierbarkeit

Wer sich vor Augen hält, daß in einem landesweiten Kommunikationsnetz am Ende Hunderte, wenn nicht Tausende von Behörden mit x-Tausenden von Mitarbeitern angeschlossen sind, erahnt die Komplexität eines derartigen Netzes. Weil jeder Mitarbeiter grundsätzlich das ganze Netz und alle angeschlossenen Computer nutzen kann, müssen ihm Netzverwalter eine persönliche Nutzungsberechtigung geben. Sie legen damit fest, daß etwa der Personalsachbearbeiter Maier bei der Oberfinanzdirektion Freiburg nur Personaldaten der im Bereich dieser Oberfinanzdirektion beschäftigten Beamten bestimmter Besoldungsgruppen an seinem Bildschirm bearbeiten und insoweit auf das Personaldatensystem UPS zugreifen darf. Ähnlich detailliert und meist noch viel komplizierter müßten die Netzverwalter die Berechtigungen aller anderen Mitarbeiter im Netz vermerken. Wenn man bedenkt, wie häufig Mitarbeiter z. B. wegen Krankheit, Urlaub, Abordnung, Stellvertretung oder Beförderung neue Aufgaben erhalten und deshalb neue Nutzungsberechtigungen bekommen müssen, kann man sich vorstellen, daß nach kurzer Zeit niemand mehr einen Überblick über die vergebenen Berechtigungen hat.

3.2.2.3 Komplexität führt zu Fehlern

Selbst wenn man annimmt, die Behörden, Mitarbeiter und Netzverwalter würden jederzeit standhaft versuchen, ihre Berechtigungen für Datenaustausch und Datenabfragen richtig zu verwalten, wäre das Risiko unbeabsichtigter Fehler unvertretbar hoch. Dazu muß man wissen: Wer welche Berechtigung hat, wird an einer Vielzahl von Stellen im Netz auf unterschiedlichste Weise mit Computersprachen festgehalten — sei es in den Rechenzentren, Rechnern des Datennetzes, Computern der Bürokommunikationssysteme, speziellen Sicherheitsprogrammen und einzelnen EDV-Verfahren. Eine einheitliche Methode gibt es hierzu nicht. Erschwerend kommt weiter hinzu: Weil die Steuerung der einzelnen Berechtigungen so kompliziert ist, ist Gang und Gäbe, daß sie sich ungewollt gegenseitig außer Kraft setzen oder modifizieren mit der Folge, daß die einzelnen Mitarbeiter mit dem System tatsächlich mehr machen können als sie eigentlich dürfen. Nur EDV-Spezialisten können da noch helfen; freilich müssen auch sie oft nach dem letzten rettenden Strohhalm greifen, dem praktischen Test. Kurzum: Wer diese unvermeidbaren Fehler ins Kalkül zieht — und das muß jeder Realist —, sieht, daß es aus der Sicht des Datenschutzes gegenwärtig und in der nahen Zukunft nicht vertretbar ist, ein solches Universalnetz zu betreiben. Es hat noch zu viele Schwachstellen, Sicherheitslücken und Grauzonen.

3.2.2.4 Verschlüsselung ist kein Allheilmittel

Immer wenn von Datenschutz und seinen Gefahren die Rede ist, kommt früher oder später die Sprache auf die Verschlüsselung (Kryptographie). Auch die Landesregierung will damit die Risiken eines landeseinheitlichen Kommunikationsnetzes in den Griff bekommen, ohne zu sagen, wie das vonstatten gehen soll. Bislang gibt es wenig Brauchbares:

— Die heutige Technik für die Verschlüsselung

Mit den auf dem Markt angebotenen Verschlüsselungsgeräten kann man Personendaten verschlüsseln, über Fernmeldeleitungen oder Funk übertragen und automatisiert abspeichern. Wenn man das macht, muß man die geheimen Schlüssel, ohne die eine Verschlüsselung nicht möglich ist, gut sichern. Ist das der Fall, dann verschlüsseln zumindest die besseren Geräte nach allgemeiner Auffassung zuverlässig. Gleichwohl gibt es keine Garantie, daß Unbefugte Verschlüsseltes nicht doch einmal entschlüsseln. Will man trotz dieses unvermeidbaren Risikos die heutigen Verschlüsselungsgeräte in einem Universalnetz einsetzen, dann gibt es Probleme mit der Verwaltung der geheimen Schlüssel. Jeder Mitarbeiter, der mit Tausenden seiner Kollegen jederzeit verschlüsselt über das Netz kommunizieren können soll, muß natürlich vorher mit jedem eine geheime Schlüsselzahl vereinbaren. Wie das in der Praxis gehen soll, ist wegen des ungeheuren Aufwands völlig unklar.

— Neue Verschlüsselungsmethoden

Eine Lösung verspricht man sich von einem faszinierenden, Mitte der 70er Jahre entwickelten Verschlüsselungskonzept, dem Kryptosystem mit öffentlichen Schlüsseln. Hier erhält jeder Netzbenutzer zwei etwa 100stellige Zahlen. Eine der beiden darf er niemandem mitteilen. Die andere muß er jedem sagen, mit dem er verschlüsselte Informationen austauschen will. Damit der Umgang mit diesen Riesenzahlen praktikabel ist, sollen sie in einer mit einem Mikroprozessor versehenen Ausweiskarte gespeichert werden. Mit einer solchen Chipkarte könnte der Netzbenutzer seine Texte nicht nur verschlüsselt versenden, sondern zusätzlich

- sich gegenüber Computern und Kommunikationspartnern ausweisen und seine Zugriffsberechtigung nachweisen,
- den von ihm versandten Text so mit einer Zahl kennzeichnen, daß der Empfänger prüfen kann, ob er tatsächlich der Ab-

sender des Textes ist (elektronische Unterschrift),

- was immer er an Informationen sichern will, verschlüsselt in Datenbanken speichern.

Der Teufel steckt jedoch auch hier im Detail:

- Auch das Kryptosystem kann nicht verhindern, daß Mitarbeiter unzulässig Informationen über Bürger austauschen.
- Schon viele haben diese neuen Kryptosysteme theoretisch untersucht; der — letztendlich entscheidende — Praxistest ist jedoch noch nicht bestanden. Diese Systeme benötigen nämlich besonders schnelle elektronische Bausteine, die sehr teuer und noch nicht entwickelt sind. Zudem sind die Chipkarten noch nicht erprobt; ihre Eignung für diese neuen Krytposysteme muß sich erst noch erweisen.

Alles in allem: Die Verschlüsselungstechnik ist noch weit davon entfernt, ein Universalnetz für den Datenschutz erträglich zu machen. Unerläßlich ist deshalb, daß die Landesregierung an ihren eigenständigen, nach außen abgeschotteten Netzen für Polizei, Finanzverwaltung, Oberschulämter, Statistisches Landesamt und dem des RSJW festhält.

3.3 Sicherheitsprobleme bei Personal Computern

Der Vorschlag im Diebold-Dornier-IKOSS-Gutachten, künftig Personal Computer in der Verwaltung einzusetzen, ist nicht neu. Schon jetzt haben viele Behörden solche leistungsfähigen Rechenzwerge. Mit ihnen drucken erstaunlich viele Gymnasien und Berufsschulen Schülerkarteikarten und Schulbescheinigungen. Sie können damit auch Elternbeiräte und Lehrer registrieren, Abiturnoten speichern und einige Verwaltungsarbeiten, die zum Schuljahresende anfallen, erledigen. Der Einsatz von Personal Computern wird weiter zunehmen; denn sie sind wichtige Bausteine bei der Bürokommunikation und billige Hilfsmittel für die Verwaltung.

3.3.1 Was der Personal Computer Neues bringt

Wer mit einem Personal Computer das Minirechenzentrum auf dem Schreibtisch hat, ist Auftraggeber, Programmierer, Maschinenbediener, Systemanalytiker, Datenträgerarchivar und Anwendungsberater in einem. Trotz dieser Fülle technischer Aufgaben ist der Personal Computer nicht für EDV-Spezialisten, sondern für Laien gedacht. Damit diese ihn für ihre Arbeit benutzen können, gibt es einfach zu bedienende Datenbanksysteme, „bedienerfreundliche" Auswertungsprogramme und einfache Programmiersprachen. Viele schaffen es, damit innerhalb von Stunden die ersten Personendaten zu speichern, wieder am Bildschirm anzuzeigen, auszuwerten und zu drucken.

3.3.2 Seine speziellen Risiken für den Datenschutz in der öffentlichen Verwaltung

In der ersten Euphorie übersehen die PC-Fans eine ganze Menge ernster Probleme.

3.3.2.1 Richtig programmieren will gelernt sein

Auch wer mit dem Personal Computer programmiert, kann sich nicht — wie die Werbung oft suggeriert — hinsetzen und einfach loslegen. Erst muß man das zu lösende Problem durchdenken, auf die EDV-Technik übertragen und ein wirksames Konzept zur Datensicherung entwickeln. Bereits dies dürfte in der Regel einen EDV-Laien überfordern. Anschließend muß er auch noch die gefundene Lösung dokumentieren und erst danach kann er mit dem Programmieren beginnen. Viele meinen, damit habe die Arbeit ihr Ende. Doch weit gefehlt: er muß die Programme noch gründlich testen, verständlich und vollständig beschreiben und dann, wenn er weiß, daß alles richtig ist, für den Einsatz freigeben. Wer dies nicht beachtet,

- — fabriziert in der Regel Programme, die bei seiner Abwesenheit (Urlaub, Krankheit, usw.) niemand versteht und anwenden kann,
- — hat in ihnen erfahrungsgemäß viele Fehler,
- — verliert auf die Dauer selbst den Überblick über seine Programme und weiß nicht mehr, welche Daten er wo hat,
- — bringt mit großer Wahrscheinlichkeit seine Behörde in die unerfreuliche Situation, auf ein EDV-Verfahren angewiesen zu sein, das niemand mehr pflegen, verstehen, fehlerfrei bedienen und wirtschaftlich handhaben kann und
- — verliert oder verfälscht unter Umständen sogar ungewollt Personaldaten.

Was außerdem noch passieren kann, erlebte ich bei einer Kontrolle des Oberschulamts Karlsruhe. Einer seiner Mitarbeiter schrieb für seinen Personal Computer mehrere Programme, die dem Oberschulamt die Organisation des Abiturs erleichtern. Mit ihrer Hilfe wird der Einsatz der Erst- und Zweitkorrekturen geplant und die Fahrtroute für die Anlieferung der Abitursaufgaben bei den Schulen festgelegt. Anstelle einer vollständigen und verständlichen Beschreibung dieser Programme übergab uns das Oberschulamt drei kurze, wenig aussagefähige Aktenvermerke sowie einige unkommentierte, handschriftliche Tabellen und einen in sehr individueller, formelhafter Form gehaltenen „Verarbeitungsplan". Wie der Personal Computer zu bedienen ist, welche Programme zu dem EDV-Verfahren gehören, über welche Personengruppen er Angaben speichert,

welche Informationen im einzelnen vermerkt und welche Auswertungen möglich sind, war daraus nicht zu entnehmen. Kurzum: An eine echte Kontrolle war wegen der unzureichenden Beschreibung nicht zu denken. Was folgt daraus? Damit die im Rahmen des Landessystemkonzepts in den Behörden eingesetzten Personal Computer ordnungsgemäß arbeiten und kontrollierbar sind, muß die Programmierung durch EDV-Laien immer eine Ausnahme sein. Meint eine Behörde, einer ihrer Mitarbeiter sei gleichwohl sachkundig genug, muß sie auf jeden Fall wissen, welche Personendaten er mit welchem Personal Computer wie verarbeitet. Selbstverständlich muß sie auch den Einsatz des Personal Computers und der Programme in der Regel schriftlich genehmigen.

3.3.2.2 Unzählige Datensammlungen können entstehen

Weil Mitarbeiter von Behörden mit einem Personal Computer im Handumdrehen neue Dateien, neue Register, Kopien elektronischer Akten oder neue Datenbanken mit Informationen über Bürger anlegen können, besteht beim Landessystemkonzept die Gefahr, daß in kurzer Zeit niemand mehr durchschaut, welche Datenverarbeitung sie tatsächlich betreiben. Diese Gefahr läßt sich selbst durch ein Bündel von Gegenmaßnahmen nur wenig verringern:

So dürfen Behörden Personal Computer nur so einsetzen, wie es sich in ihr Gesamtkonzept zur Datenverarbeitung einfügt. Zudem müssen sie sicherstellen, daß immer mindestens zwei Personen wissen, wie der Personal Computer zu bedienen ist, welche Programme und Daten er wie verwaltet. Auch die technische Ausgestaltung des Personal Computers kann zu einer Minderung der Gefahren beitragen. Manche Methode, die bei Großrechnern selbstverständlich ist, kann sich auch hier bewähren. Beispielsweise kann man den Personal Computer so programmieren, daß der Mitarbeiter nicht beliebige, sondern nur ganz bestimmte Dateien und Programme nutzen kann. Ein Mißbrauch gelingt dann nur noch dem, der die vielen technischen Internas kennt.

3.3.2.3 Sicherheitssoftware fehlt

Anders als bei Großrechnern bieten die Programme der meisten Personal Computer keine Sicherheit: Sie erlauben jedem, Daten ohne Nachweis einer Berechtigung zu verarbeiten, zeichnen die durchgeführten Arbeitsvorgänge und die verwendeten Datenträger und Programme nicht automatisiert auf und bieten auch sonst kaum Sicherheit. Wenn Behörden gleichwohl so im Rahmen des Landessystemkonzepts mit Personal Computer Personendaten verarbeiten, riskieren sie viel:

- Unbefugte können mit diesen Personal Computern heimlich enorme Datenmengen auf einen Datenträger von der Größe einer Postkarte kopieren und an Dritte weitergeben. Weil der Personal Computer nicht festhält, wer dies wann machte, ist eine spätere Aufdeckung des Mißbrauchs ein seltener Glücksfall.

- Unbefugte, auch EDV-Laien, können mit solchen bedienerfreundlichen Personal Computern ohne weiteres Personendaten verfälschen, löschen, anzeigen oder ausdrucken. Der Personal Computer notiert sich nichts davon für spätere Prüfungen.

- Schon mancher PC-Bediener hat nach einem falschen Druck auf die Tasten Daten verloren. In der Beschreibung eines Programms für Personal Computer an Schulen las ich: „Wird der Programmlauf unsachgemäß unterbrochen, bevor der Nachlauf erfolgen konnte, so kann man in den meisten Fällen davon ausgehen, daß die aktuelle Datendiskette unbrauchbar ist." Solche Programme sind zur Verarbeitung von Personendaten schlicht ungeeignet.

Da der Schutz von Personendaten nicht von der Art des Computers abhängen darf, müssen ihn auch Personal Computer sicher bieten. Auf die notwendigen Sicherheitsmaßnahmen darf man nicht deshalb verzichten, weil diese die billigen Personal Computer verteuern. Die Behörden müssen vielmehr, wann immer sie im Rahmen des Landessystemkonzepts Personal Computer einsetzen, zunächst ein vollständiges Datensicherungskonzept erarbeiten. Dabei müssen sie unter anderem überlegen, wie ihre Arbeit bei einem Ausfall des Computers weitergehen soll. Ebenso müssen sie die unbefugte Nutzung des Personal Computers mit Kennworten oder anderen Schutzcodes weitgehend verhindern. Dazu ein Tip: Wer die Kennworte verschlüsselt im Personal Computer speichert, erreicht, daß sie weder EDV-Laien noch PC-Spezialisten lesen können. Die Verschlüsselung ist einfach, wenn man das Kennwort, das der Computer immer in eine Zahl umsetzt, multipliziert, dividiert oder sonst umrechnet und das Ergebnis anstelle des Kennworts speichert. Will ein Unbefugter dann mit dem Personal Computer Daten verfälschen, kann er nicht mehr bloß das Programm starten, sondern muß erst das geheime Kennwort finden. Das wird ihn aber bei einer guten Verschlüsselung eine geraume Zeit beschäftigen.

Hinzu kommt: Weil beim Landessystemkonzept mit dem Personal Computer auch sensitive Daten gespeichert und komplizierte Verarbeitungen durchgeführt werden, geht es ohne eine vor Verfälschung sichere automatisierte Proto-

kollierung der Datenverarbeitungsvorgänge oft nicht. Wenn ein Personal Computer dies nicht kann, muß notfalls ein eigenes Sicherheitsprogramm entwickelt oder auf den Einsatz des Personal Computers ganz verzichtet werden.

Genug der technischen Details: die drei Beispiele Bürokommunikation, Landeseinheitliches Netz und Personal Computer zeigen im einzelnen, wo die große Herausforderung des Landessystemkonzepts für den Datenschutz liegt. Wenn dieser Bericht dazu beiträgt, daß die Landesregierung diese Brisanz erkennt und keine Fakten schafft, ehe die drängendsten Probleme angepackt sind, wäre viel gewonnen.

2. Abschnitt: Bericht der Kommission „Neue Führungsstruktur Baden-Württemberg"

1. Ausgangslage

Wir leben in einer schwierigen Zeit: Arbeitslosigkeit und Umweltzerstörung sind ebenso wie das rasante Vordringen der neuen Technologien und der damit einhergehende atemberaubende Ausbau des Informationswesens nur einige der zahlreichen Probleme, vor denen Staat und Gesellschaft stehen und die es zu bewältigen gilt. Schon sprechen einige vom postindustriellen Zeitalter und der dritten industriellen Revolution. All dies ist sicherlich Anlaß genug, darüber nachzudenken, ob unser Regierungs- und Verwaltungssystem in der Lage ist, diesen Herausforderungen zu begegnen, und welche organisatorischen Veränderungen sie erfordern. Deshalb erwartete ich mit einiger Spannung, wie sich die von der Landesregierung eingesetzte Kommission „Neue Führungsstruktur für Baden-Württemberg" die Antwort auf diese Fragen vorstellt und welche Lösungen sie anbietet. Für mich war vor allem von Interesse,

- ob und welche Konsequenzen die Gutachter aus dem ständig wachsenden Einsatz der modernen Informationstechnik in der Verwaltung ziehen wollen,
- wie sie deren Auswirkungen auf das Verhältnis von Legislative zu Exekutive und vor allem vom Bürger zum Staat sehen,
- welche Gegenstrategien sie gegen die immer undurchschaubarer werdende Informationslandschaft und das damit einhergehende wachsende Mißtrauen des Bürgers einschlagen möchten,
- wie sie bei den Führungskräften in der Verwaltung Sensibilität für diese Problematik wecken wollen und
- welche Organisation der staatlichen Datenverarbeitung sie für notwendig halten, damit unsere auf die Grundrechte verpflichtete Verwaltung die Persönlichkeitsrechte der Bürger auch unter den Bedingungen der modernen Informationsverarbeitung achtet und schützt.

Leider enttäuschten die Gutachter alle, die im Kommissionsbericht nach befriedigenden Antworten auf diese Fragen suchen. Da wird vielmehr in völligem Gleichklang mit dem Landessystemkonzept ein möglichst umfassender Einsatz der neuen Kommunikations- und Informationstechniken in der Verwaltung gefordert und Baden-Württemberg die Aufgabe einer „Speerspitze

der Innovation und des Fortschritts" zugewiesen. Wer jedoch erfahren will, wie den sich daraus ergebenden Risiken für Staat, Gesellschaft und Bürger zu begegnen ist, geht weitgehend leer aus. Im Gutachten finden sich dazu nur einige sehr knappe Aussagen. Die beherrschenden Themen sind Steigerung der Effizienz und Leistungsfähigkeit. Ihnen hat sich alles andere unterzuordnen. Im Bürger sehen die Gutachter nur jemand, der einen effektiv arbeitenden Staatsapparat will. Bei einer solchen Sicht der Dinge verstellt sich nur allzu leicht der Blick dafür, daß Bürger in einem so effektiv arbeitenden Staat auch unter die Räder kommen und ihre berechtigten Anliegen unterdrückt werden können. Genau dies zu verhindern, ist aber eine der wichtigsten Aufgaben unseres Rechtsstaats. Effizienz ist deshalb auch insoweit gefragt. Dazu bedarf es nicht nur der richtigen Gesetze, sondern unterstützend auch einer sachgemäßen Organisation des Staatsgefüges. Besonders deutlich zeigt sich dies am Datenschutz: Zur Sicherung unseres informationellen Selbstbestimmungsrechts vor den Gefahren aus den Bedingungen der modernen Informationstechnik reicht nicht ein gutes Datenschutzrecht. Weil sich der Umgang des Staates mit den Informationen über Bürger weitgehend hinter verschlossenen Türen abspielt und damit deren Kontrolle und zugleich dem Blick der Öffentlichkeit entzogen ist, kommt es entscheidend auch darauf an, Organisation und Zuständigkeiten auf dem Gebiet des Datenschutzes so festzulegen, daß ein möglichst effektiver Persönlichkeitsschutz garantiert ist. Nur dann sehe ich eine Chance, das zweifelsohne vorhandene Mißtrauen und Unbehagen vieler Bürger gegen die staatliche Informationsverarbeitung abzubauen und der daraus resultierenden Staatsverdrossenheit entgegenzuwirken. Bedauerlicherweise spielten solche Überlegungen für die Kommission keine entscheidende Rolle. Zwar fehlte auch bei ihr nicht das inzwischen schon obligatorische formelhafte Bekenntnis zum Datenschutz und zur Ablehnung des gläsernen Menschen. Doch wirkt sich dies nicht auf ihre Vorschläge aus — im Gegenteil: sie sind alles andere als geeignet, den Datenschutz zu verbessern.

2. Die datenschutzrelevanten Vorschläge

Thema Nr. 1 der Kommission war der Zuschnitt der Ministerien. Sie entwickelte dazu eine Konzeption mit einigen bemerkenswerten Vorschlägen.

2.1 Ministerium für Kommunikation und Kunst

Von Interesse für den Datenschutz ist vor allem der Vorschlag, ein Ministerium für Kommunikation und Kunst zu schaffen. Dieses Ministerium soll

- den bereits im Landessystemkonzept vorgesehenen Einsatz der modernen Kommunikations- und Informationstechniken in der ganzen Landesverwaltung steuern und fördern,
- für die amtliche Statistik verantwortlich sein,
- Bibliotheken und Archive betreuen,
- die Rahmenbedingungen für die Entwicklung der alten und neuen Medien setzen,
- die Kunstförderung übernehmen und zugleich ein vielfältiges Kulturangebot gewährleisten und schließlich

— auch noch die Verantwortung für den Datenschutz übernehmen.

Der Gedanke, unter dem Dach eines Ministeriums Kunst und Computer zu vereinen, entbehrt sicherlich nicht einer gewissen Originalität — zeigt er doch, wie weit sich mit Hilfe der vielgepriesenen Kommunikation der Bogen spannen läßt. Nicht mehr originell, sondern höchst bedenklich ist freilich, in dieses heterogene Gebilde auch noch den Datenschutz einzubinden. Damit soll ausgerechnet das Ministerium für die Ausgestaltung und Auslegung des Datenschutzrechts federführend sein, zu dessen wichtigsten Aufgaben gehört, den Einsatz der modernen Kommunikations- und Informationstechniken voranzutreiben, und das zudem noch für die amtliche Statistik verantwortlich zeichnet. Anders gesagt: gerade die Stelle, die für einen umfassenden Technikeinsatz einzutreten hat, soll zugleich auch die Spielregeln erarbeiten und interpretieren, nach denen dieser Technikeinsatz erfolgen soll. Zielkonflikte sind damit von vornherein vorprogrammiert. Wer von Amts wegen die moderne Kommunikations- und Informationstechnik zu forcieren und die Automation der Verwaltung voranzutreiben hat, dem muß a priori daran gelegen sein, dabei auf möglichst wenig Hindernisse und Einschränkungen zu stoßen. Wer dagegen für den Datenschutz verantwortlich ist, der muß darauf achten, den Risiken aus dem Einsatz der modernen Techniken für das informationelle Selbstbestimmungsrecht wirksam entgegenzusteuern. Ich halte nicht für möglich, diesen offenkundigen Zielkonflikt innerhalb des vorgeschlagenen Ministeriums für Kommunikation und Kunst angemessen zu lösen. Vielmehr läßt diese Konstruktion von vornherein erwarten, daß der Datenschutz den kürzeren zieht und allenfalls noch eine Feigenblattfunktion hat:

— Für ein solches Schicksal des Datenschutzes spricht schon allein, wie die Kommission die Aufgaben innerhalb des Kommunikationsministeriums verteilen will. Zwei von vier Abteilungen mit insgesamt neun Referaten sollen sich ausschließlich mit dem Einsatz der modernen Kommunikations- und Informationstechniken beschäftigen. Einer der Referatsleiter soll zudem noch in Personalunion Präsident des Statistischen Landesamts sein und damit für eine enge Anbindung der amtlichen Statistik an das Ministerium sorgen. Dieser geballten Macht soll ein einzelnes Referat „Datenschutz" gegenüberstehen, das zudem noch die damit nicht in unmittelbarem Zusammenhang stehende Aufgabe der Datenschutzkontrolle über den privaten Bereich hat. Allein schon diese Gegenüberstellung zeigt, wie die Gewichte innerhalb des Kommunikationsministeriums verteilt wären.

— Nicht hoch genug veranschlagen kann man die große politische Bedeutung, die die Landesregierung dem Einsatz der modernen Kommunikations- und Informationsverarbeitungstechniken beimißt. Bei dieser Ausgangslage wäre es reines Wunschdenken, zu erwarten, der Kommunikationsminister würde im Konfliktfall zugunsten des Datenschutzes entscheiden.

— Ein weiteres ist zu bedenken: Der Datenschutz kann nicht etwa wie andere Interessen auf die lautstarke Unterstützung organisierter Gruppen rechnen — im Gegenteil: betroffen sind in der Regel nur einzelne Bürger und dazu

gerade oft solche, die sich in einer besonders schutzbedürftigen Lage befinden und keine Lobby haben.

— Dahinstehen mag, ob die These der Kommission, Interessen- und Zielkonflikte müßten in aller Regel innerhalb eines Ministeriums ausgetragen werden, als Grundsatz sinnvoll ist. Jedenfalls nicht akzeptieren kann man sie, wenn die Gewichte innerhalb eines Ministeriums von vornherein so ungleich verteilt sind, daß ein angemessener Ausgleich nicht zu erwarten ist.

— Schließlich müssen sich die Stimmen, die der automatisierten Datenverarbeitung alles Schlimme zutrauen, durch die vorgeschlagene Konstruktion in ihrer Haltung bestätigt sehen. Schon die jetzige Zuordnung des Datenschutzes zum Innenministerium erwies sich in dieser Beziehung als wenig glücklich. Schon jetzt besteht vielfach der sicherlich nicht ganz unbegründete Eindruck, daß beim Innenministerium die Belange der Polizei klar dominieren. Diese Problematik würde aber in noch stärkerem Maße auftreten, wenn der Datenschutz bei dem Ministerium ressortieren würde, das den Einsatz der elektronischen Datenverarbeitung in der Verwaltung wo auch immer — sei es Polizei, Sozialversicherung, Personal, Schulen oder Bibliotheken — in großem Stil betreiben soll.

2.2 Zusammenlegung von Justiz- und Innenministerium

Zu Recht stieß der Vorschlag der Kommission, aus dem Innenministerium und Justizministerium ein Ministerium für Inneres und Justiz zu bilden, auf erhebliche Kritik. Gerade er zeigt mit aller Schärfe, wie die Kommission viel zu sehr auf Effizienz und Leistungsfähigkeit des Staates fixiert war und wie sie viel zu wenig Sensibilität für die Aufgabe unseres Rechtsstaats entwickelte, dem Bürger auch einen effektiven Schutz gegen den Staat selbst zu gewähren und dafür Vorkehrungen zu schaffen. Wie sehr die Kommission dieses Verfassungsgebot vernachlässigte, sieht man gerade auch am datenschutzrechtlichen Aspekt. Ob Verfassungsschutz, Polizei, Staatsanwaltschaft oder Strafvollzug: alle sammeln und speichern in großem Umfang Informationen über Bürger aus durchaus unterschiedlichen Gründen für durchaus unterschiedliche Zwecke. Faßt man diese Bereiche unter dem Dach eines Supersicherheitsministeriums zusammen, wäre zu befürchten, daß sich die jetzt schon erkennbare Tendenz verstärkt, intensiver als bisher Querverbindungen herzustellen und die Daten des einen Bereichs auch für den eines anderen zu nutzen. Wer diese Gefahr leugnen wollte, verkennt, daß Organisation nicht eine Sache ist, die man völlig losgelöst vom materiellen Recht sehen kann und damit überhaupt nichts zu tun hat. Im Gegenteil: zwischen beiden bestehen enge Wechselbeziehungen. Man muß deshalb kein Prophet sein, um vorauszusagen, daß im Fall eines Ministeriums für Inneres und Justiz auch die Zusammenarbeit zwischen Verfassungsschutz, Polizei und Staatsanwaltschaft in der Datenverarbeitung auf eine Art und Weise intensiviert würde, wie sie niemand wünschen kann.

2.3 Die Landesdatenschutzkommission

Die Gutachter erarbeiteten nicht nur Vorschläge zur Steigerung der „Effizienz und Schlagkraft" der Ministerien und ihrer nachgeordneten Behörden, sondern befaßten sich auch

mit meinem Amt und machten dazu einen Vorschlag: anstelle der Landesbeauftragten für den Datenschutz soll eine Landesdatenschutzkommission treten. Diese soll nicht mehr — wie mein Amt jetzt — organisatorisch an das Innenministerium angebunden, sondern selbständig sein. Die Mitglieder der Landesdatenschutzkommission können — so die Gutachter — aus allen Bereichen des gesellschaftlichen Lebens kommen. Nur der Vorsitzende der Kommission soll hauptamtlich tätig sein; bei den übrigen Mitgliedern reiche, meint der Kommissionsbericht, eine nebenamtliche Beschäftigung aus.

Soweit die Gutachter für eine Lösung der organisatorischen Anbindung meiner — in der Amtsausübung seit jeher unabhängigen — Dienststelle an das Innenministerium plädieren, ist ihnen beizupflichten. Der vielgerügte „böse Schein" entfiele. Sinn macht das Ganze freilich bloß, wenn mein Amt zugleich oberste Landesbehörde würde, wie es die Rechnungshöfe und beispielsweise auch der Landesbeauftragte für den Datenschutz in Berlin sind. Das wäre eine echte Alternative zu der immer wieder gewünschten Zuordnung meines Amtes zum Parlament. Von oberster Landesbehörde ist freilich im Kommissionsbericht nicht die Rede. Im Gegenteil: Der Vorschlag Nr. 92 zu meinem Amt steht im Kapitel über die Behörden unterhalb der Ministerien — ganz so, als ob mein Amt eine nachgeordnete Behörde des Innenministeriums wäre. Ein kurzer Blick in die amtliche Begründung des Landesdatenschutzgesetzes (LT-Drs. 7/2550, S. 44) hätte die Gutachter eines anderen belehrt. Mag man dies noch als Versehen abtun — keinen Zweifel, wie wenig es der Kommission letztlich um eine Stärkung der unabhängigen Datenschutzkontrolle ging, kann man mehr haben, wenn man die von ihnen propagierte Landesdatenschutzkommission näher unter die Lupe nimmt. Dieser Vorschlag hätte nur Nachteile für den Datenschutz:

— Zum einen kann ich mir nicht vorstellen, wie ein Gremium aus nebenamtlichen Mitgliedern in der Lage sein soll, alle bei meinem Amt anfallenden Entscheidungen zu treffen, erforderlichen Stellungnahmen zu verfassen und Rechtsauskünfte zu geben. Die Gutachter haben offensichtlich Vorstellungen über die Tätigkeit meines Amtes, die meilenweit von der Realität entfernt sind. Die Aufgabe einer Datenschutzbeauftragten besteht nicht nur darin, systematisch einzelne Datenverarbeitungssysteme oder einzelne Behörden daraufhin zu überprüfen, ob sie die notwendigen Schutzvorkehrungen gegen Datenmißbrauch getroffen haben, und darüber nach und nach einen Kontrollbericht zu fertigen. Eine der wichtigsten Aufgaben meines Amtes ist, in angemessener Zeit auf die vielen Sorgen und Anliegen von Bürgern zu reagieren; sie kann man nicht damit vertrösten, die Kommission werde zu gegebener Zeit über ihr Anliegen entscheiden. Nicht minder gilt es, Anfragen von Behörden zu beantworten, die möglichst bald wissen wollen, ob ihre geplanten Vorhaben und Entscheidungen datenschutzrechtlich unbedenklich sind. Da die Kommission mit ihren nebenamtlich tätigen Mitgliedern ja nicht permanent, sondern nur in größeren Abständen tagen könnte, käme es unausweichlich zu ganz erheblichen Verzögerungen. Die von den Gutachtern immer wieder zitierte „Schlagkraft" der unabhängigen Datenschutzkontrolle wäre beeinträchtigt. Ein weiteres kommt hinzu: Im Rahmen der Daten-

schutzkontrolle sind in aller Regel sehr schwierige, praktisch alle Bereiche der öffentlichen Verwaltung erfassende Rechts- und Sachfragen zu klären. Mir ist unerfindlich, wie ein nebenamtlich tätiges Mitglied in der Lage sein soll, sachgerecht an diesen Entscheidungen mitzuwirken, zumal es nicht einmal über eine qualifizierte Vorbildung verfügen muß. Alle diese Ungereimtheiten erklären sich zu einem guten Teil damit, daß die Gutachter das nicht taten, was sie in ihrem Kommissionsbericht von jeder Führungskraft als unerläßlich fordern — sich vor einer Entscheidung ausreichend über die Entscheidungsgrundlagen zu informieren. Zwar sprachen sie, wie sie selbst betonen, vor Abfassung ihres Kommissionsberichts mit Fachleuten der verschiedensten Führungsebenen in Politik und Verwaltung, holten Stellungnahmen ein und scheuten selbst Informationsbesuche nach Japan nicht. Bloß bei der Datenschutzkontrolle glaubten sie, ihren Vorschlag aus dem Handgelenk schütteln zu können, ohne sich zuvor an Ort und Stelle zu informieren. Hätten die Gutachter hier über ihrer Begeisterung für die neuen Kommunikationstechniken das alte bewährte Kommunikationsmittel des Gesprächs nicht vergessen, wäre ihnen wohl manche Fehleinschätzung nicht unterlaufen.

— Vor allem hätte ihr Vorschlag auch negative Folgen für die Qualität der Arbeit der Datenschutzkontrolle. Ganz deutlich zeigt sich dies an der Aussage im Kommissionsbericht, die vorgeschlagene Lösung gewährleiste „unabhängig von der Person einzelner auf Dauer eine wirkungsvolle, sachgerechte und ausgewogene Erfüllung der notwendigen Kontrollaufgaben". Ausgewogenheit der Datenschutzkontrolle ist also das entscheidende Anliegen der Gutachter. Wenn Worte einen Sinn haben, kann dies doch bloß bedeuten, daß künftig die Belange des Persönlichkeitsschutzes zurücktreten sollen zugunsten der Interessen der Verwaltung und einer möglichst effektiven Aufgabenerfüllung. Genau dies aber wollte der Gesetzgeber durch die neue Institution eines Landesbeauftragten für den Datenschutz verhindern, wie ein Blick in die amtliche Begründung des Landesdatenschutzgesetzes zeigt (LT-Drs. 7/2590 S. 26). Dort heißt es:

> „Zwar sind die Behörden und sonstigen öffentlichen Stellen aufgrund ihrer Bindung an Recht und Gesetz ohnehin verpflichtet, einen den gesetzlichen Anforderungen entsprechenden Datenschutz innerhalb ihres Zuständigkeitsbereiches sicherzustellen. Diese Selbstkontrolle allein erscheint jedoch nicht ausreichend, da Gesichtspunkte des Datenschutzes und Überlegungen einer wirtschaftlichen und effektiven Verwaltungsführung nicht selten miteinander in Widerspruch treten und zu einer Interessenkollision führen können."

Ich sehe keinen Grund, warum das, was im Jahr 1977 richtig war, heute nicht mehr gelten soll.

— Schließlich muß man sich beim Vorschlag der Gutachter ernsthaft fragen, ob überhaupt noch von einem unabhängigen Kontrollorgan die Rede sein kann. Ich meine: ganz sicher dann nicht mehr, wenn Mitglied der Landesdatenschutzkommission auch werden kann, wer in Institutionen beschäftigt ist, die ihrer Kontrolle unterliegen. Dann hätten wir nämlich die Situation, daß sich die Kontrolleure selbst kontrollieren.

Aus all diesen Gründen kann ich nur warnen, den Vorschlag einer Landesdatenschutzkommission zu realisieren. Unser Staatswesen ist auf das Vertrauen seiner Bürger in die Funktionsfähigkeit und Glaubwürdigkeit seiner Institutionen angewiesen. Dieses Vertrauen ist umso größer, je effektiver die zum Schutz der Bürgerrechte geschaffenen Kontrollorgane arbeiten können. Wer dies für richtig hält, dem kann nicht an einer „ausgewogenen", zahmen Datenschutzkontrolle gelegen sein, wie sie die vier Kommissionsmitglieder — ein Regierungspräsident, ein Oberbürgermeister, ein Vorstandsvorsitzender einer großen Lebensversicherung und der Vorsitzende der Geschäftsführung der größten Computerfirma in der Bundesrepublik — wollen. Hat ihnen vielleicht ihr erhebliches berufliches Interesse an einem umfassenden Einsatz der modernen Kommunikations- und Informationstechniken den Blick etwas getrübt für das, was eine funktionsfähige Demokratie auf dem Weg in die Informationsgesellschaft braucht?

3. Abschnitt: Der Gesetzgeber und der Datenschutz

1. Ausgangslage

Die öffentliche Verwaltung braucht nahezu für alles, was sie tut, Informationen über Bürger. Sobald der Gesetzgeber eine Verwaltungsaufgabe neu regeln will, stellt sich deshalb die Frage, welche Vorschriften er zum Schutze der dafür benötigten Informationen schaffen muß. In der Vergangenheit ließ der Gesetzgeber diesen Aspekt weitgehend ungeregelt oder glaubte, mit sehr vagen Generalklauseln auskommen zu können. Eine solche Zurückhaltung ist spätestens seit dem Volkszählungsurteil nicht mehr möglich. Jetzt gilt es, neben dem Neuen, was in der Gesetzgebung ohnehin ansteht, das geltende Recht daraufhin abzuchecken, ob es das informationelle Sellbstbestimmungsrecht so schützt, wie es unsere Verfassung will.

Diese Umstände lösten 1985 wichtige gesetzgeberische Aktivitäten aus. Zu nennen sind dabei vor allem
- die Bemühungen um eine Novellierung des Bundes- und des Landesdatenschutzgesetzes,
- die Vorschläge zur Schaffung der erforderlichen Rechtsgrundlagen für die Informationsverarbeitung von Polizei, Staatsanwaltschaft, Verfassungsschutz, Bundesnachrichtendienst und militärischem Abschirmdienst,
- der Erlaß des Mikrozensusgesetzes und des Volklszählungsgesetzes 1987.

Daneben gibt es noch eine ganze Reihe weiterer wichtiger Gesetzesvorhaben für den Datenschutz. Ich nenne bloß die Stichworte: maschinenlesbarer Personalausweis und maschinenlesbarer Paß, Führerschein auf Probe, ZEVIS, Novelle zum Personenstandsgesetz, Archivgesetze und Landesmediengesetz. Damit sind freilich keineswegs alle Bereiche beschrieben, in denen Gesetzgebungspläne mit Datenschutzrelevanz heranreiften. Im Gegenteil: man diskutierte mal über das Eine, mal über das Andere; zu einem Abschluß des Gesetzgebungsverfahrens kam es jedoch nur in relativ wenigen Fällen. Auch darin spiegelt sich der Stellenwert wider, den Politik und Gesellschaft dem Datenschutz zur Zeit zubilligen.

2. Die Datenschutzgesetze

Daß wir eine Novelle der Datenschutzgesetze des Bundes und der Länder brauchen, ist fast unbestritten. Weit gehen jedoch die Vorstellungen auseinander, wie dies geschehen soll. Eine der entscheidensten kontroversen Frage ist dabei, ob der bisherige Anwendungsbereich der Datenschutzgesetze auszudehnen, beizubehalten oder gar einzuschränken ist. Um die Tragweite dieses sich so spröde ausnehmenden Problems zu ermessen, muß man wissen:

— Die allgemeinen Datenschutzgesetze schützen bisher nur Personendaten, die in Dateien — vereinfacht, aber verständlicher gesagt: Karteien oder EDV-Datensammlungen — gespeichert sind. Informationen, die sich „nur" in normalen Akten, Listen oder Verzeichnissen finden, erfreuen sich dieses Schutzes dagegen nicht.

— Die allgemeinen Datenschutzgesetze regeln bislang nur, unter welchen Voraussetzungen jemand Personendaten in Dateien speichern, verändern, daraus an Dritte weitergeben darf und zu löschen hat. Sie sagen — sieht man von der Hinweispflicht des § 9 Abs. 2 LDSG ab — nicht, was es alles zu beachten gilt, wenn sich eine Behörde Informationen über einen Bürger beschaffen will.

Das Grundrecht auf informationelle Selbstbestimmung kennt diese Einschränkungen der Datenschutzgesetze nicht. Es schützt den Bürger generell — also auch gegen Informationsgier sprich: unbegrenzte Datenerhebung, und macht keinen Unterschied, ob Behörden die Daten in Karteien, EDV-Sammlungen, Akten oder ähnlichen Unterlagen festhalten. Deshalb liegt mehr als nahe, die bisherigen Einschränkungen der Datenschutzgesetze aufzugeben und in ihnen ganz allgemein zu regeln, unter welchen Voraussetzungen Behörden Personendaten sammeln, aufbewahren, nutzen und weitergeben dürfen. So sehen es denn auch alle Datenschutzbeauftragten und meinen, dieser Weg sollte beschritten werden. Leider scheinen die in Politik und Ministerien Verantwortlichen für den Datenschutz einen anderen Weg einschlagen zu wollen. Nach Bonner Plänen, die auch das Innenministerium und die anderen Ressorts des Landes befürworten, soll es im wesentlichen beim bisherigen Anwendungsbereich der Datenschutzgesetze bleiben. Sie sollen also auch in Zukunft nur die Datenverarbeitung in Dateien regeln. Dabei ist sogar noch eine wichtige Einschränkung gegenüber der bisherigen Rechtslage vorgesehen: Die Datenschutzgesetze sollen nicht einmal mehr bestimmen, welche Hinweise eine Behörde dem Bürger geben muß, wenn sie von ihm Informationen will. Statt dessen will man in den Verwaltungsverfahrensgesetzen die erforderlichen Regelungen über die Datenerhebung und -verarbeitung in Akten treffen. Eine solche Aufsplitterung des allgemeinen Datenschutzrechts ist äußerst bedenklich:

— Damit wäre die Chance vertan, das Datenschutzrecht zu vereinheitlichen. Ganz im Gegenteil: Es käme sogar zu einer erheblichen Rechtszersplitterung. Das allgemeine Datenschutzrecht wäre vielerorts geregelt: Man hätte die Datenschutzgesetze, die Verfahrensgesetze und zudem noch eine Reihe gesonderter Gesetze, weil die Verfahrensgesetze im Gegensatz zu den allgemeinen Datenschutzgesetzen nur für einen Teil der Verwaltung gelten und folglich die Datenverarbeitung in Akten für die restlichen Verwaltungsbereiche andernorts zu regeln wäre.

— Da sich bei der Datenverarbeitung in Akten oft die gleichen Probleme wie bei der Datenverarbeitung in Dateien stellen, müßte der Gesetzgeber — will er nicht Gleiches ungleich behandeln — in den Verfahrensgesetzen insoweit die gleichen Begriffe verwenden und die gleichen Regelungen treffen wie in den Datenschutzgesetzen. Er könnte sich diese unnötige Belastung und den Bürgern und der Verwaltung die sicher nicht ausbleibende Verwirrung darüber ersparen.

— Die Behörden stünden vor kaum lösbaren Problemen, wenn sie im Rahmen eines Verwaltungsverfahrens Daten in Akten und zugleich auch in Dateien verarbeiten. Wie in solchen Fällen ein noch so gewiefter Mitarbeiter wissen soll, nach welchen Bestimmungen er sich zu richten hat, ist mir unerfindlich. Eine fehlerhafte Rechtsanwendung und damit ein Vollzugsdefizit im Datenschutz wären die unausweichliche Folge.

Wer trotz dieser Nachteile die geschilderte Lösung favorisiert, tut dies aus einem ganz bestimmten Grund: Sie ist die einfachste und eleganteste Art und Weise zu verhindern, die Kontrollbefugnisse der unabhängigen Datenschutzkontrolle auf die Datenverarbeitung in Akten und auf die Datenerhebung auszudehnen. Würde man diese Probleme in den Datenschutzgesetzen regeln, gleichwohl aber den Datenschutzbeauftragten die Kontrolle insoweit vorenthalten, wäre noch schwieriger, als dies bisher schon der Fall ist, zu begründen und Bürgern und Öffentlichkeit plausibel zu machen, warum die unabhängige Datenschutzkontrolle hier nicht tätig werden dürfen soll. Gerade aber Aktivitäten dieser Art sind für viele in Parlament, Regierung und Verwaltung eine Horrorvorstellung: die öffentlichen Auseinandersetzungen im Zuge des Gesetzes zur Änderung des Landesdatenschutzgesetzes vom 30. Juni 1982 (GBl. S. 265) zeigten dies nur zu deutlich. Was damals schon galt, gilt seit dem Volkszählungsurteil 1983 erst recht: der Bürger ist zum Schutze seines informationellen Selbstbestimmungsrechts auf eine unabhängige Datenschutzkontrolle mit umfassenden Kontrollbefugnissen angewiesen.

Meine Bedenken gegen die Gesetzgebungspläne legte ich schon im Juli 1985, als ich erstmals Näheres dazu hörte, dem Innenministerium dar und informierte darüber auch die anderen Ressorts. Annehmen möchte ich, daß man mein ausführliches Schreiben las; eine Reaktion steht allerdings immer noch aus.

3. Archivgesetze

Obwohl die Arbeit der öffentlichen Archive für das Verständnis unserer Geschichte und Kultur von unschätzbarer Bedeutung ist, waren die Archive lange Zeit Stiefkind. Mit daher rührt wohl, daß wir bis heute keine Gesetze darüber haben,
— wie die Archive in den Besitz der notwendigen Unterlagen und Informationen gelangen und
— wie man diese Unterlagen der Archive nutzen darf.
Erfreulicherweise scheint sich hier nun ein Wandel anzubahnen. Dem Bundestag liegt der Entwurf eines Bundesarchivgesetzes vor; bei ihm geht es vor allem um die Arbeit des Bundesarchivs. In Baden-Württemberg erarbeitete die Landesregierung den Entwurf eines Landesarchivgesetzes mit dem Ziel, die Tätigkeit der öffentlichen Archive im Lande auf eine klare,

einwandfreie Rechtsgrundlage zu stellen. Das Wissenschaftsministerium beteiligte mich von Anfang an an dieser Arbeit in einer Art und Weise, wie ich sie mir auch sonst wünsche.

3.1 Was kommt ins Archiv?

Zur Zeit erhalten die Archive längst nicht alle Unterlagen, die sie für ihre Aufgaben benötigen. Schuld daran sind freilich nicht, wie es immer wieder fälschlicherweise heißt, die allgemeinen Datenschutzgesetze, sondern die zahlreichen Geheimhaltungsvorschriften, die es in unserer Rechtsordnung gibt. Ich nenne beispielhaft bloß die Ärztliche Schweigepflicht, das Steuer- und Sozialgeheimnis, die Verschwiegenheitspflichten der Berufspsychologen, Mitarbeiter von Ehe- und Familien- oder Suchtberatungsstellen. Keine dieser Regelungen kennt bislang eine Offenbarungsbefugnis zugunsten der Archive. Ich meine, hier sind Lockerungen am Platze. Bei der Übergabe von Unterlagen, die solche besonderen Geheimhaltungsbestimmungen schützen, an die Archive darf man aber nicht gleich das Kind mit dem Bade ausschütten. Es gilt, den schutzwürdigen Belangen der Betroffenen Rechnung zu tragen — ganz besonders bei Unterlagen mit Informationen, die unter den Schutz von Berufsgeheimnissen im Sinne von § 203 Abs. 1 StGB fallen. Diese Informationen entstanden einst im Rahmen einer persönlichen Begegnung und einer daraus erwachsenen besonderen Vertrauensbeziehung. Hier kann es deshalb zum Schutze der Bürger sogar geboten sein, archivwürdige Unterlagen vor einer Übergabe an das Archiv so zu präparieren, daß daraus nicht mehr erkennbar ist, welche konkrete Person beraten oder behandelt wurde.

3.2 Kritik

Die geplanten Archivgesetze stießen in der Öffentlichkeit und bei Vertretern der Zeitgeschichte auf Kritik. Sie befürchten, die Gesetze würden die Erforschung der Zeit des Dritten Reiches erschweren oder gar unmöglich machen. Ich nehme diese Kritik sehr ernst. Es wäre fatal, wenn der Datenschutz dazu benutzt würde, die notwendige Erforschung des düstersten Kapitels unserer Geschichte zu torpedieren. Kein Kritiker konnte freilich bislang konkret sagen, welche Regelung aus welchem Grund nicht angehen kann. Ihre Kritik blieb bislang arg allgemein; sie ließ sogar unberücksichtigt, daß die Archive in Zukunft in jedem Fall mehr Unterlagen erhalten als bislang. Auch interpretierten nicht wenige in den Entwurf eines Bundesarchivgesetzes Dinge hinein, die gar nicht drin stehen. Das rührt freilich vornehmlich daher, daß dieser Gesetzentwurf sehr kompliziert, schwer lesbar und damit selbst für die Eingeweihten kaum zu verstehen ist. Drum scheint mir in erster Linie Aufklärung von Nöten. Sollte sich dabei herausstellen, daß die Kritik tatsächlich gerechtfertigt ist, bin ich gerne bereit, an der Suche nach einer angemessenen Lösung mitzuwirken.

4. Statistikgesetze

Im Mittelpunkt der Aktivitäten des Gesetzgebers auf dem Gebiet der Statistik standen 1985 der Erlaß eines neuen Mikrozensusgesetzes und des Volkszählungsgesetzes 1987. Kernfrage

beim Mirkozensusgesetz war: Auskunftspflicht oder freiwillige Erhebung. Wie inzwischen schon eine ganze Reihe von Bürgern erfahren mußte, blieb es bei der Auskunftspflicht. Der Gesetzgeber konnte sich nicht entschließen, neue Wege zu beschreiten. Immerhin zeichnet sich ein kleiner Hoffnungsschimmer ab: man will bis 1987 Testerhebungen auf freiwilliger Basis durchführen. Sie sollen zeigen, was an der Behauptung der amtlichen Statistik dran ist, ein unvertretbarer Genauigkeits- und Qualitätsverlust wäre die Folge eines Verzichts auf die Auskunftspflicht. Die für manche schon zum Reizwort gewordene Volkszählung soll nunmehr im Jahr 1987 stattfinden. Dabei werden sich sicher nicht wenige Bürger darüber wundern, daß die Fragen im wesentlichen dieselben sind, wie sie auf den Erhebungsvordrucken für die gescheiterte Volkszählung 1983 standen. Dies alles mag sich noch im Rahmen der Verfassung halten. Zu fragen bleibt freilich, ob der Gesetzgeber bei diesem Schritt gut beraten war oder ob er nicht mit weniger Fragen mehr erreichen könnte. Immerhin steht und fällt der Erfolg einer Volkszählung mit der Bereitschaft der Bürger, die Fragen zu beantworten.

4. Abschnitt: Auswirkungen auf die Datenschutzkontrolle

1. Verlagerung der Schwerpunkte

Die Zeiten, in denen mein Amt all die Aufgaben anpacken konnte, die meine Mitarbeiter und ich für notwendig erachten, sind vorbei. Das hat verschiedene Gründe:

1.1 Stellungnahme und Anhörungen

Ein wirksamer Datenschutz läßt sich nur mit Hilfe eines Datenschutzrechts erreichen, das auch diesen Namen verdient. Der unabhängigen Datenschutzkontrolle kann es deshalb alles andere als gleich sein, in welche Richtung die gegenwärtige Diskussion um die Fortentwicklung des Datenschutzrechts läuft. Sie muß versuchen, ihre Argumente in die Waagschale zu werfen, so gut es nur geht. Meine Bemühungen schlugen sich in zahlreichen schriftlichen Stellungnahmen zu geplanten Gesetzesvorhaben nieder. Daneben hatte ich Gelegenheit, meine Vorstellungen zu einzelnen Gesetzesvorhaben und Datenschutzproblemen in einer Reihe öffentlicher Anhörungen vorzutragen, die Ausschüsse des Bundestags, Landtags und einzelne Fraktionen dieser Gremien veranstalteten. Der Innenausschuß des Deutschen Bundestags lud mich zu seinen öffentlichen Anhörungen zum Volkszählungsgesetz 1987, Personalausweisgesetz und Bundesarchivgesetz ein, der Ständige Ausschuß des Landtags zu seinem Hearing über das Landesmediengesetz. Außerdem nahm ich an Anhörungen zur Errichtung eines zentralen Verkehrsinformationssystems (ZEVIS) beim Kraftfahrt-Bundesamt und zu Personalinformationssystemen in der öffentlichen Verwaltung teil.

1.2 Bürgereingaben

Mich der Sorgen der Bürger anzunehmen, sehe ich seit jeher als eine der wichtigsten Aufgaben meines Amtes an. Die Zahl der schriftlichen Eingaben, die mich täglich errei-

chen, stieg 1985 um über 50 % gegenüber 1984. Dazu kommen die vielen telefonischen Hilferufe aus der Bevölkerung und nicht wenige Frauen und Männer finden auch persönlich den Weg in mein Amt. Dies alles erforderte verstärkte Aktivitäten. Der steigende Zuspruch durch die Bürger zeigt zugleich, wie sich der Datenschutz immer stärker in das allgemeine Bewußtsein drängt. Die Bürger nehmen nicht mehr alles schicksalhaft hin, sondern fragen, was sie akzeptieren müssen und was nicht. Zugleich sehe ich in den zahlreichen Hilferufen auch einen Vertrauensbeweis für meine Arbeit.

1.3 Kontrollen

Die intensive Beschäftigung mit dem künftigen Datenschutzrecht und den Sorgen der Bürger wirkte sich naturgemäß auf die übrige Arbeit meines Amtes aus. Aus eigener Initiative konnten wir nicht mehr soviel Kontrollen vor Ort machen, wie es eigentlich die Sache erfordert. Zwar führten wir 1985 noch über 40, teils mehrtägige Kontrollbesuche durch. Doch ging es dabei in etwa der Hälfte der Fälle um Probleme, die Bürger an uns herantrugen oder die wir bereits in früheren Jahren aufgegriffen hatten und nun zum Abschluß bringen wollten. Mehr Kontrollen aus eigener Initiative — nicht bloß im Sicherheitsbereich — halte ich auf Dauer für unerläßlich.

2. Ausstattung der Dienststelle

Die Fülle drängender Aufgaben forderte mein Amt im vergangenen Jahr aufs Äußerte. Die Grenzen der Belastbarkeit sind erreicht, teilweise überschritten. Dazu muß man wissen, daß ich seit Jahren unverändert nur 11 Mitarbeiter einschließlich der Kräfte für Registratur, Schreibdienst und Geschäftsstelle habe und sich daran auch nach dem Volkszählungsurteil anders als im Bund und anderen Ländern nichts änderte. Nunmehr ist der Zeitpunkt gekommen, zu dem ich deutlich sagen muß: wenn Baden-Württemberg an einer Datenschutzkontrolle halbwegs gelegen ist, sind personelle Konsequenzen unausweichlich. Allein das Landessystemkonzept stellt mein Amt vor äußerst umfangreiche und schwierige neue Aufgaben. Hier aus Personalmangel einfach alles laufen zu lassen, hielte ich wegen der Brisanz dieses Vorhabens für unverantwortbar. Ähnliches gilt für viele andere Themen.

Leider konnten sich Landesregierung und Landtag trotz meiner Bitte nicht entschließen, im 1. Nachtrag zum Staatshaushaltsplan 1985/86 die notwendigen zusätzlichen Stellen für mein Amt aufzubringen. Immerhin stellt man mir nun zwei neue Mitarbeiter im Wege der Abordnung in Aussicht. Das wäre gewiß schon etwas. Bloß erübrigt sich für Landesregierung und Landtag damit nicht, die Stellensituation meines Amtes von Grund auf zu verbessern. Meine Vorschläge dazu liegen seit Monaten auf dem Tisch des Innenministeriums.

Meinen Mitarbeitern danke ich herzlich dafür, daß sie auch in der sehr angespannten Situation des Jahres 1985 durch ihren Einsatz und ihr Können entscheidend zum Gelingen unserer gemeinsamen Arbeit beigetragen haben.

3. Teil: Sorglosigkeit und Datenmißbrauch nehmen nicht ab

1. Aktuelle Mißbrauchsfälle

Wie es um den Datenschutz steht, läßt sich gewiß nicht an der Zahl der Mißbrauchsfälle ablesen. Ein wichtiges Indiz sind sie freilich allemal.

1.1 Der raffinierte Kreisamtmann

Daß man die elektronische Datenverarbeitung auch zu Manipulationen im großen Stil benutzen kann, mußte ein Landratsamt schmerzhaft erfahren: Ein Kreisamtmann seines Sozialamts veruntreute von 1982 bis 1985 mit Hilfe des EDV-Verfahrens „Wiederkehrende Ausgaben" in 50 Fällen insgesamt 379 540 DM. Seine Vorgehensweise war immer gleich und bestand aus drei Schritten:

— Sozialhilfekonto anlegen

Am Monatsanfang legte der Kreisamtmann in dem EDV-Verfahren „Wiederkehrende Ausgaben" ein Sozialhilfekonto mit Fallnummer und Unterkontonummer an und speicherte darin als Zahlungsempfänger sich und sein Bankkonto und als Sozialhilfeempfänger einen Bürger, den das Sozialamt betreute, oder eine fiktive Person. Das alles konnte er nach den Dienstvorschriften des Landratsamts allein und ohne Wissen anderer Mitarbeiter des Sozialamts tun.

— Geld überweisen

Jeweils in der Mitte des Monats fertigte der Kreisamtmann dann die Zahlungsanweisungen. Dazu benötigte er zwar neben der eigenen Unterschrift, mit der er zu Unrecht die sachliche und rechnerische Richtigkeit der Auszahlungen bestätigte, auch noch die Unterschrift eines Kollegen — in der Regel die seines Stellvertreters. Das war jedoch kein Hindernis. Denn nach der Gemeindekassenverordnung bestätigt der Zweitunterzeichner mit seiner Unterschrift nicht, daß mit der Auszahlung alles in Ordnung ist, sondern nur, daß derjenige, der die sachliche und rechnerische Richtigkeit per Unterschrift feststellte, dies auch formal tun darf. Folglich erhielt der Kreisamtmann die zweite Unterschrift ohne weiteres. Das für die Auszahlungsanordnung verwendete Formular erleichterte ihm die Sache noch zusätzlich: darin sind nämlich bloß die nichtssagende Fallnummer und Unterkontonummer einzutragen, nicht aber der Zahlungsempfänger. Zudem mußte der Kreisamtmann der Auszahlungsanordnung keine Belege, etwa Rechnungen beifügen. Die einzige Kontrollinstanz, die es für ihn gab, war das Rechnungsprüfungsamt des Landratsamts. Diese Kollegen trickste der Kreisamtmann jedoch im dritten Schritt aus.

— Manipulationen vertuschen

Am Monatsende oder in den ersten Tagen des Folgemonats — auf jeden Fall stets vor dem Druck der Umsatzliste zum Zwecke der Kontrolle durch das Rechnungsprüfungsamt — änderte der Kreisamtmann die im Computer gespeicherten Angaben über den Zahlungsempfänger: er löschte seine Anschrift und sein Bank-

konto und trug statt dessen Anschrift und Kontonummer eines der Krankenhäuser ein, mit denen das Sozialamt öfter zu tun hat. Das verblüffende Ergebnis dieser Aktion war: Auf der Kontrolliste des Rechnungsprüfungsamts erschienen dann nicht Name, Anschrift und Bankkonto des tatsächlichen Zahlungsempfängers, also des untreuen Kreisamtmann, sondern des Krankenhauses. Deshalb erregten die Auszahlungen des Kreisamtmanns beim Rechnungsprüfungsamt jahrelang keinen Argwohn.

Der Schwindel flog erst auf, als der Gemeindeprüfungsanstalt bei einer systematischen Kontrolle des Landratsamts die Höhe der einzelnen überwiesenen Beträge nicht plausibel erschien und sie deshalb nach Rechnungen und anderen Belegen suchte.

Das Landratsamt zeigte sich erstaunt über meine Intervention. Es war ihm bis dahin nicht bewußt, daß der Kreisamtmann nicht nur gegen das Strafgesetzbuch, sondern auch gegen Datenschutzvorschriften verstieß: Zum einen nutzte er unbefugt Daten von Sozialhilfeempfängern, die das Sozialamt zu Recht registriert. Zum andern speicherte er über diese Hilfeempfänger unrichtige Angaben, nämlich die in Wirklichkeit nicht erhaltenen Zahlungen. Zum dritten offenbarte er der Bank unbefugt deren Namen — standen diese doch in der Regel auf den Überweisungsbelegen. Diese datenschutzrechtliche Beurteilung teilte ich dem Landratsamt mit. Außerdem beanstandete ich die Art und Weise, wie das Landratsamt das von der Datenzentrale entwickelte und betreute landeseinheitliche EDV-Verfahren „Wiederkehrende Ausgaben" einsetzte. Es darf nicht angehen, daß ein EDV-Verfahren eine Liste erstellt, auf der Personen und Organisationen als Zahlungsempfänger erscheinen können, die in Wirklichkeit überhaupt keine Zahlungen erhielten. Solche eigenartigen Listen erleichtern Manipulationen und erschweren, die Datenverarbeitung zu überprüfen. Deshalb bat ich die Datenzentrale Baden-Württemberg, alle Anwender des EDV-Verfahrens „Wiederkehrende Ausgaben" auf den Trick des ungetreuen Kreisamtmanns aufmerksam zu machen, um Ähnliches andernorts zu verhindern.

Die Reaktionen des Landratsamts und der Datenzentrale waren unterschiedlich. Das Landratsamt bemüht sich seitdem um eine Verringerung des Mißbrauchsrisikos. Neben einem Bündel organisatorischer Neuregelungen wollte es auch eine Änderung der EDV-Programme erreichen. Die Datenzentrale lehnt dies jedoch kategorisch ab. Sie will nicht einmal die anderen Anwender des Verfahrens unterrichten, weil das Verfahren auch Listen drucke, die sich zur Kontrolle besser eignen als die vom Landratsamt erstellten. Wörtlich kann man von ihr lesen: Die Verwaltungen „haben i. d. R. die organisatorischen Maßnahmen zur Kontrolle getroffen. Zumindest waren sie jederzeit in der Lage dazu." So kann es nicht angehen: Die Datenzentrale müßte ihre Anwender selbst dann informieren, wenn überhaupt keine Zweifel in dem EDV-Verfahren bestünden. Davon kann jedoch nicht die Rede sein.

Die Staatsanwaltschaft will gegen den Kreisamtmann bald Anklage erheben. Sein datenschutzrechtliches Vergehen nach § 41 Abs. 1 Nr. 1 BDSG, will sie jedoch nach § 154 a StPO dabei nicht aufgreifen. Ich kann dies nur bedauern, aber nicht hindern; wegen der Sonderregelung des Sozialgesetzbuchs habe ich in diesem Falle kein Strafantragsrecht.

1.2 Datenmißbrauch bei der Polizei

Vereinzelt hatte ich schon früher über Datenmißbrauch bei der Polizei zu berichten. Die Reihe setzte sich fort. Ich weiß, daß dies Ausnahmefälle sind und die große Zahl der Polizeibeamten korrekt verfährt. Bloß den wenigen, die hier etwas anfälllig sind, ja die sich sogar mit ihren Möglichkeiten auf Polizeidaten zugreifen zu können, gegenüber Freunden und Bekannten brüsten, sei gesagt: Mißbrauchen Sie Ihre dienstliche Stellung nicht für private Zwecke. Wenn ein Fehlverhalten ans Tageslicht kommt — und so gering sind die Chancen dafür auch wieder nicht —, können die Folgen erheblich sein. Sie müssen nicht nur mit straf-, sondern vor allem mit dienstrechtlichen Konsequenzen rechnen. Es bekommt dem Ansehen der Polizei besser und ist auch mir lieber, wenn es über mißbräuchliche Datenabrufe nichts zu berichten gibt.

1.2.1 Polizeidaten im Wirtshaus

Vor einigen Monaten machten die gravierenden Verstöße eines Angestellten bei der Datenstation der Polizeidirektion Pforzheim Schlagzeilen. Der Mitarbeiter wollte wissen, was fünf seiner Bekannten alles auf dem Kerbholz hatten, rief deshalb nach und nach in der Personenauskunftsdatei, dem Informationssystem der baden-württembergischen Polizei, deren Daten ab und ließ sie sich sogar ausdrucken. Ein Teil dieser „Kontoauszüge" hob er bei sich zu Hause auf, wo man sie bei einer Durchsuchung fand. Andere händigte er den Betroffenen in deren Wohnung aus. Einen Ausdruck übergab er jemand mit der Bitte, ihn doch an den Betroffenen weiterzuleiten, was auch geschah. Über einen weiteren Bekannten fragte er zudem die Falldatei Rauschgift des Bundeskriminalamts ab und erfuhr, daß dieser zwei Rauschgiftdelikte begangen hatte. Den Computerauszug händigte er diesem aus. Als er einmal in der Registratur aushelfen mußte, entnahm er den Polizeiakten Lichtbilder zweier Bekannter, die die Polizei im Rahmen einer erkennungsdienstlichen Behandlung aufgenommen hatte. Während er das eine Lichtbild dem Bekannten lediglich zeigte und dann in seiner Wohnung aufbewahrte, händigte er das andere dem Betroffenen in einer Gaststätte in Gegenwart von Zeugen aus. Der Polizeiangestellte interessierte sich freilich nicht nur für die Daten seiner mit dem Gesetz in Konflikt geratenen Freunde, sondern auch für die Personalien des Leiters der Kriminalpolizei und eines weiteren Polizeikollegen. Deren Daten fragte er über den Online-Anschluß der Polizei an das Kraftfahrt-Bundesamt (ZEVIS) ab. Dies alles machte er, um in seinem Bekanntenkreis mit seinen Zugriffsmöglichkeiten auf Polizeidaten und seinem Wissen renommieren zu können. Inzwischen ist er aus dem Dienst entlassen. Nachdem mehrere Betroffene und ich Strafantrag gestellt haben, wird er wohl in Kürze angeklagt.

1.2.2 Der gläserne Geschäftsführer

Seit nunmehr 2½ Jahren ermittelt eine Staatsanwaltschaft „gegen Unbekannt"; der Tatverdacht richtet sich jedoch allein gegen Polizeibeamte. Bislang steht

folgender Sachverhalt fest: Der Geschäftsführer eines Unternehmens in Südwürttemberg hatte die Aufnahme in seinen Bundesverband beantragt. Zunächst erhielt er einen positiven Bescheid. Ein 3/4 Jahr später teilte ihm der Verband dann mit, der Vorstand habe den Aufnahmebeschluß widerrufen, weil gegen ihn 5 Ermittlungsverfahren — und zwar je zwei wegen Körperverletzung und Beleidigung und eines wegen Betrugs — anhängig seien. Bemerkenswert an dem Schreiben war, daß nicht nur die Tatvorwürfe, sondern auch der Tag bzw. das Jahr der polizeilichen Anzeigen, die sachbearbeitenden Polizeidienststellen und deren Aktenzeichen angegeben waren. Aus welcher Quelle der Bundesverband diese Informationen hatte, sagte er nicht. Der Geschäftsführer war über den Inhalt des Schreibens sehr erstaunt. Er vermutete den Informanten des Bundesverbands in Kreisen der Polizei und erstattete Anzeige wegen eines Vergehens gegen das Landesdatenschutzgesetz. Auch ich stellte Strafantrag. Für die Täterschaft eines Bediensteten der Polizei spricht in meinen Augen, daß eine Reihe von Angaben im Schreiben des Verbandes — beispielsweise Art des Delikts, Tag der Anzeige und sachbearbeitende Polizeidienststelle — in der Regel nur Insidern bekannt sind. Sie allein können sich diese Daten durch eine Abfrage des polizeilichen Informationssystems oder durch Einsichtnahme in die Ermittlungsakten leicht beschaffen. Hinzu kommt, daß die Aufzählung der Daten, wie sie in dem Brief an den Geschäftsführer erfolgte, in dieser Form nur bei der Polizei üblich ist. Erhärtet wird meine Vermutung schließlich durch den gegenwärtigen Ermittlungsstand, über den ich selbstverständlich keine näheren Einzelheiten mitteilen kann. Soviel kann ich jedoch sagen: In der fraglichen Zeit bekundete ein Außenstehender gegenüber Polizeibeamten Interesse an Informationen über den Geschäftsführer. Fest steht auch, daß kurz danach Polizeibeamte die polizeilichen Informationssysteme nach Informationen über den Geschäftsführer abfragten, obwohl sie diese Angaben für dienstliche Zwecke nicht benötigten. Ob sich darüber hinaus noch ermitteln läßt, wer genau dies war, bleibt abzuwarten; die Staatsanwaltschaft ist darum intensiv bemüht. Unabhängig hiervon möchte ich jedoch auf eines hinweisen: Die polizeilichen Informationssysteme sind für die Arbeit der Polizei bestimmt. Nur in seltenen Ausnahmefällen — etwa, um Straftaten aufzuklären oder zu verhüten oder erhebliche Gefahren abzuwehren — kann es angehen, daß sie aus ihren Datenbanken Informationen an Privatpersonen oder Firmen gibt. Solch ein Ausnahmefall lag hier sicher nicht vor. Einem Verband drohen nicht schon dann erhebliche Gefahren, wenn er einen Bürger aufnimmt, gegen den die Polizei mehrere Ermittlungsverfahren führt oder führte. Es ist daher nicht Aufgabe der Polizei, den Verband vor solchen Bürgern unter Offenlegung ihres Wissens zu warnen. So verständlich es ist, daß sich ein Verband vor vermeintlichen „schwarzen Schafen" in seinen Reihen schützen will, so klar ist auch, daß dies nicht über einen Informationsaustausch zwischen Polizei und Verband geschehen darf. Ein Verband muß sich vielmehr der Möglichkeiten bedienen, die die

Rechtsordnung dafür vorsieht: er kann beispielsweise von dem, der bei ihm Mitglied werden will, ein polizeiliches Führungszeugnis verlangen.

1.2.3 Hilfe für den Geschäftsfreund

Im Zuständigkeitsbereich der Landespolizeidirektion Stuttgart II ereignete sich anderes: Ein Polizeibeamter war nebenher als Teilhaber einer privaten GmbH A tätig. Diese stand in Geschäftsbeziehungen zu einer Firma B, die weltweit Großbauprojekte organisierte. Als eines Tages ein jugoslawischer Unterhändler zu geschäftlichen Besprechungen mit der Firma B nach Stuttgart kommen wollte, erbot sich der Polizeibeamte, bei der Einreisegenehmigung behilflich zu sein. Zunächst rief er im polizeilichen Informationssystem INPOL ab, ob und welche Daten über den Unterhändler gespeichert sind. Dabei erfuhr er, daß gegen ihn seit 1975 eine Ausweisungsverfügung wegen Schwarzarbeit vorliegt und er deshalb im Falle einer Einreise festzunehmen sei. Diese Informationen gab der Polizeibeamte an den Geschäftsführer der Firma B und andere Personen weiter. Da er dies aus privaten Gründen machte, stellte ich gegen ihn Strafantrag. Die Staatsanwaltschaft erhob wegen dieser Verstöße Anklage. Das Amtsgericht Stuttgart stellte jedoch im Oktober 1985 das Verfahren in der Hauptverhandlung gegen Zahlung einer Geldbuße von 2 000 DM ein, weil der Abruf der Daten zwar unbefugt, jedoch letztlich im Interesse des Unterhändlers erfolgte. Der Polizeibeamte ist inzwischen aus dem Polizeidienst ausgeschieden.

1.2.4 Der vorgetäuschte Verkehrsunfall

Erstmals erfuhr ich von einem Bürger, der vom Wissen der Polizei profitieren wollte. Eines Tages erschien er auf der Wache eines Stuttgarter Polizeireviers und erklärte, soeben einen Pkw mit dem amtlichen Kennzeichen LB ... angefahren und leicht beschädigt zu haben. Er bat die Polizei, für ihn die Personalien des Fahrzeughalters festzustellen. Ein Polizeibeamter ermittelte daraufhin über den Direktanschluß der Polizei an das Kraftfahrt-Bundesamt die Daten des Fahrzeughalters, einer jungen Frau, und schrieb diese auf einen Zettel. Dem Bürger gelang es, einen Blick darauf zu werfen. Kurze Zeit später rief er die Frau an und sagte, er wolle sie kennenlernen. Was war geschehen? Der Bürger hatte die junge Frau am Steuer ihres Kraftfahrzeuges beobachtet. Da sie ihm gefiel und er mit ihr anbandeln wollte, erfand er kurzerhand einen Verkehrsunfall. Er wußte nämlich von früher, daß die Polizei bei Verkehrsunfällen dem Verursacher Name und Anschrift des Geschädigten mitteilt. Der Verstoß blieb ungeahndet: die junge Frau stellte keinen Strafantrag, so daß die Staatsanwaltschaft das Vergehen nach § 41 BDSG nicht verfolgen konnte und deshalb das Verfahren nach § 170 Abs. 2 StPO einstellte.

2. Wozu Gleichgültigkeit und Gedankenlosigkeit führen können

Häufig stoße ich auf Schwachstellen beim Einsatz der Technik. Fordere ich dann die Behörden auf, sie zu beseitigen, zögern

sie oft, obgleich meist nur kleinere Änderungen ihrer Arbeitsweise notwendig sind. Allzu oft stelle ich als Grund dieses Zögerns Sorglosigkeit oder Betriebsblindheit fest. Wie es dann weitergehen kann, zeigen folgende Fälle:

2.1 Die überflüssigen EDV-Listen

Unter der Schlagzeile „Geheime Listen der Stadt am Luftballon verschickt" berichtete eine Stuttgarter Tageszeitung über den Fund einer Computerliste. Auf dieser Liste war zu lesen, wieviel Wohngeld zwölf mit Name, Anschrift und ihrem Bankkonto näher bezeichnete Stuttgarter Bürger im Juni 1973 bezogen hatten. Weil damals — lange vor Inkrafttreten der Datenschutzgesetze — fast niemand Verzeichnisse über den Verbleib von EDV-Listen führte, war es mir nach nunmehr 12 Jahren — wie kaum anders zu erwarten — leider nicht mehr möglich, diesen mysteriösen Fall im einzelnen aufzuklären. Ergebnislos war die bei der Stadt Stuttgart durchgeführte Überprüfung aber dennoch nicht. Es zeigten sich dabei Mängel bei der Datenverarbeitung, die auch heute noch zu den gleichen Pannen führen können:

— Zu viele EDV-Listen

Das Rechenzentrum der Stadt Stuttgart produzierte im Wohngeldverfahren überflüssige EDV-Listen und schaffte damit unnötige Risiken. Dieses Leiden mußte ich bereits 1983 diagnostizieren, nachdem mir ein Bürger einen dicken Stapel von EDV-Listen des Sozialamts der Stadt mit Angaben über zahlreiche Sozialhilfeempfänger übergeben hatte. Zwar hatte ich damals die Stadt aufgefordert, künftig für alle Ämter nur noch die EDV-Listen zu drucken, die sie tatsächlich brauchen. Diese Verschreibung blieb offenbar ohne die von mir erhoffte Wirkung. Jedenfalls erstellte sie noch bei meinem Kontrollbesuch im Oktober 1985 im Wohngeldverfahren drei Fertigungen der sog. Auszahlungsliste, aus der alle Wohngeldempfänger eines Monats und die an sie geleisteten Zahlungen ersichtlich sind, obwohl sie in Wirklichkeit nur eine einzige Fertigung benötigt.

— Die fehlende Protokollierung

Das Rechenzentrum der Stadt Stuttgart hielt auch nicht fest, wer wann welche Unterlagen in welcher Zahl vernichtet. Wenn das nicht gemacht wird, läßt sich die Herkunft irgendwo aufgefundener Listen und EDV-Unterlagen eines Tages aber nicht mehr aufklären. Betriebliche Schwachstellen bleiben dann im Verborgenen. Auch eine wirksame Kontrolle darüber, ob nicht mehr benötigte Unterlagen tatsächlich vernichtet wurden, ist dann nicht möglich.

Wer unnötige EDV-Listen produziert und den Verbleib von Listen nicht protokolliert, hat seine Datenverarbeitung mangelhaft organisiert. Die Datenschutzgesetze fordern, die Organisation so zu gestalten, daß die Daten möglichst gut geschützt sind. Die Reaktion der Stadt Stuttgart auf meine Beanstandungen steht noch aus.

2.2 Wozu Adreßaufkleber mit Patientendaten herhalten müssen

Was geht es einen Taxifahrer an, der im Auftrag eines Krankenhauses einen Krankenhauspatienten zu befördern

hat, wann sein Fahrgast Geburtstag hat, welchen Beruf er ausübt, zu welcher Religionsgemeinschaft er sich bekennt, ob er ledig, verheiratet oder geschieden ist, wie seine Versicherungsverhältnisse sind? Was hat die Krankenkasse, das Sozialamt oder einen sonstigen Kostenträger zu interessieren, welcher Konfession der Patient angehört, welchen nahen Angehörigen das Krankenhaus im Ernstfall verständigen soll? Weshalb muß ein Krankenhauspfarrer zur Kontaktaufnahme mit dem Patienten auch die Versicherungsverhältnisse des Patienten wissen? Warum müssen dem Pfortendienst eines Krankenhauses auch alle die Informationen zur Verfügung stehen, die die Kostenträger zur Abrechnung der Krankenhausleistungen verlangen?

Solche und noch eine ganze Reihe weiterer ähnlicher Fragen stellen sich, wenn man sieht, wie zahlreiche Krankenhäuser im Land mit Adreßaufklebern umgehen. Solche Aufkleber lassen die Krankenhausverwaltungen unmittelbar nach der Aufnahme eines Patienten mit Hilfe der EDV herstellen. Sie enthalten in der Regel nicht nur die reinen Adreßdaten; aus ihnen sind meist alle Angaben zu ersehen, die die Krankenhausverwaltung bei der Aufnahme über die einzelnen Patienten erhebt. Sie geben also auch Auskunft über

- Geburtsdatum, Familienstand, Religionszugehörigkeit, Staatsangehörigkeit, Beruf und Arbeitgeber des Patienten
- Name, Anschrift, Geburtstag und Beruf des Hauptversicherers
- den Pflegesatz und die Wahlleistungen, die der Patient in Anspruch nimmt
- den Kostenträger und den einweisenden Arzt
- oft genug auch noch die Einweisungsdiagnose und den Namen des Angehörigen, mit dem das Krankenhaus im Ernstfall in Kontakt treten soll.

Um sich Schreibarbeiten zu ersparen, bringen die Krankenhausverwaltungen solche Aufkleber auf Karteikarten, Krankenakten und sonstigen Unterlagen an, stellen sie dem Pfortendienst zur Verfügung, verwenden sie beim Schriftwechsel mit Kostenträgern, mit Sozialstationen und überlassen sie auch Krankenhausseelsorgern. Auch wenn nicht überall so verfahren wird: es gibt immer noch viel zu viele Krankenhäuser, die sich solch umfangreicher Adreßaufkleber undifferenziert bedienen und sie, um sich Arbeit zu ersparen, für alle möglichen Zwecke einsetzen. Sie nehmen dabei in Kauf, daß sowohl Personen und Stellen innerhalb als auch außerhalb des Krankenhauses Kenntnis von Informationen über Patienten und ihre Angehörigen erhalten, die sie nicht zu interessieren haben und die ihnen deshalb sowohl nach den Bestimmungen des Landesdatenschutzgesetzes als auch nach den Regeln über die ärztliche Schweigepflicht, die auch von einer Krankenhausverwaltung zu beachten sind, nicht bekannt gegeben werden dürfen. Wann immer ich wegen dieser Praxis mit Krankenhäusern Kontakt hatte, bestand sehr schnell Einvernehmen darüber, daß sie nicht länger fortgesetzt werden kann. Dies zeigt mir, daß es im wesentlichen Gedankenlosigkeit und Gleichgültigkeit ist, die zu dieser Praxis geführt haben. Erstaunlich ist sie allemal.

2.3 Vom Umgang der Polizei mit Lichtbildern

Ganz gleich, ob ich zur Polizeidirektion Aalen, der Polizeidirektion Pforzheim oder sonstwo hinkomme, — immer wieder muß ich feststellen: Die Polizei macht zu viele Lichtbilder und geht mit ihnen nicht sorgfältig genug um. Offensichtlich war dies, als vor wenigen Monaten einem Stuttgarter Polizeibeamten auf dem Weg zum Gericht das dreiteilige Lichtbild eines Beschuldigten aus den Ermittlungsakten fiel. Ein Passant entdeckte es in der Nähe des Neuen Schlosses in Stuttgart. Wer auf dem Foto abgebildet war, konnte der Finder leicht feststellen: Auf der Rückseite waren wie üblich Name, Vorname, Geburtsdatum und -ort, Beruf, Körpergröße, Gewicht, Haar- und Augenfarbe des Beschuldigten sowie dessen Tätowierungen vermerkt. Obwohl die Polizei nach ihren seit 1983 geltenden Richtlinien für erkennungsdienstliche Maßnahmen in der Regel nur zwei Bilder — eines für das Bundeskriminalamt, das zweite für die Kriminalakte — fertigen soll, hielt sich die Praxis daran nur selten. Sechs, meist aber vier Bilder waren und sind üblich. Auf die Frage nach dem Warum heißt es dann meist, gelegentlich brauche man ein weiteres Bild. Es sei deshalb rationeller und wirtschaftlicher, dann nicht erst das Negativ heraussuchen und einen Abzug machen zu müssen, sondern sofort eine ausreichende Zahl an Bildern vorrätig zu haben. Dafür spricht schon etwas, bloß: „Lichtbilder auf Vorrat" stellen für den Betroffenen eine nicht zu unterschätzende Gefahrenquelle dar. Auf meine Bitte hin will sich das Innenministerium nun dafür einsetzen, daß die Polizei die ed-Richtlinien in Zukunft beachtet und nur dann mehr als zwei Lichtbilder fertigt, wenn sie von Anfang an weiß, daß sie mehr braucht — beispielsweise für Fahndungszwecke, für Ermittlungsakten oder die Lichtbildvorzeigekartei. Dagegen ist nichts zu sagen, wenn sich die generelle Praxis umorientiert.

Nicht minder wichtig ist ein anderes: die Polizei muß in ihren Unterlagen vermerken, wie viele Lichtbilder sie im Einzelfall herstellte und wohin sie kamen. Nur dann kann sie exakt über den Verbleib von Lichtbildern Auskunft geben. Fragte ich bislang bei Kontrollen danach, fielen die Antworten meist unbefriedigend aus. Das Innenministerium will nun für eine genaue Buchführung sorgen. Für die Polizeidirektion Heilbronn wird das nichts Neues bringen: Sie hält, wie ich jüngst sah, dies schon jetzt in vorbildlicher Weise in ihrem ed-Tagebuch fest.

2.4 Die Nachteile der Photokopie

Seit es Photokopiergeräte gibt, vereinfachte sich im Behördenalltag manches. Daß die Photokopie jedoch nicht nur ein Segen ist, erfahren Bürger mehr oder minder stark:

— Eine Bürgerin beobachtete in unmittelbarer Nähe eines Wohngebiets und einer stark befahrenen Straße eine Treibjagd. Da sie fand, daß dies für Anwohner, Fußgänger und Autofahrer zu gefährlich sei, schrieb sie ihr Bürgermeisteramt an und bat um Auskunft, ob dies mit rechten Dingen zuginge. Das Bürgermeisteramt machte es sich einfach: Es sandte einfach eine Photokopie ihres Schreibens an den Jagdpächter.

— Ein anderer Bürger wollte vom Regierungspräsidium Stuttgart wissen, ob es eine geplante Gemeindeverbin-

dungsstraße für sinnvoll und erforderlich halte. Noch ehe er die erbetene Auskunft erhielt, mußte er zu seiner Verwunderung erfahren, daß eine Kopie seines Schreibens bereits beim Bürgermeisteramt lag, wohin sie über das Straßenbauamt gelangt war.

Beide Bürger finden die Verfahrensweise nicht in Ordnung. Verständlich — bloß gegen Rechtsvorschriften verstößt sie nicht. Gleichwohl meine ich: die Behörden sollten zurückhaltender sein und bedenken, daß sich Bürger oft im Vertrauen darauf an sie wenden, daß nicht alles, was sie sagen oder schreiben, unbesehen an andere Behörden geht. Für diese ist oft völlig unerheblich, ob der Bürger X oder der Bürger Y den Brief schrieb; wichtig ist nur sein Inhalt. Eine Behörde, die dazu andernorts Stellungnahmen einholen will, sollte deshalb den Namen des Bürgers dann nicht weitergeben. Der Mehraufwand, der manchmal dadurch entsteht, ist nicht groß. Er sollte der Verwaltung im Interesse des Bürgers nicht zu viel sein.

3. Wie hilflos ist die Technik gegenüber Datenmißbrauch?

Häufig reagieren Behörden mit Skepsis auf meine Vorschläge, die Gefahr eines Mißbrauchs durch bessere Sicherheitstechniken zu verringern. Erstaunlicherweise räumen überwiegend EDV-Spezialisten ihrer Technik so wenig Chancen ein. Sie urteilen jedoch zu pessimistisch:

— Möglichkeiten der Technik

Wer ein EDV-Verfahren systematisch nach modernen Methoden entwickelt und einsetzt, hat eine hohe Sicherheit erreicht. Kontrollmechanismen verhindern dann weitgehend, daß andere, als die es angeht und die Zugang zum Computer oder angeschlossenen Datenterminal haben, das Verfahren überhaupt aufrufen können. Auch die Gefahr eines Mißbrauchs durch Insider können Programme wirksam verringern — etwa, indem sie eingegebene Daten auf ihre Plausibilität prüfen und die Benutzer nur genau das tun lassen, was ihrer Aufgabe entspricht. Wichtig ist auch, sinnvoll die Fähigkeit der Computer zu nutzen, alles zu protokollieren, Protokolldaten schnell auszuwerten und übersichtlich darzustellen. Vorgesetzte und andere Kontrolleure können dann die Datenverarbeitung laufend wirksam überwachen und kommen eventuellen Mißbräuchen zumindest nachträglich meist schnell auf die Spur. Wenn das EDV-Verfahren zudem einfach und benutzerfreundlich gestaltet, verständlich und vollständig beschrieben ist, scheiden auch Mißbräuche durch versteckte, mit überraschenden Funktionen versehene Programme weitgehend aus.

— Grenzen der Technik

Daß der Technik nicht möglich ist, Mißbräuche jeder Art zu verhindern, zeigt die aktuelle Diskussion über die „Computerviren". Man versteht darunter ein EDV-Programm, — „Virus" genannt — das andere im Computer oder auf seinen Datenträgern gespeicherte Programme sucht und diese anschließend verändert — sprich: infiziert. Im Extremfall kann dieses Virusprogramm sich selbst kopieren und diese Kopie in fremde Programme einfügen und dadurch seine Wirkung wie im Schneeballeffekt vervielfachen. Die möglichen Folgen dieser „Viren" sind fast grenzenlos: Die „infizierten" Programme können ihren Dienst ab einem bestimmten, in

der Zukunft liegenden Zeitpunkt einstellen. Sie können aber auch, ohne sich jemals zu erkennen zu geben, die Daten einer oder mehrerer bestimmter Personen löschen oder verändern, um jemanden zu bevorzugen oder zu benachteiligen. Sie können auch von einem Rechenzentrum in ein anderes wandern, etwa wenn das infizierte Rechenzentrum A dem Rechenzentrum B Programme übergibt. Besonders heimtückisch sind diese Mißbräuche, weil die Programmviren — wie echte Viren — nicht zu sehen sind, sich unbemerkt und schnell verbreiten und selbst von hervorragenden Spezialisten oft nicht leicht erkannt werden. Zudem ist es enorm aufwendig, die durch sie verursachten Schäden zu beseitigen; kommen noch Datensicherungsmängel hinzu, kann dies sogar unmöglich sein.

Wer kann solchen Mißbrauch betreiben? — Im Grunde jeder mit dem Computer, den er programmieren kann. Die Folgen hängen allerdings von den jeweiligen Befugnissen ab. Wer systemtechnische Spezialprogramme schreiben darf, dem stehen theoretisch fast unbegrenzte Möglichkeiten des Mißbrauchs offen. Wer diese „privilegierte Berechtigung" nicht hat, kann immerhin noch ein oder mehrere EDV-Verfahren verfälschen. Wer aber — wie etwa der Kassierer bei der Stadtkasse — zwar ein EDV-Verfahren nutzen, nicht aber selbst programmieren kann, der kann auch keine Programmviren in die Welt setzen. Fazit ist: Je besser jemand die Systeminternas von Computern kennt und je weitgehender er sie ändern kann, desto raffiniertere Programmviren kann er herstellen und um so weniger können ihn andere wegen seiner fachlichen Überlegenheit kontrollieren.

Doch auch gegen die Virengefahr ist man nicht ganz hilflos. Zum einen reicht es durchaus, wenn nur wenige der EDV-Spezialisten eines Rechenzentrums Systeminternas ändern dürfen. Zum andern kann man mit modernen Werkzeugen für die Software-Entwicklung erreichen, daß nur dokumentierte und freigegebene Programme zum Einsatz kommen. Daran muß sich dann auch halten, wer Programmviren entwickelt: er kann sie nicht einfach verstecken, sondern muß sie dokumentieren und freigeben lassen. Bei dieser Prozedur ist zu hoffen, daß der Virus erkannt wird. Zum dritten kann man die schrankenlose Verbreitung eventuell dennoch eingeschleuster Programmviren erheblich erschweren und verlangsamen, wenn man die einzelnen Arbeitsgebiete und EDV-Verfahren durch Sicherheitssoftware streng voneinander abschottet. Zum vierten ist auch eine Vorsorge für den schlimmsten Fall, daß sie ihr Unheil anrichteten, möglich, indem man Programme und Datenbanken zur Sicherheit kopiert und sicher aufbewahrt. Freilich bietet dies alles wie jede Technik keinen absoluten Schutz.

4. Teil: Sicherheitsbereich

1. Abschnitt: Polizei

1. Umgang mit Daten von Nachrüstungsgegnern

Mutlangen, Waldheide, EUCOM — das sind in Baden-Württemberg die Plätze, wo es immer wieder zu Treffen von Nachrüstungsgegnern und Blockadeaktionen kam und kommt. Die Probleme, die danach Nachrüstungsgegner an mich herantragen, sind sehr unterschiedlicher Natur.

1.1 Mutlangen

In meinem letzten Tätigkeitsbericht stellte ich eingehend dar, in welchem Umfang Polizei und Verfassungsschutz Daten über Blockierer des US-Raketenstationierungsgeländes in Mutlangen erheben und verarbeiten. Dies löste in den Medien, bei Abgeordneten, kritisierten Institutionen und Bürgern ein lebhaftes Echo aus:

1.1.1 Kritik des Präsidenten des Bundeskriminalamts

Während der Herr Innenminister von einer „gründlichen Arbeit mit wertvollen Hinweisen" sprach, kam Kritik vom Präsidenten des Bundeskriminalamts. War dies schon von der Sache her ungewöhnlich, wunderte ich mich erst recht über ihre Art und Weise. Der Präsident glaubte, meine Ausführungen als „falsch", „unseriös" und „anmaßend" abtun zu können. Vor allem warf er mir vor, den Sachverhalt und die Rechtslage falsch dargestellt zu haben. Seine Kritik erfolgte zu Unrecht: Der Sachverhalt war durchweg richtig dargestellt; die Stellungnahme der Landesregierung zu meinem Tätigkeitsbericht und die Beratungen im Landtag bestätigten dies eindrucksvoll. Auch habe ich nicht den geringsten Anlaß, meine Darstellung der Rechtslage zu korrigieren. Dazu heute nur noch so viel: Entgegen der Auffassung des Präsidenten erlaubt das BKA-Gesetz den Ländern nicht, dem Bundeskriminalamt jede Straftat und damit jede Nötigung mitzuteilen; allein diese Interpretation entspricht dem in unserer Verfassung garantierten Grundsatz der Erforderlichkeit und Verhältnismäßigkeit. Ebenso differenzieren die Richtlinien für den kriminalpolizeilichen Meldedienst in Staatsschutzangelegenheiten: sie führen Nötigungen nicht ausdrücklich als meldepflichtige Straftaten auf; auch sind diese mit den aufgezählten Delikten, z. B. Hochverrat, nicht vergleichbar. Ferner kann man Blockierern nicht — wie dies der Präsident tat — von vornherein unterstellen, ihre Aktionen seien gegen die freiheitliche demokratische Grundordnung, den Bestand oder die Sicherheit des Bundes oder eines Landes gerichtet und/oder gefährdeten auswärtige Belange der Bundesrepublik Deutschland. Schließlich halte ich nach wie vor die Speicherung von Daten der Blockierer im Nachrichtendienstlichen Informationssystem des Verfassungsschutzes (NADIS) durch das Bundeskriminalamt für höchst problematisch. Die Verfassungsschutzbehörden benötigen diese Daten nicht;

das ist nicht nur meine, sondern auch die Einschätzung des Landesamts für Verfassungsschutz Baden-Württemberg. Kurzum: wer es an der Information über die Sach- und Rechtslage fehlen ließ, war der Präsident des Bundeskriminalamts.

1.1.2 Reaktionen der Bürger

Große Resonanz fanden meine Ausführungen bei den Bürgern: Sehr viele äußerten sich zustimmend und anerkennend, einige auch kritisch. Ihre Briefe zeigten mir allerdings, daß sie mein Bemühen um eine differenzierte Betrachtungsweise der verschiedenen Datenverarbeitungsvorgänge nicht verstanden haben. Ich hatte nicht, wie sie meinten, jedwede Speicherung von Daten dieser Personen für unzulässig erklärt. Ich hatte mich auch nicht auf den — durchaus ernst zu nehmenden — Standpunkt vieler Anhänger der Friedensbewegung gestellt, Blockadeaktionen erfüllten nicht den Straftatbestand der Nötigung. Ich hatte vielmehr — ausgehend von der in der Rechtsprechung und Literatur zwar umstrittenen, aber herrschenden Meinung, solche Blockadeaktionen seien strafbar — die Ansicht vertreten, die Daten dieser Bürger, die einer strafbaren Handlung verdächtig sind, dürften grundsätzlich in der Personenauskunftsdatei, dem landesweiten Informationssystem, gespeichert werden.

Die überwiegende Zahl der Bürger, durchweg Nachrüstungsgegner, wandte sich jedoch mit konkreten Fragen an mich:

— Fast alle wollten wissen, ob und gegebenenfalls in welchem Umfang sie wegen ihrer Teilnahme an Aktionen der Friedensbewegung, insbesondere an Blockadeaktionen, in Unterlagen von Polizei und Verfassungsschutz erfaßt sind. Ich konnte sie nur auf meinen Tätigkeitsbericht verweisen und ihnen raten, Auskunftsanträge bei den Sicherheitsbehörden zu stellen. Denn nach den Datenschutzgesetzen ist es allein Sache des Landeskriminalamtes, des Landesamtes für Verfassungsschutz und des Bundeskriminalamtes, den Bürgern darüber Auskunft zu geben, ob und gegebenenfalls welche Daten über sie gespeichert sind. Wie ich inzwischen von diesen Bürgern hörte, erteilen Landes- und Bundeskriminalamt ihnen Auskunft. Eine Ausnahme machte einmal mehr der Verfassungsschutz. Das Innenministerium lehnte an das Landesamt für Verfassungsschutz gerichtete Auskunftsanträge von Bürgern durchweg mit der Begründung ab, eine Auskunft könne — gleichgültig, ob über den Auskunftsersuchenden Daten gespeichert seien oder nicht — die Möglichkeit eröffnen, im Wege des Umkehrschlusses Erkenntnisse über die Arbeit des Landesamtes für Verfassungsschutz zu gewinnen. Dies brächte die Gefahr der Ausforschung mit sich, wodurch die Erfüllung des gesetzlichen Auftrags der Verfassungsschutzbehörden beeinträchtigt würde. Um dies zu vermeiden, habe der Gesetzgeber das Landesamt für Verfassungsschutz von der Pflicht zur Auskunftserteilung freigestellt. Auch die Ermessensabwägung im konkreten Einzelfall

führe zu keinem anderen Ergebnis. Solche Schreiben erhielten Bürger — ganz gleich, ob sie hochangesehene Hochschulprofessoren oder tüchtige Hausfrauen sind. Da meine ich, wäre wahrlich eine andere Reaktion angemessen.

— Eine Ärztin, die in Mutlangen blockiert und die deswegen das Amtsgericht Schwäbisch Gmünd verurteilt hatte, fragte mich, weshalb das Gericht dies der ärztlichen Standesvertretung mitgeteilt habe. Dies geschah nach der Anordnung über Mitteilungen in Strafsachen (MiStra), einer bundesweit geltenden Verwaltungsvorschrift, wonach die Justiz die Ärztekammer von jeder Anklageerhebung und dem Ausgang des Verfahrens gegen einen Arzt zu unterrichten hat. Entsprechende Mitteilungspflichten gibt es beispielsweise bei Zahnärzten, Tierärzten und Apothekern. Sofern ein Blockierer Beamter oder Geistlicher ist, erfährt sein Dienstherr ebenfalls von dem Strafverfahren. Diese Praxis ist zwar, weil sie einer gesetzlichen Grundlage entbehrt, problematisch, verhindern kann ich sie allerdings nicht. Ich kann mich — und das habe ich in der Vergangenheit mehrfach gegenüber dem Justizministerium getan — lediglich dafür einsetzen, daß die Mitteilungspflichten der Justiz gegenüber anderen Behörden und öffentlichen Stellen generell und gerade auch in solchen Fällen eingeschränkt und auf eine gesetzliche Grundlage gestellt werden. Die Justizminister der Länder haben hierzu inzwischen einen Gesetzentwurf noch für das Jahr 1986 angekündigt.

— Viele Betroffene wollten wissen, was sie selbst gegen die Speicherung ihrer Daten in dem landesweiten Informationssystem PAD, gegen die Vormerkung im Kriminalaktennachweis und die Speicherung ihrer Daten in NADIS als Folge des praktizierten Meldedienstes unternehmen können. Ich konnte ihnen dazu folgendes sagen:

  • Gegen die dreijährige Speicherung von Daten in der Personenauskunfsdatei kann ein Blockierer bei der derzeitigen Rechtslage nicht mit Aussicht auf Erfolg angehen, wenn er deswegen verurteilt wurde. Hat die Staatsanwaltschaft oder das Gericht das Verfahren hingegen eingestellt, kann der Bürger von der Polizeidirektion Aalen Löschung seiner Daten verlangen, wenn nach den Umständen des Einzelfalls die weitere Speicherung von Daten zur vorbeugenden Bekämpfung von Straftaten nicht erforderlich ist, namentlich keine Wiederholungsgefahr besteht.

  • Ersttäter und alle in der Umgebung von Mutlangen wohnende Bürger, die mehrfach wegen Nötigung angezeigt wurden, sollten bei der Polizeidirektion Aalen Löschung der Vormerkung für den bundesweiten Kriminalaktennachweis beantragen. So verfahren können selbstverständlich auch alle anderen Bürger; ihre Aussichten, mit einem Löschungsantrag durchzudringen, dürften allerdings wesentlich geringer sein. Sie müß-

ten sich dann zu einer Klage vor dem Verwaltungsgericht entschließen.

- Wegen der Speicherung in NADIS sollten die Betroffenen einen Löschungsantrag beim Bundeskriminalamt stellen. Das Bundeskriminalamt wird ihn zwar vermutlich ablehnen, weil es die Speicherung immer noch für rechtmäßig hält. Den Bürgern bleibt dann nur der Widerspruch und notfalls die Klage vor dem Verwaltungsgericht. Dabei können sie vortragen, daß inzwischen auch das Innenministerium meint, längst nicht jeder Blockierer sei dem Bundeskriminalamt zu melden. Daraus folgt, daß auch nicht jeder in NADIS gespeichert werden darf.

1.1.3 Bilanz

Stellt sich am Schluß die Frage, was ich für die Betroffenen erreichen konnte: Sicher nicht alles, was ich für richtig und notwendig erachte; aber doch Entscheidendes. Das Innenministerium sprang nach längerem Hin und Her über seinen Schatten und rang sich zu einigen Verbesserungen durch:

— An erster Stelle ist die erkennungsdienstliche Behandlung zu nennen; hier ist jetzt die Lage wesentlich besser. Durch Erlaß vom 21. Oktober 1985 ordnete das Innenministerium an, daß die Polizei bei der Entscheidung, ob sie von einem Bürger Lichtbilder anfertigt und Fingerabdrücke nimmt, alle bekannten Umstände des Einzelfalls berücksichtigen muß. Einen Automatismus dergestalt, daß jeder bei der zweiten Nötigung erkennungsdienstlich behandelt wird, gibt es nicht mehr. Auch im Falle wiederholter Nötigung kommt es nach dem Erlaß vielmehr entscheidend darauf an, ob die Wahrscheinlichkeitsprognose gerechtfertigt ist, der Bürger werde neben weiteren Nötigungen auch andere Straftaten begehen, zu deren Aufklärung erkennungsdienstliches Material erforderlich sein kann. Bei der danach vorzunehmenden Abwägung sind insbesondere folgende Gesichtspunkte zu berücksichtigen: Das Verhalten des Betroffenen bei der Festnahme, eine etwaige Vortat des Beschuldigten, die eine erkennungsdienstliche Behandlung gerechtfertigt hätte, die wiederholte Teilnahme des Bürgers an einer Nötigung und die dem Beamten vor Ort vorliegenden Erkenntnisse über einen Bürger. Auch wenn mich der Erlaß nicht in allen Einzelheiten befriedigt, ein wesentlicher Fortschritt ist er sicher. Zu hoffen bleibt, daß die Polizei diesen Erlaß nicht nur in Zukunft anwendet, sondern auch alle zurückliegenden Fälle von Amts wegen überprüft und erforderlichenfalls korrigiert.

— Eine Korrektur ist bei der Speicherung von Daten über Blockierer in der Personenauskunftsdatei bereits geschehen. Die Polizeidienststellen haben die zunächst eingegebene Speicherungsdauer von 10 Jahren bei allen Ersttätern, die nur eine Nötigung begangen haben, nachträglich auf die von

mir geforderte Dreijahresfrist herabgesetzt. Außerdem geben sie jetzt die verkürzte Frist von vornherein ein.

— Auch in der Frage der Vormerkung von Bürgern für den Kriminalaktennachweis gab es Fortschritte. Das Innenministerium bestimmte hierzu in seinem erst dieser Tage ergangenen Erlaß vom 11. Dezember 1985, daß die Teilnahme an einer Sitzblockade in Mutlangen die Aufnahme in den bundesweiten Kriminalaktennachweis noch nicht rechtfertigt. Es soll vielmehr unterschieden werden:

  • Blockierer, die sich nur gegen die Stationierung der Waffen gerade in ihrer Nähe wenden oder ihre Aktivitäten wegen der Nähe ihres Wohn- und Aufenthaltsortes auf den Stationierungsort Mutlangen konzentrieren (örtlicher oder regionaler Bezug), sollen nicht im bundesweiten Kriminalaktennachweis erfaßt werden. Das Vorliegen dieser Voraussetzungen wird bei Bürgern, die 30 km von Mutlangen entfernt wohnen oder arbeiten, vermutet. Bei allen anderen Bürgern ist im Einzelfall zu prüfen, ob Anhaltspunkte für eine örtliche bzw. regionale Motivation vorliegen.

  • Ist letzteres nicht der Fall, soll gelten: Bei erstmaliger Teilnahme an einer Blockade erfolgt keine Vormerkung für den KAN — es sei denn, daß konkrete Anhaltspunkte für eine überregional bedeutsame Straftat vorliegen. Bei wiederholter Teilnahme an einer Blockade sollen die Daten des Betroffenen hingegen grundsätzlich im KAN gespeichert werden.

  Der Erlaß ist in seiner Tendenz sicher zu begrüßen. Ich beneide allerdings die Polizeibeamten vor Ort nicht, die ihn vollziehen müssen. Er stellt sie wegen seiner schweren Lesbarkeit vor manche Probleme. Hätte man sich mehr von der Überlegung leiten lassen, daß — unabhängig vom regionalen oder überregionalen Bezug einer Straftat — Bagatelldelikte im KAN nichts zu suchen haben, hätte man es auch einfacher sagen können.

— Erheblich umstellen muß sich die Praxis jetzt auch bei der Übermittlung von Daten an das Bundeskriminalamt. Sie ist nach dem Erlaß des Innenministeriums vom 11. Dezember 1985 nur noch ausnahmsweise — und zwar in Fällen zulässig, in denen Anhaltspunkte dafür vorliegen, daß der Betroffene künftig schwerwiegende Straftaten begehen wird. Beachtet die Polizei diese Anweisung konsequent, hört der bislang praktizierte Meldedienst zum Bundeskriminalamt weitgehend auf. Zu den problematischen Speicherungen in NADIS durch das Bundeskriminalamt kann es dann deshalb bloß noch in Ausnahmefällen kommen.

1.2 Waldheide

Wenige Tage nach dem Unglück mit einer Pershing II-Rakete auf dem US-Stützpunkt Waldheide bei Heilbronn im

Januar 1985 erreichten mich die ersten Zuschriften von Bürgern. In ihnen war von verstärkten Personenkontrollen der Polizei in der Umgebung des Stationierungsgeländes die Rede. Die Polizeibeamten vor Ort — so hieß es — stellen jeweils die Personalien der Bürger fest, fragen die polizeilichen Informationssysteme nach ihnen ab und halten den Namen der Überprüften mit Datum und Uhrzeit der Kontrolle fest. Diese Notizen bewahre die Polizeidirektion Heilbronn auf. Sie dienten ihr beispielsweise dazu festzustellen, welche Personen an den sonntäglichen Mahnwachen teilnehmen. Die Bürger wollten nun von mir wissen, ob diese Verfahrensweise zulässig ist. Wir sahen uns deshalb die Situation vor Ort 1985 in mehreren Kontrollbesuchen näher an.

Um es vorweg zu sagen: Von Anfang an spürte man das Bemühen der Heilbronner Polizeidirektion, Daten über Nachrüstungsgegner nur in dem Maß zu verarbeiten, wie es aus Sicherheitsgründen unerläßlich ist. Zwar hatte sie dabei Anlaufschwierigkeiten; auch gab es rechtliche Probleme. Nach sehr eingehender und offener Diskussion der Sach- und Rechtslage war jedoch möglich, gemeinsam einen Weg zu finden, der dem Persönlichkeitsschutz und den Belangen der Sicherheit Rechnung trägt. Ich wünschte mir, daß dieser Stil im Verhältnis zwischen Polizei und meinem Amt stets praktiziert würde. Dann wäre sicher manches einfacher.

1.2.1 Wie die Polizei zunächst verfuhr

Nicht einfach war anfangs, die polizeiliche Praxis festzustellen. Zwar gab es die wenige Tage vor unserem ersten Kontrollbesuch ergangenen Anweisungen vom 28. Januar/6. Februar 1985. Doch war darin längst nicht alles geregelt. Beispielsweise ließen sie offen, wann die Beamten vor Ort eine Anhaltemeldung fertigen sollten, welchen Inhalt diese haben sollte, ob und nach welchen Gesichtspunkten diese von der Polizeidirektion Heilbronn zu überprüfen seien, zu welchem Zweck sie aufbewahrt werden, in welchen Fällen und unter welchen Modalitäten Auskunft aus der Sammlung der Anhaltemeldungen erteilt wird. Aufgrund unserer eingehenden Gespräche stellte sich die Vorgehensweise dann so dar:

— Die Polizeibeamten vor Ort kontrollierten alle verdächtigen und auffälligen Personen in der Umgebung der Waldheide. Dabei stellten sie deren Personalien fest, führten über Funk eine INPOL- und eine PAD-Abfrage durch. Bestätigte sich ihr Verdacht nicht — wann dies der Fall war, konnte man mir nicht präzise sagen —, hatte die Sache ihr Bewenden. Anderenfalls fertigte der Beamte vor Ort eine Anhaltemeldung.

— Für diese Meldung verwendete er oft einen Vordruck, auf dem Vor- und Zuname, Geburtsdatum und Geburtsort sowie die Anschrift des Angehaltenen, gegebenenfalls die Daten seines Kraftfahrzeugs, der Grund der Kontrolle und das Abfrageergebnis (Personenfahndung positiv/negativ, Sachfahndung positiv/negativ, PAD positiv/negativ) an-

zugeben waren. Anderenfalls schrieb er einfach seine Nachricht auf normales Papier.

— Die Beamten vor Ort gaben ihre Anhaltemeldungen an die Polizeidirektion Heilbronn. Deren Lage- und Einsatzzentrum ordnete sie chronologisch und legte sie jeweils mit einer Nummer versehen in Leitz-Ordnern ab. Vor der Aufnahme habe es — so die Heilbronner Darstellung — geprüft, ob die Daten die Polizei benötige. Es gelang mir allerdings nicht festzustellen, in welchen Fällen die Polizei dies verneinte. Ein Doppel der Anhaltemeldungen erhielt das Dezernat Staatsschutz; es legte sie ebenfalls chronologisch ab.

  Bei der Durchsicht der Leitz-Ordner stellten wir 92 Anhaltemeldungen fest, darunter von einigen Personen mehrere. Als Grund der Kontrolle war meist nur „Personenkontrolle" oder „allgemeine Personenkontrolle" angegeben, nicht jedoch das Ereignis, das die Überprüfung und Meldung auslöste. Auf dieses konnte man lediglich hin und wieder aus der Ortsangabe bzw. der Uhrzeit der Kontrolle schließen — so etwa, wenn die Polizei einen Bürger spät abends an einer Stelle im Gebiet Waldheide antraf, an der sich normalerweise um diese Zeit niemand aufhält. Gelegentlich war der Grund der Kontrolle jedoch auch genauer bezeichnet. Dann hieß es etwa: „Verteilte vor Tor 1 Flugblätter gegen die Nachrüstung" oder „nahm vor Tor 1 an einer Mahnwache teil" oder „stellte ein Transparent gegen die Nachrüstung am Zaun auf", „photografierte im Schutzbereich".

— Die Polizeidirektion Heilbronn gab an, die Anhaltemeldungen aufbewahren zu müssen, um Gefahren für das Raketenstationierungsgelände abwehren zu können; zudem brauche sie diese für polizeiliche Einsätze. Freimütig räumte sie mir gegenüber ein, man könne sehr wohl darüber verschiedener Meinung sein, ob sie nicht zu viele Personen erfasse. Denn sicherlich seien auch solche in ihrer Sammlung registriert, von denen keine konkrete Gefahr für das Gelände Waldheide ausginge.

— Auskünfte aus der Sammlung der Anhaltemeldungen gab die Heilbronner Polizei im wesentlichen nur an die vor Ort eingesetzten Beamten. Nur in wenigen Fällen hatte sie die Daten der überprüften Personen mündlich auch an die Amerikaner weitergegeben — so etwa, wenn ein Bürger im Schutzbereich um das Militärgelände verbotenerweise photografierte oder den Anschein erweckte, als ob er photografiere. Wie oft die Polizeidirektion Heilbronn solche Auskünfte erteilte, konnte sie bei unserem ersten Besuch nicht sagen, weil sie bis dahin darüber keine Unterlagen führte.

— Die Polizeidirektion Heilbronn beabsichtigte, ihre Sammlung der Kontroll- und Anhaltemeldungen jährlich zu bereinigen. Meldungen über Personen, die zwischenzeitlich nicht mehr aufgefallen waren, wollte sie vernichten.

1.2.2 Was dazu zu sagen war

Die festgestellte Kontrollpraxis warf eine Reihe von Rechtsfragen mit erheblichen praktischen Konsequenzen auf:

1.2.2.1 Personenfeststellungen

Die Polizei darf unter anderem nach § 20 Abs. 1 Nr. 4 PolG einen Bürger „überprüfen" — besser mit den Worten des Gesetzes gesagt: seine Identität feststellen, wenn er sich in unmittelbarer Nähe eines besonders gefährdeten Objekts aufhält und Tatsachen die Annahme rechtfertigen, daß in oder an Objekten dieser Art Straftaten begangen werden sollen. Auf diese Regelung berief sich die Heilbronner Polizei bei ihrem Vorgehen. Dazu ist zu sagen:

— Zwei der vier gesetzlichen Voraussetzungen waren von vornherein erfüllt. Der Raketenstützpunkt Waldheide ist — das wird niemand bezweifeln — ein besonders gefährdetes Objekt. Auch rechtfertigen Tatsachen die Annahme, daß in oder an einem solchen Raketenstützpunkt Straftaten begangen werden. Ich erinnere an den Fund einer Bombe im Bereich einer US-Kaserne in Böblingen, die Anschläge auf US-Einrichtungen in Hessen und daran, daß in Stationierungsorten schon wiederholt Personen auf das Militärgelände vordrangen und damit Hausfriedensbruch begangen, teils auch weitere Straftatbestände verwirklichten. Das aber genügt für die Anwendbarkeit des § 20 Abs. 1 Nr. 4 PolG: Es muß sich weder um schwere Straftaten handeln noch müssen sich die Hinweise auf mögliche Straftaten auf das Objekt Waldheide beziehen. Allein Tatsachen, die die Annahme rechtfertigen, daß Straftaten gegen irgendwelche US-Einrichtungen in der Bundesrepublik begangen werden sollen, machen — so das geltende Recht — auch Personenkontrollen auf der Waldheide zulässig. Nicht erforderlich ist, daß von dem Bürger selbst, der sich in unmittelbarer Nähe des US-Geländes Waldheide aufhält, eine konkrete Gefahr für die öffentliche Sicherheit ausgeht oder daß er im Verdacht steht, eine strafbare Handlung begangen zu haben.

— Damit die Polizei eine Person überprüfen darf, müssen zwei weitere Voraussetzungen hinzukommen, nämlich: Der Bürger muß sich in unmittelbarer Nähe des Objekts aufhalten und die Polizei muß die Identitätsfeststellung nach dem Grundsatz der Verhältnismäßigkeit im Einzelfall für erforderlich halten dürfen. Darauf wies der Verwaltungsgerichtshof Baden-Württemberg in einem Urteil vom 31. März 1981 ausdrücklich hin. Das bedeutet: Die Polizei darf nicht jeden Bürger, der sich im Bereich des US-

Stützpunkts Waldheide aufhält — darunter sind viele Ausflügler und Spaziergänger aus dem Heilbronner Raum — einfach kontrollieren. Die Polizei muß vielmehr anhand aller erkennbarer Umstände des Einzelfalls entscheiden, ob sich ein Bürger auffällig bzw. verdächtig verhält und deshalb überprüft werden kann. So könnten etwa die verdeckte Annäherung an den Raketenstützpunkt, die Annäherung abseits öffentlicher Wege oder bei Dunkelheit, das Fertigen von Aufzeichnungen oder ein längeres Beobachten des Geländes Grund für ein polizeiliches Einschreiten sein — das alles muß es jedoch nicht, wie man gerade am letzten Beispiel besonders deutlich sieht: Der US-Stützpunkt Waldheide kann auch für den harmlosen, nicht Böses im Schilde führenden Bürger wegen des Raketenunfalls und der sonstigen Vorgänge um die Waldheide von verständlichem Interesse sein. Dafür, ob ein Bürger zu kontrollieren ist, kann das längere Beobachten des Objekts allein deshalb nicht genügen. Eine Rolle spielen kann beispielsweise auch, ob jemand an dem Gelände vorbeigeht oder stehen bleibt, wie alt jemand ist — bei einem Kind oder einem 80-Jährigen wird das längere Beobachten des Objekts kaum ein Einschreiten rechtfertigen —, in wessen Begleitung sich jemand befindet: bei einer Familie mit Kindern wird eine Personenüberprüfung meist nicht notwendig sein. Zurückhaltung ist auch geboten, wenn der Bürger beispielsweise eine Mahnwache abhält. Denn die Polizei muß dessen Recht auf freie Meinungsäußerung und Versammlungsfreiheit Rechnung tragen. Das schließt auch ein, daß Bürger, soweit es die Sicherheit erlaubt, staatlicherseits nicht überwacht werden.

Ob die Polizeidirektion diese Grundsätze zu Beginn ihrer verstärkten Kontrolltätigkeit, insbesondere auch in den Zeiten nach dem Raketenunfall immer beachtet hat, konnten wir bei unserem Kontrollbesuch nicht mit letzter Sicherheit klären: sofern die Personenüberprüfung zu keiner Anhaltemeldung führte, waren natürlich keine Unterlagen über die Kontrolle vorhanden. Fertigte die Polizei eine Anhaltemeldung, ermöglichte sie — wie ausgeführt — meist keine Nachprüfung, weil der Grund nur unzureichend vermerkt war. Die wenigen Fälle, wo aus den Unterlagen mehr zu ersehen war, erlauben keine abschließende Beurteilung: Zweifel sind jedenfalls angebracht, ob die Beamten vor Ort die Grenzen für ein Einschreiten immer richtig zogen.

1.2.2.2 Fertigen einer Anhaltemeldung

Fertigt die Polizei eine Anhaltemeldung, so greift sie damit in das informationelle Selbst-

bestimmungsrecht der überprüften Person ein. Nach dem Volkszählungsurteil ist ein solcher Eingriff nur zulässig, wenn er im überwiegenden Allgemeininteresse erforderlich ist und eine gesetzliche Grundlage hat. Da sich das Fertigen einer Anhaltemeldung weder auf die Vorschrift über die Identitätsfeststellung (§ 20 PolG) noch auf eine andere besondere Rechtsvorschrift im Polizeigesetz stützen läßt, darf die Polizei bloß dann so verfahren, wenn dies zur Abwehr einer konkreten Gefahr für die öffentliche Sicherheit erforderlich ist (§§ 1, 3 PolG). Das bedeutet: Hat ein Polizeibeamter auf der Waldheide die Identität einer Person festgestellt, darf er diese erfolgte Personenüberprüfung nicht automatisch der Polizeidirektion Heilbronn im Wege einer Anhaltemeldung mitteilen. Er muß vielmehr aufgrund der Gesamtumstände des Einzelfalls entscheiden, ob von der überprüften Person eine konkrete Gefahr ausgeht. Bei dieser Abwägung spielt eine Rolle, weshalb die Polizei die Überprüfung durchführte, welche Gründe der Bürger für sein auffälliges/verdächtiges Verhalten angab, wie er sich bei der Kontrolle verhielt, ob die Abfrage der polizeilichen Informationssysteme INPOL und PAD Anhaltspunkte dafür erbrachte, daß der Bürger schon einmal einschlägig in Erscheinung trat — etwa in einem anderen Stationierungsort auf das Militärgelände vordrang. Nur wenn die Polizei damit rechnen muß, daß der überprüfte Bürger in überschaubarer Zukunft die öffentliche Sicherheit stört — also vor allem eine Straftat begeht — und nur wenn zudem die Speicherung seiner Daten bei der Polizeidirektion eine geeignete Maßnahme ist, dieser Gefahr zu begegnen, darf der Polizeibeamte eine Anhaltemeldung fertigen. Ausnahmsweise darf er dies auch dann, wenn ein Bürger den Anschein einer konkreten Gefahr erweckt und sich der Sachverhalt nicht an Ort und Stelle abklären läßt.

Diesen Maßstab legte die Heilbronner Polizeidirektion bis zu meinem Kontrollbesuch wohl nicht an: Nicht bei jeder Meldung, die erfolgte, lag eine konkrete Gefahr oder zumindest eine Anscheinsgefahr vor.

1.2.2.3 Sammlung der Anhaltemeldungen

Die Polizeidirektion Heilbronn darf Anhaltemeldungen der Beamten vor Ort nur aufbewahren, wenn es zur Abwehr einer konkreten Gefahr erforderlich und diese Maßnahme geeignet ist, die Gefahr abzuwehren. Das bedeutet:

— Sie darf die eingehenden Meldungen nicht einfach in ihren Leitz-Ordnern abheften, sondern muß die Beurteilung der Beamten vor Ort überprüfen, muß also selbst eine Entscheidung treffen. Das konnte die Heilbronner Polizeidirektion am Anfang schon

deshalb in der Regel nicht, weil die Meldungen den Grund der Kontrolle nicht angaben. Folglich konnte sie bei unserem ersten Besuch auch nicht sagen, ob und gegebenenfalls wodurch von einem in der Sammlung der Anhaltemeldungen Erfaßten eine konkrete Gefahr für das Objekt Waldheide ausging. Unabdingbare Voraussetzung für eine solche Beurteilung ist, daß die Beamten auf der Waldheide den Anlaß der Kontrolle, aber auch das Ergebnis ihrer Überprüfung und insbesondere die Aussagen des Überprüften präzise festhalten.

— Klarheit muß auch darüber bestehen, anhand welcher Unterlagen der Staatsschutz der Heilbronner Polizeidirektion das Vorliegen einer konkreten Gefahr beurteilt: Er darf sicher noch einmal die polizeilichen Informationssysteme des Bundes und des Landes abfragen, er darf auch auf eigene Erkenntnisse zurückgreifen, die sich in seinen Akten befinden. Er darf aber diese Daten nur verwerten, wenn sie relevant sind: Daß ein auf der Waldheide überprüfter Bürger schon einmal eine fahrlässige Körperverletzung oder einen Warenhausdiebstahl begangen hat, ist kein Indiz dafür, daß von ihm eine konkrete Gefahr für den Raketenstützpunkt ausgeht. Anders sieht es hingegen aus, wenn der Überprüfte der Polizei einschlägig bekannt ist — etwa wegen eines Hausfriedensbruchs oder einer Sachbeschädigung in Mutlangen. Kurzum: der Staatsschutz darf eine eingegangene Anhaltemeldung in seine Sammlung nur aufnehmen, wenn er nach allen Umständen des Einzelfalls zu dem Schluß kommt, daß der Überprüfte in überschaubarer Zukunft eine Straftat gegen den Raketenstützpunkt Waldheide begehen wird und diese Information geeignet ist, diese Gefahr abzuwehren. Er darf dies zudem nur so lange tun, wie von dem Überprüften eine konkrete Gefahr für das Objekt Waldheide ausgeht. Lag nie eine konkrete Gefahr vor oder fiel sie weg, muß die Polizeidirektion die Unterlagen unverzüglich vernichten.

Auch in diesem Punkt bestehen Zweifel, ob die Polizeidirektion Heilbronn von Anfang an so verfuhr. Insbesondere hat es wohl beim Staatsschutz an einer Prüfung der eingehenden Anhaltemeldungen daraufhin, ob von der überprüften Person eine konkrete Gefahr ausgeht, gefehlt: Das niemand behindernde Abhalten einer Mahnwache vor dem Eingangstor zum Militärgelände oder auch das Mitführen eines Transparentes gegen die Nachrüstung begründen für sich allein keine konkrete Gefahr. Es ist vielmehr zu bedenken, daß solche Verhaltensweisen auch im militärischen Schutzbereich erlaubt sind, sofern es keine gegenteilige An-

ordnung gibt. Noch mehr: sie stehen auch an solchen Orten unter dem Schutz des Grundgesetzes.

Nicht dem Gesetz entsprach auch die Heilbronner Praxis, nur in jährlichen Zeitabständen die Sammlung der Anhaltemeldungen zu bereinigen.

1.2.2.4 Weitergabe von Daten

Die Heilbronner Polizei darf Daten aus ihrer Sammlung der Anhaltemeldungen nur zur Abwehr einer konkreten Gefahr weitergeben — an amerikanische Dienststellen auch nach Maßgabe des NATO-Truppenstatuts und des Zusatzabkommens hierzu. Danach arbeiten die deutschen Behörden und die Behörden der Truppen eng zusammen, um die Durchführung des NATO-Truppenstatuts und dieses Abkommens sicherzustellen. Die Zusammenarbeit erstreckt sich insbesondere auf die Förderung und Wahrung der Sicherheit sowie den Schutz der Truppen, namentlich auf den Austausch aller Nachrichten, die für diese Zwecke von Bedeutung sind.

Ob die Polizeidirektion Heilbronn diese Grenzen beachtete, konnten wir bei unserem ersten Besuch nicht feststellen, weil Aufzeichnungen fehlten, wann sie welche Information an die Amerikaner weitergab. Um diese Vorgänge für die Zukunft kontrollierbar zu machen, schlugen wir vor, solche Auskünfte nur noch auf schriftliche Auskunftsersuchen hin schriftlich zu geben und diese Entscheidung zudem einem ihrer leitenden Beamten vorzubehalten.

1.2.3 Konsequenzen

Um sicherzustellen, daß die Polizeidirektion Heilbronn und die Polizeibeamten auf der Waldheide bei der Erhebung und Verarbeitung von Daten im Zusammenhang mit der Waldheide die gesetzlichen Bestimmungen in jedem Falle beachten, bat ich die Polizeidirektion Heilbronn, ihre Dienstanweisung neu zu fassen und dabei all dem, was ich hier schrieb, Rechnung zu tragen. Sie hat dies inzwischen getan. Alle Polizeibeamten, die in Sachen Waldheide tätig sind, haben damit klare Anweisungen in der Hand und verfahren, wie die Heilbronner Polizei mir inzwischen versicherte, auch danach. Zudem konnte ich bei einem Kontrollbesuch vor wenigen Wochen feststellen, daß die Sammlung der Anhaltemeldungen inzwischen bereinigt ist: sie enthielt nur noch 8 Personen mit insgesamt 42 Einzelmeldungen; die Zahl der Meldungen über diese 8 Personen lag zwischen 2 und 14. Die gesetzlichen Voraussetzungen für ihre Aufnahme in die Sammlung lagen vor.

1.2.4 Die Folgen von Nötigungen durch Sitzblockade

Wie in Mutlangen kommt es auch auf der Waldheide hin und wieder zu Nötigungen durch Sitzblockade. Auch insoweit bemühte sich die Polizeidirektion Heilbronn von Anfang an um eine differenzierte Praxis: Blockierer, bei denen sie nicht damit rechnen muß, daß sie andere strafbare Handlungen als Nötigungen begehen, behandelt sie nicht erkennungsdienstlich. Zurückhaltung übt sie auch bei der KAN-Vormerkung: zwar gilt auch für sie der Grundsatz, nur die in ihrem Bezirk wohnenden Blockierer grundsätzlich nicht im KAN zu erfassen. Doch sieht sie bei außerhalb ihres Bezirks wohnenden Bürgern, insbesondere bei Ersttätern, von der Vormerkung im KAN ab und praktiziert damit bereits seit längerem eine Linie, wie sie sich nunmehr aus dem Mutlangen-Erlaß des Innenministeriums vom 11. Dezember 1985 ergibt.

Nicht dem Gesetz entspricht nur ihre Praxis, jeden auf der Waldheide in Erscheinung tretenden Ersttäter im Rahmen des kriminalpolizeilichen Meldedienstes in Staatsschutzangelegenheiten an das Landeskriminalamt zu melden, das die Daten an das Bundeskriminalamt weitergab, das diese wiederum in NADIS einstellte. Nach dem Mutlangen-Erlaß des Innenministeriums vom 11. Dezember 1985 will sie jedoch diese Praxis ändern und nur noch Blockierer melden, bei denen mit schwerwiegenden Straftaten zu rechnen ist.

1.3 EUCOM

Weniger im Blickpunkt der Öffentlichkeit stand in letzter Zeit das Hauptquartier der amerikanischen Streitkräfte in Europa (EUCOM) in Stuttgart-Vaihingen. Da mich aber auch dazu Anfragen erreichten, informierte ich mich bei der Landespolizeidirektion Stuttgart II, in welchem Umfang sie nach Blockadeaktionen Daten von Blockierern erhob und speicherte. Dabei stellte ich fest: nur zwei Aktionen waren unter diesem Aspekt von Interesse. Das eine Mal — es war der 16. November 1983 — schritt die Polizei gegen 47 Blockierer der Hauptzufahrt zum EUCOM ein. Da sie damals dieses Verhalten allein als Ordnungswidrigkeiten wertete, kam es zu keiner problematischen Datenverarbeitung. Das andere Mal — es war am 10. Dezember 1983 — nahm die Polizei 134 Personen vorübergehend wegen Nötigung fest. Dann lief alles ähnlich wie in Mutlangen. Knapp zwei Jahre später stellte sich bei meinem Kontrollbesuch die Lage so dar:

— Die Landespolizeidirektion Stuttgart II hatte in der Personenauskunftsdatei alle Erstblockierer anstatt mit der angemessenen Dreijahresfrist mit einer Speicherfrist von 10 Jahren — bei Jugendlichen von 5 Jahren — erfaßt.

— Hingegen hatte sie keinen der Blockierer für den bundesweiten Kriminalaktennachweis vorgemerkt.

— Nur einen der Festgenommenen behandelte sie für Zwecke der vorbeugenden Bekämpfung von Straftaten erkennungsdienstlich. Dies war zulässig, weil er bereits mit 11 Taterkenntnissen registriert war und am 10. Dezember 1983 nicht nur blockiert, sondern sich auch seiner Festnahme widersetzt hatte.

— Zwei Bürger behandelte die Landespolizeidirektion Stuttgart II erkennungsdienstlich, ohne daß sich mit letzter Sicherheit klären ließ, weshalb dies geschah. Entgegen den ed-Richtlinien war nämlich der Grund hierfür nicht in den Akten vermerkt. Man kann daher nur vermuten, daß die erkennungsdienstliche Behandlung zum Zwecke der Identitätsfeststellung erfolgte. Im Gegensatz dazu stehen allerdings die zeugenschaftlichen Erklärungen der die Blockierer wegtragenden Polizeibeamten. Sie besagen nämlich, daß die Personalien der Blockierer bei Einlieferung in den Polizeigewahrsam bereits feststanden. Wie dem auch sei — nachdem die beiden Bürger allenfalls zum Zwecke der Identitätsfeststellung erkennungsdienstlich behandelt werden durften, hätte die Landespolizeidirektion Stuttgart II die vorhandenen Lichtbilder und die Index-Karteikarten schon längst vernichten und die Eintragungen im ed-Buch löschen müssen — nämlich gleich, nachdem die Identität der beiden feststand. Dies schreiben die ed-Richtlinien ausdrücklich vor. Weshalb dies nicht geschah, konnte mir niemand sagen.

Aufgrund dieser Feststellungen forderte ich die Landespolizeidirektion Stuttgart II auf, die Dauer der Speicherung von Daten dieser Erstblockierer in der Personenauskunftsdatei auf drei Jahre herabzusetzen und die ed-Daten und ed-Unterlagen der beiden Bürger zu löschen und zu vernichten. Die Landespolizeidirektion Stuttgart II unterrichtete mich inzwischen davon, daß sie die Speicherungsdauer in 129 Blockiererfällen auf drei Jahre verkürzt und das beanstandete ed-Material vernichtet hat.

2. Direktzugriff der Fachhochschule für Polizei und der Landespolizeischule auf ZEVIS, INPOL und PAD

Die Fachhochschule für Polizei in Villingen-Schwenningen und die Landespolizeischule in Freiburg und ihre Außenstelle in Karlsruhe können ebenso wie alle Polizeidienststellen im Lande Online auf die beim Kraftfahrt-Bundesamt in Flensburg geführte Datei ZEVIS zugreifen. In ZEVIS sind bislang die Daten der zirka 15 Millionen zugelassenen Fahrzeuge aus den Ländern Baden-Württemberg, Bayern, Rheinland-Pfalz, Saarland und Schleswig-Holstein und der Zulassungsstellen Bonn und Düsseldorf sowie die Daten der über 4 Millionen Fahrzeuge mit Versicherungskennzeichen sowie die Daten der mehr als 600 000 Bürger gespeichert, denen die Fahrerlaubnis entzogen wurde. Wie die Polizeidienststellen verfügen auch die Fachhochschule für Polizei und die Landespolizeischule darüber hinaus über Direktanschlüsse an die Personen- und die Sachfahndungsdatei beim Bundeskriminalamt und die Personenauskunftsdatei des Landes. Dafür gibt es keine Rechtsgrundlage:

— Der Anschluß der beiden Ausbildungsstätten an ZEVIS läßt sich ebensowenig wie der aller Polizeidienststellen des Landes auf § 10 BDSG stützen. Denn nach § 2 Abs. 2 Nr. 2 BDSG ist es so, daß mit der Einrichtung des Direktzugriffs der gesamte Datenbestand von ZEVIS an die Fachhochschule für Polizei und die Landespolizeischule als übermittelt gilt. Da aber beide zur Erfüllung ihrer Aufgaben, nämlich der Aus- und Fortbildung von Polizeibeamten, nicht alle in ZEVIS gespeicherte Daten kennen müssen, ist der Online-Anschluß schon aus diesem Grund unzulässig. Ich gehe doch noch einen Schritt weiter: Fachhochschule für Polizei und Landes-

polizeischule benötigen überhaupt keine Originaldaten, da sie selbst nicht Aufgaben der Gefahrenabwehr oder der Strafverfolgung wahrnehmen. Für die Aus- und Fortbildung der Beamten genügt es, wenn sie mit einem Testdatenbestand üben können. Ein solcher ließe sich auch leicht einrichten, weil die Abfrage- und Recherchiermöglichkeiten in ZEVIS begrenzt sind. Das Kraftfahrt-Bundesamt teilte mir auf Anfrage mit, daß es ab der zweiten Jahreshälfte 1986 einen „realitätsgerechten" Testdatenbestand zur Verfügung stellen könne. Ich regte deshalb beim Innenministerium an, sich um eine solche Lösung zu bemühen, falls ihm an einer praxisnahen Aus- und Fortbildung seiner Polizeibeamten gelegen ist. Für die Zwischenzeit forderte ich es auf, den Online-Anschluß der beiden Schulen an ZEVIS abzuschalten. Dafür war nicht nur maßgeblich, daß eine Rechtsgrundlage hierfür fehlt, sondern eine solche auch nicht geschaffen werden soll. Der vorliegende Entwurf eines Gesetzes zur Änderung des Straßenverkehrsgesetzes, der unter anderem den Online-Anschluß der Polizei an ZEVIS legalisieren soll, sieht dies jedenfalls nicht vor: Zum Online-Abruf berechtigt sind danach ausschließlich die Polizeidienststellen des Bundes und der Länder und auch nur zur Verfolgung von Straftaten und Ordnungswidrigkeiten und zur Abwehr von Gefahren für die öffentliche Sicherheit oder Ordnung. Die Fachhochschule für Polizei und die Landespolizeischule sind jedoch nach dem Polizeigesetz und der zweiten Durchführungsverordnung dazu keine Polizeidienststellen; auch werden sie nicht zu einem der genannten Zwecke tätig. Daß sie Beamte für diese Zwecke schulen, bedeutet nicht, daß sie selbst Gefahrenabwehr oder Strafverfolgung betreiben. Nur am Rande bemerkt sei hier, daß nach einer von mir durchgeführten Länderumfrage keine andere Polizeischule in der Bundesrepublik über einen Online-Anschluß an ZEVIS verfügt. Auch das stützt meine Behauptung, ein solcher Anschluß sei nicht erforderlich.

— Dasselbe gilt für die Online-Anschlüsse der beiden Schulen an INPOL, das polizeiliche Informationssystem des Bundes und der Länder, und an die Personenauskunftsdatei, das landesweite Informationssystem. Auch sie sind nicht durch § 10 BDSG bzw. § 10 LDSG gedeckt. Die Anschlüsse an INPOL stehen darüber hinaus auch nicht mit den Feststellungsanordnungen des Präsidenten des Bundeskriminalamts für die Personenfahndungs- und Sachfahndungsdatei in Einklang. Danach sind zur Abfrage beider Dateien nämlich nur die Polizeidienststellen der Länder und das Bundeskriminalamt sowie einige weitere, im einzelnen aufgeführte Stellen befugt: Fachhochschule für Polizei und Landespolizeischule gehören dazu nicht. Ich forderte deshalb das Innenministerium auf, auch diese beiden Anschlüsse aufzuheben.

Die Reaktion des Innenministeriums hierüber war höchst bemerkenswert: Nicht etwa deswegen, weil es zum wiederholten Male meine Kontrollkompetenz für ZEVIS mit der auch nicht richtiger werdenden Begründung bestritt, Datenübermittlungen des Kraftfahrt-Bundesamtes an Stellen der Länder fielen allein in die Zuständigkeiten des Bundes. Bemerkenswert war vielmehr vor allem, in welchem Ton und mit welcher Begründung es meine Forderung nach Abschaltung der Online-Anschlüsse zurückwies:

„Vordergründig ist natürlich nicht zu bestreiten, daß Landespolizeischule und Fachhochschule für Polizei weder Zwecke der Strafverfolgung noch der Gefahrenabwehr verfolgen. An beiden Einrichtungen durchgeführte Veranstaltungen zielen jedoch allein darauf ab,

die Beamten für die Erfüllung dieser Aufgaben zu schulen. Die dazu notwendigen Daten sind damit auch zur Aufgabenerfüllung in diesem Sinne erforderlich."

So einfach ist es also beim Innenministerium: Wer sich — wie ich — am Gesetz orientiert, die Begriffe Gefahrenabwehr und Strafverfolgung wie üblich auslegt, muß sich den Vorwurf gefallen lassen, vordergründig zu argumentieren. Maßgeblich ist offensichtlich nicht mehr das Gesetz, sondern das, was das Innenministerium für notwendig erachtet. Alles andere ist, wie es das Innenministerium an anderer Stelle formuliert, überzogener Datenschutz, für den es selbst im vielzitierten Volkszählungsurteil keine Stütze gäbe. Ich meine, daß es sehr wohl ein berechtigtes Anliegen des Bürgers ist, daß seine in ZEVIS und in polizeilichen Informationssystemen gespeicherten Daten nur für Zwecke der Strafverfolgung und Gefahrenabwehr und nur den Polizeidienststellen zur Verfügung stehen. Daß den Schulen Testdaten genügen, räumt im übrigen auch das Innenministerium ein, wenn es ausführt, gegen eine Umstellung des ZEVIS-Anschlusses auf einen vom Kraftfahrt-Bundesamt angebotenen, geeigneten Testdatenbestand bestünden selbstverständlich keine Bedenken. Für die beiden anderen Dateien INPOL und PAD kann jedoch nichts anderes gelten: Auch hier genügten Testdaten. Fraglich kann damit allein sein, daß der Aufwand für deren Einrichtung zu groß wäre. Das ist jedoch nicht der Fall, wenn man keine überzogenen Anforderungen an sie stellt. Damit die Polizeibeamten im Lande die Möglichkeiten der Personenauskunftsdatei kennenlernen und üben können, bedarf es nicht — wie das Innenministerium meint — einer Testdatei mit 500 000 Datensätzen. Es genügt dafür ein wesentlich kleinerer Bestand, der sich mit vertretbarem Aufwand anlegen ließe. Ich hoffe sehr, daß das Innenministerium in dieser Frage noch umdenkt.

3. Die freiwillige ed-Behandlung Prostituierter

Die Polizei darf einen Bürger erkennungsdienstlich behandeln, wenn es zur Durchführung eines Strafverfahrens oder zur vorbeugenden Bekämpfung von Straftaten oder zur Feststellung der Identität erforderlich ist oder wenn er ohne festen Wohnsitz umherzieht. Prostituierte werden hierzulande jedoch auch dann erkennungsdienstlich behandelt, wenn keine dieser Voraussetzungen vorliegt. „Erkennungsdienstliche Behandlung mit Einwilligung" nennt die Polizei das. Ob die Prostituierten tatsächlich immer damit einverstanden sind, daß die Polizei sie photografiert und — was allerdings nur zum Teil geschieht — Fingerabdrücke nimmt, wenn sie sich bei ihr „anmelden", sehen die Beteiligten unterschiedlich: Die Polizei bejaht es selbstverständlich, während die Betroffenen meinen, von Freiwilligkeit könne keine Rede sein. „Jetzt müssen wir noch ein Lichtbild von Ihnen machen" so oder ähnlich formulieren es nach Angaben der Prostituierten die Polizeibeamten. Eine Belehrung über die Rechtslage, einen Hinweis auf die Freiwilligkeit gebe es — so die Prostituierten — nicht, geschweige denn, daß die Polizei ihre Einwilligung in die Datenverarbeitung einhole. Die Prostituierten erfahren danach regelmäßig auch nicht,

- ob die örtliche Polizeidienststelle nur ein Lichtbild von ihnen fertigt, das dann bei ihr verbleibt — so macht es die Landespolizeidirektion Stuttgart II — oder ob sie die auch sonst übliche Zahl von Lichtbildern herstellt und eine Aufnahme dem Bundeskriminalamt übersendet,
- daß die örtliche Polizeidienststelle ihre Fingerabdrücke an das Landeskriminalamt weiterleitet,

— daß die Polizei Lichtbilder, Fingerabdrücke und Personenbeschreibungsdaten speichert und erforderlichenfalls zur Erfüllung polizeilicher Aufgaben an andere Polizeidienststellen und Behörden übermittelt.

Nicht aufgeklärt werden die Prostituierten meist auch darüber, daß sie ihre Einwilligung jederzeit widerrufen können. Das hat nicht nur, aber vor allem für Frauen Bedeutung, die die Prostitution aufgeben und verständlicherweise den Wunsch hegen, daß die Polizei keine Unterlagen mehr über ihre frühere Tätigkeit besitzt. Sie wollen wissen, was sie tun können, damit ihre erkennungsdienstlichen Unterlagen vernichtet werden.

Wegen dieser Informationen über die Praxis der Polizei machte mein Amt das Innenministerium auf die geschilderte, mit dem Landesdatenschutzgesetz nicht zu vereinbarende Praxis aufmerksam. Dieses ordnete inzwischen durch Erlaß vom 22. November 1985 an, daß die Prostituierten per Vordruck auf die Freiwilligkeit der erkennungsdienstlichen Behandlung hinzuweisen sind und ihre Einwilligung in die Datenverarbeitung schriftlich einzuholen ist. Der Vordruck klärt die Frauen auch darüber auf, daß sie ihre Einwilligung jederzeit widerrufen können. Davon haben inzwischen einige Gebrauch gemacht, die der Prostitution nicht mehr nachgehen.

4. Max-Planck-Institut untersucht KpS-Fristen

Die von den Polizeien des Bundes und der Länder erarbeiteten und Anfang 1981 verabschiedeten KpS-Richtlinien legten für die Polizei erstmals sog. Regelspeicherfristen fest: Bei Erwachsenen sollte die Polizei gespeicherte Daten regelmäßig nach 10 Jahren löschen. Bei Jugendlichen sollte sie spätestens nach 5, bei Kindern spätestens nach 2 Jahren prüfen, ob eine Löschung möglich ist. In Fällen von geringer Bedeutung sollte die Löschung regelmäßig nach 3 Jahren erfolgen. Schon kurze Zeit nach Einführung der Richtlinien machten jedoch Teile der baden-württembergischen Polizei unter Führung des Landeskriminalamts Front gegen die Regelspeicherfristen. Sie seien zu kurz bemessen, trügen den Besonderheiten des Einzelfalls nicht Rechnung, seien Schuld daran, wenn der Polizei wertvolles Material verloren gehe, verursachten einen zu großen Aufwand.

Mich haben diese Argumente nie überzeugt. Die KpS-Richtlinien lassen der Polizei bei richtiger Handhabung ausreichend Spielraum. Oberster Grundsatz ist nämlich: Die Speicherung ist so lange zulässig, wie es zur rechtmäßigen Aufgabenerfüllung der Polizei erforderlich ist. Hierbei sind das öffentliche Interesse, zu Zwecken der Strafverfolgung oder Gefahrenabwehr auf polizeiliche Erkenntnisse zurückgreifen zu können, und das durch das Grundrecht auf freie Entfaltung der Persönlichkeit geschützte Interesse des einzelnen, solchen Einwirkungen der öffentlichen Gewalt nicht ausgesetzt zu sein, gegeneinander abzuwägen. Im Sinne einer verallgemeinernden Interessenabwägung legen die Richtlinien sodann Regelspeicherfristen fest. Sie gelten jedoch, wie es schon der Name sagt, nur für den Regelfall. In atypischen Fällen kann, ja muß die Polizei kürzere und ausnahmsweise auch längere Fristen festlegen. Die KpS-Richtlinien sehen selbst eine Verlängerung vor: „Wenn Tatsachen die Annahme rechtfertigen, daß wegen Art und Ausführung der Tat, die der Betroffene begangen hat oder derer er verdächtig war, die Gefahr der Wiederholung besteht oder die Aufbewahrung der Unterlagen aus anderen schwerwiegenden Gründen zur

Aufgabenerfüllung weiterhin erforderlich ist", kann die Polizei im Einzelfall angemessene Speicherungsfristen festsetzen.

Die Polizei sah dies jedoch anders und bekämpfte die Fristenregelung mit allen Mitteln. So ließ sich das Landeskriminalamt beispielsweise von allen Dienststellen Fälle melden, in denen Personen nach Löschung ihrer Daten in der Personenauskunftsdatei erneut bei der Polizei in Erscheinung traten. Ferner untersuchte das Landeskriminalamt in einer Stichprobe die Rückfälligkeit von Personen, die die Polizeidirektion Esslingen in der Personenauskunftsdatei erfaßt hatte. Es kam dabei zu dem Schluß, die Regelspeicherfristen bei Kindern und Jugendlichen reichten nicht aus. Eine Nachprüfung durch mich ergab allerdings, daß dem Landeskriminalamt bei seiner Untersuchung verschiedene rechnerische und methodische Fehler unterlaufen waren.

Um gesicherte Erkenntnisse darüber zu gewinnen, ob und in welchem Umfang Straftäter bzw. Straftatverdächtige, deren Daten in der Personenauskunftsdatei gelöscht wurden, später wieder in Erscheinung treten, wollte das Innenministerium schließlich das Landeskriminalamt mit einer Untersuchung beauftragen. Die im Rahmen des maschinellen PAD-Löschungsverfahrens anfallenden Löschprotokollbänder sollten zu diesem Zweck 2 Jahre lang jeweils halbjährlich mit dem aktuellen PAD-Datenbestand abgeglichen werden. Das Innenministerium bot mir an, mich an diesem Projekt zu beteiligen. Ich erklärte meine Bereitschaft, an einer Untersuchung über die Geeignetheit der Aufbewahrungsfristen in den KpS-Richtlinien mitzuwirken, obwohl ich für eine solche Untersuchung keine Notwendigkeit sah und sehe. Wenn sie überhaupt einen Sinn machen soll, gilt es — das machte ich sehr deutlich —, dabei vor allem drei Gesichtspunkte zu beachten:

— Das Innenministerium darf zur Durchführung des Projekts die in den KpS-Richtlinien festgelegten Regellöschungsfristen nicht für das ganze Land aufheben. Die Untersuchung muß sich vielmehr auf eine bis maximal drei repräsentative Polizeidienststellen beschränken.

— Untersucht werden darf nicht nur, wie viele Kinder, Jugendliche, Erwachsene nach Löschung ihrer Daten in der Personenauskunftsdatei in welchem zeitlichen Abstand erneut darin erfaßt wurden und mit welchem Tatvorwurf. Vielmehr muß auch weiteres geschehen:

  • Nachzugehen ist der Frage, in wie vielen Fällen nach Ablauf der Regelfrist gelöschte Daten schon vorher im Wege der Einzelfallöschung hätten gelöscht werden müssen. Ich darf dies an einem Beispiel verdeutlichen: Der 30jährige Herr X war wegen Diebstahls in der Personenauskunftsdatei erfaßt. Nach 10 Jahren löschte die Polizei seine Daten. Zwei Jahre später ermittelte die Polizei gegen ihn wegen Erschleichens von Beförderungsleistungen. Herr X wäre danach ein sog. Wiederholungstäter. Dies muß jedoch nicht so sein: Ist Herr X nämlich in dem gegen ihn durchgeführten Strafverfahren wegen Diebstahls freigesprochen worden, weil er nicht der Täter war, so hätte die Polizei seine Daten unverzüglich in der Personenauskunftsdatei löschen müssen und damit nicht bis zum Ablauf der Regelspeicherfrist warten dürfen. Herr X wäre somit bei richtiger Sachbehandlung kein Wiederholungs-, sondern — falls sich der neue Tatvorwurf als zutreffend erweist, was ja keineswegs gesagt ist — allenfalls Ersttäter. Da sol-

che Fälle alles andere als selten sind — insbesondere aus den Anfängen der Personenauskunftsdatei, als es noch keine Einzelfallöschung wegen des Verfahrensausgangs bei der Justiz gab —, muß man die Regellöschfälle generell daraufhin untersuchen, ob sie nicht in Wirklichkeit Einzellöschfälle sind. Ich gehe davon aus, daß sich die Zahl der vermeintlichen Wiederholungstäter auf diese Weise nicht unerheblich verringert. In vielen Fällen wird es sich allerdings gar nicht mehr feststellen lassen, ob ein Regellöschungsfall nicht bei richtiger Sachbehandlung und im Wege der Einzelfallöschung hätte gelöscht werden müssen. Das liegt daran, daß die Justiz vor 1981 die Polizei vielfach nicht über den Ausgang eines Ermittlungs- bzw. Strafverfahrens unterrichtete, obwohl dies schon damals vorgeschrieben war. Auch diese Zahl muß jedoch ermittelt werden, weil sich in diesen Fällen nicht mit Sicherheit sagen läßt, daß ein Bürger, der zum zweiten Mal mit der Polizei zu tun hat, ein Wiederholungstäter ist.

- Nachzugehen ist auch der Frage, ob im Zeitpunkt der Regellöschung Tatsachen erkennbar waren, die nach den KpS-Richtlinien eine Verlängerung gerechtfertigt hätten. Diese Frage zielt darauf ab, ob in Einzelfällen auftretende Probleme nicht bereits mit den geltenden KpS-Richtlinien hätten gelöst werden können. Wäre dies der Fall, ginge es wohl nicht an, die KpS-Fristen generell zu verlängern.

— Die Untersuchung darf sich nicht auf einen Abgleich zwischen den Löschprotokollbändern und dem aktuellen Personenauskunftsdatei-Bestand beschränken, sondern muß auch die Ermittlungsakten miteinbeziehen. Denn nur so kann man feststellen, ob eine Regellöschung nicht in Wirklichkeit eine Einzelfallöschung hätte sein müssen oder ob im Zeitpunkt der Regellöschung Tatsachen erkennbar waren, die eine Verlängerung der Frist nach den KpS-Richtlinien gerechtfertigt hätten.

Während Innenministerium und ich uns rasch über die Forschungsfragen und auch darüber einigen konnten, daß nur ein renommiertes Forschungsinstitut wie das Max-Planck-Institut für ausländisches und internationales Strafrecht in Freiburg für eine solche Untersuchung in Frage kommt, gestalteten sich die Verhandlungen über die konkrete Durchführung des Vorhabens schwierig. Sie wurden zusätzlich dadurch erschwert, daß das Innenministerium hinter meinem Rücken und obwohl es meine Haltung dazu kannte, durch Erlaß vom 7. Juli 1983 die Löschung der in der Personenauskunftsdatei gespeicherten Daten ab Mitte 1982 für das ganze Land aussetzte. Ab diesem Zeitpunkt nahm das Landeskriminalamt die zur Löschung heranstehenden Daten von zig-Tausenden von Bürgern zwar aus der aktuellen Personenauskunftsdatei heraus, speicherte sie jedoch auf Löschprotokollbändern. Allein von 1982 bis 1984 waren hiervon über 85 000 Personen betroffen. Dies stellte, da die Polizei auf die darauf gespeicherten Daten mit Hilfe eines entsprechenden Programms jederzeit hätte zugreifen können, keine Löschung im Sinne des Landesdatenschutzgesetzes dar. Ich protestierte deshalb gegen diese Maßnahme — jedoch vergeblich: das Innenministerium beharrte auf dem formal zutreffenden Standpunkt, das Landesdatenschutzgesetz schreibe nur eine Sperrung und keine Löschung der Daten vor. Gesperrt seien die Daten jedoch allemal, da die Polizei sie nicht mehr nutze. Das Innenministerium übersah dabei, daß die Aussetzung der Löschung für das ganze Land über einen längeren Zeitraum hinweg

ein Vorgang ist, den ein Datenschutzbeauftragter im Interesse der betroffenen Bürger nicht hinnehmen kann. Nicht umsonst hat sich ja auch die deutsche Polizei 1981 entschieden, mehr zu tun als die Datenschutzgesetze fordern und nach Fristablauf die Daten zu löschen und nicht bloß zu sperren.

Trotz dieser schweren Belastung der Verhandlungen konnte das Vorhaben Mitte 1985 unter Dach und Fach gebracht werden. Mit Ergebnissen der Untersuchung ist frühestens Ende 1987 zu rechnen. Auch sind alle Daten aus der Personenauskunftsdatei, die für Forschungsvorhaben nicht unbedingt benötigt werden, seit Ende November gelöscht.

2. Abschnitt: Zentrale Namenskarteien der Staatsanwaltschaften

1. Ausgangslage

Jede Staatsanwaltschaft führt ein zentrales Namensregister. In ihm sind alle Personen erfaßt, gegen die ein Ermittlungsverfahren bei ihr anhängig ist oder war. Das Namensregister ist traditionell eine Sammlung von Karteikarten. Die Sache läuft dabei so ab: Geht bei der Staatsanwaltschaft eine Anzeige ein, legt sie über den Beschuldigten eine Karteikarte an. Ist eine solche bereits vorhanden, vermerkt sie das neue Verfahren zusätzlich auf ihr. Die Kartei hat unterschiedliche Funktionen. Sie dient in erster Linie dem Auffinden von Akten. Auch ermöglicht sie, in zunächst abgeschlossenen, dann aber erneut aufgerollten Verfahren auf frühere Akten zurückzugreifen. Bei neu eingehenden Anzeigen läßt sich über die Kartei feststellen, ob gegen den Beschuldigten bereits Verfahren anhängig waren. Schließlich gibt die Staatsanwaltschaft aus der Kartei auch Auskünfte an verschiedenste Stellen, z. B. an Anwälte, Geschädigte, Gerichte, Polizei und Versicherungen.

Als ich mich 1980 erstmals mit den Zentralen Namenskarteien befaßte, stellte ich fest, daß sie in einigen Punkten nicht dem Landesdatenschutzgesetz entsprechen: Nicht einmal bei einem rechtskräftigen Freispruch wegen erwiesener Unschuld zogen die Staatsanwaltschaften Konsequenzen. Auch ließ die Bereinigung der Karteien nach Ablauf angemessener Fristen zu wünschen übrig. Das Justizministerium erkannte einst zwar meine daraus abgeleiteten Forderungen im Grundsatz an, glaubte jedoch, sie mit dem vorhandenen Personal nicht realisieren zu können. Es beschritt einen anderen Weg und erklärte kurzerhand 1982 die Zentralen Namenskarteien zu sog. internen Dateien. Darunter versteht man Dateien, die eine Behörde ausschließlich für ihre eigenen Zwecke nutzt und aus der sie keine Informationen an andere weitergibt. Mit diesem legalen „Trick" erreichte das Justizministerium, daß sich die Staatsanwaltschaften beim Speichern, Weitergeben, Sperren und Löschen von Daten der Zentralen Namenskartei nicht an das Landesdatenschutzgesetz halten mußten und nicht meiner Kontrolle unterlagen. Einen Nachteil dabei mußten sie allerdings in Kauf nehmen: Ihre Bediensteten bei der Zentralen Namenskartei konnten telefonische Anfragen von Rechtsanwaltskanzleien, unter welchem Aktenzeichen ein Ermittlungsverfahren gegen ihren Mandanten läuft, nicht mehr wie ehedem sofort anhand der Kartei beantworten; sonst wäre diese ja keine interne Datei mehr gewesen. Die Bediensteten waren vielmehr genötigt, Anrufer an den zuständigen Staatsanwalt bzw. die Geschäftsstelle zu verweisen, um dort das Aktenzeichen aus der Ermittlungsakte zu erfahren. Diese

Verfahrensweise ist zweifellos umständlich. Sie läßt sich allerdings nicht, wie mancher Staatsanwalt oder Rechtsanwalt meinte, auf den Datenschutz oder gar mich zurückführen. Im Gegenteil: Aus der Sicht des Datenschutzes wäre es sehr viel besser und mir wäre es sehr viel lieber gewesen, die Staatsanwaltschaften hätten weiterhin die Auskünfte aus der Zentralen Namenskartei geben können und diese Kartei nach und nach so bereinigt, wie es das Landesdatenschutzgesetz erfordert. Immerhin sah auch das Justizministerium, daß es in diesem Punkt etwas tun muß: seit 1. Januar 1984 müssen die Staatsanwaltschaften ihre Karteikarten nach sechs bzw. neun Jahren vernichten. Dies gilt auch für in der Vergangenheit angelegte Karteikarten. Diese Regelung hat einen ziemlichen Schönheitsfehler: wegen desselben Delikts bleibt ein Beschuldigter bei der einen Staatsanwaltschaft sechs, bei der anderen neun Jahre gespeichert.

2. Zentrale Namensdatei (ZENDA) der Staatsanwaltschaft Stuttgart

Die Staatsanwaltschaft Stuttgart stellte am 1. Januar 1985 als erste Staatsanwaltschaft im Lande ihre Zentrale Namenskartei auf EDV um. Grund dafür war wohl, daß sie ihre Kartei mit ca. 1,2 Millionen Karteikarten und einem jährlichen Zuwachs von weit mehr als 100 000 Karteikarten kaum mehr handhaben konnte. Mit der Automatisierung änderte sich auch die Rechtslage: Eine automatisierte Datei unterliegt — unabhängig davon, ob aus ihr Auskunft an Dritte erteilt wird oder nicht — in vollem Umfang dem Landesdatenschutzgesetz und der Datenschutzkontrolle. Ich sah mir deshalb bei einem Kontrollbesuch die Zentrale Namensdatei der Staatsanwaltschaft Stuttgart eingehend an und stellte fest:

2.1 Die bisherige Vorgehensweise

Die Staatsanwaltschaft erfaßt bei Eingang einer Strafanzeige im wesentlichen
- den Familiennamen, Vornamen, Geburtsnamen, das Geburtsdatum, den Geburtsort und das Geburtsland des Beschuldigten,
- den Tag der Anzeige,
- den Tatvorwurf, wie er sich aus der polizeilichen Anzeige ergibt,
- die Speicherungsdauer, nämlich 30 Jahre bei Leichensachen, 20 Jahre bei Brandsachen und im übrigen 5 Jahre

im Computer. Sobald sie bei sich das Verfahren abgeschlossen hat, speichert sie auch die Erledigungsart — nämlich Anklage, Strafbefehlsantrag oder Einstellung. Den Ausgang des gerichtlichen Verfahrens vermerkt sie nicht. Auch sperrt oder löscht sie Daten je nach Ausgang des Verfahrens nicht: Die Daten eines Bürgers, dessen Unschuld sich im Ermittlungsverfahren herausgestellt hat oder der im Strafverfahren rechtskräftig freigesprochen wurde, bleiben mindestens 5 Jahre im Computer und stehen der Staatsanwaltschaft uneingeschränkt zur Verfügung.

Auf telefonische Anfragen reagierte die Staatsanwaltschaft so: Die ZENDA-Bediensteten verwiesen den Anrufer an die zuständige Geschäftsstelle. Diese prüfte, ob der Anrufer ein berechtigtes Interesse an der Auskunft hat, und identifizierte ihn — gegebenenfalls durch Rückruf. Bei Anrufen

von Rechtsanwaltskanzleien ging es einfacher zu: sie mußten lediglich die ihnen von der Anwaltskammer zugeteilte, der Staatsanwaltschaft bekannte Codenummer nennen. Diese entsprach der Mitgliedsnummer der Rechtsanwälte in der Anwaltskammer, an die heranzukommen für Dritte kein Problem ist: Die Rechtsanwaltskammer druckt sie beispielsweise auf Adreßklebern aus, die sie für den Versand ihrer Kammermitteilungen an die Rechtsanwälte verwendet.

2.2 Meine Einwände

Diese Verfahrensweise begegnete in mehrfacher Hinsicht Bedenken:

2.2.1 Tatvorwurf

Der in der ZENDA eingetragene Tatvorwurf kann unrichtig sein. Dies ist schon dann der Fall, wenn die Polizei einem Beschuldigten, der mit seinem Auto auf einen Polizeibeamten losfährt, versuchten Mord vorwirft, während die Staatsanwaltschaft nur von einem gefährlichen Eingriff in den Straßenverkehr ausgeht. Der Tatvorwurf kann aber auch im Laufe des Ermittlungs- oder Strafverfahrens unrichtig werden: etwa wenn die Polizei oder Staatsanwaltschaft einem Beschuldigten zunächst Totschlag vorwerfen, sich später jedoch herausstellt, daß sich der tödliche Schuß versehentlich aus der Waffe des Beschuldigten löste und damit nur eine fahrlässige Tötung vorliegt. In beiden Fällen ist der Beschuldigte durch den ursprünglichen Eintrag „versuchter Mord bzw. Totschlag" in ZENDA beschwert. Dafür genügt die Besorgnis, der Eintrag in ZENDA habe bei etwaigen künftigen Ermittlungen der Staatsanwaltschaft gegen ihn oder einen andern, den er möglicherweise anzeigte, Einfluß auf Entscheidungen der Staatsanwaltschaft. Ich forderte deshalb, den Tatvorwurf unverzüglich zu berichtigen, wenn er sich zu Gunsten eines Beschuldigten ändert.

2.2.2 Verfahrenserledigung

Ähnlich liegen die Dinge beim Eintrag „Verfahrenserledigung". Erfaßt wird bisher nur der Verfahrensabschluß bei der Staatsanwaltschaft, also beispielsweise die Anklageerhebung. Nicht registriert sie hingegen, wenn — um ein Beispiel zu nennen — das zuständige Gericht die Eröffnung der Hauptverhandlung ablehnt, weil gegen den Angeklagten kein hinreichender Tatverdacht besteht. Dies verfälscht das Bild, das über einen Bürger vermittelt wird: gespeichert wird nur das ihn Be-, nicht auch das ihn Entlastende. Um das für die Zukunft zu vermeiden, muß die Staatsanwaltschaft den Angeklagten entlastende Verfahrenserledigungen in ZENDA vermerken.

2.2.3 Sperren und Löschen

Ein Hauptproblem ist jedoch, daß die Staatsanwaltschaft bei bestimmten Verfahrensausgängen die in ZENDA gespeicherten Daten nicht sperrt — d. h. nicht

mehr nutzt —, geschweige denn löscht. Dies aber ist notwendig, wenn

— in einem Ermittlungsverfahren jeglicher Tatverdacht gegen einen Beschuldigten entfallen ist;

— unter keinem rechtlichen Gesichtspunkt ein strafbares Verhalten des Beschuldigten vorliegt;

— das Fehlen einer Prozeßvoraussetzung endgültig feststeht; dies ist beispielsweise der Fall, wenn bei einer Straftat, die nur auf Antrag einer Behörde oder des Verletzten verfolgt wird, innerhalb der dreimonatigen Antragsfrist kein Strafantrag gestellt werden, oder wenn eine Tat verjährt ist;

— das Gericht die Eröffnung der Hauptverhandlung aus einem der vorgenannten Gründe abgelehnt hat;

— das Gericht das Verfahren wegen eines Verfahrenshindernisses (z. B. Verjährung, fehlender Strafantrag, verbrauchter Strafklage) nach Eröffnung des Hauptverfahrens durch Beschluß außerhalb der Hauptverhandlung oder durch Urteil rechtskräftig eingestellt hat;

— der Angeklagte rechtskräftig freigesprochen wurde.

Hier benötigt die Staatsanwaltschaft die in ZENDA gespeicherten Daten regelmäßig nicht mehr zur Erfüllung ihrer Aufgaben. Sie dürfen deshalb bei einer Abfrage des Computers nicht mehr auf dem Bildschirm erscheinen (sog. Sperrung der Daten). Nur dann ist gesichert, daß beispielsweise ein Bürger, dessen Unschuld sich in einem Ermittlungs- oder Strafverfahren herausstellte, wenigstens annähernd so gestellt ist, als hätte es ein solches Verfahren gar nie gegen ihn gegeben. Nur unter den engen Voraussetzungen des Landesdatenschutzgesetzes — etwa zur Behebung einer bestehenden Beweisnot — darf die Staatsanwaltschaft auf diese Daten ausnahmsweise noch zugreifen, indem sie einen besonderen Code in den Computer eingibt.

Entgegen der Meinung mancher Bürger kann man hingegen nicht fordern, die Daten zu sperren, wenn die Staatsanwaltschaft das Verfahren aus anderen als den obengenannten Gründen einstellte — etwa mangels eines für die Anklageerhebung ausreichenden Tatverdachts. Ein solches Verfahren kann die Staatsanwaltschaft nämlich wieder aufnehmen, sofern die Tat nicht verjährt ist und sie neue Tatsachen erfährt.

2.2.4 Auskünfte an Rechtsanwälte

Nicht befriedigen konnte auch das Verfahren bei der Auskunftserteilung an Rechtsanwälte. Es bot keine Gewähr, daß der Anrufer tatsächlich Auskunft erhalten durfte:

— Problematisch war schon, daß die Codenummer die Mitgliedsnummer des Rechtsanwalts war.

— Der fehlende Wechsel der Codenummern in angemessenen Zeitabständen erhöhte noch die Gefahr, daß Personen sie erfahren, die zur Abfrage nicht berechtigt sind.

— Kritisch zu bewerten war schließlich, daß weder die Staatsanwaltschaft noch die Rechtsanwaltskammer erfuhren, wenn ein Mitarbeiter (z. B. eine Sekretärin) aus einer Rechtsanwaltskanzlei ausschied und damit zur Abfrage nicht mehr befugt war.

Um die Mißbrauchsmöglichkeiten einzudämmen, schlug ich vor, daß die Rechtsanwaltskammer für jedes Mitglied einen Code vergibt, der nicht mit der Mitgliedsnummer identisch und ihr auch nicht ähnlich ist. Diesen wechselt sie regelmäßig und zudem dann, wenn er möglicherweise Unbefugten bekannt wurde. Die Anwaltskammer leitet jedem Rechtsanwalt den persönlichen Code in verschlossenem Umschlag zu. Außerdem verpflichtet sie ihn, einen neuen Code bei ihr anzufordern und zu verwenden, wenn ein ursprünglich Abfrageberechtigter aus der Kanzlei ausscheidet oder wenn nicht auszuschließen ist, daß seine Codenummer Unbefugten bekannt wurde.

Die Stuttgarter Staatsanwaltschaft und Rechtsanwaltskammer wollen meinen Bedenken in vollem Umfang Rechnung tragen. Damit ist — das weiß ich wohl — für beide ein gewisser Mehraufwand verbunden. Auf der andern Seite konnte ich der Staatsanwaltschaft jedoch auch Entlastung verschaffen: Sie kann jetzt wieder Auskünfte über gespeicherte Daten unmittelbar aus der Datei ZENDA erteilen und muß die Anrufer nicht mehr an Geschäftsstelle oder Staatsanwalt verweisen.

3. Abschnitt: Gesetzgebung

1. Zur Situation

Nach dem Volkszählungsurteil war klar: der Gesetzgeber muß Rechtsgrundlagen für die Informationsverarbeitung der Sicherheitsbehörden schaffen. Änderungen der Strafprozeßordnung, des Bundeskriminalamtsgesetzes, des Bundesgrenzschutzgesetzes, der Polizeigesetze der Länder und der Verfassungsschutzgesetze des Bundes und der Länder sind damit unausweichlich. Auch gilt es, die Aufgaben und Befugnisse des Militärischen Abschirmdienstes und die Zusammenarbeit zwischen den Sicherheitsbehörden auf eine gesetzliche Grundlage zu stellen. Darin waren sich die Vertreter der Sicherheitsbehörden und des Datenschutzes schnell einig. Beide Seiten machten sich deshalb ans Werk. Die Innenministerkonferenz ließ ihre Arbeitskreise Regelungen für die Polizeigesetze und den Entwurf eines neuen Bundesverfassungsschutzgesetzes ausarbeiten. Der Bund sollte Entwürfe für ein MAD-Gesetz und ein Zusammenarbeitsgesetz vorlegen. Auch die Datenschutzbeauftragten blieben nicht untätig: sie verabschiedeten am 25. Januar 1985 einen Forderungskatalog zum Polizeigesetz und am 16. September 1985 zum Verfassungsschutzgesetz.

Anfang März 1985 teilte ich dem Innenministerium in einer umfangreichen Stellungnahme meine Vorstellungen zum Polizeigesetz mit. Ohne in irgendeiner Weise auf diese Ausarbeitung einzugehen, übersandte es mir im Mai 1985 Vorentwürfe zum Polizei- und zum Verfassungsschutzgesetz, mit denen sich die Innenministerkonferenz schon befaßt hatte. Nicht übersandte es mir den inzwischen ebenfalls vorliegenden Entwurf eines Zusammenarbeitsgesetzes, obwohl auch dieser die Datenverarbei-

tung durch Sicherheitsbehörden der Länder regelt und somit für mich von großem Interesse ist. Ich mußte ihn mir daher bei einem meiner Kollegen besorgen; fast alle Datenschutzbeauftragten hatten den Entwurf von ihrem Innenressort erhalten. Zu diesen drei Entwürfen nahm ich im August bzw. Oktober 1985 gegenüber dem Innenministerium umfassend Stellung. Mein Ergebnis war, daß die Entwürfe, so wie sie aussehen, abzulehnen sind: nicht nur, weil sie in vielen Einzelpunkten nicht befriedigen, sondern vor allem wegen zweier grundsätzlicher Bedenken:

— Zum einen gehen sie von einem falschen Ansatzpunkt aus: Es kann nicht Aufgabe des Gesetzgebers sein, die derzeitige Praxis einfach festzuschreiben, ja in manchen Punkten sogar noch darüber hinauszugehen. Es ist vielmehr notwendig — wie es Prof. Benda, der frühere Präsident des Bundesverfassungsgerichts, in einer gutachtlichen Äußerung zu Verfassungsfragen des Berliner Meldegesetzes formulierte —, auch über viele Jahre für selbstverständlich gehaltene Verhaltensweisen und Regelungen zu überdenken. Die Sicherheitsbehörden sollen Daten verarbeiten dürfen, soweit dies zur Erfüllung ihrer Aufgaben nachweisbar unerläßlich ist, mehr aber auch nicht.

— Zum anderen regeln sie viele Fragen nicht vollständig und oftmals auch nicht hinreichend präzise. Ich weiß wohl, daß Forderungen nach mehr Regelung angesichts der vielbeklagten Normenflut nicht populär sind. Ich meine aber, daß im Sicherheitsbereich, in dem durch das Erheben und Verarbeiten von Daten ganz erheblich in das informationelle Selbstbestimmungsrecht der Bürger eingegriffen wird, klare Grenzen gezogen werden müssen. Das liegt im Interesse des Bürgers, aber auch der Behörden.

Wie sich das Innenministerium zu meinen Überlegungen stellt, weiß ich bis heute leider nicht. Alles, was ich schrieb, blieb ohne Resonanz. Einem Rundfunkinterview des Landespolizeipräsidenten zum Entwurf eines Polizeigesetzes konnte ich nur zwei Dinge entnehmen: zum einen hält er — anders als viele andere und ich — den Entwurf für eine Einschränkung gegenüber dem geltenden Recht. Zum andern meint er, bis zu einer endgültigen Verabschiedung des Entwurfs gingen sicher noch mehrere Jahre ins Land. Ein Drittes las ich in einer Tageszeitung, die ein internes Schreiben des Landespolizeipräsidenten an den Herrn Innenminister veröffentlichte: die Polizei rät beim jetzigen Verfahrensstand von einer öffentlichen Diskussion des Entwurfs und einer Behandlung im Landtag ab; die Regierung müsse erst die Möglichkeit haben, sich selbst ein schlüssiges und mit Bund und Ländern abgestimmtes Konzept für die polizeiliche Informationsverarbeitung zu machen. Ich meine, daß es dann für eine Diskussion zu spät ist, weil die Positionen festgelegt sind. Die Regierung muß sich jetzt der Diskussion mit mir stellen. Es darf nicht so sein, daß immer nur ich meine Vorstellungen gegenüber dem Innenministerium darlege, ohne jemals in der Sache eine Antwort zu erhalten. Mich würde selbstverständlich interessieren, in welchen Punkten das Innenministerium mit mir übereinstimmt, noch mehr jedoch, in welchen Punkten es aus welchen Gründen anderer Auffassung ist. Nur über einen solchen Dialog, der natürlich nicht nur im Austausch von Schreiben bestehen darf, wird es möglich sein, zu sachlich fundierten Lösungen im Spannungsfeld zwischen Persönlichkeitsschutz und effektiver polizeilicher Aufgabenerfüllung zu kommen. Das Innenministerium sollte deshalb keine

Zeit verlieren, ihn endlich in Gang zu setzen, da die Schaffung datenschutzrechtlicher Vorschriften im Sicherheitsbereich keinen Aufschub duldet.

Weder eine öffentliche Diskussion noch einen Dialog mit mir gab es bislang über den Entwurf eines Verfassungsschutzgesetzes, obwohl dieser — jedenfalls in seiner ursprünglichen Fassung — kaum weniger brisant ist als der Entwurf zum Polizeigesetz. Zu beidem wird es vermutlich auch nicht mehr kommen, weil die Bonner Koalitionsfraktionen Presseberichten zufolge den Entwurf noch im Januar 1986 abschließend beraten wollen. Es bleibt deshalb nur zu hoffen, daß er den von den Datenschutzbeauftragten des Bundes und der Länder gemeinsam erarbeiteten Forderungskatalog berücksichtigt und ich auch meine sonstigen Überlegungen darin wiederfinde.

Noch nicht so weit gediehen sind die Arbeiten an der Änderung der Strafprozeßordnung. Der Bundesminister der Justiz legt bislang erst ein „Problempapier zu den rechtlichen Grundlagen für Fahndungsmaßnahmen, Fahndungshilfsmittel und die Akteneinsicht" vor, in denen er unter anderem Formulierungsvorschläge für die künftige Regelung der Rasterfahndung, der polizeilichen Beobachtung und der Einsicht in Strafakten unterbreitet. Sie entsprechen meinen Vorstellungen weit eher als die anderen Entwürfe, so daß ich eine insgesamt positive Stellungnahme genüber dem hiesigen Justizministerium abgeben konnte. Ich wies darin aber zugleich darauf hin, daß es mit den vorgesehenen Regelungen nicht sein Bewenden haben kann. Es bedarf vielmehr weiterer Vorschriften über das Erheben, Speichern, Weitergeben und sonstige Nutzung von in Dateien und Akten erfaßten Daten. Das hängt vor allem damit zusammen, daß die polizeiliche Datenverarbeitung nicht nur der Gefahrenabwehr, sondern in erheblichem Umfang auch der Strafverfolgung dient. Notwendig ist daher, weitgehend parallele Regelungen in das Polizeigesetz und die Strafprozeßordnung aufzunehmen. Erfreulich ist, daß mir das Justizministerium seine gegenüber dem Bundesminister der Justiz abgegebene Äußerung übersandte. Auch wenn ich seine Auffassung in einer Reihe von Punkten nicht teile, kenne ich jetzt doch wenigstens seine Haltung, so daß ich zu gegebener Zeit in eine Sachdiskussion mit ihm eintreten kann.

2. Polizeigesetz

Um nur einen annähernden Eindruck zu vermitteln, welch schwierige Entscheidung bei der Regelung über die polizeiliche Datenverarbeitung bevorsteht, greife ich einige Probleme des Entwurfs eines Polizeigesetzes heraus:

2.1 Gefahrenvorsorge

Nach dem Entwurf soll die Polizei Daten über einen Bürger nicht nur — wie es das geltende Recht zuläßt — zur Abwehr einer konkreten Gefahr, sondern schon dann erheben, speichern und nutzen dürfen, „soweit dies die Vorsorge zur Gefahrenabwehr erfordert". Begründet wird dies damit, daß die Polizei eine konkrete Gefahr oftmals nur abwehren könne, wenn sie bereits vor Eintritt der Gefahr Daten vorrätig habe; als Beispiele werden genannt: Daten über Abschleppunternehmer, Sachverständige und Dolmetscher. Gewiß hat niemand etwas dagegen, daß die Polizei deren Daten vorhält; es liegt vielleicht sogar in ihrem Geschäftsinteresse. Problematisch ist etwas ganz anderes: auf diese Be-

stimmung könnte die Polizei auch die Erhebung und Speicherung von Daten anderer Personen stützen. Sie könnte beispielsweise auf den Gedanken kommen, alle ihr bekannten Demonstranten — unabhängig davon, ob sie schon einmal eine Demonstrationsstraftat begangen haben oder es Anhaltspunkte dafür gibt, daß sie dies tun werden — aus Vorsorge zur Gefahrenabwehr erfassen. Sie könnte auch auf Grund dieser Vorschrift ganze Risikogruppen, z. B. Homosexuelle, registrieren mit der Begründung, diese würden erfahrungsgemäß häufig Straftaten begehen. Ich kann nur davor warnen, im Polizeibereich durch die Einführung eines neuen, nicht näher definierten Begriffs der „Vorsorge zur Gefahrenabwehr" die Grenze für das Erheben und Speichern von Daten über Bürger durch die Polizei sehr weit vorzuverlagern und von dem Erfordernis einer konkreten Gefahr ganz generell abzugehen.

2.2 Vorbeugende Bekämpfung von Straftaten

Der Entwurf läßt die Erhebung von Daten über einen Bürger auch generell zur vorbeugenden Bekämpfung von Straftaten zu. Diese unterscheidet sich von der konkreten Gefahrenabwehr dadurch, daß sie in deren Vorfeld stattfindet: Es gibt tatsächliche Anhaltspunkte dafür, daß jemand eine Straftat begeht, jedoch kann mit ihr in überschaubarer Zukunft nicht hinreichend wahrscheinlich gerechnet werden. Wie bei der Vorsorge zur Gefahrenabwehr wird auch hier die Datenerhebung sehr weit ins Vorfeld vorverlagert. Das halte ich nur bei Straftaten von erheblichem Gewicht für gerechtfertigt, beispielsweise bei Mord, Totschlag, bestimmten Staatsschutzdelikten oder Raub. Zu weit geht mir — wie es der Entwurf tut —, die Erhebung von Daten auch zur vorbeugenden Bekämpfung eines Bagatelldiebstahls oder des Erschleichens von Beförderungsleistungen zuzulassen.

2.3 Nichtstörer und „andere Personen"

Daß die Polizei Daten über Personen erheben und speichern darf, von denen eine konkrete Gefahr für die öffentliche Sicherheit ausgeht — anders gesagt: bei denen wahrscheinlich ist, daß sie in überschaubarer Zukunft eine Straftat begehen (sog. Störer) —, ist jedermann verständlich. Problematisch wird es jedoch, wenn man — wie der Entwurf — der Polizei gestatten will, auch Daten von Nichtstörern zu erheben und zu speichern, also von „unverdächtigen", harmlosen Bürgern, die mehr oder weniger zufällig in Zusammenhang mit einer „verdächtigen" Person geraten, weil sie beispielsweise diese Person kennen oder weil ihr Name im Notizbuch des „Verdächtigen" aufgeführt ist oder weil sie das Pech haben, einem „Verdächtigen" in der Bahn gegenüberzusitzen. So etwas kann jedem von uns passieren, ohne daß er sich deswegen etwas vorzuwerfen hätte. Nun geht der Datenschutz nicht so weit zu fordern, Daten solcher Bürger dürfte die Polizei schlechterdings nicht erheben und speichern. Schon bisher lassen die Polizeigesetze zu, daß die Polizei auch Maßnahmen gegen Nichtstörer treffen kann, wenn es eine gegenwärtige erhebliche Gefahr abzuwehren gilt, wenn also beispielsweise das Leben eines anderen Menschen unmittelbar gefährdet ist. Der vorliegende Entwurf geht jedoch um einiges weiter:

— Er läßt die Erhebung von Daten nicht nur zur Abwehr einer gegenwärtigen erheblichen Gefahr, sondern schon

zur Abwehr einer „ganz normalen Gefahr" und generell zur vorbeugenden Bekämpfung von Straftaten zu.

— Er erlaubt in diesen Fällen die Erhebung von Daten über „andere Personen", wobei völlig unklar ist, wer „andere Personen" sind und worin sie sich von Nichtstörern unterscheiden.

— Er erlaubt die Speicherung von Daten dieser Personen in Dateien, soweit dies zur Abwehr der Gefahr erforderlich ist.

— Er ermöglicht die Speicherung von Daten über Personen, bei denen keine Anhaltspunkte dafür bestehen, daß sie Straftaten begehen, wenn dies zur Verhütung oder zu künftigen Aufklärungen bestimmter im Gesetz aufgeführter Straftatbestände erforderlich ist. Die Speicherung darf bis zu drei Jahren dauern. Eine Unterrichtung der Betroffenen über die Speicherung, von der sie ja regelmäßig nichts wissen, ist nicht vorgesehen.

Diese Regelungen verwischen die bisher im Polizeigesetz immer klar gezogene Grenze zwischen Störern und Nichtstörern. Letztere verdienen einen anderen Umgang mit ihren Daten.

2.4 Öffentliche Veranstaltungen und Versammlungen

Nach dem Entwurf soll die Polizei bei öffentlichen Versammlungen und Veranstaltungen Daten über Bürger erheben dürfen — und zwar auch durch Video- und Tonaufnahmen, wenn „tatsächliche Anhaltspunkte die Annahme rechtfertigen, daß Gefahren für die öffentliche Sicherheit oder Ordnung entstehen." Diese Formulierung wird den Anforderungen des Volkszählungsurteils und des Brokdorf-Beschlusses des Bundesverfassungsgerichts nicht gerecht. Beide machen nämlich deutlich, daß der Staat bei der Beobachtung und Registrierung von Demonstranten äußerst zurückhaltend verfahren muß, um den Grundrechten des Bürgers auf informationelle Selbstbestimmung und auf Versammlungsfreiheit gerecht zu werden. Daraus folgt:

— Der Gesetzgeber muß — was der Entwurf nicht tut — bei der Datenerhebung zwischen der (zufälligen) Ansammlung von Menschen und einer unter den Schutz des Art. 8 des Grundgesetzes fallenden Versammlung unterscheiden. In oder im Zusammenhang mit einer Versammlung darf die Polizei Daten nur in engen Grenzen erheben — etwa, wenn im Einzelfall konkrete Anhaltspunkte dafür bestehen, daß bei der Versammlung eine Straftat begangen wird.

  Noch strengere Regeln müssen für Videoaufnahmen und Tonaufzeichnungen durch die Polizei gelten, weil sie die Rechtssphäre des Bürgers stärker tangieren. Sie sollten nur zur Abwehr einer gegenwärtigen erheblichen Gefahr und allenfalls noch zur vorbeugenden Bekämpfung einer erheblichen Straftat zulässig sein.

2.5 Speicherung von Daten aus Ermittlungsverfahren für Zwecke der vorbeugenden Bekämpfung von Straftaten in Dateien

Hinter dieser — dem Laien sicher kaum verständlichen — Überschrift verbirgt sich folgendes: Ermittelt die Polizei ge-

gen einen Bürger wegen einer Straftat, legt sie eine Ermittlungsakte an. Außerdem erfaßt sie seine Daten in der Personenauskunftsdatei, dem polizeilichen Informationssystem von Baden-Württemberg. Ferner legt sie eine Kriminalakte an. Ist das Verfahren bei der Justiz abgeschlossen, benötigt die Polizei die Daten nicht mehr für Zwecke der Strafverfolgung. Der Entwurf sieht nun vor, daß die Polizei all diese Daten zur vorbeugenden Bekämpfung von Straftaten — also für einen andern Zweck — in Dateien speichern darf. Problematisch an dieser Vorschrift, die die derzeitige Praxis der Polizei festschreibt, ist, daß dies völlig unabhängig von der Schwere einer Straftat geschehen darf: auch wenn einem Bürger nur eine fahrlässige Körperverletzung oder eine Beleidigung zum Vorwurf gemacht wurde, darf die Polizei seine Daten nach Abschluß des Ermittlungs- oder Strafverfahrens weiterspeichern — und zwar in beliebigen, auch landesweiten polizeilichen Informationssystemen. Unerheblich ist, ob der Bürger schon einmal etwas mit der Polizei zu tun hatte, wie lange er straffrei lebt (Vorleben), ob die Gefahr besteht, daß er erneut mit dem Gesetz in Konflikt kommt (Wiederholungsgefahr), ob die Datenspeicherung überhaupt geeignet ist, etwaige künftige polizeiliche Ermittlungen gegen ihn zu fördern.

Dies ließe sich vielleicht noch verstehen, wenn der Bürger wegen dieser Tat verurteilt wurde. Das ist jedoch nicht Voraussetzung: Auch wenn ihn das Gericht aus Mangel an Beweisen freisprach, die Staatsanwaltschaft das Ermittlungsverfahren aus demselben Grund oder wegen Geringfügigkeit oder gegen Zahlung einer Geldbuße einstellte, muß er befürchten, daß die Polizei seine Daten auf Jahre hinaus speichert und ihm bei einem erneuten Zusammentreffen vorhält. Eine solche Datenspeicherung aber wird vor allem da zum reinen Selbstzweck, wenn der Tatvorwurf geringfügig ist, der Bürger deswegen nicht verurteilt wurde und bei ihm keine Wiederholungsgefahr besteht. Um dies zu vermeiden, muß der Gesetzgeber die Speicherung von in Strafermittlungsverfahren gewonnenen Daten für Zwecke der vorbeugenden Bekämpfung von Straftaten auf solche Fälle beschränken, in denen nach Art und Ausführung der Tat und nach der Persönlichkeit des Bürgers die Gefahr der Begehung weiterer Straftaten von erheblichem Gewicht besteht.

2.6 Weitergabe von Daten aus Unterlagen der Polizei

Der Entwurf läßt die Weitergabe von Daten aus Unterlagen der Polizei sogar an Private in sehr weitem Umfang zu. Das halte ich nicht für richtig: Der Inhalt von Dateien und Akten der Polizei ist — wie es in den KpS-Richtlinien von 1981 zu Recht heißt — „vertraulich und grundsätzlich nur für den Dienstgebrauch innerhalb der Polizeien des Bundes und der Länder bestimmt", weil es sich um äußerst sensitive und häufig auch um „weiche" Daten handelt — sprich: Verdachtsmomente und Vorgänge, deretwegen der Betroffene nicht verurteilt wurde. Behörden müssen sich deshalb im Grundsatz mit dem zufrieden geben, was sie aus dem Bundeszentralregister oder anderen Registern — z. B. dem Verkehrszentral- und dem Gewerbezentralregister — erfahren können, und Private mit dem, was sie beispielsweise aus einem polizeilichen Führungszeugnis ersehen können. Daß sie auf diesem Weg nur die „halbe Wahrheit" über einen Bürger erfahren, darf nicht dazu führen, die durch das Bundes-

zentralregistergesetz errichteten Schranken auf dem Umweg über Auskünfte der Polizei zu unterlaufen. Der Gesetzgeber sollte deshalb Auskünfte der Polizei an andere als Polizeidienststellen und -behörden nur zur Abwehr einer konkreten Gefahr, zur Abwendung einer erheblichen sozialen Notlage und zur Verfolgung öffentlich-rechtlicher oder zivilrechtlicher Ansprüche zulassen.

Zu diesen Restriktionen muß jedoch noch ein zweites hinzukommen: Es kann nicht, wie es der Entwurf vorsieht, genügen, daß die Stelle, die Auskunft aus Unterlagen der Polizei begehrt, allein über das Vorliegen der Voraussetzungen für eine Auskunft entscheidet. Wegen der Sensitivität der Daten und der möglichen Folgen einer Weitergabe für den Betroffenen muß dies auch die Polizei tun.

2.7 Löschen von Daten in Dateien

Nach dem Entwurf sind in Dateien gespeicherte Daten zu löschen, wenn „bei der in bestimmten Zeitabständen vorzunehmenden Überprüfung (Regelüberprüfung) oder aus Anlaß einer Einzelfallbearbeitung" festgestellt wird, daß ihre Kenntnis für die Polizei nicht mehr erforderlich ist. Nach welchen Zeitabständen eine Regelüberprüfung stattfinden soll, soll die Polizei für jede Datei durch Verwaltungsvorschrift festlegen. Dieser Weg ist verfassungsrechtlich bedenklich, weil er eine der wichtigsten Fragen der Entscheidung des Parlaments entzieht und dem Gebot, die Dateiverarbeitung bei der Polizei für den Bürger so gut es irgend geht transparent zu machen, nicht gerecht wird. Ebenso wie im Bundeszentralregistergesetz muß es auch im Polizeigesetz Regelfristen für die Löschung bzw. Überprüfung gespeicherter Daten geben. Sie sollten auf keinen Fall länger als die in den KpS-Richtlinien festgelegten Fristen — 2 Jahre für Kinder, 3 Jahre bei Bagatelldelikten, 5 Jahre bei Jugendlichen, 10 Jahre bei Erwachsenen — sein. Dazu ist im Hinblick auf eine Entscheidung des hessischen Verwaltungsgerichtshofs aus dem Jahre 1982 zu prüfen, ob für Erwachsene nicht eine kürzere Regelspeicherfrist festgelegt werden muß. Für den Gesetzgeber stellt sich weiterhin die Frage, ob in den Fällen, in denen der Bürger nicht verurteilt wurde, die Speicherungsfrist herabzusetzen ist. In jedem Falle empfiehlt sich, die gesetzliche Regelung so zu formulieren, daß die Polizei bei der Bemessung der Frist nach unten und — unter bestimmten Voraussetzungen — ausnahmsweise auch nach oben abweichen kann, um den Besonderheiten des Einzelfalls Rechnung zu tragen.

Außer der Regellöschung ist auch die Einzelfallöschung — also die Löschung vor Ablauf der Regelfrist, etwa aufgrund einer Entscheidung der Justiz — im Gesetz selbst so präzise wie möglich zu regeln. Die Formulierung des Entwurfs, die Daten seien zu löschen, wenn die Polizei aus Anlaß einer Einzelfallbearbeitung feststellt, daß sie diese nicht mehr braucht, löst das Problem nicht. Vielmehr muß der Gesetzgeber die dafür maßgeblichen Kriterien festlegen. Er muß darüber befinden, ob es für die Löschung von Daten darauf ankommen soll, ob jemand wegen „erwiesener Unschuld" oder nur „in dubio pro reo" freigesprochen wurde. Soll diese im Strafverfahren abgeschaffte Differenzierung hier weitergehen, muß das Gesetz dies ausdrücklich vorsehen.

Unbefriedigend an der Regelung im Entwurf ist schließlich, daß sie nur für die Löschung von Daten in Dateien und nicht für die Aktenaussonderung gilt. Das würde bedeuten, daß die Polizei bei einem Freispruch wegen erwiesener Unschuld von Gesetzes wegen zwar die Daten in der Personenauskunftsdatei löschen, nicht jedoch die über das Verfahren angelegten Ermittlungs- und Kriminalakten vernichten muß. Eine solche Verfahrensweise würde den schutzwürdigen Belangen des Betroffenen nicht gerecht. Sein Persönlichkeitsrecht wird nämlich nicht nur durch die Speicherung von Daten in Dateien, sondern auch durch das Vorhandensein von Akten bei der Polizei tangiert. Auswirken würde sich die Beschränkung auf Dateien vor allem im Staatsschutzbereich, wo die Polizei in sehr starkem Maße nur mit Akten und „internen" Dateien arbeitet. Die Forderung muß daher lauten: Einbeziehung aller Akten und sonstigen Datenträger in die Regelung über die Löschung. Dabei kann man die Besonderheiten der Speicherung von Daten in Akten selbstverständlich angemessen berücksichtigen.

2.8 Auskunft

Eines der wichtigsten Datenschutzrechte des Bürgers ist sein Auskunftsrecht gegen jede Behörde, die möglicherweise Daten über ihn speichert. Es soll dem Bürger die Orientierung ermöglichen, welche Stellen welche Informationen über ihn speichern und verarbeiten. Im Sicherheitsbereich ist dies besonders wichtig, da sich die Datenverarbeitung der Polizei meist ohne Wissen und Mitwirkung des Bürgers vollzieht, so daß sie für ihn weniger transparent, zugleich aber von den möglichen Folgen her gefährlicher ist als in vielen anderen Bereichen. Dennoch hat der Bürger nach geltendem Recht keinen Auskunftsanspruch gegen die Polizei, sondern nur einen Anspruch auf fehlerfreie Ermessensausübung bei der Entscheidung über seinen Auskunftsanspruch. Daran hält bedauerlicherweise der Entwurf im Grundsatz fest. Unbefriedigend ist auch, daß er Auskunft aus Akten nicht einbezieht. Ich meine: jeder Bürger muß grundsätzlich auch gegenüber der Polizei einen Auskunftsanspruch haben, der sich auf Dateien und Akten bezieht, wobei man die Besonderheit, daß in Akten Erfaßtes manchmal schwer aufzufinden ist, angemessen berücksichtigen kann. Darüber hinaus muß der Bürger grundsätzlich auch erfahren können, für welchen Zweck die Polizei Daten speichert — z. B. zur Abwehr einer konkreten Gefahr, zur vorbeugenden Bekämpfung von Straftaten —, auf welche Rechtsgrundlage und für wie lange dies voraussichtlich geschieht, woher die Polizei die Daten hat und an wen sie sie weitergibt.

2.9 Zusätzlicher Regelungsbedarf

Kritik verdient der Entwurf jedoch nicht nur, weil er vieles unbefriedigend regelt, sondern auch, weil er manche verbesserungsbedürftigen Vorschriften — z. B. über die Identitätsfeststellung und die erkennungsdienstliche Behandlung — und manche regelungsbedürftigen Fragen überhaupt nicht aufgreift. Zu letzterem nur zwei Beispiele:

— Kriminalakten

Der Entwurf enthält keine Regelungen über das Anlegen und Führen von Kriminalakten. Offensichtlich

glaubten die Verfasser, hierfür bedürfe es keiner besonderen Rechtsvorschrift. Diese Auffassung läßt sich jedoch spätestens seit der Entscheidung des bayer. Verfassungsgerichtshofs vom 9. Juli 1985 nicht mehr vertreten. Darin heißt es wörtlich:

> „Aus den Verwaltungsvorschriften, die für die Kriminalaktensammlungen gelten (gemeint sind die KpS-Richtlinien), ergibt sich hier doch, daß es hier nicht um die schlichte Aufbewahrung von Aktengut geht. Diese Aktensammlungen haben eine sonst für Behördenakten im allgemeinen nicht bestehende besondere, das Persönlichkeitsrecht der Bürger berührende Bedeutung. Das ergibt sich aus dem Zweck dieser Sammlungen, aus dem großen Kreis der Stellen, die vom Akteninhalt Kenntnis erhalten können (das sind beispielsweise alle Polizeidienststellen, die Verfassungsschutz-, die Gewerbe- und die Waffenbehörden), aus den hierzu in Form von Dateien geführten Kriminalaktennachweisen, aus dem begrenzten Auskunftsrecht der Betroffenen und aus der Dauer der Aktenaufbewahrung. Gesammelte Kriminalakten können ein umfangreiches, sich über einen langen Zeitraum erstreckendes Persönlichkeitsbild vermitteln. Derjenige, über den die Akten geführt werden, hat nur im Falle seiner Anhörung die Möglichkeit, auf den Inhalt der Akten Einfluß zu nehmen. Insbesondere die Weitergabe von Auskünften aus der Aktensammlung an andere Stellen kann das Persönlichkeitsrecht des Betroffenen berühren ...
>
> All diese Umstände sprechen dafür, die Personen, über die Kriminalakten nach Maßgabe der genannten Richtlinien geführt werden, in ihrem allgemeinen, grundrechtlich gesicherten Persönlichkeitsrecht als schutzbedürftig anzuerkennen. Es erscheint deshalb ... geboten, daß der Gesetzgeber die Materie regelt, die bisher Gegenstand der KpS-Richtlinien ist."

Regelungsbedürftig ist vorrangig, unter welchen Voraussetzungen die Polizei Kriminalakten über jemand anlegen darf. Soweit dies wegen eines Ermittlungsverfahrens geschieht, muß dasselbe gelten wie bei der Speicherung von Strafverfolgungsdaten für Zwecke der vorbeugenden Bekämpfung von Straftaten in Dateien: Es muß nach Art und Ausführung der Tat und nach der Persönlichkeit des Bürgers die Gefahr bestehen, daß er weitere erhebliche Straftaten begeht. Kriminalakten oder Akten, die man als solche bezeichnen kann, legt die Polizei darüber hinaus jedoch auch an, wenn ein Bürger einen Selbsttötungsversuch unternimmt oder eine Polizeidienststelle von einer anderen Polizeidienststelle eine Erkenntnisanfrage — „Was ist dort über Herrn X bekannt?" — erhält. Deshalb muß der Gesetzgeber auch entscheiden, ob und gegebenenfalls mit welcher Maßgabe und vor allem wie lange die Polizei in derartigen Fällen Kriminalakten führen darf.

— Automatisierte Datenverarbeitung

Ein Hautpmangel des Entwurfs ist schließlich, daß er keine ausreichenden Vorschriften über die automatisierte Datenverarbeitung vorsieht. Sie sind erforderlich, weil die automatisierte Datenverarbeitung — insbesondere die Speicherung von Daten in einem landesweiten Informationssystem wie der Personenauskunftsdatei, auf das rund 23 000 Polizeibeamte jederzeit zugreifen können — eine besondere Gefahr für die Betroffenen darstellt, der nach dem Volkszählungsurteil auch durch besondere Sicherungen begegnet werden muß. Zwei Punkte möchte ich herausgreifen: Zum einen darf die Polizei in der Personenauskunftsdatei nicht, wie dies derzeit der Fall ist, jeden

Ermittlungsvorgang speichern. Daß Herr X eine fahrlässige Körperverletzung beging oder daß Herr Y einen anderen beleidigte, indem er ihm den Vogel zeigte, hat in einem landesweiten Informationssystem nichts zu suchen; es gehört allenfalls in eine örtliche/regionale Datei; so verfährt beispielsweise Bayern. Zum anderen wirft besondere Probleme auf, daß in ein und derselben Datei mitunter Daten für unterschiedliche Zwecke und sehr unterschiedliche Personengruppen erfaßt sind. Zwei Beispiele zur Verdeutlichung: 1981 stellte ich fest, daß in der Personenauskunftsdatei außer den Daten mehrerer hunderttausend Personen, gegen die die Polizei wegen einer Straftat ermittelt hatte, auch die Daten mehrerer 100 Prostituierter gespeichert waren, die bislang keine Straftat begangen hatten und auch keiner solchen verdächtig waren. Ähnlich läge die Problematik, wenn die Polizei im Staatsschutzbereich eine Datei errichtete, in der mutmaßliche Terroristen ebenso gespeichert wären wie etwa Blockierer in Mutlangen oder Heilbronn. Für die Zukunft sollte eine eindeutige Rechtsvorschrift solche Zusammenspeicherungen ausschließen. Dateien der Polizei dürfen — anders als in der Vergangenheit, die durch einen gewissen Wildwuchs gekennzeichnet war —, keine beliebige Struktur mehr aufweisen, sondern müssen sich an einheitlichen Prinzipien orientieren. Der Gesetzgeber muß hierfür die nötigen Vorgaben machen.

Vor allem wegen dieser Gründe meine ich, daß die Polizei ihren Entwurf von Grund auf überarbeiten muß. Dabei ist Eile geboten, um so bald wie möglich im Interesse von Polizei und Bürgern ein verfassungsgemäßes Polizeirecht zu erhalten.

3. Verfassungsschutzgesetz

Der Entwurf, zu dem ich gegenüber dem Innenministerium Stellung nahm, datiert vom 14. März 1985. Aus der Presse erfuhr ich, daß ihn die Bonner Koalitionsfraktionen inzwischen veränderten. Seinen aktuellen Stand kenne ich nicht. Den ursprünglichen Entwurf kritisierte ich vornehmlich deshalb, weil er

- die Aufgaben der Verfassungsschutzbehörden nicht präzise genug beschrieb und es folglich auch an präzisen Befugnisnormen fehlte,
- die Durchführung von Sicherheitsüberprüfungen völlig unzureichend regelte,
- dem Verfassungsschutz eine Blankoermächtigung zur Anlegung von Dateien erteilte,
- die Erhebung von Daten nicht auf „verdächtige" Personen begrenzte,
- die Speicherungsvorschrift zu weit faßte, insbesondere keine Eingrenzung für die Speicherung von Daten im Rahmen von Sicherheitsüberprüfungen enthielt,
- die Speicherung von Daten Minderjähriger nicht einschränkte,
- keine ausreichenden Vorschriften für die Datenverarbeitung in Akten traf,
- anderen als Sicherheitsbehörden in zu weitem Umfang erlaubte, Daten an den Verfassungsschutz zu übermitteln bzw. vom Verfassungsschutz Daten zu erhalten,

— in seinen Regelungen über die Weitergabe von Daten Verwertungsverbote, das Trennungsgebot Polizei/Verfassungsschutz und den Grundsatz der Zweckbindung nicht berücksichtigte,

— keine Fristen für die Überprüfung und Löschung von Daten vorsah und

— keine Regelung über die Erteilung von Auskünften durch den Verfassungsschutz enthielt.

Den aktuellen Stand des Entwurfs eines Verfassungsschutzgesetzes kenne ich nicht. Ich muß mich deshalb beschränken zu sagen, welche Anforderungen an ein Verfassungsschutzgesetz unbedingt zu stellen sind:

— Die Aufgaben des Verfassungsschutzes sind präzise zu regeln, weil sich daran Folgerungen mit Eingriffscharakter knüpfen. So gilt es beispielsweise zu verdeutlichen, was eine „Bestrebung" ist, die gegen „die freiheitliche demokratische Grundordnung, den Bestand oder die Sicherheit des Bundes oder eines Landes gerichtet ist".

— Die nachrichtendienstlichen Mittel, die der Verfassungsschutz einsetzen darf, muß das Gesetz selbst soweit wie möglich nennen.

— Es geht nicht an, den Verfassungsschutz — wie offenbar beabsichtigt — pauschal zu ermächtigen, daß er generell von öffentlichen Stellen Daten anfordern kann und alle amtlichen Register einsehen darf. Die Notwendigkeit für eine so weitgehende Regelung ist bislang nicht dargetan. Anhand der bisherigen Erfahrungen ist vielmehr sehr genau zu prüfen, ob die bestehenden Datenschutzvorschriften — etwa im Meldegesetz — dem Verfassungsschutz tatsächlich zu enge Fesseln anlegen. Nur wenn sich dies feststellen ließe, könnte man daran denken, die Befugnisse des Verfassungsschutzes behutsam zu erweitern. Keinesfalls bedarf es eines Einsichtsrechts des Verfassungsschutzes in alle, sondern allenfalls in bestimmte Register.

— Die Strafverfolgungsbehörden dürfen im Rahmen der Telefonüberwachung oder bei der Durchsuchung einer Wohnung erlangte Erkenntnisse über einen Bürger nur eingeschränkt an den Verfassungsschutz weitergeben.

— Der Verfassungsschutz darf im Rahmen der Extremistenbeobachtung die Daten eines Bürgers — was der ursprüngliche Entwurf nicht vorsah — nur personenbezogen auswertbar speichern, wenn ein Bezug dieses Bürgers zum Extremismus feststellbar ist. Hinzukommen muß, daß die Speicherung zur Beobachtung extremistischer Bestrebungen erforderlich ist. Es gilt, damit der gegenwärtigen Praxis, immer mehr von der Beobachtung von Organisationen zur Erfassung von Einzelpersonen überzugehen, entgegenzuwirken.

— Der Schutz Minderjähriger vor Datenspeicherungen in Dateien des Verfassungsschutzes ist über den mir bekannten Entwurf hinaus auszubauen: Unter 16jährige sollten überhaupt nicht, andere Minderjährige nur ausnahmsweise erfaßt werden. Nach kurzer Zeit ist zu prüfen, ob ihre Daten zu löschen sind.

— Nicht angehen kann, dem Verfassungsschutz einen Freibrief für die Einrichtung und den Ausbau von Dateien auszustellen. Es gilt vielmehr, einschränkende Kriterien festzulegen

sowie organisatorische und verfahrensrechtliche Vorkehrungen vorzusehen, die der Gefahr einer Verletzung der Persönlichkeitsrechte des Bürgers entgegenwirken.

— Verfassungsschutz und Polizei müssen kraft Verfassungsrechts getrent sein. Daraus folgt beispielsweise, daß es keine Online-Verbindungen zwischen ihnen geben darf. Ein entsprechendes Verbot ist in das Gesetz aufzunehmen.

— Außer einer abschließenden Aufzählung aller Verfahren, an denen der Verfassungsschutz im Rahmen von Sicherheitsüberprüfungen mitzuwirken hat, ist notwendig, auch die Durchführung der Überprüfung näher zu regeln. Dazu gehören unter anderem Regelungen über die Intensität der Prüfung, die sich an der Gefährdung im Einzelfall zu orientieren hat.

— Neu geregelt werden muß die Auskunft des Verfassungsschutzes an Bürger wegen ihrer gespeicherten Daten. Dabei gilt sicherzustellen, daß der Verfassungsschutz Auskunftsverlangen nicht — wie es derzeit noch weitestgehend Praxis des Landesamts für Verfassungsschutz Baden-Württemberg ist — schematisch ablehnt. Er sollte beispielsweise eine Auskunft erteilen, wenn die Speicherung von Daten über einen Bürger nur auf einer Sicherheitsüberprüfung beruht; im übrigen sollte eine Abwägung im Einzelfall stattfinden. Im Falle einer Auskunftsverweigerung sollte er in seinen Unterlagen die Gründe hierfür schriftlich festhalten müssen. Den Auskunftssuchenden sollte man auf die Möglichkeit hinweisen, sich an den Datenschutzbeauftragten zu wenden. Die Bearbeitung von Auskunftsersuchen muß getrennt von anderen Informationssammlungen erfolgen. Gesetzlich ausgeschlossen werden muß, daß ein Auskunftsantrag zum Nachteil eines Bürgers verwertet wird. Ferner ist zu bestimmen, daß Unterlagen über Auskunftsanträge nach kurzer Frist zu vernichten sind.

— Unerläßlich ist es, im Gesetz angemessene Regelspeicherfristen für die Löschung von Daten in Dateien und darüber hinaus auch in Akten vorzusehen. Bei der Speicherungsdauer ist zwischen den verschiedenen Aufgaben des Verfassungsschutzes zu differenzieren.

Das sind nur einige wichtige Aspekte. Abzuwarten bleibt, ob sich der von den Bonner Koalitionsfraktionen ausgehandelte Gesetzentwurf an diesen Maßstäben messen lassen kann.

5. Teil: Hochschulen und Forschung

Hochschulen und ihre Forschungseinrichtungen fristen kein Eigenleben. Vielmehr kommt der Bürger mit ihnen auf vielfältige Weise in Kontakt: als Patient, als Student, als Mitarbeiter und manchmal ist er auch, ohne daß er es weiß, Gegenstand ihrer Forschung. Dabei stellen sich immer wieder eine ganze Reihe teilweise schwieriger Datenschutzfragen.

1. Forschungsvorhaben

Auch wenn es der Forschung letztendlich gar nicht um den einzelnen geht, kommt sie doch häufig nicht ohne Personendaten aus. Um Ergebnisse erzielen zu können, muß sie nämlich viel-

fach Bürger auswählen, befragen, untersuchen und bei Dritten Informationen über sie einholen. Dabei lassen die Forscher leider immer wieder außer Betracht, daß die Forschung keinen absoluten Vorrang, sondern jeder Bürger grundsätzlich das Recht hat, selbst über die Verwendung seiner Daten zu bestimmen. Welche Probleme es im einzelnen gibt, sollen einige ausgewählte Forschungsvorhaben beleuchten:

1.1 „Öffentlichkeitsbeteiligung bei der Genehmigung von umweltrelevanten Großvorhaben"

Mitunter begegnen mir nach Jahren in völlig anderem Zusammenhang Dateien und Karteien wieder, mit denen ich mich schon einmal zu befassen hatte. So ging es mir jüngst mit der Datensammlung der ca. 28 000 Einwender gegen den Bau des Kernkraftwerks Neckarwestheim — Block II. Während es einst einiges an dem Umgang des Wirtschaftsministeriums mit diesen Einwenderdaten auszusetzen gab, wollte nun das Kernforschungszentrum Karlsruhe GmbH mein Plazet, daß es aus der Einwendersammlung des Wirtschaftsministeriums nach dem Zufallsprinzip eine bestimmte Anzahl von Namen und Adressen von Einwendern auswählen darf, um diese zu befragen. Ohne eine solche Befragung sei sein Forschungsvorhaben „Öffentlichkeitsbeteiligung bei Genehmigung von umweltrelevanten Großvorhaben" nicht sinnvoll, das es zusammen mit dem Forschungsinstitut für öffentliche Verwaltung in Speyer und unter methodischer Betreuung des Zentrums für Umfragen, Methoden und Analysen e. V. in Mannheim durchführen wolle. Ich mußte die Forscher enttäuschen. § 11 LDSG läßt ein solches Verfahren nicht zu. Das Wirtschaftsministerium dürfte die Adreßdaten der Einwender ohne deren Wissen dem Kernforschungszentrum nur überlassen, wenn es sicher sein könnte, damit „schutzwürdige Belange" der Einwender nicht zu beeinträchtigen. Das anzunehmen, erschiene verwegen. Denn gerade unter den Einwendern in atomrechtlichen Genehmigungsverfahren dürften sich viele Bürger befinden, die eine Zusammenarbeit mit dem Kernforschungszentrum Karlsruhe wegen ihrer persönlichen Einstellung zur Errichtung von Kernkraftwerken prinzipiell ablehnen. Zudem könnten sich unter den Einwendern auch Arbeitnehmer des Kernforschungszentrums Karlsruhe befinden, die im Falle einer Nennung ihres Namens berufliche Nachteile befürchten.

Zwar vereinbar mit dem Datenschutz, aber keineswegs empfehlenswert wäre ein anderes Verfahren: Das Wirtschaftsministerium könnte selbst ein von der Forschungsgruppe verfaßtes Schreiben an die Einwender versenden. Dabei müßte unmißverständlich zum Ausdruck kommen, warum es dies tut. Zugleich müßte man den Einwendern ausdrücklich sagen, daß es ihnen überlassen bleibt, ob sie mit der Forschungsgruppe in Kontakt treten und an der Befragung teilnehmen wollen oder nicht. Da bei einer solchen Verfahrensweise das Kernforschungszentrum Karlsruhe keine Einwenderadressen erhielte, wäre eine Beeinträchtigung deren schutzwürdiger Interessen nicht zu befürchten. Gegen diesen Weg spricht freilich ein anderer Grund, der mit dem Datenschutz direkt nichts zu tun hat: zumindest ein Teil der

Einwender dürfte wegen ihrer prinzipiellen Ablehnung von Kernkraftwerken auch für eine solche Aktion des Wirtschaftsministeriums wenig Verständnis haben.

1.2 Wählerverhalten im Bundestagswahlkreis Tübingen

Das Institut für Politikwissenschaft der Universität Tübingen wollte im Rahmen einer Untersuchung über die Bundestagswahl 1983 im Wahlkreis Tübingen einen repräsentativen Querschnitt der Bevölkerung befragen. Es bat deshalb die Gemeinden, ihm aus ihren für die Bundestagswahl angelegten Wählerverzeichnissen Namen und Adressen zufällig ausgewählter Wahlberechtigter mitzuteilen. Übersehen hatte es dabei, daß eine solche Auskunft nicht zulässig ist. Die Bundeswahlordnung läßt wie die übrigen Wahlordnungen Auskünfte aus dem Wählerverzeichnis nur zu, wenn amtliche Stellen in Zusammenhang mit der Wahl darauf angewiesen sind. Das war hier nicht der Fall. Gleichwohl mußte das Forschungsprojekt deshalb nicht scheitern. Ich sagte den Gemeinden, sie könnten statt dessen dem Institut nach dem Zufallsprinzip ausgewählte Adreßdaten der über 18jährigen Bürger — das sind weitestgehend, aber nicht durchweg die Wahlberechtigten — aus dem Melderegister übermitteln. Zuvor mußte ihnen das Forschungsinstitut allerdings versichern, daß es die so ausgewählten Bürger eingehend über die Herkunft der Adreßdaten aus dem Melderegister und die Ziele des Forschungsvorhaben aufklärt und dabei vor allem deutlich macht, was mit den Angaben geschieht, daß die Teilnahme der Bürger an der Befragung völlig freiwillig ist und ihre Entscheidung, nicht teilzunehmen, keine Nachteile mit sich bringt. Trotz dieser Belehrung machte das Institut für Politikwissenschaft nicht alles ganz richtig. In seinem Anschreiben an die Bürger fand sich die mißverständliche Formulierung, wie ich sie bei ähnlichen Projekten immer wieder feststelle: „Die Fragebögen werden sofort nach der Erhebung anonym verarbeitet." Wer so schreibt, übersieht, daß man einen Befragten trotz Weglassen von Namen und Adreßdaten in der Regel noch sehr wohl anhand anderer Angaben identifizieren kann. So war es hier, weil im Fragebogen auch nach dem Beruf gefragt war. Gibt der Befragte dann Apotheker, Pfarrer, Zahnarzt oder einen ähnlichen, in einer kleinen Gemeinde selten vorkommenden Beruf an, so ist es relativ einfach herauszubekommen, wer er ist. Anstatt fälschlicherweise eine anonyme Auswertung des Fragebogens zu versprechen, sollte man den Befragten genau das sagen, was man im einzelnen mit ihren Angaben macht. Das Tübinger Institut sagte mir sofort zu, in Zukunft so zu verfahren.

1.3 Unternehmerbefragung

Probleme mit der Anonymität hatte auch das betriebswirtschaftliche Institut der Universität Stuttgart bei einem Forschungsvorhaben über Existenzgründer. Es versandte an ausgewählte Unternehmer einen Fragebogen und fragte u. a. nach Fremdkapital, Anlagevermögen, Zinsaufwand, Umsatz- und Betriebsergebnis. Dazu hieß es wörtlich: „Da Sie auf dem Fragebogen ihre Adresse nicht angeben, ist die absolute Anonymität der eingetragenen Zahlen gewährleistet." Dem war allerdings nicht so, wie sich bei einer Durchsicht des Fragebogens schnell zeigte. Das Institut wollte nämlich vom Unternehmer auch Einzelheiten über den

Beginn seiner selbständigen Tätigkeit, die Rechtsform seines Unternehmens, Wirtschaftsbereich und die Branche („ihre genaue Bezeichnung") sowie den Land- oder Stadtkreis der Niederlassung wissen. Mit diesen Angaben und einem — allgemein zugänglichen — Dienstleistungsverzeichnis der Industrie- und Handelskammer kann man ohne größere Schwierigkeiten herausbekommen, um wen es sich handelt. Der Hinweis auf die absolute Anonymität, der sicherlich zur Bereitschaft der Befragten mitzumachen beitrug, erwies sich damit als falsch. Auch dieses Institut will es in Zukunft besser machen.

1.4 Abhören von Notrufen zur Spracherforschung

Wer in einem Notfall aufgeregt die Nummer der Feuerwehr wählt, denkt sicher nicht daran, daß sein Anruf auf Tonband aufgezeichnet wird. Die Feuerwehr hält jeweils Name des Anrufers, Unglücksort, Unglückszeit und die Schilderung, was im einzelnen passiert ist, fest. Damit kann sie im Nachhinein erforderlichenfalls kontrollieren, ob sie auf einen Notruf sachgerecht reagierte. Diese mit § 201 Abs. 1 Nr. 1 des Strafgesetzbuches vereinbarte Gesprächsaufzeichnung darf die Feuerwehr selbstverständlich nicht an andere Personen, auch nicht an Wissenschaftler weitergeben. Gerade darum aber ging es einer Studentin bei ihrer Doktorarbeit. Sie wollte die Tonbandmitschnitte daraufhin untersuchen, welche Auswirkungen die Aufregung durch einen Unglücks- oder Notfall auf das Sprachvermögen des Anrufers hat. Ich mußte ihr sagen, daß dies so nicht geht. Die Notrufzentrale darf ihr die Tonbänder nur geben, wenn sie entweder zuvor das Einverständnis der früheren Anrufer dazu einholt — ein sicherlich recht schwieriges, wenn nicht aussichtsloses Unterfangen — oder wenn sie aus den Tonbändern zuvor alles herauslöscht, womit die Studentin die Anrufer identifizieren könnte. Ob sich die Branddirektion zu einer dieser aufwendigen Maßnahmen bereit fand, weiß ich nicht. Verpflichtet war sie jedenfalls dazu nicht.

1.5 Patientenfragebogen der Europäischen Dialyse- und Transplantationsgesellschaft

Durch meinen Kollegen aus Nordrhein-Westfalen erfuhr ich von einem bundesweiten Meldeverfahren über Patienten, die sich in einer Dialysebehandlung befinden oder einer Nierentransplantation unterzogen haben. 95 % der bundesdeutschen Dialyse- und Transplantationszentren melden seit geraumer Zeit ihre Patienten mit Namen und einer Vielzahl von medizinischen Daten an die Europäische Dialyse- und Transplantationsgesellschaft mit Sitz in London, ohne daß die Patienten zuvor um ihr Einverständnis gefragt werden. 160 000 nierenkranke Patienten aus ganz Europa sind inzwischen dort im Computer erfaßt. Das alles geschieht, um anhand dieses Datenmaterials den Verlauf einer Nierenerkrankung und ihre bestmögliche Behandlung weiter zu erforschen. Ich bezweifle nicht, daß diese grenzüberschreitende Zusammenarbeit von Ärzten und Forschern zur Verbesserung des medizinischen Wissensstandes beitragen kann. Unverständlich ist für mich allerdings, daß man — wie ich bei einigen meiner Kontrolle unterliegenden Kliniken feststellen mußte, z. B. dem Katharinenhospital Stuttgart, Kreiskrankenhaus Heidenheim und der Abteilung Innere Medizin IV des Universitätsklinikums

Tübingen — die Einwilligung des Patienten in die Offenbarung seiner Daten an die wissenschaftliche Gesellschaft in London bislang nicht einholte. Dies war und ist im Hinblick auf die ärztliche Schweigepflicht unerläßlich. Es genügt nicht, daß ein Teil der Patienten von der Existenz des Registers weiß. Erst jetzt wollen die in der Dialyse- und Transplantationsgesellschaft zusammengeschlossenen Ärzte daran gehen, die Patienten über das Verfahren ausdrücklich aufzuklären und sie um ihre schriftliche Einwilligung bitten.

1.6 Perinatalerhebung

Das erklärte Ziel dieser Studie ist, die Qualität der Geburtshilfe zu sichern, wenn möglich weiter zu verbessern. Dazu sollen möglichst viele Krankenhäuser im Land einer von der Landesärztekammer eingerichteten Geschäftsstelle nach jeder Geburt sehr detaillierte Angaben über die persönlichen und sozialen Verhältnisse der Schwangeren, über die Schwangerschaft, die Entbindung, das Neugeborene und den Gesundheitszustand der Mutter zuleiten. Aufgabe der Geschäftsstelle ist, diese Einzelangaben statistisch auszuwerten. Anhand dieser Statistiken können dann die einzelnen Krankenhäuser Vergleiche mit der Situation in den übrigen Krankenhäusern anstellen. Außerdem will man die Sammelstatistiken zur wissenschaftlichen Forschung bereitstellen.

Da die Perinatalerhebung nicht nur in Baden-Württemberg, sondern auch in anderen Bundesländern stattfinden soll, befaßten sich die Datenschutzbeauftragten der Länder und des Bundes mit der Frage, wie dies in Einklang mit der ärztlichen Schweigepflicht und den Datenschutzgesetzen geschehen kann. Unser Vorschlag sieht so aus:

— Jedes Krankenhaus, das sich an der Perinatalerhebung beteiligen will, darf nur Einzelangaben melden, die so anonymisiert sind, daß man sie zumindest faktisch nicht mehr bestimmten Personen zuordnen kann. Dafür genügt es nicht — wie ursprünglich beabsichtigt —, nur den Namen der Schwangeren wegzulassen, statt der genauen Anschrift die vollständige Postleitzahl ihres Wohnorts und statt des Geburtsdatums ihr Geburtsjahr mitzuteilen. Soll die Meldung faktisch anonym sein, ist unbedingt erforderlich, auf die Mitteilung der vollständigen Postleitzahl des Wohnorts der Schwangeren zu verzichten und sich statt dessen mit der Weitergabe deren ersten beiden Ziffern zu begnügen.

— Diese Bemühungen um eine Anonymisierung reichen allerdings nur dann, wenn zugleich gesichert ist, daß die gemeldeten Einzelangaben nach wie vor unter den Schutz des Datenschutzrechts fallen und die Auswertungsstelle nicht frei darüber verfügen darf. Deshalb müssen die meldenden Krankenhäuser mit der Geschäftsstelle der Landesärztekammer vereinbaren, daß sie die mitgeteilten Angaben im Auftrag des Krankenhauses speichert, nur zum Erstellen der geplanten Statistiken nutzt und vor allem nicht an andere weitergibt.

Die Landesärztekammer erklärte sich bereit, dies zu tun. Die Perinatalerhebung ist inzwischen angelaufen.

2. Blutspendedienst

Wer für andere Menschen Blut spendet, denkt sicher nicht an den Datenschutz. Für ihn ist mit dem Ausfüllen einiger Formulare vor der Blutabnahme und dem kleinen Pflaster am Arm danach alles erledigt. Ganz so ist es nicht. Erhebung der Anamnese und Untersuchungen vor der Blutentnahme hinterlassen ebenso wie Auskünfte von Gesundheitsämtern und Hausärzten über Spender sensible Datenspuren. Dem Schutz der Spender dienen — genauso wie dem des Patienten, der sich in ärztliche Behandlung gibt — das Arztgeheimnis und die Datenschutzgesetze. Wie es mit der Einhaltung dieser Regeln im Blutspendealltag steht, sah ich mir vor Ort bei den Blutspendediensten des Universitätsklinikums Freiburg, der Städtischen Krankenanstalten Karlsruhe, des Klinischen Laboratoriums der Chirurgischen Klinik und des Instituts für Immunologie der Universität Heidelberg und des Instituts für Anaesthesiologie und Transfusionsmedizin der Universität Tübingen näher an. Dabei zeigte sich, daß es auch hier einige — durchaus lösbare — Probleme mit dem Datenschutz gibt.

2.1 Was der Spender offenbaren muß

Wer spendet, muß gesund sein. Damit der Arzt des Blutspendedienstes dies verläßlich feststellen kann, müssen Spendewillige ein Aufnahmeformular ausfüllen. Sie werden darin nicht bloß nach Name, Anschrift, Telefon und Geburtsdatum gefragt, sondern auch um detaillierte Auskünfte über ihre bisherige Krankheitsgeschichte gebeten. So weit, so gut. In manchen Formularen fand sich freilich auch „Kleingedrucktes", das mir zu weit ging. Schon 1983 machte mich eine Bürgerin auf die — bis Anfang 1985 verwendete — Klausel im Formular der Blutzentrale des Stuttgarter Katharinenhospitals aufmerksam:

> „Ebenfalls entbinde ich die Haus- und Krankenhausärzte sowie die Staatlichen und Städtischen Gesundheitsämter von ihrer ärztlichen Schweigepflicht, um dem leitenden Arzt der Blutzentrale dadurch die Möglichkeit zu geben, sich über meinen Gesundheitszustand durch Befragen dieser Ärzte zusätzlich zu informieren."

Ähnliches fand sich nun bei der Blutspendezentrale der Chirurgischen Universitätsklinik Heidelberg:

> „Ich bin damit einverstanden, daß die Blutspendezentrale Auskunft über frühere Krankheiten bei Ärzten und ärztlichen Dienststellen einholen, andererseits bei evtl. krankhaften Befunden Mitteilung an den von mir genannten Hausarzt machen kann."

Im Formular des Blutspendedienstes des Tübinger Instituts für Anaesthesiologie und Transfusionsmedizin hieß es dazu:

> „... erkläre ich mich mit der Blutentnahme für Blutkonserven einverstanden und ermächtige die Abteilung Transfusionsmedizin, Auskünfte über meinen Gesundheitszustand einzuholen."

Die Blutspendedienste ließen sich diese Klauseln jeweils durch Unterschrift der Spender bestätigen. Eine wirksame Einwilligung war dies freilich nicht. Nach den Datenschutzgesetzen und den Regeln über die ärztliche Schweigepflicht ist eine Einwilligung nur rechtmäßig, wenn derjenige, der sie abgibt, bei ihrer Abgabe erkennen und abschätzen kann, worin er im einzelnen einwilligt. § 5 Abs. 2 LDSG schreibt

zu seinem Schutze sogar ausdrücklich vor, daß er über die Bedeutung der Einwilligung zu unterrichten ist. Diesen Anforderungen tragen so pauschale Erklärungen, wie man sie hier den Spendern abverlangte, nicht Rechnung — sind sie doch nichts anderes als eine Blankovollmacht mit nicht absehbaren Auswirkungen. Daß die Spender solche Vollmachten erteilen mußten, obwohl es höchst selten vorkommt, daß ein Blutspendedienst eine Auskunft des behandelnden Arztes oder Gesundheitsamts benötigt, erstaunte mich zu hören. Aus all diesen Gründen legte ich den Blutspendediensten nahe, auf solche unnötigen und unwirksamen Einwilligungserklärungen „auf Vorrat" zu verzichten. Sollte ein Blutspendedienst ausnahmsweise einmal eine ärztliche oder amtsärztliche Auskunft über einen Blutspender brauchen, sollte er dies mit ihm besprechen und dabei sagen, von wem und zu welchem Zweck er eine Auskunft einholen möchte, und den Spender dafür um sein — in der Regel schriftlich zu erteilendes — Einverständnis bitten. Der Blutspendedienst des Tübinger Instituts für Anaesthesiologie und Transfusionsmedizin griff diesen Vorschlag bereitwillig auf. Auch die Karlsruher Krankenanstalten, deren „Kleingedrucktes" sich auf Anfragen beim Gesundheitsamt beschränkte, schloß sich dieser Praxis an. Die Antwort von Heidelberg steht noch aus.

2.2 Weitergabe von Blutspenderdaten

Mancher Spender wird mit Erstaunen hören, wohin seine Daten gelangen.

— Information des Hausarztes

Gelegentlich kommt vor, daß sich bei der Untersuchung des Spenders ein krankhafter oder anomaler Befund herausstellt, der eine ärztliche Behandlung ratsam erscheinen läßt. Manche Blutspendedienste treffen für diesen Fall Vorsorge: So fand ich beispielsweise im „Kleingedruckten" des Formulars des Blutspendedienstes der Chirurgischen Klinik Heidelberg und des Blutspendedienstes des Universitätsklinikums Freiburg die Einwilligung des Spenders, er sei in einem solchen Fall mit der Weitergabe des Befunds an seinen Hausarzt einverstanden. So, meine ich, geht es nicht: Denn eigentlich müßten doch die Blutspendedienste den Spender selbst über den Befund informieren und ihm dann völlig überlassen, ob und was er — beispielsweise einen Besuch beim Hausarzt — zu unternehmen gedenkt. Deshalb sollte, wenn man es schon anders machen will, die Einwilligung keinesfalls im „Kleingedruckten" enthalten sein. Wenn der Spender diese Klausel überhaupt liest, kann sie bei ihm den Eindruck hervorrufen, er könne nur Blut spenden, wenn er mit der Offenbarung des Untersuchungsergebnisses an seinen Hausarzt einverstanden ist. So ist es aber doch nicht. Die Blutspendedienste müssen die Spender vielmehr ausdrücklich darauf hinweisen, daß sie frei entscheiden können, ob ihr Arzt den Befund erfährt oder nicht. Der Freiburger Blutspendedienst will meinem Vorschlag folgen; die Äußerung von Heidelberg steht noch aus.

— Spendername auf Blutkonserve

Blutspendedienste beschriften die fertige Blutkonserve in der Regel mit Angaben zur Blutgruppe oder Blutfor-

mel und einer laufenden Nummer. Sollte es ausnahmsweise einmal nötig sein, ist auf diese Weise möglich, die näheren Umstände der Herstellung der Blutkonserve und den Namen des Spenders zu ermitteln. Allein das Tübinger Institut für Anaesthesiologie und Transfusionsmedizin macht es anders: Es beschriftet die fertige Blutkonserve mit dem Namen des Spenders und seinem Geburtsdatum. Die so gekennzeichneten Blutkonserven gibt es an verschiedenste medizinische Einrichtungen. Auf diese Weise erfahren deren Mitarbeiter — also eine von vornherein gar nicht absehbare Zahl — ohne Grund die Personalien des Spenders. Gewiß ist es nicht ehrenrührig, daß jemand Bescheid weiß, daß eine bestimmte Blutkonserve etwa vom 25jährigen Herrn Fischer stammt. Aber erforderlich ist dies sicher nicht und ebensowenig mit dem Arztgeheimnis zu vereinbaren. Es reicht völlig aus, die Blutkonserven so zu kennzeichnen, daß man im Ausnahmefall den Namen des Spenders ermitteln kann. Dem Tübinger Institut leuchtet dies noch nicht so recht ein, obwohl die anderen Blutspendedienste damit doch gut fahren. Es will noch juristischen Rat einholen.

— Der zentral erfaßte Spender

Blutspendedienste aus dem ganzen Bundesgebiet melden dem Tübinger Institut für Anaesthesiologie und Transfusionsmedizin Spender, deren Blut in einem aufwendigen Verfahren nach HLA-Bestandteilen typisiert wurde. Solches besonders typisiertes Blut benötigt die Medizin bei Transplantationen und spezifischen Zellübertragungen. Damit jede Universitätsklinik oder andere medizinische Einrichtung im Bedarfsfall möglichst rasch erfahren kann, wo solches Blut vorhanden ist, begann das Tübinger Institut schon vor Jahren mit dem Aufbau seiner zentralen Datenbank über solche Blutspender. Blutspendedienste aus dem ganzen Bundesgebiet melden ihm inzwischen ihre HLA-Spender. Das Meldeverfahren, das die zentrale Datenbank inzwischen auf ca. 20 000 gespeicherte HLA-Spender anwachsen ließ, hatte nur einen Haken: Die Spender wußten in der Regel von ihrer zentralen Erfassung in Tübingen nichts. Wer beispielsweise bei den Blutzentralen des Universitätsklinikums Freiburg und Katharinenhospital Stuttgart Blut spendete, erfuhr nicht und mußte auch nicht damit rechnen, daß sein Name nach Tübingen geht und er dort im Computer landet. Weder das Arztgeheimnis noch die Bestimmungen des Landesdatenschutzgesetzes beachtete man hier ausreichend. Der Stuttgarter und Freiburger Blutspendedienst waren auf meine Erläuterungen hin rasch bei der Hand, ihre Meldeverfahren zu ändern. Auch das Tübinder Institut erklärte sich erfreulicherweise bereit, alle meldenden Blutspendedienste im Bundesgebiet zu informieren, daß solche Meldungen nur mit Einwilligung der Spender zulässig sind.

— Spenderdaten an Privatlabor

Auch die Städtischen Krankenanstalten Karlsruhe praktizierten ein mit dem Arztgeheimnis und dem Landesdatenschutzgesetz nicht zu vereinbarendes Verfahren. Ihr Blutspendedienst wählte nach dem Zufallsprinzip täglich einen Spender aus und sandte ohne dessen Wissen seine mit Namen und Geburtsdatum gekennzeichnete Blutpro-

be an ein Karlsruher Labor. Nach dem wenigen, was ich trotz mehrmaligen Fragens von den Verantwortlichen erfahren konnte, untersuchte dieses Labor die Proben auf die sog. HLA-Antikörperzusammensetzung, speicherte die Namen der Spender und Laborwerte im Computer und meldete die Ergebnisse der Laboruntersuchungen an den Blutspendedienst Karlsruhe. Ob, wie lange und zu welchem Zweck das Institut die Spenderdaten speicherte, konnte man mir nicht sagen; es gäbe über die Zusammenarbeit keine schriftliche Vereinbarung. Das merkwürdige Verfahren ist inzwischen eingestellt.

2.3 Aufbewahrung von Blutspenderdaten

Wer einmal drin ist, kommt so schnell nicht wieder heraus. Mit dieser kurzen Formel könnte man die Aufbewahrung der Spenderdaten durch die Blutspendedienste charakterisieren. Daß sie die Daten ihrer Dauerspender in ihrer Spenderdatei nicht löschen, leuchtet ein. Was aber geschieht mit denen, die nur einmal spenden wollten, ihre Spendertätigkeit eingestellt haben oder für eine Spende aufgrund der ersten ärztlichen Untersuchung oder Laboranalyse nicht in Frage kommen? Die Praxis war bis auf den Blutspendedienst des Heidelberger Instituts für Immunologie überall ähnlich:

— Der Blutspendedienst des Universitätsklinikums Freiburg führte eine Kartei der „archivierten" Spender, die bis 1958 zurückging. In einem Schränkchen fanden sich auch noch EDV-Disketten aus der Computerfrühzeit mit Spenderdaten. Man erklärte zwar, daß man schon seit langem für diese Alt-Disketten keine Verwendung mehr habe; an eine Vernichtung hatte man jedoch nicht gedacht. Inzwischen holte man dies nach.

— In den Städtischen Krankenanstalten Karlsruhe und bei der Blutbank der Chirurgischen Klinik Heidelberg hatte man sich ebenfalls noch wenige Gedanken über die Vernichtung alter Karteikarten gemacht. Sie kamen in der Regel in einen verschlossenen Lagerraum.

— Im Tübinger Institut für Anaesthesiologie und Transfusionsmedizin verfuhr man gleichfalls nach dem Prinzip, wer einmal mit uns Kontakt hatte, den speichert der Computer auf Dauer. Auf unsere Fragen nach dem Grund hieß es, man brauche die Daten so lange, um kontrollieren zu können, ob ein früher schon einmal aus medizinischen Gründen abgewiesener Bewerber einen erneuten Spendeversuch startet und dabei seine schon einmal festgestellte Ungeeignetheit verschweigt.

Diese Praxis befriedigt nicht. Ich forderte alle Blutspendedienste auf, die Aufbewahrungszeiten nach folgenden Gesichtspunkten neu zu regeln: Die Daten ungeeigneter Spender und solcher Personen, die nicht mehr für eine Spende bereitstehen — etwa, weil sie verzogen sind —, sind grundsätzlich nach Ablauf von 10 Jahren zu löschen oder zumindest für jede weitere Nutzung zu sperren. Diese 10-Jahresfrist ergibt sich aus der in § 11 der ärztlichen Berufsordnung festgelegten Dokumentationsfrist und den vom Wissenschaftlichen Beirat der Bundesärztekammer und vom Bundesgesundheitsamt herausgegebenen Richtlinien zur Blutgruppenbestimmung und Bluttransfusion. Während die meisten von mir angesprochenen Blutspendedienste die

Aufbewahrung nunmehr so handhaben wollen, meint das Tübinger Institut für Anaesthesiologie und Transfusionsmedizin, ungeeignete Spender sollten weiterhin 30 Jahre gespeichert bleiben. Diese Argumentation überzeugt für die ganz überwiegende Zahl der Spender nicht. Denn selbst wenn einmal der sehr unwahrscheinliche Umstand eintreten sollte, daß ein ungeeigneter Spender nach mehr als 10 Jahren versucht, den Blutspendedienst über seinen früheren Ausschluß als Spender zu täuschen, kann dies jedenfalls dann keinen Schaden anrichten, wenn sich der krankhafte Befund bei der auf jeden Fall erfolgenden erneuten Voruntersuchung wiederum nachweisen läßt. Ob es, wie Tübingen geltend macht, einige wenige Sonderfälle gibt, wo dieser erneute Nachweis nicht gelingt, ließ sich bisher noch nicht endgültig klären.

3. Studentenwerke

Neun Studentenwerke in Baden-Württemberg kümmern sich um Dinge, die mit dem Studium nicht direkt zu tun haben, gleichwohl aber aus dem Studentendasein nicht wegzudenken sind. Sie sorgen beispielsweise für die Verpflegung der Studenten in der Mensa, vermieten die Zimmer der Studentenwohnheime und gewähren Ausbildungsförderung. Kritische Fragen von Bürgern nach dem Umgang der Studentenwerke mit Studentendaten waren Anlaß, mich diesem Komplex näher zu widmen. Das Studentenwerk Freiburg bot sich für eine Kontrolle geradezu an, weil es ein computerunterstütztes Verfahren bei der Verwaltung von Wohnheimplätzen einsetzt, das als Pilotprojekt für die übrigen Studentenwerke dienen soll. Leider gestaltete sich die Zusammenarbeit mit der Geschäftsführung des Studentenwerks Freiburg nicht einfach.

3.1 Kontrolle mit Hindernissen

Am Anfang standen unvollständige und widersprüchliche Aussagen des Studentenwerks, ob und welche Studentendaten es automatisiert speichert. Konnte man dies noch als Panne entschuldigen, die bei jeder Verwaltung vorkommen kann, wurde die Angelegenheit zum Ärgernis, als sich meine Mitarbeiter vor Ort umschauen wollten. Zu Beginn des Kontrollbesuchs gab es als Begrüßung den Einwand des Geschäftsführers, das Studentenwerk unterliege nicht der Kontrolle des Landesbeauftragten für den Datenschutz. Den Hinweis auf die gesetzliche Regelung, wonach das Studentenwerk als Anstalt des öffentlichen Rechts unzweifelhaft zu den im Landesdatenschutzgesetz genannten öffentlichen Stellen zählt, die der Aufsicht des Landes und damit meiner Kontrolle unterstehen, akzeptierte man nur unter dem Vorbehalt „der weiteren rechtlichen Prüfung". Während des Besuchs nahm die Kooperationsbereitschaft leider nicht zu. Da wurde etwa ein Angestellter, der gerade bereitwillig zur Beantwortung von Fragen meiner Mitarbeiter ansetzte, mit nachdrücklicher „Fürsorge" vom Geschäftsführer darüber belehrt, er wolle doch sicherlich jetzt gerade zum Mittagessen gehen und hätte deshalb gewiß gar keine Zeit, unsere Fragen zu beantworten. Trotz dieser Hindernisse konnten wir die Prüfung der Datenverarbeitung beim Studentenwerk schließlich zu Ende bringen. Dabei fand sich einiges, was geändert werden muß.

3.2 Wie kommt der Student an einen Wohnheimplatz?

Das Studentenwerk Freiburg verwaltet wie die anderen Studentenwerke auch Studentenwohnheime. Wer dort ein Zimmer mieten will, muß einen umfangreichen Bewerberfragebogen ausfüllen. Der Student muß neben zahlreichen Angaben über seine Person auch seine eigenen und zugleich die finanziellen Verhältnisse seiner Eltern detailliert auflisten. Unter anderem wird er gefragt nach

— den einzelnen Leistungen, die er aus öffentlichen Mitteln bezieht (z. B. Leistungen nach dem Bundesausbildungsförderungs- und Bundesversorgungsgesetz oder aus Waisenrente),

— seinen privaten Einkünften, wobei die Höhe der Zuwendungen seines Unterhaltsverpflichteten und Ehegatten und die eigenen Arbeitseinkünfte anzugeben sind,

— der Höhe des Einkommens und der genauen Berufsbezeichnung von Vater, Mutter und Ehegatten,

— der Zahl der Geschwister mit Angabe, ob diese vom Elternhaus noch finanziell abhängen.

Dazu ist aus der Sicht des Datenschutzes zu sagen: Gegen das Prinzip des Studentenwerks, bei der Zimmervergabe finanziell schlecht gestellte Studenten zu bevorzugen, ist gewiß nichts einzuwenden. Dafür — aber auch nur insoweit — darf es detailliert nach den finanziellen Verhältnissen fragen. Gibt ein Student jedoch von vornherein an, sein Einkommen liege über der „Bedürftigkeitsgrenze", ist klar, daß er nur zum Zuge kommen kann, wenn das Studentenwerk alle Studenten mit geringem Einkommen schon untergebracht hat und trotzdem noch Zimmer frei sind oder aber im Laufe des Semesters plötzlich frei werden. Trotzdem beharrte das Studentenwerk zunächst darauf, auch weiterhin in solchen Fällen vom Studenten detaillierte Auskunft über seine finanziellen Verhältnisse zu verlangen: Es will, daß solche Studenten beispielsweise ohne Grund offenbaren, daß der Vater Rechtsanwalt oder Chefarzt ist und im Jahr 100 000 oder 200 000 DM verdient, die Mutter Unternehmerin ist und entsprechendes mehr. Erst auf meinen weiteren Vorstoß zeigte das Freiburger Studentenwerk erste Einsicht: es will die geforderte Änderung seines Verfahrens nun doch näher bedenken.

3.3 Auskünfte des Amts für Ausbildungsförderung

In manchen Fällen waren dem Studentenwerk Freiburg nicht einmal die detaillierten Auskünfte finanziell schlecht gestellter Bewerber genug. Dem, der keine plausiblen Angaben über seine Einkünfte aus Ausbildungsförderung machte, konnte passieren, daß der Sachbearbeiter eben mal Auskünfte bei seinem Kollegen im Amt für Ausbildungsförderung einholte. Dieses Vorgehen ist mit dem Sozialdatenschutz unvereinbar. Denn das Amt für Ausbildungsförderung muß seine BAföG-Akten gegenüber anderen Abteilungen des Studentenwerks grundsätzlich geheimhalten. Obwohl das Amt für Ausbildungsförderung und die Wohnheimverwaltung unter dem gemeinsamen Dach „Studentenwerk", vereint sind, darf es keinen Austausch von Sozialdaten für Zwecke der Wohnheimverwaltung geben. Unbenommen bleibt den Studentenwerken, in Zweifelsfällen die

Studenten aufzufordern, ihre Angaben nachzuweisen. Das Studentenwerk Freiburg will dies alles bislang nicht einsehen. Seine Aufsichtsbehörde, das Landesamt für Ausbildungsförderung, teilte zunächst meine Ansicht und sagte zu, dafür zu sorgen, daß die Studentenwerke in Zukunft durchweg korrekt verfahren. Inzwischen ist seine so begrüßenswert klare Position etwas ins Wanken geraten: es will alles noch einmal mit den Geschäftsführern der Studentenwerke besprechen. Zu hoffen bleibt, daß es dabei zu seiner anfänglichen Haltung zurückfindet.

3.4 Mängel in der Datensicherheit

Wer die Hürden des Bewerbungsverfahrens erfolgreich durchlaufen hat und Mieter eines Zimmers im Studentenwohnheim ist, kommt mit einer Vielzahl von Daten in dessen Computer; er wird, wie es so schön heißt, „computerunterstützt verwaltet". Das Freiburger Studentenwerk testet das dafür zur Verfügung stehende EDV-Programm als Pilotanwender für die anderen Studentenwerke. Es hatte, wie sich bei unserer technischen Prüfung herausstellte, eine ganze Reihe von Mängeln, die ich nach § 18 Abs. 1 LDSG beanstanden mußte. Beispielhaft seien aufgezählt:

— Unwirksamer Paßwortschutz

Paßwortschutz macht nur einen Sinn, wenn jeder Mitarbeiter, der auf die EDV-Verfahren zugreifen kann, ein anderes Paßwort hat und dieses zudem häufig wechselt. Das Studentenwerk Freiburg „schützte" seine Programme der Wohnheimverwaltung nur durch ein Paßwort, das für alle Mitarbeiter gleich war und das es seit der Einführung des Verfahrens am 1. Januar 1985 bis zum Kontrollbesuch am 15. Mai 1985 unverändert ließ. Man wußte nicht einmal, wie es zu ändern war; der Hersteller der Programme hatte dies noch gar nicht mitgeteilt.

— Fehlendes Datenträgerverzeichnis

Zum Abbuchen der Mietzahlungen tauscht das Studentenwerk Freiburg mit der Bad.-Württ. Bank Disketten aus. Um Unregelmäßigkeiten im nachhinein prüfen zu können, muß man Nachweise führen, wer, wann welche Disketten hatte. Die dafür erforderlichen Aufzeichnungen fehlten.

— Fehlerprotokollierung

Treten beim Einsatz von EDV-Programmen Fehler auf, muß man diese schriftlich festhalten, den Programmhersteller verständigen und auf ihre Beseitigung achten. Anders das Studentenwerk: es begnügte sich bei einem Fehler lediglich mit dem Versuch, den Programmlauf gleichwohl zu einem erfolgreichen Ende zu bringen. Maßnahmen, den Fehler statt bloß zu umgehen, richtig zu beseitigen, unternahm es in der Regel nicht.

— Unvollständige Dokumentation

Jedes EDV-Verfahren ist präzise zu beschreiben. Dazu gehört die Dokumentation aller Datenarten, die gespeichert werden sollen, und der vorgesehenen Datensicherungsmaßnahmen. Auch daran fehlte es in Freiburg.

Bis auf die unvollständige Dokumentation, die spätestens nach Abschluß der Testphase in Ordnung zu bringen ist, sollen inzwischen, wie mir das Studentenwerk mitteilte, die Mängel bei der Datensicherheit behoben sein.

4. Was im ärztlichen Attest über einen erkrankten Kandidaten stehen darf

Einige Aufregung gab es wegen des Erlasses des Ministeriums für Wissenschaft und Kunst vom 1. Juli 1985 zum Rücktritt von einer Fachhochschulprüfung aus Gesundheitsgründen. Studenten wandten sich an mich; einzelne Ärzte und der Präsident der Landesärztekammer protestierten; Landtagsabgeordnete brachten im Landtag einen Antrag ein, den Erlaß zurückzuziehen. Was war geschehen? Das Ministerium hatte den Fachhochschulen empfohlen, den Studenten per Aushang am schwarzen Brett bekanntzugeben, wie ein ärztliches Zeugnis über die Prüfungsunfähigkeit eines erkrankten Kandidaten auszusehen hat. Wörtlich war darin zu lesen: „Für ein ärztliches Zeugnis ist zu fordern, daß es die volle Anamnese des Patienten, die Diagnose (angewendete Untersuchungsmethoden und Schlußfolgerungen aus Anamnese und Untersuchungsergebnis) sowie die Art der Behandlung wiedergibt". Im Klartext hieß dies, daß sich jeder Student, der wegen Krankheit von einer Prüfung zurücktreten will, vor dem Prüfungsausschuß quasi „bis aufs Hemd" ausziehen müßte. Relativ rasch war geklärt: diese Anforderungen ließen sich nicht aus dem maßgeblichen § 14 Abs. 2 der Verordnung über die Prüfung an Fachhochschulen ableiten. Dort ist die Sache nämlich so geregelt:

— Will ein Student einer Fachhochschule von einer Prüfung zurücktreten, muß er dem Prüfungsausschuß unverzüglich seine Gründe schriftlich mitteilen und diese glaubhaft machen. Was heißt dies? Glaubhaftmachen ist im Rechtssinne weniger als Nachweisen. Ein Mittel der Glaubhaftmachung ist stets die eigene Erklärung des Kandidaten. Hinzukommen muß nach § 14 Abs. 2 der Verordnung die „ärztliche Bescheinigung über die Prüfungsunfähigkeit". An ihren Inhalt sind, wie schon der Wortlaut zeigt, keine hohen Anforderungen zu stellen. Andererseits kommt schon der schlichten Bescheinigung des Arztes über die Prüfungsunfähigkeit ein hoher Stellenwert zu, weil sie der Arzt als Außenstehender und zudem Sachverständiger abgibt. Kann der Prüfungsausschuß in Zusammenschau dieser Bescheinigung, der vom Kandidaten vorgetragenen Tatsachen oder den äußeren Umständen der Erkrankung keinen vernünftigen Zweifel an der Triftigkeit des Grundes haben, dann muß er es damit bewenden lassen. Es besteht keinerlei Anlaß, in solchen Fällen vom Kandidaten auch noch eine ärztliche Bescheinigung über weitere Details seiner Erkrankung zu verlangen. Kurzum: Das geltende Recht erlaubt nicht, im Falle eines Rücktritts aus Krankheit schematisch ein ärztliches Zeugnis mit voller Anamnese, Diagnose und Art der Behandlung zu fordern.

— Natürlich wird es immer wieder Einzelfälle geben, in denen der Prüfungsausschuß wegen besonderer Umstände Zweifel haben kann, ob das Urteil des Arztes über die Prüfungsunfähigkeit tatsächlich gerechtfertigt ist. Auch dann aber ist nicht Schematismus, sondern Augenmaß am Platz: Der Prüfungsausschuß muß je nach Sachlage bei den Anforderungen an die ärztliche Bescheinigung differenzieren und stets das für den Kandidaten schonendste Vorgehen wählen. Das kann je nachdem ein amtsärztliches Zeugnis, eine etwas detaillier-

tere Darstellung des Arztes, welche Auswirkungen der Krankheit den Kandidaten gerade an der Ablegung der Prüfung hindern, ja im Extremfall selbst einmal ein so umfangreiches Attest sein, wie es das Ministerium in seinem Erlaß vom 1. Juli 1985 generell forderte. Der Schlüssel zu einer verfassungsgemäßen Praxis liegt in der Orientierung am Einzelfall. Nur dann kann der Prüfungsausschuß den Grundsatz der Verhältnismäßigkeit beim Eingriff in das allgemeine Persönlichkeitsrecht der Kandidaten beachten und zugleich das Prinzip der Chancengleichheit für alle Prüfungskandidaten wahren.

Das Ministerium brachte es nicht übers Herz, sich dieser Beurteilung anzuschließen, sondern rang sich lediglich zu einem Teilrückzug auf Raten durch. Zunächst hieß es auf meine erste Anfrage, zu einem ordnungsgemäßen Zeugnis gehöre „sicher in vielen Fällen nicht die volle Krankheitsgeschichte". Auf die Regelung des § 14 Abs. 2 der Verordnung für die Prüfung an Fachhochschulen ging das Ministerium aber nicht weiter ein, sondern zitierte statt dessen gar nicht einschlägige Bestimmungen aus der Verordnung für die Ausbildung und Prüfung der Juristen. In seiner kurze Zeit später folgenden Antwort auf eine Landtagsanfrage räumte es dann ein, der Prüfungsausschuß müsse bei den im Einzelfall zu belegenden Tatsachen das Gebot der Verhältnismäßigkeit beachten. Kurz danach legte es dem Wissenschaftsausschuß des Landtags den Entwurf eines ergänzenden Erlasses an die Fachhochschulen vor, der aber gleichwohl im wesentlichen an den alten Positionen festhielt. Ergebnis der Beratungen im Landtag, bei denen ich dem Ministerium Formulierungshilfe anbot, war: es überarbeitete seinen Entwurf noch zweimal. Entgegen meinen Einwänden blieb es aber weiter dabei, die medizinischen Befundtatsachen müßten im Zeugnis enthalten sein; allerdings sei der medizinische Sachverhalt je nach Lage des Einzelfalls zu beschreiben und müsse „in der Regel nicht die volle Krankheitsgeschichte (Anamnese, Diagnose, angewendete Untersuchungsmethode sowie Art der Behandlung)" enthalten. Ein — entscheidender — Schritt des Ministeriums zu einer Einigung hat damit noch gefehlt: Das Ministerium hätte auf seine kategorische Forderung nach Angabe einer medizinischen Befundtatsache im ärztlichen Zeugnis verzichten und statt dessen die glaubhafte Erklärung des Kandidaten und die schlichte ärztliche Prüfungsunfähigkeitsbescheinigung in der Regel ausreichen lassen müssen. Vielleicht war dies zu viel verlangt. Es wäre wohl zu deutlich geworden, daß die Verordnung über die Prüfung an Fachhochschulen selbst den Rücktritt ausreichend regelt und der erste und alle folgenden Erlasse besser unterblieben wären.

5. Gerangel um Studenten

Studenten kosten nicht nur Geld, sie können dem Stadtsäckel auch Geld bringen. Früher funktionierte dies so: die Hochschulstädte erhielten aus dem Topf des kommunalen Finanzausgleichs für jeden Studenten unabhängig davon, ob er bei ihnen seinen Hauptwohnsitz oder bloß einen Nebenwohnsitz hatte, einen Kopfbetrag. Das Versiegen dieser Einnahmequelle beklagten die Hochschulstädte — voran die Stadt Stuttgart —, seit das Land ab 1983 im Zuge einer Änderung seiner Berechnungsmethode bloß noch für Studenten mit Hauptwohnsitz zahlte. Seitdem brachten dem Hochschulort Studenten, die aufs Jahr gesehen den Mittelpunkt ihrer Lebensbeziehungen und damit ihren Hauptwohnsitz in ihrem Heimatort haben, kein Geld mehr. Der Kampf der Hochschulstädte und Heimatgemeinden um den Hauptwohnsitz-

einwohner begann: ohne das Melderecht immer ausreichend zu beachten, versuchten Hochschulstädte des lieben Geldes wegen, Studenten bei sich „einzugemeinden". Daneben stellten sie jedoch auch finanzpolitische Forderungen und argumentierten: sie könnten die Belastungen durch die studentischen Einwohner nur tragen, wenn sie auch einen speziellen Sonderlastenausgleich für die Studenten mit Nebenwohnsitz erhielten. Ein monatelanges Gerangel um den Sonderlastenausgleich begleitete sodann 1985 die Einbringung des Regierungsentwurfs zur Änderung des kommunalen Finanzausgleichsgesetzes und seine parlamentarischen Beratungen. Schließlich standen vor allem zwei Lösungsansätze zur Diskussion. Der eine war für den Datenschutz völlig problemlos: hier sollten die Hochschulstädte pro immatrikulierten Studenten einen Pauschalbetrag erhalten. Dem anderen — ein Gegenvorschlag der Stadt Stuttgart und des Städtetags — mußte ich aus der Sicht des Datenschutzes entschieden widersprechen:

Um herauszufinden, wie viele Studenten bloß einen Nebenwohnsitz am Hochschulort haben, sah er vor, alle Hochschulen durch Gesetz zu verpflichten, den Einwohnermeldeämtern die Namen all der Studenten mit Geburtstag und Adresse mitzuteilen, die gegenüber ihrer Hochschule die Hochschulstadt als Wohnsitz angegeben hatten. Durch einen automatisierten Abgleich dieser Daten mit den Melderegistern sollten die Hochschulstädte dann die Zahl der Studenten ermitteln, die bei ihnen nur einen Nebenwohnsitz haben. Was sprach dagegen?

— Eine Weitergabe der Studentendaten von den Hochschulen an die Hochschulstädte wäre ein ganz erheblicher Eingriff in das informationelle Selbstbestimungsrecht der Studenten. Solche Eingriffe lassen sich nicht, wie die Urheber des Vorschlags meinten, mit angeblich größerer Einzelfallgerechtigkeit rechtfertigen. Wer die Zahl der Studenten mit Nebenwohnsitz kennt, vermag noch lange nicht die tatsächlichen Belastungen der Kommunen durch sie genau abzuschätzen. Dazu sind die Beziehungen der Studenten zu ihren Wohnsitzgemeinden zu unterschiedlich. Zudem ist Einzelfallgerechtigkeit im Finanzausgleich ohnehin unerreichbar; für ihn sind vielmehr Typisierung und Pauschalierung charakteristisch.

— Nicht stach auch das Argument, die Einwohnermeldeämter der Hochschulstädte würden über die Studenten nicht mehr Informationen erhalten, als sie ohnehin schon haben. Zusätzlich hätten sie erfahren, daß jemand Student der Hochschule ist. Eine vergleichbare Angabe muß keine andere Bevölkerungsgruppe der Meldebehörde machen. Die vorgeschlagene Regelung hätte deshalb quasi zu einem Sondermelderecht für ledige Studenten geführt. Das wiederum geht nicht an, weil das Meldegesetz abschließend bestimmt, welche Angaben die Meldebehörde erheben darf und welches Verfahren sie dabei einzuhalten hat. Es will, daß der Bürger seine Angaben direkt gegenüber der Meldebehörde macht und die Meldebehörde sich nicht hintenherum weitere beschafft. Dazu wäre es aber bei dem vorgeschlagenen Abgleich für eine besondere Bevölkerungsgruppe, die Studenten, gekommen.

— Völlig verquer war das Argument der Befürworter, ihr Verfahren sei sogar besonders datenschutzfreundlich, weil die Hochschulstädte dann nicht mehr Anlaß hätten, wegen der Frage nach „Haupt- oder Nebenwohnsitz" die Lebensweise der Studenten zu erfassen. Hier scheint man völlig aus dem Auge verloren zu haben: die korrekte Anwendung des Melderechts steht nicht zur Disposition der Meldebehörden. De-

ren Aufgabe ist vielmehr, seine Vorschriften so anzuwenden, wie es dem Willen des Gesetzgebers entspricht und nicht je nach finanziellen Interessen ihrer Stadt. Geschieht dies gleichwohl, müßte das Land dem im Wege der Rechtsaufsicht entgegentreten.

— Beim Datenabgleich hätte es, anders als die Befürworter meinten, auch praktische Schwierigkeiten zuhauf gegeben. Ich stellte fest, daß einige Hochschulen die Semesteranschrift ihrer Studenten gar nicht kennen und daher der Meldebehörde auch nicht liefern könnten. So ist es beispielsweise bei der Universität Stuttgart und der Fachhochschule für Technik Stuttgart mit zusammen ca. 19 000 Studenten. Bei weiteren 14 Hochschulen mit ca. 8 200 Studenten wäre, da sie keine EDV einsetzen, ein automatisierter Abgleich nicht möglich gewesen. Sie hätten unter enormem Aufwand ihre Studentenkarteikarten einzeln durchschauen und herausschreiben müssen, welche ledigen Studenten die Hochschulstadt als ihren Wohnsitz angegeben haben. Bei drei weiteren Hochschulen mit ca. 3 570 Studenten hätte man zudem erhebliche technische Schwierigkeiten mit einem automatisierten Abgleich.

Alles in allem: der vorgeschlagene Datenabgleich hätte zu datenschutzpolitisch ganz und gar unerwünschten Ergebnissen geführt und wäre wohl bei den Studenten wegen seiner Undurchsichtigkeit auf wenig Verständnis gestoßen. Ob mein Einsatz gegen diesen Vorschlag die ausschlaggebende Rolle spielte, weiß ich nicht. Ich jedenfalls bin froh, daß der Landtag diese Berechnungsmethode schließlich verwarf und sich für die Pauschbetragslösung entschied.

6. Teil: Gesundheit und Soziales

1. Krebsregister

Im April 1985 traf die Landesregierung für das geplante Krebsregister eine wichtige Entscheidung: Die Ärzte sollen dem Register ihre Patienten, wenn es irgend angeht, anonym und nicht mit ihrem vollen Namen und weiteren Identifizierungsdaten melden. Dazu will sie ihnen, wie mein Amt im Mai 1984 vorschlug, einen Verschlüsselungscomputer an die Hand geben. 50 Stück stehen inzwischen bereit. Ihre Eignung will das Sozialministerium 1986 in einem Feldversuch im Raum Tübingen—Reutlingen erproben. Unter dem Aspekt des Datenschutzes ist dabei von Interesse:

— Der Verschlüsselungscomputer hat die Größe der Tastatur einer Schreibmaschine; ein etwa gleich großer Drucker ist angeschlossen. Für diese Art von Rechner entschieden sich die Experten, damit es die Ärzte und ihre Mitarbeiter möglichst einfach haben. Zudem könnte dieser Rechner, wenn man ihn entsprechend programmiert, nicht nur die Identifizierungsdaten der Krebskranken verschlüsseln, sondern die ganze Meldung des Arztes an das Register ausdrucken. Außerdem könnte man ihm wichtige aktuelle Informationen für die Ärzte zur Diagnose und Behandlung des Krebses einprogrammieren. Kurzum: Der Verschlüsselungscomputer ist et-

was größer und auch teurer als der zunächst ins Auge gefaßte Taschencomputer; dafür aber vielseitiger verwendbar.

— Für den anonymen Probelauf, der von Januar bis Dezember 1986 erfolgen soll, ist wichtig, daß die Verschlüsselung der Identifizierungsdaten nicht im Einzelfall dadurch unterlaufen wird, daß sich aus den weiteren zu machenden Angaben über den Patienten Rückschlüsse auf dessen Identität ziehen lassen. Ich bat das Sozialministerium, bei der Gestaltung der Meldebögen hierauf zu achten.

Zu hoffen bleibt, daß der Feldversuch dazu beiträgt, neue Wege für die epidemiologische Krebsforschung zu eröffnen.

2. Das Gesundheitsamt

Gesundheitsämter haben vielfältige Aufgaben. Dabei treffen ärztliche Tätigkeit und hoheitliches Handeln in nahezu einmaliger Weise zusammen. Aus diesem Spannungsverhältnis ergeben sich immer wieder auch Probleme mit dem Datenschutz.

2.1 Die schulärztliche Untersuchung

Die „Schulgesundheitspflege" ist keine Erfindung unserer Tage. Diese staatliche Fürsorgemaßnahme geht vielmehr auf eine Zeit zurück, als es noch um die allgemeine ärztliche Versorgung nicht allzu gut bestellt war. Wer nun denkt, wegen des inzwischen erreichten Standards unseres Gesundheitssystems würde die Schulgesundheitspflege an Bedeutung verlieren, irrt. Auch hier haben die Möglichkeiten des Computers einem Bereich der Schulgesundheitspflege, der Schularztuntersuchung, eine neue Dimension verliehen. Im ministeriellen Amtsdeutsch heißt dies: Ausbau der Schuluntersuchung zur „epidemiologisch auswertbaren vollständigen Querschnittsuntersuchung einer Jahrgangskohorte der Gesamtbevölkerung". Dazu will das Sozialministerium die von den Schulärzten festgestellten Befunde, die bislang die einzelnen Gesundheitsämter meist auf Karteikarten in unterschiedlicher Weise erfassen, in einer automatisiert auswertbaren, zentralen Befunddokumentation zusammenführen. Nicht zuletzt wegen vermehrter Eingaben von Eltern sah ich mir das Verfahren bei der schulärztlichen Untersuchung näher an. Dabei kam folgendes heraus:

— Verpflichtung zur Teilnahme an einer schulärztlichen Untersuchung.

  Kinder, die vor ihrem ersten Schultag eine Aufforderung zur schulärztlichen Reihenuntersuchung erhalten, müssen daran — entgegen der Auffassung des Sozialministeriums — nicht teilnehmen. Nach den §§ 91 i. V. m. 74 Abs. 2 und 3 des Schulgesetzes sind nämlich nur Schüler zur Teilnahme an Schulgesundheits- und Schuleignungsuntersuchungen verpflichtet. Kinder, die noch keine Schule besuchen, sind aber keine Schüler. Natürlich spricht nichts dagegen, wenn die Eltern mit ihrem Kind freiwillig zur Untersuchung kommen, weil so körperliche und geistige Entwicklungsmängel schon vor Eintritt in die Schule festgestellt werden können. Bloß verpflichtet sind sie dazu nicht.

— Freiwilligkeit von Anamnesefragen

Während der Schulzeit besteht die Pflicht, eine ärztliche Untersuchung zu dulden. Dazu gehört allerdings nicht, umfangreiche Anamnesefragen zu beantworten. So können Schulärzte die Eltern nicht zwingen, Angaben

- über alle bisher durchgemachten Krankheiten des Kindes und seiner Entwicklungsfortschritte,
- Erkrankungen der Mutter und Komplikationen während der Schwangerschaft,
- „besondere" Krankheiten in der Familie,
- Alter der Geschwister und
- Kindergartenbesuch

zu machen. Die allgemein gehaltene, unpräzise Vorschrift des § 91 des Schulgesetzes erlaubt keinesfalls einen so weitgehenden Eingriff in das Persönlichkeitsrecht von Eltern und Kindern. Wäre dem nicht so, könnte man mit ihr unter Hinweis auf die ärztliche Anamnese fast beliebige Fragen nach den Lebensumständen und den Familienverhältnissen stellen. Kurzum: Die Beantwortung von Fragen der Anamnese steht den Eltern frei.

— Zweck der Schulgesundheitsuntersuchung

Zweck der Schulgesundheitsuntersuchung ist, gesundheitliche Gefährdungen des einzelnen Schulkindes zu erkennen und seinen Eltern gegebenenfalls zu sagen, daß sich eine Behandlung empfiehlt. Die angefallenen Untersuchungsdaten dürfen die Gesundheitsämter unter Wahrung der gebotenen Anonymität für statistische Zwecke auswerten. Dabei sollten sie einen Ratschlag beherzigen, den das königlich württembergische Ministerium des Innern in seinem Erlaß vom 15. April 1913 gab:

> „... die Schulärzte haben bei ihrer Tätigkeit sich gegenwärtig zu halten, daß nicht die Gewinnung einer möglichst einwandfreien Statistik die Hauptsache ist, sondern, daß es vor allem darauf ankommt, solche Maßnahmen vorzuschlagen, die geeignet sind, die der Gesundheit der Jugend drohenden Gefahren abzuwenden oder die Gesundheitsverhältnisse des heranwachsenden Geschlechts zu verbessern. Der Schularzt wird eine um so ersprießlichere Wirksamkeit entfalten können, je mehr es ihm gelingt, das Vertrauen der Eltern, Lehrer und Gemeindeverwaltungen zu erwerben. Nur wenn er sich dieses Vertrauens erfreuen darf, werden seine Ratschläge die gehörige Beachtung finden."

Dies alles machte ich dem Sozialministerium deutlich. Es will nun entgegen seiner früheren Vorstellung die Eltern auf die Freiwilligkeit der Anamnesefragen aufmerksam machen und geeignete Maßnahmen treffen, daß die Gesundheitsämter nur solche Befunddaten zur zentralen Auswertung weitergeben, die anonymisiert sind.

2.2 Die amtsärztliche Untersuchung

In der Vergangenheit mußten wir uns immer wieder damit beschäftigen, wie die Gesundheitsämter beim Erstellen amtsärztlicher Zeugnisse vorgehen sollen. Nicht wenige Bedienstete, aber auch Ärzte der Gesundheitsämter und ich meinen, es genüge, wenn die Personalbehörde in der Regel nur das Ergebnis der amtsärztlichen Untersuchung erfahre. Die Personalbehörden argumentieren dagegen anders. Drum

ist so mißlich, daß es bislang keine befriedigende Rechtsvorschrift gibt. Immer wieder hatte das Sozialministerium eine solche angekündigt; doch es folgte nichts. Nun scheint es anders zu werden.

Mir liegt eine Verwaltungsvorschrift des Sozialministeriums über amtsärztliche Untersuchungen im öffentlichen Dienst im Entwurf vor. Sie geht vom Grundsatz aus, daß die Dienststelle, die das amtsärztliche Zeugnis angefordert hat, in der Regel nur eine zusammenfassende gutachtliche Beurteilung erhalten soll. Bei Einstellungsuntersuchungen soll sie nur mit ausdrücklicher Einwilligung des Probanden Einzelbefunde erfahren können. Damit trägt das Sozialministerium meinen, schon im 4. Tätigkeitsbericht dargestellten Überlegungen Rechnung (LT-Drs. 8/4600 S. 93). Gegen verschiedene andere Vorschriften seines Entwurfs mußte ich dagegen Bedenken anmelden: so bezweifle ich, ob es erforderlich und sinnvoll ist, den Amtsarzt zu verpflichten, bei jeder amtsärztlichen Untersuchung unterschiedslos eine umfangreiche, standardisierte Familienanamnese zu erheben. Es soll zum Beispiel jeder angeben müssen, wann und woran seine Großeltern starben. Abgesehen davon, daß viele diese Frage gar nicht zuverlässig beantworten können, scheint mir insgesamt in der Frage der Familienanamnese ein auf den Einzelfall abgestelltes Vorgehen wesentlich angemessener.

Das Sozialministerium ließ auf mein Schreiben vom September 1985, in dem ich ihm meine Bedenken und Vorschläge vortrug, nichts mehr hören. So weiß ich nicht, ob es sie berücksichtigen will. Zu hoffen bleibt dies ebenso wie, daß es bald zu einer einheitlichen datenschutzfreundlichen Praxis im Lande kommt.

2.3 Ein sinnloser Meldedienst

Nicht immer bedenken Gesetzesväter beim Erlaß einer Regelung ausreichend, ob sie damit auch tatsächlich das erreichen, was sie wollen. Ein Musterbeispiel dafür ist die Vorschrift des § 5 Abs. 4 Nr. 4 des Landesmeldegesetzes. Damals — bei ihrem Erlaß — wollte der Landtag etwas Gutes tun und den Katastrophenschutz unterstützen. Er entschied sich deshalb — abweichend vom Regierungsentwurf — dafür, daß das Einwohnermeldeamt bei der Anmeldung auch danach fragen darf, ob der neue Einwohner in einem Heil- oder Heilhilfsberuf ausgebildet ist. Um diese Vorstellungen des Gesetzgebers in die Tat umzusetzen, verpflichtete das Innenministerium durch verschiedene Vorschriften die Einwohnermeldeämter, diese Angaben auch tatsächlich zu erheben und den Gesundheitsämtern alle Personen zu melden, die die Frage nach der Ausbildung in einem Heil- oder Heilhilfsberuf bei der Anmeldung bejahen. Zwar nicht alle, aber doch die meisten Gemeinden kamen, wie befohlen, dieser Aufforderung nach. Die Sache hat jedoch einen Haken: die Gesundheitsämter wissen gar nicht, was sie mit diesen Meldungen anfangen sollen. Da sie aus ihnen nicht ersehen können, ob nun der einzelne Bürger speziell eine Ausbildung zum Arzt, Zahnarzt, Krankengymnasten, Masseur etc. absolviert hat, wie lange die Ausbildung zurückliegt und ob er diesen Beruf überhaupt noch ausübt, sind die Meldungen für die Gesundheitsämter unbrauchbar. Immer wieder sagten sie mir dies. Die Folge davon ist: die Gesundheitsämter legen die Meldungen irgendwo ab, Daten-

friedhöfe entstanden. Sozialministerium und Innenministerium, die ich auf die Sinnlosigkeit dieses Meldedienstes aufmerksam machte, hatten inzwischen ein Einsehen. Das Innenministerium will die Meldebehörden anweisen, von weiteren Mitteilungen an die Gesundheitsämter abzusehen, und bei der nächsten Änderung der Meldeverordnung die Frage nach einer Ausbildung in einem Heil- oder Heilhilfsberuf auf dem Anmeldevordruck streichen.

2.4 Die Liste der Medizinalpersonen

Die Gesundheitsämter in Baden-Württemberg sind in einer wenig beneidenswerten Lage, weil die wichtigsten Rechtsvorschriften für ihre Arbeit noch aus der Zeit des Dritten Reiches stammen. Da damals ganz andere Vorstellungen über die Aufgaben des öffentlichen Gesundheitsdienstes herrschten als heute und sich seitdem auch die rechtlichen Verhältnisse wesentlich gewandelt haben, stehen sie immer wieder vor der Frage, ob bestimmte Regelungen des alten Gesetzes über die Vereinheitlichung des Gesundheitswesens vom 3. Juli 1934 (RGBl. I, S. 351) und der dazu ergangenen Durchführungsverordnungen heute überhaupt noch zu praktizieren sind. Die zwangsläufige Folge solch unzureichender Rechtsgrundlagen sind Rechtsunsicherheit und uneinheitliche Praxis. Dies zeigt sich auch an der „Liste der Medizinalpersonen", die Gesundheitsämter an sich nach § 1 der 3. Durchführungsverordnung zum Gesetz über die Vereinheitlichung des Gesundheitswesens zu führen haben.

Schon 1980 stellte ich bei Kontrollbesuchen der Gesundheitsämter fest, daß die einzelnen Ämter bei der Führung dieser Listen sehr unterschiedlich vorgehen. Vor allem waren sie sich sehr unsicher, welchen Zweck diese Listen haben und wie sie an die zu deren Führung notwendigen Informationen gelangen können. Dementsprechend unterschiedlich war auch die Intensität, mit der sie sich mit der Führung dieser Listen abgaben. Schon damals sagte mir das Sozialministerium zu, es werde der Frage nachgehen, ob und inwieweit die Gesundheitsämter überhaupt noch an der „Uberwachung von Medizinalpersonen" mitzuwirken haben und ob, wenn ja, dafür eine gesetzliche Meldepflicht eingeführt werden soll. Offensichtlich erwies sich diese Prüfung als sehr schwierig: sie war 1985 immer noch nicht abgeschlossen. Statt dessen sammelten die Gesundheitsämter die Daten von Medizinalpersonen in allerdings unterschiedlichem Maße munter weiter. Weil inzwischen klar war, daß die „Medizinalpersonen" selbst dem Gesundheitsamt nichts melden müssen, wandte sich eine Reihe von Gesundheitsämter an Krankenhäuser und Kliniken und holte dort Auskünfte über deren Beschäftigte ein, um die Liste der Medizinalpersonen richtig zu führen. Genau so kann es nicht gehen: hiermit greifen die Gesundheitsämter in das informationelle Selbstbestimmungsrecht dieser Personen ein, ohne dafür gesetzlich ermächtigt zu sein. Eine solche Rechtsnorm zu schaffen, halte ich, nachdem eigentlich niemand so recht weiß, was die „Liste der Medizinalpersonen" soll, für recht problematisch. Ich trug dies alles an das Sozialministerium heran. Es hatte ein Einsehen mit den Gesundheitsämtern und mit den Angehörigen der Berufe des Gesundheitswesens: es will die Gesundheitsämter jetzt endlich anweisen, bis auf weiteres keine Listen über „Medizinalpersonen" mehr zu führen.

3. Sonderregister über psychisch Kranke beim Einwohnermeldeamt

Als mir eines Tages eine Bürgerin schrieb, das Einwohnermeldeamt von Bad Schussenried führe eine Spezialkartei über psychisch Kranke, wollte ich dies zunächst nicht recht glauben. Doch ein Kontrollbesuch vor Ort belehrte mich eines anderen.

3.1 Bisheriges Verfahren

Das Psychiatrische Landeskrankenhaus Bad Schussenried meldete alle Patienten, die sich seit mindestens 6 Monaten bei ihm aufhalten, auf einer Sammelliste dem Einwohnermeldeamt Bad Schussenried. Ehe es dies jeweils tat, befragte es zwar seine Patienten per Vordruck, ob sie sich selbst anmelden wollen oder ob es dies für sie tun soll. Kreuzte der behandelnde Arzt auf dem Vordruck die Rubrik „Patient ist geschäftsfähig, weigert sich aber, die Anmeldung durchzuführen" an, meldete das Psychiatrische Landeskrankenhaus diesen Patienten trotzdem. Die Anschrift der Patienten gab es jeweils mit „Klosterhof PLKH 1" an; andere Personen, z. B. Pfleger und Ärzte, die ebenfalls im Psychiatrischen Krankenhaus wohnten, erhielten diesen Zusatz nicht; ihre Adresse lautete korrekt „Klosterhof 1".

Die Gemeinde Bad Schussenried speicherte die Daten der gemeldeten Patienten mit dem Adreßzusatz „PLKH" in ihrem automatisierten Melderegister. Ihr Rechenzentrum — der Zweckverband Interkommunale Datenverarbeitung Ulm — druckte ihr über jeden Einwohner eine Karteikarte aus. Diese stellte die Gemeinde Bad Schussenried in ihr parallel zum automatisierten Melderegister geführtes manuelles Melderegister ein — es sei denn, es war die Kartei eines Patienten des Psychiatrischen Landeskrankenhauses. Diese Ausdrucke, die alle auch den Zusatz „PLKH" enthielten, kamen jeweils in das Sonderregister des Einwohnermeldeamts über psychisch Kranke. Ergänzend dazu führte die Gemeinde auch noch eine Sonderkartei der verstorbenen oder verzogenen Patienten des Psychiatrischen Landeskrankenhauses.

Nicht genug damit: Die Gemeinde Bad Schussenried und das Psychiatrische Landeskrankenhaus verglichen in regelmäßigen Abständen ihre Datenbestände. Zu diesem Zweck erstellte der Zweckverband Interkommunale Datenverarbeitung Ulm im Auftrag der Gemeinde aus dem automatisierten Melderegister eine Liste aller gemeldeten Patienten. Dies ging recht einfach, weil er bloß die Personen ausdrukken mußte, deren Adresse mit dem Zusatz „PLKH" versehen war. Das Psychiatrische Landeskrankenhaus ließ sich zu diesem Zweck aus seiner Patientenstammdatei eine Patientenliste ausdrucken. Beide Listen glich man ab.

Dies alles geschah, weil es angeblich der Gemeinde die Verwaltungsarbeit erleichterte.

3.2 Meine Bewertung

Das geschilderte Vorgehen verstieß in mehrfacher Hinsicht gegen den Datenschutz.

— Zwar ist das Psychiatrische Landeskrankenhaus nach § 25 Abs. 1 Satz 3 des Meldegesetzes gehalten, Patienten

nach 6 Monaten Aufenthalt anzumelden, wenn diese selbst wegen Krankheit oder Gebrechlichkeit dazu nicht in der Lage sind. Es muß jedoch dabei den Willen des Patienten respektieren. Ist der Patient in der Lage, sich anzumelden, tut dies aber nicht, hat das Psychiatrische Landeskrankenhaus lediglich die nach § 19 des Meldegesetzes jedem Wohnungsgeber obliegende Anzeigepflicht.

Ebenso war nicht korrekt, bei der Adresse der Patienten den Zusatz „PLKH" aufzuführen. Dieser Zusatz ist kein Teil der Anschrift, sondern lediglich ein Erkennungsmerkmal für Patienten. Es geht nicht an, auf diese Weise Patienten zu brandmarken.

— Das Einwohnermeldeamt durfte den Zusatz „PLKH" selbstverständlich nicht im automatisierten Melderegister speichern. Erst recht ging wegen des besonderen Schutzes, den psychisch Kranke genießen, nicht an, über sie Sonderregister anzulegen.

— Auch der Abgleich der Patientendaten zwischen Psychiatrischem Landeskrankenhaus und Gemeinde verstieß gegen das Meldegesetz. Ein solcher Abgleich ist dort nicht vorgesehen; auch ist er nicht notwendig. Wenn das Psychiatrische Landeskrankenhaus die ihm nach dem Meldegesetz obliegende Pflicht zur Anmeldung als Wohnungsgeber korrekt erfüllt, kann die Gemeinde auch ohne solchen Datenabgleich prüfen, ob ihm alle meldepflichtigen Patienten tatsächlich gemeldet sind.

Auf meine Beanstandungen hin reagierten das Psychiatrische Landeskrankenhaus und die Gemeinde Bad Schussenried sehr aufgeschlossen. Die festgestellten Mängel sind inzwischen behoben: vor allem ist das Brandmal „PLKH" im Melderegister gelöscht; auch gibt es keine Spezialregister über psychisch Kranke mehr.

4. Gesetzliche Krankenversicherung

Nahezu 90 % der Bevölkerung sind berechtigt, Leistungen der gesetzlichen Krankenversicherung in Anspruch zu nehmen. Deshalb ist von besonderem Interesse, wie unsere Krankenkassen mit den Daten der Versicherten, Beitragspflichtigen und Leistungserbringer umgehen.

4.1 Der Online-Anschluß

Die Krankenkassen erledigen schon seit längerer Zeit viele ihrer Aufgaben mit Hilfe der automatischen Datenverarbeitung. Dazu nehmen sie in aller Regel die Dienste ihrer Landesverbände in Anspruch. Diese haben nach § 414 c RVO die Aufgabe, ihre Mitglieder unter anderem durch Entwicklung und Abstimmung von Verfahren und Programmen für die automatische Datenverarbeitung und den Betrieb von Rechenzentren zu unterstützen. Da die gesetzlichen Krankenkassen in großen Mengen sehr sensible Daten von Versicherten und Beitragspflichtigen verarbeiten, hielten wir für nötig, uns durch einen Kontrollbesuch bei einem Landesverband — dem Verband der Ortskrankenkassen Südwest — ein Bild vor Ort über dessen Vorgehen zu verschaffen. Dieser Verband betreibt in Sigmaringen und in Lahr zwei

Rechenzentren. Ihnen sind insgesamt 21 Ortskrankenkassen aus den Regierungsbezirken Tübingen und Freiburg angeschlossen. Beim Kontrollbesuch stellte sich vor allem folgende Problematik:

— In den Rechenzentren kommt das unter der Federführung des Bundesverbandes der Ortskrankenkassen entwickelte EDV-Verfahren IDVS II zum Einsatz. Dieses sieht vor, daß die Daten aller einem Rechenzentrum angeschlossenen Kassen in einem gemeinsamen Datenbestand geführt werden. Jede dem Rechenzentrum angeschlossene Krankenkasse kann auf die meisten Daten aller übrigen Krankenkassen direkt zugreifen. So kann zum Beispiel die AOK Konstanz unter anderem folgende Daten eines bei der AOK Waldshut Versicherten abfragen:

  — Name, Anschrift, Geburtsdatum des Versicherten,
  — Betriebsnummer des Arbeitgebers,
  — Grad der Minderung der Erwerbsfähigkeit,
  — Art und Zeitpunkt der ausgestellten Krankenscheine,
  — Zeiten der Arbeitsunfähigkeit,
  — Krankenhausdaten (u. a. Beginn und Ende der Behandlung),
  — Leistungsart bei Sachleistungen (z. B. Schwangerschaftsgymnastik, Armprothese oder Stützmieder).

  Als Begründung für diesen umfassenden Direktzugriff nannte der Verband beim Kontrollbesuch Zweckmäßigkeitsüberlegungen. So könnte man auf diese Weise z. B. bei einem Wechsel der Kassenzugehörigkeit Vorerkrankungszeiten einfach feststellen; Rückfragen bei der bisherigen Krankenkasse würden sich erübrigen.

— Dieser Direktzugriff widerspricht dem Sozialgeheimnis im Sinne von § 35 des Zehnten Buchs des Sozialgesetzbuchs (SGB X). Nach dieser Bestimmung hat jeder Anspruch darauf, daß die einzelnen Sozialleistungsträger — sprich Krankenkassen — die Einzelangaben über seine persönlichen und sachlichen Verhältnisse als Sozialgeheimnis wahren und nicht unbefugt offenbaren. Gerade letzteres ist aber der Fall: Denn bei den vom Verband der Ortskrankenkassen eingesetzten EDV-Verfahren offenbart eine Ortskrankenkasse alle Daten, auf die ein Direktzugriff besteht, auch den anderen, demselben Rechenzentrum angeschlossenen Ortskrankenkassen. Eine solche umfassende Offenbarung ist nicht befugt, weil keiner der in den §§ 65 bis 77 SGB X im einzelnen geregelten Offenbarungstatbestände erfüllt ist. Insbesondere sind die Voraussetzungen des § 69 Abs. 1 Nr. 1 SGB X nicht gegeben. Danach ist nämlich eine Offenbarung von Daten nur zulässig, soweit dies tatsächlich zur Erfüllung einer Aufgabe nach dem Sozialgesetzbuch erforderlich ist. So ist es aber hier nicht: es steht vielmehr von vornherein objektiv fest, daß die anderen Ortskrankenkassen weitaus die meisten Daten, auf die sie Online zugreifen können, nicht zur Erfüllung ihrer Aufgaben benötigen. Für eine Ortskrankenkasse können allenfalls einzelne, von einer anderen Ortskrankenkasse gespeicherte Daten solcher Personen von Interesse sein, die jetzt bei ihr ver-

sichert sind. In allen anderen Fällen, in denen ein solcher Wechsel der Kassenzugehörigkeit nicht stattfand, besteht nicht die geringste Notwendigkeit für eine Offenbarung an andere Ortskrankenkassen.

In meinem Prüfbericht machte ich den Landesverband Südwest auf diese Rechtslage aufmerksam und forderte ihn auf, das den Kassen zur Verfügung gestellte EDV-Verfahren baldmöglichst so abzuändern, daß kein Direktzugriff auf Daten anderer Krankenkassen mehr besteht. Seine Reaktion war bisher jedoch enttäuschend. Er verwies in seiner Antwort lediglich darauf, daß es sich bei dem Verfahren IDVS II um ein bundeseinheitliches AOK-Programmpaket handele, das unter Federführung des Bundesverbands der Ortskrankenkassen entwickelt worden sei. Er habe meine Bedenken an den Bundesverband der Ortskrankenkassen weitergeleitet. Damit macht sich der Landesverband die Sache etwas zu leicht. Auch er ist dafür verantwortlich, daß seine Mitgliedskassen nur solche EDV-Verfahren einsetzen, bei denen die Einhaltung der Vorschriften über den Datenschutz gewährleistet ist. Dem kann er sich nicht durch einen Verweis auf seinen Bundesverband entziehen.

4.2 Der Mutterpaß

Wer Sozialleistungen beantragt, muß dabei regelmäßig Nachweise vorlegen. Nicht selten sind dies Urkunden, die man aus einem ganz anderen Anlaß erstellte und die deshalb auch Informationen enthalten, die den Sozialleistungsträger überhaupt nicht zu interessieren haben. Welche Probleme mit dem Datenschutz es dabei geben kann, zeigt ein Vorgang bei der Ortskrankenkasse Reutlingen, über den mich ein Arzt informierte. Diese Krankenkasse forderte Mütter, die nach der Entbindung den in § 198 RVO vorgesehenen Pauschbetrag von 100 DM in Anspruch nehmen wollten, dazu auf, den Mutterpaß vorzulegen. Damit sollten sie nachweisen, daß sie sich den in den Mutterschaftsrichtlinien vorgesehenen Vorsorgeuntersuchungen unterzogen hatten. § 198 RVO macht davon die Zahlung des Pauschbetrags abhängig.

Muß die Mutter in solchen Fällen überhaupt einen besonderen Nachweis erbringen? — war die erste Frage, die mich beschäftigte. Ortskrankenkassen müssen sich — wie alle anderen Sozialleistungsträger auch — keinesfalls alles und jedes nachweisen lassen. Vielmehr steht es nach §§ 20, 21 SGB X in ihrem pflichtgemäßen Ermessen, ob und welche Beweise sie zur Ermittlung des Sachverhalts einsetzen wollen. Dabei ist der Grundsatz der Verhältnismäßigkeit zu beachten: es muß also die durch die Beweiserhebung eintretende Belastung in einem angemessenen Verhältnis zu dem mit ihr angestrebten Zweck stehen. Mißt man den Vorgang an diesem Maßstab, so meine ich, reicht es aus, weil es um einen relativ geringen Pauschbetrag geht, wenn sich die Ortskrankenkasse von der Mutter bestätigen läßt, daß sie sich den notwendigen Vorsorgeuntersuchungen unterzog. Da der Arzt die einzelnen Untersuchungen der Mutter jeweils mit der Krankenkasse abrechnet, dürfte die Wahrscheinlichkeit, daß die Mutter eine unrichtige Versicherung abgibt, gering sein. Für ein solches Vorgehen spricht auch, daß nach den Feststellungen der Krankenkasse ca. 90 % der Frauen die Vorsorgeuntersuchungen in Anspruch nehmen.

Meint man gleichwohl, eine solche Bestätigung durch die Mutter reiche nicht, stellt sich die weitere Frage, ob die Ortskrankenkasse auf der Vorlage des Mutterpasses bestehen oder ob die Mutter den gewünschten Nachweis nicht auch auf andere Weise erbringen kann — etwa durch die Vorlage einer Bescheinigung des Vorsorgearztes. Dies ist uneingeschränkt zu bejahen: ein Mutterpaß kann nämlich eine ganze Reihe sehr sensibler Angaben enthalten, die für die Gewährung des Pauschbetrags ohne jede Bedeutung sind. Es wäre unverhältnismäßig und damit unzulässig, wenn eine Versicherte gezwungen wäre, solche Angaben zu offenbaren, wenn sie den Nachweis auf für sie schonendere Art und Weise führen könnte. Kurzum: Die Krankenkassen sollten den Müttern überlassen, welchen Weg sie wählen.

Die Ortskrankenkasse Reutlingen zeigte Verständnis für diese Überlegungen. Sie verzichtete sofort auf die Vorlage des Mutterpasses und begnügt sich jetzt mit der Erklärung der Mutter, daß sie regelmäßig an den Vorsorgeuntersuchungen teilnahm.

4.3 Offenbarung von Sozialdaten an Gerichte

Sozialdaten genießen zu Recht einen besonderen Schutz. Sozialleistungsträger müssen sie grundsätzlich geheim halten; sie dürfen sie nur unter den Voraussetzungen der §§ 67 bis 77 des Zehnten Buchs des Sozialgesetzbuchs (SGB X) Dritten offenbaren. Leider verkennen sie und manche Gerichte, daß sich daraus auch Beschränkungen bei einer Weitergabe von Informationen an Gerichte ergeben können. Die weitverbreitete Übung von Sozial- und Jugendämtern, unterschiedliche Verwaltungsvorgänge in einer Akte zusammenzufassen, weil sie sich auf dieselbe Person oder Familie beziehen, führt allzu oft dazu, daß sie bei Rechtsstreitigkeiten über Sozialleistungen den Gerichten auch Unterlagen vorlegen, die für die Entscheidungsfindung des Gerichts völlig unerheblich sind. Darüber hinaus müssen Sozialleistungsträger bei Rechtsstreitigkeiten das Sozialgeheimnis auch bei ihrem Sachvortrag beachten. Daß dies nicht immer geschieht, zeigt folgender Fall:

Die AOK Schwäbisch Gmünd wollte sich nicht damit abfinden, daß die bisher bei ihr versicherten Mitarbeiter einer im Bauhandwerk und Straßenbau tätigen Firma nach deren Aufnahme in die Bauhandwerks-Innung bei der Innungskrankenkasse Schwäbisch Gmünd versichert sein sollten. Sie erhob deshalb beim Sozialgericht Feststellungsklage über die Krankenkassenzugehörigkeit gegen die IKK Schwäbisch Gmünd und machte geltend, die Voraussetzungen für die Aufnahme der Firma in die Bauhandwerks-Innung seien nicht vorgelegen; deshalb seien die Mitarbeiter der Firma nach wie vor bei ihr versichert. Im Rahmen dieses Rechtsstreits legte die AOK Schwäbisch Gmünd dem Sozialgericht eine Lohnsummenliste mit Informationen über die Mitarbeiter der Firma vor. Aus dieser Liste waren Name, Geburtstag, Art der Beschäftigung, Dauer der Beschäftigung im Jahr 1983 und die in dieser Zeit erhaltene Lohnsumme jedes Mitarbeiters zu ersehen. Die AOK Schwäbisch Gmünd hatte diese Information der Jahresmeldung entnommen, die ihr die Firma nach § 5 der Zweiten Datenerfassungs-Verordnung (2. DEVO) für Zwecke der Sozialversicherung erstatten

mußte. Die Vorlage dieser Lohnsummenliste an das Sozialgericht hatte die weitere Folge, daß auch die Mitarbeiter der Firma, die am Prozeß als Beigeladene beteiligt waren, erfuhren, wieviel ihre Kollegen im einzelnen verdienen.

Dieses Vorgehen der AOK Schwäbisch Gmünd mußte ich nach § 18 Abs. 1 LDSG aus folgenden Gründen beanstanden: Das Sozialgesetzbuch erlaubt nur, im gerichtlichen Verfahren Sozialdaten zu offenbaren, soweit dies zur Durchführung des Verfahrens tatsächlich erforderlich ist. Erforderlich ist nur, was bei objektiver Würdigung der Rechtslage unter Berücksichtigung des Grundsatzes der Verhältnismäßigkeit für die Entscheidung des Gerichts erheblich sein kann. Das war die Lohnsummenliste sicher nicht. Für die Entscheidung über die Feststellungsklage war allenfalls bedeutsam, welche Berufsgruppen im Betrieb der Firma vertreten sind, wie viele Mitarbeiter den einzelnen Berufsgruppen angehören und wie sich die Lohnsummen zusammensetzen. Davon ging im Grund auch die AOK Schwäbisch Gmünd aus. Allerdings glaubte sie, gleichwohl zur Vorlage der Lohnsummenliste berechtigt zu sein, weil sie damit die Richtigkeit ihrer Angaben über die Berufsgruppen beweisen wollte. Dem steht entgegen, daß im Verfahren vor dem Sozialgericht der Amtsermittlungsgrundsatz gilt und es deshalb in erster Linie Sache des Gerichts ist, die erforderliche Sachaufklärung zu betreiben, über die Beweisbedürftigkeit der Angaben der Prozeßbeteiligten zu entscheiden, die Beweismittel zu bestimmen und gegebenenfalls Beweise zu erheben. Dies schließt zwar nicht aus, daß Prozeßbeteiligte von sich aus Beweise vorlegen. Zu weit ginge freilich, gewissermaßen auf Verdacht zum Beweis für die Richtigkeit eines Parteivortrags Sozialdaten in großem Umfang und von großer Sensibilität zu offenbaren — vor allem dann, wenn der Parteivortrag von den übrigen Prozeßbeteiligten ohnehin kaum zu bestreiten ist. Schon der Grundsatz der Verhältnismäßigkeit verlangt zunächst abzuklären, ob das Gericht den vorgetragenen Sachverhalt überhaupt für beweisbedürftig hält und, wenn ja, welche Beweismittel es als geeignet ansieht. Dazu bestand um so mehr Anlaß, als die AOK Schwäbisch Gmünd wegen § 108 des Sozialgerichtsgesetzes damit rechnen mußte, daß diese Sozialdaten allen Verfahrensbeteiligten — auch den beigeladenen Mitarbeitern der Firma — bekannt werden.

Die AOK Schwäbisch Gmünd war über meine Beanstandung sehr betroffen: Sie bedauerte den Vorfall, sieht die Rechtslage inzwischen so wie ich und will sie bei künftigen Verfahren vor Sozialgerichten berücksichtigen.

4.4 Verhindert der Sozialdatenschutz das Aufdecken von Manipulationen?

Hin und wieder werden Befürchtungen laut, der Datenschutz verhindere im Bereich der gesetzlichen Krankenversicherung die gebotene Aufklärung und Ahndung von Manipulationen. Daß dem jedoch keineswegs so ist, zeigt folgender Fall:

Ein Apotheker war in den Verdacht geraten, gemeinsam mit Kassenärzten betrügerische Manipulationen begangen zu haben. Daraufhin leitete die Apothekerkammer ein standes-

rechtliches Ermittlungsverfahren gegen den Apotheker ein. In dessen Verlauf bat ihr Kammeranwalt die Kassenärztliche Vereinigung, ihr die Unterlagen zur Verfügung zu stellen, die sie im Rahmen ihrer Ermittlungen gegen die beteiligten Kassenärzte gesammelt hat. Die Kassenärztliche Vereinigung wandte sich an mich und wollte meinen Rat. Der sah so aus:

Ich hatte keine Bedenken gegen die Herausgabe dieser Unterlagen. Denn die Bestimmungen zum Schutz des Sozialgeheimnisses lassen jedenfalls dann, wenn ein hinreichend konkreter Verdacht der betrügerischen Zusammenarbeit zwischen Kassenärzten und Apotheker besteht, dies zu. Rechtsgrundlage dafür ist § 69 Abs. 1 Nr. 1 SGB X, wonach eine Kassenärztliche Vereinigung Sozialdaten offenbaren darf, soweit dies zur Erfüllung einer gesetzlichen Aufgabe nach dem Sozialgesetzbuch erforderlich ist. So war es hier: Die Kassenärztlichen Vereinigungen haben nämlich nach § 368 n RVO unter anderem die Aufgabe, gegenüber den Krankenkassen und ihren Verbänden die Gewähr dafür zu übernehmen, daß die kassenärztliche Versorgung den gesetzlichen und vertraglichen Erfordernissen entspricht. Zur kassenärztlichen Versorgung zählt dabei unter anderem auch die Verordnung von Arznei- und Heilmitteln. Folglich ist es eine Aufgabe der Kassenärztlichen Vereinigungen, daran mitzuwirken, daß Ärzte nur notwendige Arzneimittel verordnen. Im Rahmen dieser Aufgaben kann es sehr wohl im Sinne von § 69 Abs. 1 Nr. 1 SGB X erforderlich sein, Polizei und Staatsanwaltschaft Auskünfte für Zwecke strafrechtlicher Ermittlungsverfahren zu geben. Dies ist allgemein anerkannt. Daneben kommt aber auch die Einleitung oder Unterstützung von berufsgerichtlichen Verfahren in Betracht. Auch solche Verfahren können dazu beitragen, daß die Regelungen der Reichsversicherungsordnung über die Versorgung mit Arzneimitteln beachtet und die Versichertengemeinschaft vor einer unberechtigten Inanspruchnahme geschützt wird. Daran vermag auch der Umstand nichts zu ändern, daß sich das berufsgerichtliche Verfahren nicht gegen einen Kassenarzt, sondern gegen einen Apotheker richtet. Zumindest dann, wenn der konkrete Verdacht einer betrügerischen Zusammenarbeit zwischen Kassenarzt und Apotheker besteht, kann die Einleitung oder Unterstützung eines berufsgerichtlichen Verfahrens gegen den beteiligten Apotheker eine notwendige Maßnahme zur Erfüllung der Aufgaben der Kassenärztlichen Vereinigung sein. Auch ein solches Verfahren kann dazu beitragen, gemeinsame Manipulationen von Kassenarzt und Apotheker zu unterbinden. Schließlich ist zu bedenken: Die Kassenärztlichen Vereinigungen sind wie die Krankenkassen und die Kassenärzte am Gesamtsystem der gesetzlichen Krankenversicherung beteiligt. Dieses System kann seiner Aufgabe nur gerecht werden, wenn sich alle Beteiligten an die dafür bestehenden Regelungen halten und gegen Verstöße mit den ihnen zur Verfügung stehenden Mitteln vorgehen. Insbesondere haben sie alles zu tun, um zu verhindern, daß die Versichertengemeinschaft durch Manipulationen geschädigt wird.

7. Teil: Der Mitarbeiter im öffentlichen Dienst

1. Personaldatensysteme

Die Personaldatensysteme der öffentlichen Verwaltung sind über ihre ursprüngliche Aufgabe, die Bezüge der Bediensteten zu berechnen und auszuzahlen, längst hinausgewachsen. Mit allen Systemen neueren Datums können die Behörden die wichtigsten Aufgaben der Personalverwaltung erledigen, z. B. Beurlaubungen, Versetzungen, Beförderungen und Ernennungen verfügen, Teilzeitbeschäftigung sowie Arbeits- und Dienstjubiläen berechnen und — seien es standardisierte, seien es spontan formulierte — Abfragen und Auswertungen machen. Zwei Personaldatensysteme — das automatisierte Verfahren zur Unterstützung der personalverwaltenden Stellen der Oberfinanzdirekion Freiburg (UPS) und das Personal- und Stellenverwaltungssystem am Arbeitsplatz (PSA) für die Universitäten — kann man auch bei Bewerbungen einsetzen: sie bestätigen dem Bewerber den Eingang seiner Bewerbung, erstellen Übersichten zur Vorbereitung der Bewerbergespräche und drucken Listen der nicht zum Zuge gekommenen Bewerber aus.

Wer die Personaldatensysteme in der Wirtschaft kennt, mag dies als klein, unbedeutend und problemlos abtun: die Reizworte „Zeiterfassungssystem, Kantinen- und Tankabrechnungssystem und EDV-Systeme zur Personalentwicklung, -planung und -betreuung mit Schulungsergebnissen und Beurteilungen" tauchen hier nicht auf. Der Eindruck täuscht jedoch: auch einige Personaldatensysteme der öffentlichen Hand registrieren Beurteilungsnoten und sind für Zwecke der Personalentwicklung und -planung konzipiert. Ein Beleg dafür ist die Reaktion des Kultusministeriums auf meine — inzwischen erfüllte — Forderung, seinen Online-Anschluß an die Lehrerdatenbank der Oberschulämter aufzuheben: „Das Ministerium hat ständig eine Vielzahl von Personalentscheidungen aller Art zu treffen, für deren Vorbereitung die schnelle Aufbereitung von entscheidungserheblichen Daten unerläßlich ist." Kein Wunder also, daß es beim Einsatz dieser leistungsfähigen Systeme Probleme gibt.

1.1 Lehrerdatenbank

Der Aufbau der Lehrpersonendateien bei den einzelnen Oberschulämtern, über die ich schon berichtete, schreitet weiter fort. Ein Kontrollbesuch beim Oberschulamt Karlsruhe zeigte, daß das System immer noch nicht ausgereift ist.

1.1.1 Direktzugriff der Oberschulämter

Wenn ein Oberschulamt einen Lehrer neu in die Lehrpersonendatei aufnimmt, erhält er eine Identnummer. Gleichzeitig kommt er mit folgenden Daten in die Identnummerndatei:

- Identnummer
- Kennzeichen für das Oberschulamt, das den Lehrer betreut oder betreute,
- Abteilung des Oberschulamts, das den Lehrer betreut oder betreute,
- Personalnummer des Landesamtes für Besoldung und Versorgung ohne Sachgebietsangabe
- Familienname
- Vorname
- Geburtsdatum.

Auf all diese Angaben kann nicht nur das Oberschulamt zugreifen, in dessen Bezirk der Lehrer tätig ist. Auch die Personalsachbearbeiter der übrigen Oberschulämter können sie „online" abrufen. Wenig überzeugend war, was das Oberschulamt Karlsruhe beim Kontrollbesuch dazu sagte: Man könne damit schnell feststellen, ob ein anderes Oberschulamt Personalakten über den Lehrer führe; auch sei einfacher, bei fehlgeleiteten Schreiben an Lehrer ihr jeweiliges Oberschulamt ausfindig zu machen.

Das kann freilich kein Grund für einen so umfassenden Datenzugriff sein. Weil die Oberschulämter nur jeweils für die Lehrer ihres Bezirks zuständig sind, lassen ihn die Datenschutzgesetze nicht zu. Ich forderte deshalb im Sommer 1985 das Oberschulamt Karlsruhe auf, den Online-Zugriff umgehend aufzuheben. Eine Antwort steht noch aus.

1.1.2 Berichtigung der gespeicherten Lehrerdaten

Die in der Lehrerdatenbank über die einzelnen Lehrer gespeicherten Angaben sind in der Mehrzahl der Fälle unvollständig oder unrichtig. Das Oberschulamt Karlsruhe sagte uns beim Kontrollbesuch im April 1985, daß bei ca. 90 % aller Lehrer die Zeitangaben über „Beschäftigung", „Dienststelle der Person", „Status" und „Funktionen" nicht stimmen. Grund dieses erstaunlichen Phänomens ist: alle Oberschulämter entschieden sich 1982 beim Aufbau der Lehrpersonendatei dafür, bei einigen Zeitangaben, die ihnen das Landesamt für Besoldung und Versorgung nicht auf Magnetband liefern konnte, kurzerhand stets den 1. März 1982 zu speichern. Praktisch sah das so aus: Eine Lehrerin wurde am 8. September 1980 zur Studienassessorin ernannt; die Lehrpersonendatei speicherte dagegen als Datum ihrer Ernennung den 1. März 1982. Alle Oberschulämter sind gegenwärtig dabei, anhand der Personalakten die Daten jedes einzelnen Lehrers zu überprüfen und erforderlichenfalls zu berichtigen. Weil dies sehr aufwendig ist, werden sie damit kaum vor Mitte 1986 fertig. Solange aber dürfen die Oberschulämter die falschen Daten nicht weiter speichern; sie müssen — das verlangt § 27 BDSG — sofort alle unrichtigen Zeitangaben löschen. Dies forderte ich bereits im Juni 1985 vom Kultusministerium. Trotz mehrerer Mahnungen hat es mir bislang nicht geantwortet.

1.1.3 Automatisierte Protokolle unerläßlich

Der Computer des Oberschulamts Karlsruhe kann — so meinte das Amt — trotz seiner großen Leistung nicht protokollieren, welche Programme wann ablaufen und was sie machen. Um dennoch später wenigstens sagen zu können, welche Auswertungen er wann erstellte, führte das Oberschulamt bis zu unserem Kontrollbesuch eine Übersicht von Hand. Diese Verlegenheitslösung hat jedoch zwei Schwachstellen: Zum einen ist nicht sicher, daß diese Übersichten vollständig sind. Zum andern sind sie nicht aussagekräftig genug, weil sie die allermeisten Arbeiten mit dem Computer nicht erfassen. So ersieht man aus ihnen nicht, wann jemand Lehrerdaten kopierte, diese mit anderen Daten

abglich oder wann ein Programm diese veränderte. Weil man das alles aber auch später noch eindeutig feststellen können muß, ist eine exakte Protokollierung unerläßlich. Mein Amt erläuterte dem Oberschulamt Karlsruhe auch, wie es dies mit dem Standardprogramm seines Computers erreichen kann. Leider erfuhr ich auch zu dieser Frage noch nichts.

1.2 PAISY (Personal-Abrechnungs- und administratives Informationssystem)

PAISY ist bekannt als Personaldatensystem, das nahezu jede Abrechnungsart — sei es für Krankenhäuser, Waldarbeiter oder Musiker — beherrscht und unbeschränkt viele Personaldaten verarbeiten kann. Die Stadt Mannheim setzt eine auf ihre Verhältnisse abgestimmte Version von PAISY ein. Damit kann sie die Bezüge ihrer Beamten, Angestellten und Arbeiter abrechnen und dabei unter anderem auch die Mieten für Dienstwohnungen oder Mitgliedsbeiträge zur Gewerkschaft einbehalten. Natürlich unterstützt PAISY auch das Personalamt auf vielfältige Weise. Dieses äußerst flexible und daher nicht leicht durchschaubare System ist allerdings nicht mehr so tüchtig, wenn es darum geht, den Datenschutz zu sichern.

1.2.1 Fehlzeiten

Die Stadt speichert in PAISY Angaben über Fehlzeiten der Bediensteten — z. B. Krankheit, unentschuldigtes Fehlen, unbezahlter Urlaub — und faßt sie in Fehlzeitenlisten zusammen. Diese sind aus technischen Gründen allerdings nicht so gestaltet, daß die Stadt damit arbeiten könnte; im Gegenteil: sie sind unbrauchbar. Man müßte viele dicke EDV-Listen gleichzeitig durchsehen, um den erforderlichen Überblick über die Fehlzeiten zu bekommen. Geeignete Listen kann die Stadt derzeit nicht erstellen. Die Speicherung der Fehlzeiten in PAISY geht folglich zur Zeit ins Leere; sie ist eine unzulässige Vorratsspeicherung. Ich beanstandete deshalb diesen Vorgang und forderte die Stadt auf, die gespeicherten Fehlzeiten unverzüglich zu löschen und die unbrauchbaren Listen umgehend zu vernichten. Letzteres ist geschehen; im übrigen prüft die Stadt immer noch die Rechtslage.

Die Stadt wollte von mir — ungeachtet ihrer gegenwärtigen technischen Schwierigkeiten — wissen, inwieweit es überhaupt angeht, Fehlzeiten automatisiert zu verarbeiten. Dazu ist zu sagen: Grundsätzlich darf ein Arbeitgeber Fehlzeiten für Zwecke des Dienst- und Arbeitsverhältnisses verarbeiten. So kann es für den Arbeitgeber von Interesse sein zu erfahren, ob und — bejahendenfalls — in welchem Umfang Erkrankungen von Mitarbeitern auf betriebliche Ursachen — z. B. die Gestaltung der Arbeitsplätze oder Umwelteinflüsse — zurückzuführen sind. Auch muß der Dienstherr unter Umständen wissen, wann und wie oft ein Mitarbeiter krank ist, um zu verhindern, daß er einen Arbeitsplatz erhält, dessen gesundheitlichen Anforderungen er nicht gewachsen ist. Andererseits darf das automatisierte Verarbeiten von Fehlzeiten nicht dazu führen, daß eine „Jagd" auf häufig erkrankte Mitarbeiter stattfindet.

1.2.2 Sperren von Personaldaten

Sobald die Stadt PAISY so ändert, daß es geeignete Fehlzeitenlisten erstellt, steht sie vor einem neuen Problem: Ihre PAISY-Version kann offenbar Fehlzeitendaten nicht, wie es das Datenschutzrecht fordert, sperren. Gerade aber dies müßte geschehen, wenn etwa ein städtischer Arbeiter aus unbekannten Gründen nicht zum Dienst erscheint, die Stadt daraufhin „unentschuldigt gefehlt von ... bis ..." in PAISY speichert und der Arbeiter danach behaupten würde, er hätte sich vorher doch entschuldigt, nur sei dies offenbar in der Hektik des Geschäfts untergegangen. Man sollte meinen, daß die Stadt in solchen Fällen die registrierte Information „unentschuldigt gefehlt" löschen und eventuell statt dessen „entschuldigt gefehlt" speichern könnte. Dies leistet — so ihre Aussage — ihr PAISY jedoch nicht. Die Stadt speichert vielmehr die Fehlzeiten im Abrechnungsteil von PAISY als Lohnart mit der Folge, daß sie sie wegen dessen Abrechnungssystematik nicht mehr löschen kann, auch wenn man sie gar nicht für die Abrechnung braucht. Die Stadt kann sie nur stornieren, indem sie die gleiche Fehlzeit noch einmal einträgt — aber mit negativem Vorzeichen, damit es sich abrechnungstechnisch ausgleicht. Das freilich ist keine Sperrung oder Berichtigung im Sinne des Datenschutzrechts: ließe sich nämlich die Stadt eine Liste aller Mitarbeiter ausdrucken, die irgendwann einmal unentschuldigt fehlten, erschiene auch unser Arbeiter zu Unrecht in dieser Liste.

1.2.3 Automatisierte Prüfungen unerläßlich

Wer das Personalrecht kennt, weiß, daß es voll komplizierter Vorschriften steckt. Der Computer kann zum Teil überprüfen, ob sie richtig angewandt werden: er vergleicht die Personaldaten miteinander und prüft sie auf ihre Plausibilität. Über 120 mögliche Plausibilitätsprüfungen hat das Personalamt der Stadt Mannheim zusammengestellt. Seine PAISY-Version kann jedoch nur wenige davon durchführen: nicht einmal kontrolliert es die Datenfelder „Eintrittsgrund", „Austrittsgrund" und „Wiedervorlagegrund". Das Risiko, daß die Stadt viele Personaldaten falsch verarbeitet, ist daher hoch. Nachdem ich die Stadt darauf hinwies und die Programmierung dieser über 120 Plausibilitätsprüfungen verlangte, teilte sie mir mit, dies sei ihr mangels Geld und Personal nicht möglich. Sie wolle die Risiken anders in den Griff bekommen: ihr Personalamt werde sich immer wieder EDV-Listen mit Mitarbeiterdaten ausdrucken lassen und diese auf ihre Richtigkeit hin von Hand prüfen. Das ist keine akzeptable Lösung: Zum einen entstehen dabei große Mengen dicker EDV-Listen mit sensitiven Mitarbeiterdaten, die alle sicher verwahrt und später vernichtet werden müssen und somit ein neues Sicherheitsproblem ergeben. Zum andern wirkt die manuelle Kontrolle nicht sofort bei der Dateneingabe, sondern erst Tage oder Wochen danach. Sie verhindert also im Gegensatz zu der automatisierten Prüfung nicht von vornherein die Verarbeitung unrichtiger Daten. Zum dritten ist die manuelle Prüfung anhand von Listen bei weitem nicht so effektiv

wie automatisierte Kontrollen. Ich beanstandete deshalb deren Fehlen nach § 18 Abs. 1 LDSG. Eine Antwort der Stadt liegt mir noch nicht vor.

1.3 PSA (Personal- und Stellenverwaltungssystem am Arbeitsplatz)

PSA ist ein neues Personaldatensystem für die baden-württembergischen Hochschulen. Das Wissenschaftsministerium betreute die Entwicklung. Eine Universität erprobte es bereits. PSA soll die Hochschulen unter anderem bei Berufungs- und Bewerbungsverfahren, Einstellungen, Versetzungen, Kündigungen, der Stellenverwaltung und Statistik unterstützen. Kaum waren die Pläne für PSA bekannt, wandten sich beunruhigte Bürger an mein Amt. So kam es, daß wir uns schon während der Entwicklungsphase mit PSA befaßten. Im wesentlichen ging es um folgendes:

1.3.1 Umgang mit Bewerberdaten

Probleme gab es mit Bewerberdaten:

— Das Wissenschaftsministerium hatte ursprünglich vor, auch den Tag der Eheschließung, der Scheidung oder des Todes des Ehegatten des Bewerbers zu speichern. Dies ging zu weit: Denn der Arbeitgeber „Öffentliche Verwaltung" darf ebenso wie jeder private Arbeitgeber Daten von Bewerbern nur erheben, soweit er sie zur Entscheidung über die Bewerbung benötigt. Das aber trifft hier nicht zu.

— Ursprünglich war nicht klar, ob die Hochschulen — wie die Datenschutzgesetze fordern — den Bewerber über seine Einspeicherung in PSA unterrichten werden. Ich wies das Wissenschaftsministerium auf dieses Erfordernis hin und schlug vor, das Programm so zu gestalten, daß jeder Bewerber nicht nur eine Nachricht über die Tatsache der Speicherung, sondern auch über ihren Zweck und ihre Dauer erhält. Auch sorgte ich dafür, daß die Hochschulen die Daten nicht zum Zuge gekommener Bewerber in PSA unverzüglich löschen.

1.3.2 Fehler beim Einsatz vermeiden

Kritisieren mußte ich, daß ein Zeit- und Aktivitätenplan für den Einsatz des neuen Personaldatensystems bei den Hochschulen fehlte. Dies aber fordert § 8 LDSG vornehmlich aus zwei Gründen: Wenn zum einen die Hochschulen nicht lange vor dem Einsatz wissen, welcher Aufwand auf sie zukommt, können sie sich enorm verschätzen und müssen dann eilig das neue System irgendwie zum Laufen bringen. Wie leicht man hier ein paar Wochen übersieht, zeigt der inzwischen erstellte Zeitplan: Er gibt für den einen Teil von PSA 19 und für den anderen Teil 17 Wochen als Vorbereitungszeit an. Zusammen muß man also über sechs Monate sorgfältig vorausplanen. Weil zum andern Planer und Entwickler von PSA am besten wissen, was die Hochschulen vor einem Einsatz des Systems zu tun haben, müssen sie ihnen dafür auch einen Plan vorlegen. Wie wichtig dies ist, zeigt der mir inzwischen zugegangene „grobe Ak-

tivitätenplan", der 39 Punkte nennt — z. B. Programmtest, Programmfreigabe, Regelung des Datenzugriffs und Schulung.

2. Änderungsmitteilung über persönliche Verhältnisse

Das Landesamt für Besoldung und Versorgung fordert Beamte auf, die Änderung ihrer persönlichen Verhältnisse per Vordruck mitzuteilen. Die Fragen gehen ins Detail: Wer etwa die Geburt eines Kindes anzeigt, muß auch erklären, ob das Neugeborene ehelich ist. Wer weiß, wie kompliziert die Berechnung der Bezüge oder des Kindergeldes ist, bezweifelt nicht, daß hier genaue Fragen zu stellen sind. Zu Recht zweifeln konnte aber ein Lehrer an dem Erlaß des Oberschulamts Tübingen vom 7. Mai 1985, wonach alle Lehrer dem Oberschulamt je eine Durchschrift ihrer Änderungsanzeigen über ihre persönlichen Verhältnisse an das Landesamt für Besoldung und Versorgung zuzusenden haben.

Richtig ist, daß auch das Oberschulamt als Personalbehörde wissen muß, ob sich Name oder Anschrift des Lehrers änderten. Anders sieht die Sache aber aus bei Angaben, die nur für die Berechnung der Bezüge, des Kindergeldes oder der Beihilfen im Krankheitsfall erforderlich sind. Sie gehen die Personalverwaltung nichts an. Zwar führt diese die Hauptpersonalakten. Zu ihnen gehören aber nicht, wie es ausdrücklich in einer Verwaltungsvorschrift des Kultusministeriums heißt, die Besoldungs- und Beihilfeakten. Sie hat allein das Landesamt für Besoldung und Versorgung zu führen. Das Oberschulamt darf deshalb von seinen Lehrern keine Angaben wie Beschäftigungsverhältnis des Ehegatten, Geburtsdatum des geschiedenen Ehegatten, Unterhaltsverpflichtung, Aufnahme von anderen Personen in der Wohnung, Ehelichkeit des Neugeborenen, Aufnahme des Kindes in den Haushalt, Kindergeldbezug und Änderung der Bankverbindung verlangen, weil sie ganz offensichtlich allein für den Bezug von Kindergeld relevant sind.

Auf meine Intervention hin will das Landesamt für Besoldung und Versorgung jetzt seinen Vordruck so gestalten, daß auf der Durchschrift für die personalverwaltende Stelle nur noch die Angaben zu lesen sind, die diese wirklich benötigt. Das Oberschulamt Tübingen dagegen konnte zunächst „nicht erkennen, inwieweit mit dem im Bezug genannten Erlaß Belange des Datenschutzes tangiert worden sind". Ich hoffe, daß sich dies noch ändert und es seinen Erlaß entsprechend der Rechtslage korrigiert.

3. Registrieren von Telefondaten

Das Thema „Registrieren von Telefondaten" bewegt viele Mitarbeiter des öffentlichen Dienstes und Personalräte. Immer wieder erreichen mich Anfragen, ob es denn zulässig sei, daß ihr Dienstherr bei ihren Telefongesprächen nicht nur Datum und Uhrzeit eines Gesprächs und die angefallenen Gebühreneinheiten, sondern auch die angewählte Rufnummer erfaßt. Eine Reihe gegensätzlicher Gerichtsurteile führte dazu, daß von einer gefestigten Rechtsauffassung keine Rede sein kann. So sage ich natürlich den Fragern, wie ich die Dinge sehe, weise jedoch gleichzeitig auf die bestehende Rechtsunsicherheit hin. Ich meine, es gilt folgendes zu unterscheiden:

3.1 Privatgespräche

Ich sehe keine Rechtsgrundlage, die erlauben würde, bei Privatgesprächen die vollständige Rufnummer des Gesprächspartners zu speichern. Gleichwohl geschieht dies bei den meisten Landesbehörden. Eine solche Vorgehensweise ist in der Regel nicht unabweisbar geboten und damit nicht erforderlich im Sinne der Datenschutzgesetze: Um die Telefongebühren für geführte Privatgespräche einziehen zu können, reicht es aus, daß die Abrechnungsstelle Datum und Uhrzeit des Gesprächs, die angefallene Gebühreneinheit und die angewählte Rufnummer ohne die beiden letzten Ziffern kennt. Mit diesen Angaben kann sie in aller Regel die Gespräche in Rechnung stellen und der Mitarbeiter prüfen, ob er das Gespräch tatsächlich geführt hat.

3.2 Dienstgespräche

Anders beurteile ich die Rechtslage bei Dienstgesprächen. Hier läßt sich durchaus die Auffassung vertreten, daß in diesen Fällen auch die Speicherung der Telefonnummer des Gesprächsteilnehmers geboten ist. Denn die Mitarbeiter haben auch beim Telefonieren die Haushaltsgrundsätze der Wirtschaftlichkeit und Sparsamkeit zu beachten. Aufgabe ihrer Dienstvorgesetzten ist andererseits, die Einhaltung dieser Grundsätze zu überwachen. Dafür kann die Registrierung der Telefonnummer des Gesprächsteilnehmers ein geeignetes und notwendiges Mittel sein.

3.3 Sonderfällle

Eine andere Beurteilung erfordern allerdings Dienstgespräche von Institutionen oder Personen, die eine besondere Vertrauensstellung einnehmen. Zu denken ist hier vor allem an den Personalrat. Zwar ist selbstverständlich auch der Personalrat verpflichtet, bei der Nutzung der Fernsprechanlage die Grundsätze der Wirtschaftlichkeit und Sparsamkeit zu beachten. Dies darf aber nicht dazu führen, daß durch die Registrierung seiner Telefonate seine rechtlich garantierte Unabhängigkeit tangiert oder beeinträchtigt wird. Dies aber wäre so, wenn Datum und Uhrzeit seiner Gespräche aufgezeichnet würde. Erst recht unzulässig wäre, wenn dazu auch noch eine Speicherung der Telefonnummer des Gesprächspartners hinzukäme. Denn auf diese Weise könnte die Dienststelle kontrollieren, mit wem der Personalrat Kontakt hatte.

Nicht erlaubt ist auch, bei Dienstgesprächen von Mitarbeitern, die einer besonderen — auch rein behördeninternen — Schweigepflicht unterliegen, die Telefonnummer des Gesprächspartners zu speichern. Dazu zählen vor allem die Mitarbeiter von Beratungsstellen im Sinne von § 203 Abs. 1 Nr. 4 StGB — also Ehe-, Erziehungs- oder Jugendberater. Eine Speicherung und Auswertung dieser Telefonnummern wäre nicht mit deren Geheimhaltungspflichten zu vereinbaren. Der Dienstvorgesetzte könnte dann nämlich erfahren, welche Bürger Kontakte mit den Beratungsstellen hatten. Das darf er aber kraft Gesetzes nicht.

4. Die Trennung von Beihilfestelle und Personalstelle

Wer Beihilfe in Anspruch nehmen will, muß der Beihilfestelle Arztrechnungen, Rezepte, Gutachten und ähnliche Unterlagen

vorlegen. Auf diese Weise erfährt sie teilweise sehr detaillierte Informationen über den Gesundheitszustand und über persönliche Probleme eines Mitarbeiters. Sie muß deshalb diese Informationen geheimhalten und darf sie auch nicht der Personalstelle zur Verfügung stellen. Kommt es bei Personalmaßnahmen auf die gesundheitlichen Verhältnisse eines Mitarbeiters an, dann kann sich die Personalstelle darüber nur insoweit ein Bild verschaffen, als ihr das Beamten- und Tarifrecht dies erlaubt.

Diese Rechtslage würde geradezu konterkariert, wenn ein Dienstherr seine Verwaltung so organisieren würde, daß dieselben Mitarbeiter Personalsachen und Beihilfeangelegenheiten zu bearbeiten, ja gar zu entscheiden hätten. Mit einer solchen Organisation ließe sich nicht verhindern, daß die im Beihilfeverfahren gewonnenen Erkenntnisse über die gesundheitlichen Verhältnisse eines Mitarbeiters in Entscheidungen über Personalmaßnahmen einfließen. Sie ließe sich deshalb nicht mit den Anforderungen vereinbaren, die zum Schutz des informationellen Selbstbestimmungsrechts aller Bediensteten zu stellen sind.

Das alles, meine ich, sollte eigentlich für jedermann einsichtig sein. Leider ist dem nicht so. Bei einer ganzen Reihe von Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts bearbeiten dieselben Mitarbeiter Beihilfe- und Personalangelegenheiten. Um hier Abhilfe zu schaffen, schlug ich dem Finanzministerium in meiner Stellungnahme zum Entwurf eines Gesetzes zur Änderung des Landesbeamtengesetzes (LT-Drs. 9/2434) vor, die Trennung von Beihilfe- und Personalstelle ausdrücklich vorzuschreiben. Leider berücksichtigte das Ministerium bislang meinen Vorschlag nicht.

5. Ärztliche Unterlagen über Polizeibeamte

Ein Polizeibeamter besuchte einen Augenarzt und bekam eine Brille verordnet. Kurze Zeit später stand sowohl in seinem Polizeiführerschein als auch in seiner allgemeinen Fahrerlaubnis der Eintrag: „Der Inhaber dieses Führerscheins muß beim Führen von Kraftfahrzeugen die geeigneten Augengläser tragen." Wie konnte es ohne weiteres Zutun des Beamten zu einer so schnellen Reaktion der Behörden kommen? Meine Ermittlungen ergaben folgendes: Geht ein Polizeibeamter zum Arzt, so hat er in der Regel mit der Abrechnung der Behandlungskosten nichts zu tun, weil sie zwischen den Kassenärztlichen Vereinigungen und den zuständigen Polizeidienststellen — der Landespolizeidirektion, Bereitschaftspolizeidirektion oder Landespolizeischule — erfolgen. Bei der Abrechnung der augenärztlichen Untersuchung des Beamten nutzte die Landespolizeidirektion Karlsruhe die ihr vorgelegten ärztlichen Unterlagen nicht nur für diesen Zweck, sondern unternahm wegen der hierin enthaltenen Informationen über den Gesundheitszustand des Beamten im Rahmen „ihrer Fürsorgepflicht" zur „Gefahrenabwehr" und „zur Arbeitserleichterung für den Polizeibeamten" weitere Schritte. So fragte sie zunächst beim behandelnden Facharzt nach, ob der Beamte die Brille auch beim Führen eines Dienstkraftfahrzeuges tragen müsse. Als sich dies bestätigte, unterrichtete sie hiervon das Polizeipräsidium, bei dem der Beamte seinen Dienst tat. Das Polizeipräsidium trug in den Dienstführerschein die Auflage ein und informierte zudem die Führerscheinbehörde, die dem Polizeibeamten eine entsprechende Auflage erteilte.

Zwar müssen Polizeibeamte gut sehen können. Eine so weitreichende Maßnahme des Dienstherren halte ich aber für unzulässig:

— Die Kassenärztlichen Vereinigungen legen die Arztbelege, Rezepte, Gutachten usw. den Heilfürsorgestellen zur Kostenabrechnung vor. Nur zur Wahrnehmung dieser Aufgabe erhalten die Polizeidienststellen also die ärztlichen Unterlagen. Sie dürfen sie deshalb nicht für etwas anderes verwenden. Tun sie dies nicht, greifen sie in das informationelle Selbstbestimmungsrecht der Polizeibeamten ein. Da es hierfür an einer Rechtsgrundlage fehlt, ist es ihnen verwehrt, Informationen aus dem Heilfürsorgeverfahren anderweitig zu verwenden. Sie dürfen nur das tun, was ihnen §§ 53, 54, 91 und 145 des Landesbeamtengesetzes erlauben.

— Ebenfalls nicht zu rechtfertigen ist, daß die ärztliche Abteilung der Polizeidirektion Karlsruhe den behandelnden Arzt ohne Wissen des Polizeibeamten um Informationen anging. Auch hierfür fehlt es an einer gesetzlichen Grundlage.

Das Innenministerium teilte mir auf meine Anfrage mit, die Vorgehensweise der Landespolizeidirektion Karlsruhe sei nicht die übliche Praxis: grundsätzlich gingen Informationen aus den Heilfürsorgeverfahren anderen nichtärztlichen Stellen nicht zu; lediglich zur Rechnungslegung würden bestimmte Abrechnungsunterlagen an die Landesoberkassen weitergegeben. Im Einvernehmen mit dem Rechnungshof und dem Finanzministerium strebe es aber auch hier an, eine Änderung herbeizuführen. Zu hoffen bleibt, daß dies bald geschieht.

8. Teil: Andere Schwerpunkte

1. Abschnitt: Die Gemeinde

Viele Bürger haben mit ihrer Gemeinde Probleme wegen des Datenschutzes. Was sie alles an mich herantragen, ist nicht immer von grundsätzlicher Bedeutung, oft aber gerade für den einzelnen recht wichtig. So lag einer engagierten Tierschützerin sehr am Herzen zu erfahren, ob der Datenschutz denn wirklich die Stadtverwaltung hindere, ihr zu sagen, an wen die Stadt ihre jungen Braunbären aus dem Tiergehege verkauft habe. Häufiger ging es um trockenere Themen: viele Bürger wollen wissen, wann die Gemeinde eine Auskunftssperre im Melderegister eintragen muß; Wähler empören sich — und nicht zu Unrecht —, daß ein Kandidat vor der Bürgermeisterwahl mit Hilfe seiner Partei an die Anschriften der Wahlberechtigten kam. Der Umgang mit Standesamtsurkunden ist bei allen in der Familienforschung Engagierten ein Dauerthema. Auch das öffentlich ausgehängte Aufgebot vor der Eheschließung stört viele Bürger nicht ohne Grund. Ein Bürger bat um Auskunft, ob er zur Planung einer Ortskernsanierung der Gemeinde Einzelheiten aus seinen Lebensumständen mitteilen muß. Nicht weniger oft fragen die Gemeinden selbst um Rat — etwa, was sie bei der Befragung für das Erstellen eines örtlichen Mietspiegels beachten müssen. Gerne wollen manche auch Schützenhilfe bei kommunalpolitisch heißen Eisen: War es richtig, daß ein Oberbürgermeister ein Gerichtsurteil mit Angaben über Grundeigentum und Vermögensverhältnissen namentlich genannter Bürger ungekürzt im Amtsblatt veröffentlichte? Diese Aufzählung soll und kann nur einen schwachen Eindruck von den vielfältigen Problemen vermitteln, die es bei Gemeinden mit dem Datenschutz gibt.

1. Was Kreditschutzorganisationen von Gemeinden über Bürger wissen wollen

CREDITREFORM

STUTTGART
Seit 1879 im Dienste der internationalen Wirtschaft

Ort: _____

Straße u. Hausnr.: _____

Firma: _____
Name:

Geschäftszweig: _____

Bitte Namen und Anschrift genau nachprüfen

Korr.: Pr.: Bearb.: Stuttgart ab: an:

Für die Erledigung dieser Anfrage sind wir selbst termingebunden. Wir bitten Sie daher um **sofortige Rücksendung** des ausgefüllten Fragebogens. Vielen Dank.

Ihre Mitteilung erfolgt ohne Verbindlichkeit für Sie und wird von uns vertraulich behandelt. Auch wir bitten Sie um diskrete Behandlung unserer Anfrage.

Betr.: nur Firmen und Vertreter

Genaue Firmenbezeichnung: _____
Rechtsform (Gewerbebetrieb, Einzelkaufmann, oHG, KG, GmbH, GmbH & Co. KG, AG, Genossenschaft): _____
_____
Seit wann am Platze? Von wo zugezogen? _____
Wann und von wem gegründet? _____
Jetziger Inhaber, Geschäftsführer oder Gesellschafter: _____
Im Handelsregister eingetragen und wo? _____
Oder besteht nur Eintrag im Gewerberegister? Seit wann? _____
Fabrikation, Großhandel, Einzelhandel oder Vertretung? _____
Was wird hergestellt oder gehandelt? (bitte vollständige Angaben) _____
_____
Wo befindet sich Fabrikationsbetrieb oder Geschäftslokal? (genaue Anschrift) _____
_____
Bei Ladengeschäft ungefähre Größe und Zahl der Schaufenster: _____
Bestehen Zweigbetriebe und wo? _____
Wie ist der Geschäftsgang (sehr gut, gut, mäßig, schlecht)? _____
Zahl der Beschäftigten: _____
Jahresumsatz: _____
Anzahl der Kraftfahrzeuge: (welche?) _____

Betr.: Firmen, Privatpersonen, Vertreter und Landwirte

Vor- und Zuname (bei Frauen auch Mädchenname): _____
Beruf und jetzige Tätigkeit: _____
Geburtsdatum und Geburtsort: _____
Seit wann am Platze wohnhaft? _____
Von wo zugezogen? _____
Familienstand (ledig, verh., gesch.) und Zahl der Kinder: _____
Bei wem und als was beschäftigt? _____
Ist Ehefrau berufstätig und wo? _____
Allgemeine Beurteilung: _____
_____
Güterstand: _____

Betr.: Firmen, Privatpersonen, Vertreter und Landwirte

Ist Haus- oder Grundeigentum vorhanden? Wenn ja, wo? (genaue Anschrift) _____
_____
Auf wen eingetragen im Grundbuch? _____
Wenn Einheitswert nicht bekannt, dann ungefährer Schätzwert: _____
Höhe der Belastung: _____
Wenn kein Hausbesitz vorhanden, dann Höhe der Miete (monatlich): _____
Wert des Warenlagers: _____
Wert der Geschäftseinrichtung: _____
Höhe der Außenstände: _____
Höhe der Verpflichtungen: _____
Wert der Kraftfahrzeuge: _____
Bankkredit (Höhe): _____
Was ist Ihnen über die Zahlungsweise bekannt (pünktlich, langsam, schlecht)? _____
Sind Ihnen ernste Beanstandungen bekannt und welche? _____
_____
Halten Sie eine Geschäftsverbindung für zulässig? _____
Welche Bankverbindungen bestehen? _____

Betr.: nur Landwirte

Ist der Hof Eigentum oder gepachtet? _____
Wieviel ha Eigenland und wieviel Pachtland? _____
Wie wird der Hof bewirtschaftet (gut, mäßig, schlecht)? _____
Welches sind die Hauptanbauprodukte? _____
_____
Viehbestand (Schweine, Kühe etc.): _____
Welche Maschinen sind vorhanden? _____

Bemerkungen: _____

Falls die angefragte Person oder Firma inzwischen verzogen sein sollte, so berichten Sie uns bitte ausführlich über das, was Ihnen bekannt ist, und geben Sie uns die genaue derzeitige Anschrift bekannt.

Falls in den Verhältnissen eine wesentliche Veränderung eintreten sollte, benachrichtigen Sie uns bitte sofort. Die Gebühr vergüten wir Ihnen nachträglich.

Nicht wenige Kreditschutzorganisationen wollen die Gemeinden als universelles Auskunftsbüro benutzen, wenn sie ihnen umfangreiche Fragebögen über Gemeindebürger ins Rathaus schicken. Oft wissen die Gemeinden dann nicht so recht, ob und was sie jetzt machen sollen. Vorweg sei ihnen gesagt: zur Antwort verpflichtet sind sie in keinem Fall. Manche Fragen dürfen, aber müssen sie nicht beantworten; andere Antworten dürfen sie kraft Gesetzes nicht geben. Das ist der Grund, warum es für die Gemeinden so schwer ist, sich richtig zu verhalten. Eine Stütze mag ihnen sein zu wissen:

Fragen nach Vorname, Familienname, Geburtsdatum, Geburtsort, Familienstand, Kinder und Zuzug können sie anhand des Melderegisters beantworten. Das Meldegesetz erlaubt den Gemeinden, Auskunfteien und Kreditschutzorganisationen

- jederzeit Auskunft über Familienname, Vorname, akademische Grade und Anschrift einer bestimmten Person zu geben,
- bei Vorliegen eines berechtigten Interesses zusätzlich auch z. B. Tag und Ort der Geburt, Familienstand, Tag des Zuzugs, bisherigen Wohnort mitzuteilen — es sei denn, das Interesse des Bürgers an der Geheimhaltung seiner Daten überwiegt das Auskunftsinteresse. In der Regel hat sie keines, wenn sie den Bürger selbst befragen kann.

Über Firmenbezeichnungen, Rechtsform der Firma, Inhaber, Geschäftsführer, Zahl der Beschäftigten und die ausgeübte Tätigkeit wissen die Gemeinden Bescheid, weil sie Gewerbeanzeigen erhalten und Gewerbekarteien erstellen. Ob sie daraus Auskunft geben dürfen, beurteilt sich, da spezielle Rechtsvorschriften fehlen, wie folgt: Die Gemeinde darf dies nur tun, wenn sie damit nicht schutzwürdige Belange des Bürgers beeinträchtigt. Eine Verwaltungsvorschrift des Wirtschaftsministeriums hat diese Rechtslage dahin konkretisiert, daß die Gemeinde einer anfragenden Kreditschutzorganisation

- jederzeit Auskunft über Name und Anschrift eines einzelnen Gewerbetreibenden und Art der angemeldeten Gewerbetätigkeit geben kann
- weiter Angaben über einen einzelnen Gewerbetreibenden, z. B. Zahl seiner Beschäftigten und den Geschäftsführer, nur geben darf, wenn die Kreditschutzorganisation ihr berechtigtes Interesse für jede gewünschte Angabe einzeln glaubhaft macht.

— Fragen nach Grundeigentum, Größe des landwirtschaftlichen Eigenlandes, Höhe der eingetragenen Belastungen ließen sich durch einen Blick in das Grundbuch beantworten. Auskünfte aus dem Grundbuch dürfen die Gemeinden aber nach § 12 der Grundbuchordnung nur geben, wenn die Kreditschutzorganisation oder Auskunftei ihr berechtigtes Interesse an den gewünschten Angaben konkret dargelegt hat. Dies ist, wenn sie der Gemeinde einfach ein standardisiertes Auskunftsformular zusenden, mit Sicherheit nicht der Fall.

— Fragen nach dem Viehbestand und den Hauptanbauprodukten eines Hofes dürfen die Gemeinden nicht beantworten. Da sie für diese Angaben auf überregionale Statistiken zurückgreifen müßten — z. B. die jährliche Bodennutzungserhebung oder die Viehzählung, an deren Erstellung sie mit-

wirken —, stehen die Regelungen des Bundesstatistikgesetzes solchen Auskünften entgegen. Hierbei geht es nämlich um nichts anderes als um Einzelangaben über persönliche und sachliche Verhältnisse, die strikt geheimzuhalten sind.

— Die Höhe der Miete oder finanzieller Verpflichtungen können die Gemeinden ebenso wie die genaue Berufstätigkeit und den Arbeitgeber eines Bürgers aus zahlreichen ihrer Unterlagen ersehen. So wirken die Gemeinden an Verfahren wegen Sozialhilfe, Wohngeld und Renten mit und erfahren dabei höchst sensible Daten der Antragsteller. Gleiches gilt beispielsweise für Erhebungsverfahren zur Grund- und Gewerbesteuer. Das Sozialgeheimnis und das Steuergeheimnis verbieten den Gemeinden jedoch aus gutem Grund, Auskünfte aus diesen Unterlagen an Kreditschutzorganisationen und Auskunfteien zu geben.

— Über Anzahl der Kraftfahrzeuge, Güterstand, Wert des Warenlagers und, ob der Hof „gut, mäßig oder schlecht" bewirtschaftet ist, weiß sicher auch mancher Gemeindebedienstete Bescheid. Die Gemeinde ist jedoch erst recht nicht verpflichtet, dies mitzuteilen.

— In keinem Fall kann die Gemeinde der Bitte einer Auskunftei der Kreditschutzorganisation entsprechen, sie laufend über Änderungen in den Verhältnissen des Bürgers zu unterrichten.

Alles in allem: in der Regel können Auskunfteien und Kreditschutzorganisationen nur eine Melderegisterauskunft oder einfache Einzelauskunft aus den Gewerbeanzeigen erhalten. Verpflichtet ist die Gemeinde, wie gesagt, auch dazu nicht. Die Entscheidung, ob sie dies tun will, steht vielmehr in ihrem pflichtgemäßen Ermessen.

2. Information des Gemeinderats und der Öffentlichkeit über datenschutzrelevante Vorgänge

In Fällen dieser Art konnte ich Bürgermeister oder Gemeinderat nicht immer mit einem eindeutigen „Ja" oder „Nein" weiterhelfen. Dazu liegen die Dinge oft zu kompliziert oder fehlen klare Rechtsvorschriften. Auch wäre nötig, daß die Gemeindeordnung zum Datenschutz mehr als bislang sagt. Drei Beispiele aus diesem Komplex greife ich heraus:

— Eine Gemeinderatsfraktion wollte von der Stadtverwaltung die Gewerbebetriebe erfahren, die mit besonders problematischen Emissionen zur Luftverschmutzung beitragen. Was war zu bedenken? Grundsätzlich darf eine Stadtverwaltung ihr bekanntgewordene Betriebs- und Geschäftsgeheimnisse und zum persönlichen Lebensbereich gehörende Geheimnisse nicht offenbaren. Das freilich tut sie nicht, wenn sie darüber den Gemeinderat in nichtöffentlicher Sitzung informiert. Im Gegenteil: sie muß dies wegen des Informationsrechts des Gemeinderats tun. Eine andere Frage ist, ob der Gemeinderat darüber in öffentlicher Sitzung verhandeln kann. Dies ja — es sei denn, das öffentliche Wohl oder berechtigte Interessen einzelner erfordern anderes. So verlangt es § 35 der Gemeindeordnung. Folglich ist bei jedem einzelnen Gewerbebetrieb aufs Neue abzuwägen zwischen dem Interesse der Bevölkerung, wie sich ein solcher Betrieb auf die Luftver-

schmutzung auswirkt und welche Risiken damit für die Bürger einhergehen, und den Interessen dieses Betriebs, nicht alle Einzelheiten zu seinem Nachteil preisgeben zu müssen. Das freilich kann nicht ich abschließend tun, sondern nur der Kenner aller Einzelheiten der örtlichen Szene.

— In einem anderen Fall fragte ein Bürgermeister, ob er der Presse vor einer öffentlichen Gemeinderatssitzung die für die Gemeinderäte bestimmten Sitzungsunterlagen überlassen darf. Das Landespressegesetz hilft bei der Antwort nicht weiter. Es gibt zwar der Presse ein allgemeines Informationsrecht, sagt aber nicht, in welcher Form die Gemeinde diesen Informationsanspruch erfüllen muß. Der Gemeindeordnung wiederum kann man nur entnehmen, daß selbst Gemeinderäte zu ihrer Vorbereitung auf eine Gemeinderatssitzung nicht beliebige Unterlagen erhalten können. Die Stadt darf ihnen mit der Einladung zur Sitzung nur solche Unterlagen zusenden, die für die Verhandlung erforderlich sind und dies nur insoweit, als nicht das öffentliche Wohl oder berechtigte Interessen einzelner entgegenstehen. Innerhalb dieser Grenzen ist auch eine Vorabinformation der Presse durch Zusenden von Unterlagen möglich. Doch meine ich, daß es bessere Formen für ihre Information gibt.

— Wenn die Stelle eines Schulleiters zu besetzen ist, darf auch die Gemeinde als Schulträger mitreden. Damit sie dazu in der Lage ist, muß sie das Oberschulamt über alle eingegangenen Bewerbungen unterrichten und ihr gleichzeitig sagen, welchen Bewerber es für den geeignetsten hält. Gelegentlich werde ich dann gefragt, ob die Gemeinde auch das Recht hat, vom Oberschulamt Einzelheiten über die Qualifikation der Bewerber — beispielsweise Dienstzeugnisse und Prüfungsnoten — zu erfahren. Das Schulgesetz gibt hierauf die Antwort: sein § 40 Abs. 1 Nr. 2 schränkt den Grundsatz der Geheimhaltung der Personalakten dahin ein, daß das Oberschulamt auf Wunsch der Gemeinde sachdienliche Informationen zur Eignung geben muß. So weit, aber nicht darüber hinaus hat das Oberschulamt die persönlichen und dienstlichen Verhältnisse eines Bewerbers dem Gemeinderat offenzulegen. Was daraus für den Einzelfall folgt, hängt entscheidend von den konkreten Umständen ab. Je nachdem kann es sein, daß einem Gemeinderat auch einmal Noten aus Dienstzeugnissen und Prüfungen bekanntzugeben sind.

3. Zweitwohnungssteuer

Wer Eigentümer oder Mieter einer Zweitwohnung in einer schönen Fremdenverkehrsgemeinde ist und dort nicht ständig wohnt, hat meist auch schon mit der Zweitwohnungssteuer Bekanntschaft gemacht. In der Juristerei gab es wegen dieser Angabe lebhaften Streit; das Bundesverfassungsgericht hat inzwischen ihre Zulässigkeit bestätigt. Auch für den Datenschutz ist die Zweitwohnungssteuer ein Thema. So wollten schon manche Bürger von mir wissen, ob sie wirklich die ihnen von den Gemeinden zugeschickten umfangreichen Erhebungsbögen zur Festsetzung der Zweitwohnungssteuer ausfüllen müssen. Zu beantworten haben sie nach den Vorschriften des Kommunalabgabengesetzes und der Abgabenordnung all die Fragen, die zur Feststellung, ob und in welcher Höhe sie gegebenenfalls Zweitwohnungssteuer zu zahlen haben, erforderlich sind. Die Ge-

meinden müssen dies im Erhebungsbogen klar sagen. Das machen aber viele, wie ich immer wieder feststellen mußte, nicht. Viele Mißverständnisse hätten sie bei den Steuerpflichtigen auch vermeiden können, wenn ihre Vordrucke ein wenig geschickter gestaltet wären. Manch einer stellt beispielsweise Fragen, die sich nur an den Eigentümer richten können, auch dem Mieter, der sie gar nicht beantworten braucht, und umgekehrt. Ähnliche Ungeschicklichkeiten unterliefen auch bei der Ermittlung von Steuerbefreiungsgründen: sicher muß, wer seine Wohnung aus beruflichen Gründen nutzt und deswegen von der Zweitwohnungssteuer befreit ist, Arbeitgeber und Arbeitsstätte nennen. Aber was soll das denn beim Urlauber? Wenn sie aus der Anordnung der Fragen nicht erkennen können, daß diese Frage sich gar nicht an sie richtet, machen die einen brav unnötige Angaben und empören sich die anderen, was die Gemeinde dies eigentlich angeht. Alle Gemeinden sollten daher ihre Fragebögen einmal daraufhin durchsehen, ob sie korrekt und für den Bürger verständlich sind.

4. Kurtaxe

Erstaunt fragte mich die Einwohnerin einer Fremdenverkehrsgemeinde, ob sie denn tatsächlich der Gemeinde melden müsse, wenn sie Besuche von Bekannten oder Verwandten bekomme und diese — selbstverständlich kostenlos — bei ihr übernachteten. Anlaß für ihre Anfrage war folgende Regelung in der Kurtaxesatzung:

„§ 5

(1) Von der Entrichtung der Kurtaxe, nicht aber von der Meldepflicht sind befreit:

a) ...

b) Familienbesucher von Einwohnern der Gemeinde XY, welche unentgeltlich in deren Haushalt aufgenommen werden.

c) ..."

Wer dies unbefangen liest, kann tatsächlich meinen, der Besuch der Großmutter wäre meldepflichtig. Ich konnte die Bürgerin allerdings beruhigen. Bei weiterem Suchen fand sich in der Kurtaxesatzung noch ein § 10 „Meldepflicht". Danach muß nur der die Gemeinde informieren, der andere gegen Entgelt beherbergt. Nur dafür ist auch im Kommunalabgabengesetz eine Ermächtigung vorhanden.

2. Abschnitt: Die Gebäudebrandversicherungsanstalten

1. Die Pflichtversicherung

Die Württembergische Gebäudebrandversicherungsanstalt und die Badische Gebäudeversicherungsanstalt sind für jeden Hausbesitzer und Wohnungseigentümer ein Begriff. Denn sie alle müssen jedes Jahr aufs Neue einen Obulus entrichten und sind dafür gegen Schäden ihrer Anwesen durch Brand, Blitzschlag, Explosion und Absturz von Luftfahrzeugen (Brandversicherung) sowie gegen Schäden durch Sturm, Hagel, Hochwasser, Überschwemmung, Schneedruck, Lawinen, Bergsturz, Erdrutsch, Erdfall und Erdbeben (Elementarschadensversicherung) versichert.

Um diesen Versicherungsschutz zu gewähren, benötigen die Anstalten umfangreiche Informationen über die versicherten Grundstücke, Häuser und Wohnungen. Die Eigentümer müssen deshalb eine Menge Angaben machen, Unterlagen vorlegen und Schätzungen vornehmen lassen. Auf diese Weise erfahren die Anstalten, wie hoch die Herstellungskosten eines Gebäudes waren und welchen Wert das Anwesen jetzt besitzt. Auch kennen sie die Wohnverhältnisse der einzelnen Bewohner; denn die Einschätzungsunterlagen enthalten sehr detaillierte Angaben über das Zubehör. Diesen Unterlagen ist beispielsweise zu entnehmen, ob und wie viele Einbauschränke, eingebaute Regale, Kücheneinbauten, Herde, Öfen, Boiler, Stromspeicher, Kamine und sanitäre Einrichtungen wie WCs, Badewannen, Duschen, Waschbecken usw. das Gebäude hat. Um die im Rahmen dieser Gebäudeversicherung anfallenden Massengeschäfte leichter bewältigen, vornehmlich die jährliche Umlage erheben zu können, setzen die Anstalten schon seit einiger Zeit Computer ein. Ihre Einschätzungsunterlagen, die noch nicht automatisiert geführt werden, bewahren — von einigen Ausnahmen abgesehen — die Gemeinden auf.

Weil beide Anstalten so sensitive Daten über so viele Bürger haben, führten meine Mitarbeiter und ich bei ihnen Kontrollbesuche durch. Dabei zeigten sich eine Reihe von Problemen, die teilweise schon seit Jahren einer Lösung harren.

2. Die Zweckentfremdung

Jeder Eigentümer, der einer Gebäudeversicherungsanstalt und ihren Schätzern Informationen zukommen lassen muß, nimmt zunächst einmal an, die Anstalt werde diese Informationen nur für Zwecke der Brand- und Elementarschadensversicherung verwenden. Nur dafür schuf schließlich der Gesetzgeber die Auskunftspflicht. In Wirklichkeit aber liegen die Dinge leider nicht so einfach. Denn neben den Gebäudeversicherungsanstalten interessieren sich eine ganze Reihe anderer Stellen für diese Informationen und nutzen sie in ihrem Sinn.

2.1 Die umfangreiche Amtshilfe

Am eifrigsten interessiert sich die Steuerverwaltung für die von den Gebäudeversicherungsanstalten gesammelten Informationen. Sie will diese Daten, damit sie mit deren Hilfe die Einheitswerte von Grundstücken ermitteln kann. Deshalb teilt die Württembergische Gebäudebrandversicherungsanstalt den Finanzämtern das Ergebnis jeder Einschätzung eines Gebäudes und seines Zubehörs mit — Einschätzungsverzeichnis genannt. Im Gebiet der Badischen Gebäudeversicherungsanstalt erfolgt die Information der Finanzämter durch die Gemeinden mit Hilfe eines automatischen Mitteilungsdienstes. Reges Interesse an den Einschätzungswerten hat aber auch die Vermessungsverwaltung. Sie will diese Informationen, um die Gebühr festsetzen zu können, die für die Aufnahme eines Gebäudes in das Liegenschaftskataster zu zahlen ist. Deshalb übersenden die Gemeinden im Gebiet der Badischen Gebäudeversicherungsanstalt in deren Auftrag den Vermessungsämtern jeweils automatisch einen Durchschlag des Einschätzungsverzeichnisses. Differenzierter ist die Praxis im Gebiet der Württembergischen Gebäudebrandversicherungsanstalt. Hier holen sich die Vermessungsämter vielfach nur von Fall zu Fall bei den Gemeinden Auskunft aus den Einschätzungsunterlagen ein.

Aus der Sicht des Datenschutzes ist dazu zunächst einmal festzuhalten: Bei den Angaben in den Einschätzungsunterlagen handelt es sich um zwangsweise für Zwecke der Gebäudeversicherung erhobene Daten. Solche Daten darf man, wie das Bundesverfassungsgericht in seinem Volkszählungsurteil vom 15. Dezember 1983 ausführt, grundsätzlich nur für den Zweck nutzen, für den sie erhoben wurden. Zieht man sie für andere Zwecke heran, ist dies ein zusätzlicher Eingriff in das Grundrecht jedes Bürgers auf informationelle Selbstbestimmung. Er darf bloß erfolgen, wenn es dafür eine gesetzliche Grundlage gibt, die dem rechtsstaatlichen Gebot der Normenklarheit entsprechen muß. Mißt man die beschriebenen Informationsweitergaben an diesem Maßstab, so bedeutet dies:

2.1.1 Mitteilungen an die Finanzämter

Für den Mitteilungsdienst an die Finanzämter existiert keine diesen Anforderungen entsprechende Rechtsgrundlage. Eine solche sind insbesondere nicht die Amtshilfevorschriften der Abgabenordnung. Denn zum einen ist schon sehr fraglich, ob man einen so umfassenden Mitteilungsdienst überhaupt noch als Amtshilfe ansehen kann, die doch ihrem Wesen nach Hilfe im Einzelfall ist. Vor allem aber führt das Bundesverfassungsgericht im Volkszählungsurteil nachdrücklich aus, die allgemeine Pflicht zur Amtshilfe sei keine Rechtfertigung für eine Weitergabe zwangsweise erhobener Daten. Ebensowenig läßt sich der praktizierte Mitteilungsdienst mit der in § 93 der Abgabenordnung geregelten allgemeinen Auskunftspflicht gegenüber Finanzbehörden legitimieren. Denn diese Regelung gilt für nichts anderes als für einzelne Steuerverfahren und kann allenfalls eine Mitteilung im Einzellfall begründen. Schließlich scheidet auch § 10 LDSG als Rechtsgrundlage schon deshalb aus, weil die Finanzbehörden keinesfalls jede einzelne Information, die sie bisher erhalten, tatsächlich auch zwingend benötigen. Beide Gebäudeversicherungsanstalten halten eine Klärung dieser Frage durch die beteiligten zuständigen Ministerien für notwendig. Dafür habe ich Verständnis. Weniger Verständnis kann ich für das Verhalten des Wirtschaftsministeriums aufbringen, das mir mitteilte, es könne derzeit noch nicht abgesehen werden, bis wann mit einer Klärung zu rechnen sei.

2.1.2 Mitteilungen an die Vermessungsbehörden

Auch die laufende, unaufgeforderte Weitergabe der Einschätzungsverzeichnisse im Bereich der Badischen Gebäudeversicherungsanstalt erfolgt ohne ausreichende Rechtsgrundlage. Insbesondere rechtfertigt § 10 LDSG diese exzessive Datenweitergabe nicht. Die abweichende Praxis im Gebiet der Gebäudebrandversicherungsanstalt Württemberg zeigt deutlich genug, daß die Vermessungsämter ihre Aufgaben durchaus auch wahrnehmen können, wenn sie nicht automatisch über jede Einschätzung eines Gebäudes oder einer Wohnung informiert werden. Dies sieht auf meine Beanstandung hin inzwischen auch die Badische Gebäudeversicherungsanstalt so und stellte deshalb den Mitteilungsdienst an die Vermessungsämter ein.

Zu weit geht aber auch die Praxis in Württemberg, den Gemeinden im Einzelfall auf Anfrage Auskunft zu geben. Wer so verfährt, berücksichtigt nämlich nicht, daß die Vermessungsämter die Möglichkeiten haben, die zur Gebührenfestsetzung notwendigen Informationen unmittelbar beim Gebührenschuldner zu erheben. Er ist nämlich kraft Gesetzes verpflichtet, die für die Gebührenfestsetzung notwendigen Angaben zu machen. Nur wenn sich dieser weigert oder nicht in der Lage ist, seine Pflicht zu erfüllen, kann eine Auskunft der Gebäudebrandversicherungsanstalt an die Vermessungsämter in Betracht kommen. Eine andere Vorgehensweise läßt sich auch nicht, wie das Innenministerium meint, mit dem „Umsetzungsbonus" rechtfertigen, den das Bundesverfassungsgericht in ständiger Rechtsprechung Gesetzgebung und Verwaltung dann einräumt, wenn es eine bislang für verfassungsgemäß gehaltene Regelung für verfassungswidrig erklärt. Das Innenministerium übersieht bei dieser Argumentation nämlich, daß das Bundesverfassungsgericht einen Umsetzungsbonus nur dann zubilligt, wenn andernfalls die Funktionsfähigkeit einer staatlichen Einrichtung gefährdet wäre. Davon kann hier ganz sicherlich keine Rede sein.

2.2 Die Nutzung durch die Gemeinden

Wer Informationen besitzt, will sie in der Regel auch umfassend nutzen. So verwenden viele Gemeinden die Angaben aus den Einschätzungsunterlagen nicht nur für Zwecke der Gebäudeversicherung, sondern auch für ihre eigenen Aufgaben: sie unterrichten beispielsweise ihren Gutachterausschuß nach dem Bundesbaugesetz und geben die Informationen auch dem Amt für Wohnungswesen. Die Gebäudeversicherungsanstalten wissen seit langem um diese Praxis. Irgendwelche Anweisungen, in welchem Umfang und unter welchen Voraussetzungen die Gemeinden die Einschätzungsunterlagen für Gemeindezwecke nutzen dürfen, erließen sie jedoch nicht.

Diese Praxis steht mit dem Datenschutzrecht nicht in Einklang. Nach den gesetzlichen Regelungen über die Gebäudeversicherung kommt den Gemeinden nur eine Hilfsfunktion bei der Gebäudeversicherung zu. Sie sind gewissermaßen der verlängerte Arm der Gebäudeversicherungsanstalt und bewahren die Einschätzungsunterlagen nur für Zwecke der Gebäudeversicherung auf. Nicht die Gemeinden entscheiden, welche Informationen in den Einschätzungsunterlagen festzuhalten sind, sondern die Gebäudeversicherungsanstalten. Nur diese sind für die Richtigkeit der Daten verantwortlich. Aus diesem Grund sind sie im Sinne des Datenschutzrechts die „speichernde Stelle", während die Tätigkeit der Gemeinden als gesetzlich angeordnete „Datenverarbeitung im Auftrag" zu bewerten ist. Daraus folgt: die Gemeinden können nicht nach eigenem Gutdünken entscheiden, wie sie die bei ihnen aufbewahrten Informationen der Gebäudeversicherung verwenden. Dies ist vielmehr Sache der Gebäudeversicherungsanstalten. Folglich dürfen die Gemeinden die Einschätzungsunterlagen nicht beliebig, sondern nur im Einvernehmen mit ihrer Gebäudeversicherungsanstalt nutzen. Diese wiederum hat sich dabei an § 10 LDSG zu orientieren. Obwohl ich schon im

März 1985 beide Gebäudeversicherungsanstalten, das Wirtschaftsministerium und das Innenministerium über diese Problematik unterrichtete, steht eine Antwort in der Sache immer noch aus. Nach Auskunft des Wirtschaftsministeriums ist damit noch längere Zeit nicht zu rechnen. Dafür habe ich kein Verständnis. Ich meine, daß die für den Schutz des informationellen Selbstbestimmungsrechts der Versicherungspflichtigen so wichtige Frage, wer über die Verwendung von Informationen aus den Einschätzungsunterlagen zu entscheiden hat, baldmöglichst einer Klärung zugeführt werden muß.

3. Datensicherung

Bei der technischen Kontrolle der Datenverarbeitung zeigten sich erhebliche Unterschiede zwischen den beiden Anstalten. Während ich mir bei der Württembergischen Gebäudebrandversicherungsanstalt leicht ein Bild über die Details der Datenverarbeitung machen konnte und nur wenige Mängel feststellen mußte, lagen die Verhältnisse bei der Badischen Gebäudeversicherungsanstalt anders. Hier war eine umfassende Überprüfung überhaupt nicht einmal möglich, weil keine nur annähernd ausreichende Beschreibung der Datenverarbeitung vorhanden war. Beide Anstalten zogen aus meinen Feststellungen Konsequenzen: Die Württembergische Gebäudebrandversicherungsanstalt sicherte mir zu, sie werde bei ihrem derzeit in Entwicklung befindlichen neuen EDV-Verfahren meine Kritik berücksichtigen. Die Badische Gebäudeversicherungsanstalt beauftragte, um aus ihrer verfahrenen Situation herauszukommen, die Datenzentrale, ihre Datenverarbeitung gründlich unter die Lupe zu nehmen und ein Gutachten zu erstellen, wie sie am besten die Mängel im einzelnen behebt. Ich hoffe sehr, daß dies zügig vorangeht.

3. Abschnitt: Handels- und Gaststättenzählung 1985

Einige Aufregung verursachte die Handels- und Gaststättenzählung 1985. Verständlich war dies gewiß — denn es handelte sich hier um die erste Bundesstatistik, die nach dem Volkszählungsurteil als Totalerhebung stattfand. Das Statistische Landesamt forderte dazu die ca. 175 000 Unternehmen des Handels- und Gaststättengewerbes in Baden-Württemberg auf, Fragen nach der Beschäftigtenzahl, dem Umsatz, der Zahl der Betten und noch zahlreichen weiteren Informationen über ihr Unternehmen zu beantworten.

1. Die mangelhafte Rechtsgrundlage

Die Verantwortlichen für die Statistik in Bund und Ländern — in Baden-Württemberg ist es das Finanzministerium — ließen diese Zählung durchführen, obwohl allen klar war, daß das Handelsstatistikgesetz vom 10. November 1978 (BGBl. I, S. 1733), auf das sie sich bei der Befragung stützten, nicht den Anforderungen gerecht wird, die von Verfassungs wegen an ein solches Statistikgesetz zu stellen sind. Vor allem bestimmt dieses Gesetz nicht, welche Hilfsmerkmale erhoben werden. Außerdem fehlen präzise Regelungen über die Trennung der Hilfsmerkmale von den eigentlichen Erhebungsmerkmalen und ihre Löschung. Wenn die Verantwortlichen trotz dieser Mängel den Startschuß für die Handels- und Gaststättenzählung gaben, hät-

ten sie wenigstens dafür sorgen müssen, daß die erhobenen Daten nur für deren Zwecke und für nichts anderes Verwendung finden. Dies ist jedoch nicht der Fall. So will man die Adreßdaten der Unternehmen, die die Statistischen Ämter von der Steuerverwaltung erhielten und zur Organisation der Zählung benötigen, ebenso wie die Angaben der auskunftspflichtigen Betriebe auch für die Erstellung anderer Bundesstatistiken als der Handels- und Gaststättenzählung verwenden — beispielsweise für die Volkszählung 1987, die Statistik über die Beherbergung im Reiseverkehr, die Lohnstatistik und verschiedene Steuerstatistiken. Das Finanzministerium räumte mir gegenüber zwar ein, daß diese Art der Verwendung an sich im Handelsstatistikgesetz abgesichert werden müßte, glaubte aber — Recht hin, Recht her — nicht darauf verzichten zu können, „da nur auf diese Weise die Aufgaben der amtlichen Statistik erfüllt werden können".

2. Die unrechtmäßige Verarbeitung von Steuerdaten

Anlaß zur Kritik hatte ich auch aus anderem Grund: Die Oberfinanzdirektionen Stuttgart, Karlsruhe und Freiburg stellten dem Statistischen Landesamt zur Organisation der Zählung bis Frühjahr 1985 auf Magnetbändern nicht nur, wie dies § 6 Abs. 2 des Handelsstatistikgesetzes vorsieht, Anschriften und Gewerbekennziffern aller Unternehmen des Handels- und des Gastgewerbes des Landes zur Verfügung, sondern dazu noch als „Serviceleistung" deren Steuernummer und Kennzeichnung für Umsatzsteuer und Gewerbesteuer. Da es für diese „Serviceleistung" keine Rechtsgrundlage gab, offenbarten die Oberfinanzdirektionen unbefugt Verhältnisse der Auskunftspflichtigen, von denen sie in einem Besteuerungsverfahren Kenntnis erhalten hatten, und verletzten damit das Steuergeheimnis. Das Statistische Landesamt legte mit diesen Informationen eine Adreßdatei an. In dieser Datei speicherte sie neben ca. 175 000 Anschriften von auskunftspflichtigen Unternehmen auch deren Steuernummer. Da dieses Datum nicht zur Durchführung der Handels- und Gaststättenzählung 1985 erforderlich war, verstieß dieses Vorgehen gegen § 9 Abs. 1 LDSG.

Auf meine Beanstandung hin teilte mir das Finanzministerium vorab mit, daß das Statistische Landesamt inzwischen alle im Rahmen der Handels- und Gaststättenzählung 1985 gespeicherten Steuernummern und Kennzeichen für die Umsatz- und Gewerbesteuer gelöscht hat. Zu einer abschließenden Stellungnahme zu meiner Beanstandung sah sich das Ministerium allerdings noch nicht in der Lage. Dazu will es erst eine Sitzung der AO-Referenten des Bundes und der Länder abwarten.

9. Teil: Sorgen der Bürger

Jedes Jahr berichte ich über die Sorgen der Bürger und schildere markante und typische Fälle. Zweierlei Motive bewegen mich dabei: zum einen hat das Parlament Anrecht zu erfahren, was die Menschen erleben. Zum anderen hoffe ich, daß die sich in manchen Ereignissen offenbarende Not und Beschwernis auch bei denen Verständnis für den Datenschutz weckt, die bislang nicht zu seinen Freunden zählen. Verhehlen will ich nicht, daß mich die Reaktion

der politisch Verantwortlichen auf die Sorgen der Bürger manchmal schon enttäuschte. Nach wie vor ist es schwer, der Bevölkerung die Grenzen meiner Kontrollbefugnisse deutlich zu machen. Wie soll auch ein juristisch Unverbildeter verstehen, was eine Datei ist und welche Konsequenzen sich daraus ergeben, wenn selbst viele Behörden und manche Politiker mit diesem Begriff nichts anzufangen wissen. Gleichwohl halten die für den Datenschutz Verantwortlichen seine Fahne unbeirrt hoch und die Datenschutzbeauftragte mit seiner Hilfe von mancher erforderlichen Kontrolle fern. Einem Ondit zufolge sollen die Bonner Koalitionsfraktionen sich freilich inzwischen einig sein, daß sich die Datenschutzbeauftragten der Anliegen von Bürgern immer annehmen können — auch wenn deren Daten nicht in Dateien, sondern „bloß" in Akten festgehalten sind. Bewahrheitet sich dies, bliebe Baden-Württemberg dann wohl nichts anderes übrig als zumindest insoweit die 1982 erfolgte Beschneidung meiner Kompetenzen rückgängig zu machen. Das würde manchem Bürger im Lande zugute kommen.

1. Vorsicht Forellenzucht

Ein 54jähriger Herr von Bildung und glücklicherweise auch Humor hielt sich zur Vertiefung seines Wissens mehrere Tage in einem Schwarzwaldkurort auf. Recht erschrocken war er, als während eines abendlichen Spaziergangs plötzlich ein Polizeifahrzeug hielt und die beiden entsteigenden Polizeibeamten ihn aufforderten, seinen Personalausweis vorzuzeigen. Da er diesen nicht bei sich hatte, belehrten ihn die Beamten, es sei Vorschrift, den Personalausweis ständig mit sich zu führen. Auf die weitere Frage nach dem Grund der Überprüfung soll ein Polizeibeamter wörtlich gesagt haben: „Das ist nicht Ihr Problem, sondern unser Problem. Der Staatsbürger soll ruhig wissen, daß die Polizei keineswegs untätig ist, sondern ihren Aufgaben nachkommt". Und der andere Polizeibeamte habe dahin gehend ergänzt, „er halte jedes ihm unbekannte Gesicht für überprüfungswürdig". Nach diesem Discours über den Grund der Überprüfung — so unser Bürger — hätten ihn die Polizeibeamten eingehend darüber befragt, woher er gerade komme, wo er wohne, mit welchem Verkehrsmittel er angereist sei, wo er die Nacht verbringe, wie er heiße. Unser Bürger beantwortete all diese Fragen und gab insbesondere auch an, im Hotel X zu übernachten. Einer der Beamten notierte dies alles und sei daraufhin zum Streifenwagen gegangen, von wo aus er unverkennbar den Hotelier angerufen und sich nach ihm erkundigt habe. Dabei habe er offensichtlich erfahren, daß eine Fortbildungsstätte am Ort das Hotelzimmer gebucht hatte. Denn der Polizeibeamte habe ihn anschließend gefragt, ob er in der Fortbildungseinrichtung zu tun habe, was er bejahte. Daraufhin hätten ihn die Beamten entlassen. Als der Bürger jedoch noch ihren Dienstausweis sehen wollte, hätten sie ihm angekündigt, er werde noch von ihnen hören. Tags darauf erkundigten sich die beiden dann tatsächlich beim Leiter der Fortbildungseinrichtung nach seinen Personalien.

Der Bürger hielt das Vorgehen der Polizeibeamten nicht für korrekt und bat deshalb das Innenministerium um Überprüfung. Dieses belichtete das Verhalten der Polizeibeamten in seiner Antwort so: Die Feststellung der Personalien sei „zur vorbeugenden Verbrechensbekämpfung" erforderlich gewesen. Schließlich hätten die Polizeibeamten ihn seinerzeit auf Höhe einer neben der Fahrbahn gelegenen Forellenzuchtanlage angetroffen. Die Feststellung seiner Personalien habe dazu gedient, ihn — „rein vorsorglich" — von einem „möglichen Fischdieb-

stahl" abzuhalten, „mit welchem aufgrund der vorgefundenen Situation die Beamten mit ausreichender Wahrscheinlichkeit rechnen durften". Zulässig gewesen sei die Rückfrage beim Leiter der Ausbildungseinrichtung, da die Vergewisserung über die Identität des Bürgers auf andere, einfachere und weniger belastende Weise nicht möglich gewesen sei. Den Bürger überzeugte der Hinweis auf den möglichen Fischdiebstahl keineswegs. Deshalb berichtete er mir die „lustige Geschichte mit ernstem Hintergrund". Ich kann die Vorgehensweise der Polizei nicht gutheißen:

— Nach dem Polizeigesetz darf die Polizei die Identität eines Bürgers unter anderem dann feststellen, wenn es eine konkrete Gefahr für die öffentliche Sicherheit oder Ordnung abzuwehren gilt. Dies ist beispielsweise der Fall, wenn das Bevorstehen einer Straftat angenommen werden kann. Hätte es seinerzeit Anhaltspunkte dafür gegeben, daß unser Bürger einen Fischdiebstahl begehen will, hätte die Polizei ihn überprüfen dürfen. Solche Anhaltspunkte gab es aber nicht; nicht einmal das Innenministerium bezweifelte in seiner Antwort an den Bürger dessen Sachverhaltsdarstellung. Fest steht also, daß die Polizeibeamten den möglichen Fischdiebstahl seinerzeit nicht als Grund für die Identitätsüberprüfung nannten und daß ein Polizeibeamter sagte, er halte jedes ihm unbekannte Gesicht für überprüfungswürdig. Dies und die weitere Überlegung, daß ein unbekanntes Gesicht noch kein Grund für eine polizeiliche Überprüfung sein kann, hätte für das Innenministerium Anlaß sein müssen, anders zu reagieren.

— Nicht richtig handelten die beiden Polizeibeamten, wenn sie den Grund für die Überprüfung nicht nannten. Der zur Angabe seiner Personalien Aufgeforderte muß erkennen können, warum gegen ihn eingeschritten wird.

— Unzutreffend war auch, wenn die Polizeibeamten gesagt haben sollten, der Bürger müsse seinen Personalausweis stets mit sich führen. Das Gesetz verpflichtet Bürger lediglich, einen Personalausweis oder Paß zu besitzen — nicht aber, ihn bei sich zu haben. Weil dem so ist, muß jeder freilich gegebenenfalls Nachteile auf sich nehmen, wenn die Polizei bei einer Kontrolle seine Personalien nicht gleich feststellen kann.

— Bedenken bestehen schließlich auch dagegen, wie die beiden Polizeibeamten die Identität des Betroffenen feststellten. Das Polizeigesetz läßt zu diesem Zweck die „erforderlichen Maßnahmen" zu. Was das heißt, sagt es hingegen nur beispielhaft. Auf jeden Fall muß die Polizei jeweils den Weg wählen, der einerseits eine rasche und zuverlässige Feststellung der Identität ermöglicht, andererseits aber den Bürger möglichst wenig belastet oder gar bloßstellt. Ob es danach zulässig war, die angegebenen Personalien beim Gastwirt nachzuprüfen, oder ob es nicht trotz vorgerückter Stunde andere, unseren Bürger weniger belastende Überprüfungsmöglichkeiten gegeben hätte, mag dahinstehen. Nicht rechtmäßig war jedenfalls die Rückfrage der Polizeibeamten beim Leiter der Fortbildungsstätte am nächsten Morgen. Dies folgt schon daraus, daß sie am Abend vorher zunächst zu erkennen gaben, daß ihnen die Auskunft des Hoteliers genügt. Außerdem war diese Rückfrage schwerlich geeignet, der Polizei weitere, über die Auskunft des Gastwirts hinausgehende Erkenntnisse zu vermitteln und eine zweifelsfreie Feststellung der Identität des Bürgers zu er-

möglichen. Bedenken müssen hätten die beiden Polizeibeamten aber auch, daß sie unseren Bürger mit ihrer Rückfrage bei der Erwachsenenbildungsstätte unnötig in Mißstände brachten. Alles in allem: eine ziemlich verunglückte Personenüberprüfung.

2. Terroristenfahndung

Nicht minder erschrocken waren wohl einige unbescholtene Bürger, die an einem Tisch in einem vollbesetzten Stuttgarter Tanzlokal saßen, als ihnen kurz nach Mitternacht plötzlich mehrere bewaffnete Polizeibeamte entgegentraten und ihre Ausweise sehen wollten. Terroristenfahndung lautete die Begründung. Nach der Ausweiskontrolle brachten die Polizeibeamten die jungen Leute in einem Polizeifahrzeug zu ihrer Dienststelle, der Landespolizeidirektion Stuttgart II. Dort sagte ihnen die Polizei, sie habe zwei Hinweise erhalten, daß sich in dem Tanzlokal ein per Fahndungsplakat gesuchter Terrorist aufhalte. Demjenigen, den die Polizei als Terroristen verdächtigte, nahm sie, obwohl er ihr bereits im Tanzlokal seinen ordnungsgemäßen Ausweis vorgelegt hatte, sodann einen Fingerabdruck und überspielte diesen an das Bundeskriminalamt in Wiesbaden. Als von dort die Mitteilung kam, dieser Mann sei mit dem Terroristen nicht identisch, ließ sie ihn wieder frei. Er wandte sich daraufhin an mich, weil er fürchtete, nunmehr in Dateien der Polizei erfaßt zu sein. Eine vorher nicht angekündigte Kontrolle am 12. Februar 1985 bei der Polizei ergab, daß über den Vorfall keine Daten gespeichert und auch die Fingerabdrücke bereits wieder vernichtet waren. Schlagzeilen hatte die Begebenheit schon Tage zuvor — nämlich am 6. Februar 1985 — in der Stuttgarter Zeitung gemacht.

3. Razzia

Sehr in Sorge war ein Vater, dessen Tochter zusammen mit rund 150 weiteren jungen Leuten in einer Discothek in eine Rauschgiftrazzia der Polizei geraten war. Er fürchtete, seine Tochter sei nunmehr als Angehörige der Rauschgiftszene registriert, zumal die Polizei beim Betreten des Lokals Aufnahmen von allen Anwesenden gefertigt habe. Bei einer Überprüfung vor Ort stellten wir folgendes fest: Die Polizei hatte aufgrund einer Anordnung des Bürgermeisteramts in der Discothek eine Razzia durchgeführt, weil sie als Treffpunkt der Rauschgiftszene galt. Dies hatte eine frühere Razzia in diesem Lokal gezeigt. Auch hatte das Bürgermeisteramt den Inhaber der Discothek bereits früher abgemahnt, weil er den Handel mit Rauschgiften nicht unterband. Beim Eindringen in das Lokal hatte die Polizei — wie sie es nennt — Übersichtsaufnahmen gefertigt, um zu wissen, wer überhaupt anwesend war, wer bei wem stand, wer unter Umständen etwas in der Hand hielt. Diese Photos wollte sie für den Fall, daß es zu Strafverfahren gegen einzelne Anwesende kommen sollte, als Beweismaterial verwenden. Nach dem Schießen der Bilder stellte die Polizei die Personalien aller Discothekenbesucher fest und fragte über Funk ab, ob und wer davon im bundesweiten Fahndungssystem INPOL und/oder im landesweiten Informationssystem PAD gespeichert ist. Gegen vier Discothekenbesucher leitete die Polizei ein Ermittlungsverfahren ein, weil sie bei ihnen Rauschgift beschlagnahmt hatte. Zur Zeit unserer Kontrolle hatte die Polizei die Übersichtsaufnahmen bereits wieder vernichtet — angeblich deshalb, weil die Bildqualität sehr schlecht war. Außer den Tatverdächtigen

hatte sie niemanden in ihren Dateien erfaßt. Ich konnte daher den besorgten Vater beruhigen: Seine Tochter war nicht registriert. Natürlich war er darüber erleichtet. Aber nicht nur für ihn blieb unbefriedigend, daß die Polizei Bilder von Unverdächtigen aufnahm, obwohl es dafür keine (eindeutige) Rechtsgrundlage gibt.

4. Wer eine Kaserne photographiert

Zwei Bürgern war folgendes widerfahren: Sie hatten 1982 die amerikanische Kaserne Cook Barracks in Göppingen photographiert. Die Polizei hatte dies beobachtet und die Personalien der beiden festgestellt; die Polizeidirektion Göppingen leitete gegen sie ein Ermittlungsverfahren wegen eines Vergehens gegen die Landesverteidigung ein. Da die Ermittlungen jedoch rasch allenfalls den Verdacht einer Ordnungswidrigkeit nach dem Schutzbereichsgesetz erbrachten, gab die Staatsanwaltschaft Stuttgart das Verfahren an das Landratsamt Göppingen ab. Dieses fand schließlich Jahre später im Benehmen mit der Wehrbereichsverwaltung V heraus, daß das Gebiet um die Kaserne nicht im Schutzbereich lag, und stellte im Januar 1985 das Bußgeldverfahren gegen die beiden Bürger ein. Daraufhin wandten sich die Photographen an mich, weil sie annahmen, daß die Polizei aufgrund des Vorgangs Daten über sie speichert und sie diese gelöscht haben wollten. Bei meiner Kontrolle im Sommer 1985 stellte ich dann auch fest, daß sie immer noch in der Personenauskunftsdatei — dem landesweiten Informationssystem der Polizei — gespeichert waren, da die Polizeidirektion Göppingen bis dahin den Verfahrensausgang nicht kannte. Aufgrund der neuen Sachlage löschte sie diese Daten. Das muß freilich nicht heißen, daß alle in polizeilichen Unterlagen gesammelten Informationen über die beiden vernichtet sind. Möglich, ja sogar sehr wahrscheinlich ist vielmehr, daß die Polizeidirektion Göppingen die Daten der beiden Bürger einst im Rahmen des kriminalpolizeilichen Meldedienstes in Staatsschutzsachen an das Landes- und dieses wiederum an das Bundeskriminalamt meldete. Dies ließ sie mich jedoch nicht prüfen, weil sie — falls es so war — die Daten aus Akten und nicht aus Dateien übermittelt hätte, so daß insoweit eine Kontrollbefugnis meines Amtes nicht besteht. Ich konnte deshalb den beiden Bürgern nur raten, beim Landes- und beim Bundeskriminalamt Auskunft über die über sie gespeicherten Daten zu verlangen, da diese Ämter aufgrund von Verwaltungsvorschriften aus dem Jahre 1981 gehalten sind, den Bürgern nicht nur über etwaige Datenspeicherungen in Dateien, sondern auch über einschlägige Informationen aus Akten Auskunft zu geben. Ob die beiden Bürger meinen Rat befolgten und ob sie dann auch Auskunft erhielten, wozu das geltende Recht nicht verpflichtet, weiß ich nicht. Unabhängig davon zeigt aber der Vorgang einmal mehr, wie unbefriedigend die seit 1982 geltende Regelung über meine Kontrollbefugnis für den Bürger ist: ihm wird auf diese Weise eine umfassende Prüfung der Rechtmäßigkeit von Datenspeicherungen bei der Polizei durch mich vorenthalten.

5. Beschlagnahme einer Adreßkartei

Die negativen Folgen dieser Regelung zeigt auch eine weitere Begebenheit: Im April 1985 wurde ich mit Eingaben von Verbänden und Bürgern förmlich überschwemmt. Die Karlsruher Polizei hatte — wie auch in der Presse zu lesen war — im Rahmen eines Ermittlungsverfahrens auf Anordnung des Amtsgerichts Koblenz bei der Deutschen Friedensgesellschaft —

Vereinigte Kriegsdienstgegner (DFG-VK) — eine Hausdurchsuchung durchgeführt und die Abonnentenkartei der „Südwest-Kontakte", des Mitteilungsblattes der DFG-VK beschlagnahmt. Die Bezieher der Südwest-Kontakte, gegen die kein Tatverdacht bestand, bezweifelten die Rechtmäßigkeit der Beschlagnahme; auch fürchteten sie, nunmehr in Unterlagen der Polizei und des Verfassungsschutzes registriert zu sein. Sie baten mich deshalb, beides zu überprüfen. Zur Beschlagnahme mußte ich ihnen sagen, daß nach geltendem Recht allein die Justiz deren Rechtmäßigkeit in dem dafür vorgesehenen Verfahren zu beurteilen hat. Im übrigen führten meine Nachforschungen zu der Feststellung, daß die Abonnenten der Südwest-Kontakte nicht in ihren Rechten nach dem Landesdatenschutzgesetz verletzt sind. Deren Daten sind insbesondere nicht — wie auch der Antwort der Landesregierung vom 3. Mai 1985 auf die Mündliche Anfrage eines Abgeordneten zu entnehmen war — in einer Datei der Polizei erfaßt. Sie schildert die Sache vielmehr so: die Polizei habe nach dem Zufallsprinzip 22 Adressen aus der Adressenkartei photokopiert und diese zu den Akten des Ermittlungsverfahrens, das gegen andere Personen geführt wird, genommen. Daß die Polizei so und nicht anders verfuhr — beispielsweise Akten über die einzelnen Bezieher der „Südwest-Kontakte" anlegte —, konnte ich allerdings nicht nachprüfen, weil mir — wie gesagt — seit der Änderung des Landesdatenschutzgesetzes im Sommer 1982 die Kontrolle der Datenverarbeitung in Akten verwehrt ist.

6. Die Bewerbung beim Konsulat

Eine Englischstudentin wurde mißtrauisch, als das amerikanische Generalkonsulat in Stuttgart ihre Bewerbung um eine Aushilfsstelle mit der Begründung ablehnte, sie sei nicht ausreichend qualifiziert, obwohl es ihr kurz zuvor noch eine mündliche Einstellungszusage erteilt hatte. Sie glaubte, den Grund darin zu erkennen, daß die Staatsanwaltschaft Stuttgart 1981 gegen sie wegen eines Vergehens nach dem Betäubungsmittelgesetz ermittelt hatte. Das Verfahren habe sie freilich nach kurzer Zeit eingestellt, weil kein Tatverdacht gegen sie bestand. Vermutlich seien ihre Daten jedoch noch gespeichert und im Zusammenhang mit der Bewerbung oder schon vorher an amerikanische Stellen übermittelt worden. Meine Nachforschungen ergaben, daß 1981 das Zollfahndungsamt Stuttgart gegen die Frau wegen eines Betäubungsmitteldelikts ermittelt hatte. Das Landeskriminalamt, das hiervon erfuhr, speicherte daraufhin die Daten der Studentin in der Personenauskunftsdatei, die zum Abruf durch alle Polizeibeamten im Lande bereitsteht, und in der bundesweiten Falldatei Rauschgift, auf die die Zollverwaltung, der Bundesgrenzschutz und die Polizeien des Bundes und der Länder zugreifen können. Die Staatsanwaltschaft Stuttgart stellte das Ermittlungsverfahren jedoch bereits im September 1981 ein. Darüber erhielt — aus welchen Gründen auch immer — das Landeskriminalamt hingegen keine Information. Erst durch meine Anfrage vom Februar 1985 erfuhr es hiervon. Es löschte sodann die Daten, nachdem es den Einstellungsbescheid der Staatsanwaltschaft eingesehen hatte. Keine Anhaltspunkte fand ich dafür, daß Polizeidienststellen des Landes das amerikanische Generalkonsulat über das frühere Ermittlungsverfahren unterrichtet hätten. Das muß allerdings nicht bedeuten, daß der von der Bürgerin vermutete Zusammenhang nicht besteht. Möglich wäre es, nachdem seinerzeit das Zollfahndungsamt Stuttgart die Ermittlungen führte, daß Bun-

desbehörden die Daten an amerikanische Dienststellen weitergaben. Ich riet deshalb der Bürgerin, sich auch an den Bundesbeauftragten für den Datenschutz zu wenden.

7. Schweigepflicht und Suizidversuch

Wer in ein Krankenhaus muß, sollte eigentlich gewiß sein können, daß dessen Mitarbeiter um die Bedeutung der ärztlichen Schweigepflicht wissen und diese auch im persönlichen Gespräch mit Bekannten wahren. Daß dem leider nicht immer so ist, erfuhr ich von jemand — nennen wir ihn Herrn Lukas —, der nach einem Suizidversuch auf die Intensivstation eines Krankenhauses eingeliefert wurde. Wenige Tage nach seiner Entlassung überraschte ihn seine Vermieterin mit der Nachricht, sie wisse von dem Suizidversuch und dem anschließenden Aufenthalt auf der Intensivstation; eine ihr bekannte Mitarbeiterin des Krankenhauses habe ihr dies erzählt, als sie dort jemand besuchte. Leider ließ sich trotz intensiver Bemühungen nicht mehr feststellen, wer die ärztliche Schweigepflicht so gravierend verletzt hat. Wenigstens aber sollte der Vorfall für Krankenhäuser Anlaß sein, verstärkt darauf zu achten, daß man es auch innerhalb des Krankenhauses mit der Schweigepflicht ernster nimmt. Daß bislang hier manches im Argen liegt, läßt sich leider kaum bestreiten.

8. Werbung über alles

Die stolzen Eltern eines Neugeborenen waren äußerst betroffen, als sie eine unbekannte Dame besuchte und ihnen im Auftrag der Volksbank ein Sparbuch überreichte, worin Name, Adresse und Geburtsdatum ihres Kindes eingetragen waren. Die Betroffenheit der Eltern steigerte sich noch, als sie kurze Zeit später auch Werbesendungen einer Kindernahrungsmittelfirma erhielten — glaubten sie doch, sich gerade vor solchen Werbeaktionen ausreichend gesichert zu haben. Weil sie früher jedesmal nach der Geburt eines ihrer älteren Kinder unzählige Werbesendungen erhalten hatten und Vertreterbesuche über sich ergehen lassen mußten, erklärten sie diesmal noch im Kreiskrankenhaus Waiblingen bei der Anmeldung der Geburt ausdrücklich und schriftlich, daß sie mit einer Veröffentlichung der Geburt nicht einverstanden sind. Meine Recherchen in diesem zunächst mysteriös erscheinenden Vorfall ergaben, daß es im Kreiskrankenhaus Waiblingen jedenfalls noch bis Anfang 1985 immer wieder vorkam, daß Mitarbeiter der Verwaltung in Widerspruch zu § 11 LDSG und zur ärztlichen Schweigepflicht Daten über Neugeborene und ihre Eltern ohne deren Wissen zu Werbezwecken weitergaben. Das Kreiskrankenhaus gelobte für die Zukunft Besserung. Erstaunlich und letztlich auch bedrückend bleibt, daß Mitarbeiter eines so großen Kreiskrankenhauses noch im Jahre 1985 offensichtlich nicht das Geringste dabei fanden, Kenntnisse, die sie bei ihrer Arbeit erhalten hatten, Werbung treibenden Firmen zu geben.

9. Der mißtrauische Patient

Manche Bürger haben wenig Zutrauen in die Objektivität ärztlicher Gutachter. Einer beschwerte sich, wie häufig die begutachtenden Ärzte in Rehabilitationsverfahren ärztliche Unterlagen zuziehen, die bei früheren Anlässen angefallen seien. Dies führe dazu, daß der begutachtende Arzt jeweils die Aussagen der früheren Gutachten übernehme und sich kein eigenes Bild mehr von ihm mache. Seine Klage gipfelte in der

Forderung, ich solle alle über ihn vorhandenen ärztlichen Unterlagen einziehen und in Verwahrung nehmen, bis geklärt sei, ob sie tatsächlich auch der Wahrheit entsprächen. Diesen Wunsch konnte ich nicht erfüllen, weil dies nicht meines Amtes ist. Doch konnte ich dem Bürger folgende Tips geben: Er hat durchaus die Möglichkeit, auf die Zuziehung ärztlicher Unterlagen einzuwirken. So darf niemand Unterlagen, die sich noch im Besitz von Ärzten und Krankenhäusern befinden, ohne Einverständnis des Bürgers beiholen. Aber auch dann, wenn ein ärztliches Gutachten schon im Besitz einer Krankenkasse, eines Rentenversicherungsträgers, einer Berufsgenossenschaft oder eines anderen Sozialleistungsträgers ist, darf man es nicht ohne weiteres in einem laufenden Rehabilitationsverfahren zu Rate ziehen. Denn jeder, der will, kann dies durch seinen ausdrücklichen Widerspruch verhindern. Allerdings geht er damit das Risiko ein, die Sachaufklärung erheblich zu erschweren. Dies wiederum kann sein Sozialleistungsträger zum Anlaß nehmen, seinen Antrag allein deshalb abzulehnen — also ein zweischneidiges Schwert.

10. Was Schwerbehinderte hinnehmen müssen

Wen das Versorgungsamt als Schwerbehinderten anerkannt hat, der kann nicht darauf vertrauen, der festgestellte Grad seiner Erwerbsminderung sei damit ein für allemal festgeschrieben. Das Versorgungsamt kann vielmehr unter den Voraussetzungen der §§ 44 ff. des Zehnten Buchs des Sozialgesetzbuchs seine Feststellungen korrigieren. Hat es beispielsweise konkrete Anhaltspunkte, daß sich inzwischen der Grad der Minderung der Erwerbsfähigkeit veränderte, darf es ein Überprüfungsverfahren einleiten. Das kann bei einem Beinamputierten dazu führen, daß es sich bei dessen Arbeitgeber erkundigt, ob der Schwerbehinderte seine Arbeit nur sitzend verrichtet oder auch stehen oder gehen oder gar heben und tragen muß. Dabei muß es in der Regel nicht einmal dem Schwerbehinderten sagen, daß es eine solche Anfrage startet. Anders ist es nur, wenn das Versorgungsamt von Stellen Auskunft will, die nach geltendem Recht eine solche ohne Einverständnis des Schwerbehinderten nicht geben dürfen. Diese Rechtslage versuchte ich einem Schwerbehinderten klarzumachen, der sich bei mir wegen der für ihn und seine Leidensgenossen sicherlich wenig erfreulichen Überprüfungsmöglichkeiten der Versorgungsämter beklagte.

11. Die unterbliebene Adoption

Wer sich bei einem Jugendamt um die Adoption eines Kindes bemüht, muß dabei sehr detaillierte Angaben über seine Lebensumstände machen. Das Jugendamt benötigt diese Informationen, damit es die Adoption in der richtigen Weise vermitteln kann. Was passiert mit solchen Angaben, wenn die Adoptionsbewerber ihre Absicht aufgeben? Können sie dann verlangen, daß diese Angaben gelöscht werden? Mit diesen Fragen konfrontierte mich ein Ehepaar, das den verständlichen Wunsch hatte, daß das Stadtjugendamt Mannheim seine Unterlagen über sie vernichtet, nachdem sie ihren Antrag auf Adoption eines Kindes zurückgenommen hatten. Ich mußte dem Ehepaar sagen, daß es nach derzeitigem Recht einen solchen Rechtsanspruch nur hat, soweit das Jugendamt seine Informationen in einer Datei speichert, nicht aber, wenn es diese „nur" in Akten führt. Erfreulicherweise berief sich das

Stadtjugendamt Mannheim nicht auf diese unbefriedigende, dem Bürger letzlich nicht vermittelbare Rechtslage, sondern war sofort bereit, der Bitte des Ehepaares uneingeschränkt zu entsprechen.

12. Was Väter nichtehelicher Kinder erleben

Jugendämter müssen dafür sorgen, daß die Väter nichtehelicher Kinder Unterhalt bezahlen. Obwohl es für sie gewiß nicht immer einfach ist, an die dazu erforderlichen Informationen zu gelangen, müssen sie gleichwohl die rechtlichen Schranken beachten. Verschiedene Anfragen von Vätern zeigen mir, daß dies nicht immer geschieht. So schickte das Stadtjugendamt Mannheim einem Vater einen Fragebogen mit der Aufforderung zu, auch Name, Geburtsdatum, Geburtsort, Wohnung, berufliche Tätigkeit, Berufsausbildung und Familienstand seiner eigenen Eltern — also der Großeltern des unehelichen Kindes — und Name, Geburtsdatum, Geburtsort und berufliche Tätigkeit der Ehefrau — die mit dem Kind überhaupt nichts zu tun hat — anzugeben. Zugleich wies es den Vater in einem Begleitschreiben darauf hin, er sei aufgrund von § 1605 BGB verpflichtet, diese Auskünfte zu geben. Dieser Hinweis war falsch: § 1605 BGB verpflichtet den Vater eines nichtehelichen Kindes nur zu Auskünften über sein Einkommen und Vermögen, soweit dies zur Feststellung seiner Unterhaltspflicht erforderlich ist. Andere Angaben muß er nicht machen. Das Stadtjugendamt Mannheim änderte inzwischen sein Musterschreiben und versicherte mir, es wolle in Zukunft korrekt über den Umfang der Auskunftspflicht informieren. — Korrekt verfahren will in Zukunft auch das Kreisjugendamt Friedrichshafen, das für seine Anfragen beim Arbeitgeber des Vaters des nichtehelichen Kindes eine Verdienstbescheinigung mit demselben Formular anforderte, das auch das Sozialamt für solche Auskünfte verwendet, und dadurch den irreführenden Eindruck erweckte, der Arbeitgeber müsse die gewünschten Angaben machen. Denn in diesem Formular heißt es, der Arbeitgeber sei aufgrund von § 116 des Bundessozialhilfegesetzes zur Auskunft verpflichtet. In Wirklichkeit besteht eine solche Auskunftspflicht aber nur bei Anfragen des Sozialamtes, nicht aber des Jugendamts als Amtspfleger eines nichtehelichen Kindes. Hier ist es vielmehr dem Arbeitgeber überlassen, ob er antworten will oder nicht. Noch ein weiteres bedachte das Kreisjugendamt Friedrichshafen nicht: es hätte die Verdienstbescheinigung beim Arbeitgeber erst anfordern dürfen, nachdem der Vater des nichtehelichen Kindes die ihm gesetzte Frist, eine Verdienstbescheinigung beizubringen, ungenutzt verstreichen ließ.

13. Weitergabe von Elternlisten

Manche Kindergärten haben ihre liebe Not mit dem Datenschutz, weil sie immer noch nicht wissen, wann und wem sie die Adressen der Eltern ihrer Kinder weitergeben dürfen. Elternbeiräte und ihre Vorsitzenden können sie ohne weiteres erhalten. Denn sie haben nach dem Kindergartengesetz die Aufgabe, den Kontakt zum Elternhaus herzustellen. Dies aber können sie nur tun, wenn sie wissen, wer die Eltern sind und wo sie wohnen. Der Datenschutz steht also dem Wunsch der Elternbeiräte, die Adressen zu erhalten, nicht im Wege. Nicht ganz so einfach liegen die Dinge, wenn andere Personen Namen und Adressen der Eltern der Kindergartenkinder erfah-

ren wollen. Solchen Ansinnen darf der Kindergarten nur entsprechen, wenn die anfragende Person ein berechtigtes Interesse an diesen Informationen hat und schutzwürdige Belange der Eltern der Kinder nicht beeinträchtigt werden. Ob dem so ist oder nicht, muß der Kindergarten in jedem Einzelfall aufs Neue entscheiden. Dabei darf er nicht übersehen, daß man aus Adressenlisten mehr als die Anschrift herauslesen kann. Ein Vater gab mir dazu ein gutes Beispiel: Er konnte der vom Kindergarten seines Sohnes verteilten Adressenliste genau entnehmen, welche Eltern getrennt leben, wer „nur" Stiefvater war, welches Kind nur von der Mutter erzogen wurde und einiges mehr. Dies wird oft viel zu wenig bedacht. Dabei könnten Kindergärten solch unerwünschte Begleiterscheinungen oft schon vermeiden, wenn sie beim Elternabend eine Liste mit der Bitte herumreichen, sich einzutragen, wenn man gegen eine Weitergabe seiner Adresse an die anderen Eltern der Kindergartenkinder nichts einzuwenden hat.

14. Beurteilung von Schulanfängern durch die Hintertür

Um Kindern den Schulanfang so leicht wie möglich zu machen, hospitieren Grundschullehrer immer wieder an Kindergärten. So weit, recht und gut. Bloß was, wenn solche Informationsbesuche zu einer Schulreifebeurteilung hinter dem Rükken der Eltern umfunktioniert werden? Ein solches Ansinnen stellte ein Mentor an einen ihm zur Ausbildung zugewiesenen Lehrer. Dieser sollte während seines Besuchs im Kindergarten den Entwicklungszustand der kommenden Schulanfänger feststellen und seine Beobachtungen über die einzelnen Kinder der Grundschule mitteilen, damit sie diese Informationen in ihrer Kartei vermerkt. Ein solches Vorgehen verbietet der Datenschutz; es wäre nur mit Einwilligung der zuvor genau informierten Eltern über Sinn und Zweck der Beurteilung möglich. Selbst dann besteht aber noch die Gefahr, daß manche Eltern bloß deshalb ja sagen, um sich nicht von vornherein das Wohlwollen des zukünfigen Lehrers ihres Kindes zu verscherzen. Ich meine, in eine solch schwierige Situation sollte man Eltern gar nicht erst bringen. Wohl besser wäre, auf vorgezogene Schultauglichkeitsbeurteilungen ganz zu verzichten und es bei der im Schulgesetz vorgesehenen Eignungsprüfung zu Beginn des ersten Schuljahres zu belassen.

15. Von Häsle, Fröschle und Herrn Specht

Wer es als Schüler besonders schlimm getrieben hat, dem kann passieren, daß seine Untaten noch Jahre später Lehramtsanwärtern während der Klausur in pädagogischer Psychologie Kopfzerbrechen bereiten. So war es am Freiburger Seminar für Schulpädagogik. Einer seiner Professoren schilderte in einem Prüfungsfall ausführlich einen Schüler, der ihm Jahre zuvor arg zugesetzt hatte. Der Klausurname ließ einen — wenig erfolgreichen — Kandidaten Schlimmes befürchten. Er glaubte, damit den einstigen Umtreiber ausfindig machen zu können, und sah dessen Persönlichkeitsrechte verletzt. Richtig ist: Prüfungsfälle aus der Praxis müssen so gefaßt sein, daß eine Identifizierung der Personen nicht möglich ist. Unser Schüler hörte auf Häsle — ein bei Pädagogen ebenso beliebter Phantasiename wie Fröschle oder Specht. Aber auch wer wirklich so heißt und im Rückblick auf seine Schulzeit meint, manches aus jener Zeit sei klausurgeeignet, kann gleichwohl

unbesorgt sein. Denn mir versicherte das Freiburger Studienseminar, bei solchen Namen handle es sich um für Prüfungszwecke besonders „einprägsame Tier-Charakter-Bilder". Wer wollte dies schon bezweifeln?

16. Reisekostenabrechnungen von Beratungslehrern

Reisekostenabrechnungen nimmt die Verwaltung sehr genau. Man kann die Kontrolle des sparsamen Umgangs mit Haushaltsmitteln aber auch zum Schaden des Persönlichkeitsrechts übertreiben. Ein Sonderschullehrer gab mir dazu einen interessanten Hinweis: Eltern von Kindern, die schon in den ersten Lebensjahren Anzeichen einer möglichen Behinderung erkennen lassen, können sich an die Frühberatungsstellen der Sonderschulen wenden. Sinn macht dies freilich nur, wenn den Beratungslehrern dann gelingt, das volle Vertrauen der Eltern zu gewinnen. Oft ist dazu nötig, daß sie die Familien auch zu Hause aufsuchen. Einem Beratungslehrer, der dies tat, stellte sich ein unerwartetes Hindernis in den Weg: sein Staatliches Schulamt, bei dem er seine Reisekostenabrechnung einzureichen hatte, wies ihn an, er solle künftig nicht nur das Ziel der Reise, sondern stets auch in Spalte 19 des Reisekostenvordrucks R 17 den Namen des jeweils besuchten Kindes eintragen. Das bereitete dem Beratungslehrer Kopfzerbrechen, weil auf diese Weise nicht nur sein Chef, sondern auch das Staatliche Schulamt und die Landesoberkasse jeweils den vertraulich zu behandelnden Namen des Kindes erfahren würden. Ich sah dies auch so und wandte mich an das Oberschulamt Freiburg. Es pflichtete mir bei, daß außer dem Beratungslehrer bloß noch dessen Chef — also der Leiter der Beratungsstelle — die Namen der besuchten Familien kennen müsse. „Spalte 19" im Reisekostenabrechnungsformular bleibt deshalb wieder leer.

17. Wenn Ehrungen peinlich werden

Wen ein Vorgesetzter mit lobenden Worten in den Ruhestand verabschiedet, freut sich meist darüber. Wenn aber der Redner dabei aus den Personalakten zitiert und der versammelten Zuhörerschaft persönlichen und beruflichen Werdegang bis hin zur Herkunft und politischen Betätigung und vielem anderen offenlegt, dann kann es sein, daß er damit dem Geehrten die Freude an der Abschiedsfeier verdirbt. So jedenfalls ging es einem Lehrer, der mich fragte, ob solche Abschiedsreden eigentlich mit dem Personalaktengeheimnis vereinbar seien. Natürlich gilt auch hier, was sonst Rechtens ist: Grundsätzlich muß der Mitarbeiter mit der Weitergabe von Informationen aus seiner Personalakte an die Öffentlichkeit einverstanden sein. Freilich meine ich nicht, daß man bei Ehrungen eine ausdrückliche Einwilligung fordern kann. Viele, die geehrt werden sollen, würden nicht schlecht staunen, wenn ihnen ihre Personalbehörde zuvor die Laudatio zur Billigung vorlegen würde. Nur wenn für diese erkennbar ist, daß sich bestimmte Informationen aus der Personalakte nicht für eine Rede in der Öffentlichkeit eignen, weil sie dem zu Ehrenden zu nahetreten oder ihn bloßstellen oder gar verletzen könnten, dann darf sie dieses Wissen nicht verwenden. Auch ist ihr verwehrt, in eine Abschiedsrede an sich harmlose Informationen aus der Personalakte einfließen zu lassen, wenn der zu Ehrende zuvor bat, seine Lebensumstände nicht anzusprechen.

18. Der kopierte Personalausweis

Wer sein Auto zulassen will, weiß, daß er dabei eine Reihe persönlicher Angaben machen und deren Richtigkeit durch Vorlage seines Personalausweises nachweisen muß. Ein Bürger, der dies alles korrekt erledigt hatte, konnte nicht verstehen, warum die Führerscheinstelle der Stadt Karlsruhe gleichwohl noch seinen Personalausweis photokopierte und die Photokopie zu ihren Unterlagen nahm. Ich stellte fest, daß diese Führerscheinstelle seit ihrem Verzicht auf schriftliche Zulassungsanträge immer dann so verfuhr, wenn die antragstellenden Bürger ihre Ausweise vor dem Abholen der Fahrzeugpapiere benötigten, sie aus grundsätzlichen Erwägungen bis dahin nicht aus der Hand geben wollten, vor der Aushändigung der Fahrzeugpapiere noch eine Hauptuntersuchung durch den TUV erfolgen mußte oder noch ein Sachverständigengutachten beizubringen war. Ich mußte der Stadt Karlsruhe sagen, daß eine solche Verfahrensweise nicht Rechtens ist. Denn eine Photokopie eines Personalausweises enthält einige Angaben mehr — beispielsweise Größe, Farbe der Augen, unveränderliche Kennzeichen, das Lichtbild und die Personalausweisnummer — als sie jeder, der sein Auto zulassen will, aufgrund von § 23 der Straßenverkehrszulassungsordnung gegenüber der Zulassungsstelle nachweisen muß. Eine Führerscheinstelle darf deshalb einen Personalausweis nur photokopieren, wenn sie dem Inhaber zunächst erklärt hat, warum sie dies tun will und wohin die Photokopie kommt, und der Ausweisinhaber ausdrücklich damit einverstanden ist. Die Stadt Karlsruhe änderte inzwischen ihre Praxis: ihre Führerscheinstelle fertigt jetzt grundsätzlich keine Kopien von Personalausweisen mehr an.

19. Was im Grundbuchauszug alles stehen kann

Wie sehr das Grundbuchrecht in manchem vom alllgemeinen Datenschutzrecht abweicht, macht folgende Begebenheit deutlich: Um sein Haus beleihen zu können, beantragte ein Bürger einen Grundbuchauszug beim Grundbuchamt. Er erhielt ihn auch in Form einer Photokopie. Was ihn jedoch überraschte, war, daß darin auch eine in den Jahren 1964 bis 1969 angeordnete Zwangsversteigerung des Hauses vermerkt war — wenn auch versehen mit einem Löschungsvermerk. Der Bürger befürchtete nun, seine Bank werde ihm deswegen den beantragten Kredit verweigern, und bat deshalb das Grundbuchamt, ihm einen maschinenschriftlichen Grundbuchauszug auszuhändigen, in dem die gelöschten Eintragungen über die Zwangsversteigerung fehlen. Dieser Bitte entsprach das Grundbuchamt nicht. Der Bürger wandte sich deswegen an mich. Ich mußte ihm sagen, daß er keinen Rechtsanspruch auf eine maschinenschriftliche Grundbuchabschrift hat, sondern das Grundbuchamt den Grundbuchauszug als Abschrift oder als Photokopie herstellen darf. Wählt es die Photokopie, gibt diese — zwangsläufig — den Inhalt des Grundbuchs vollständig wieder; dazu gehören auch „gelöschte" Eintragungen. Denn anders als im allgemeinen Datenschutzrecht bedeutet Löschen im grundbuchrechtlichen Sinne nicht Unkenntlichmachung der Eintragung. Sie ist lediglich rot zu unterstreichen und damit noch in der Photokopie zu lesen. Anders ist es hingegen, wenn das Grundbuchamt eine Grundbuchabschrift fertigt. Dann braucht es gelöschte Einragungen nur mit einer laufenden Nummer und dem Vermerk „gelöscht" aufzunehmen. Das hat jedoch keine Datenschutzgründe, sondern bezweckt allein, dem Grundbuchamt Arbeit zu ersparen. Das wird schon daran deutlich, daß man aus dem Hinweis auf die Löschung ersehen

kann, daß das Grundbuch an dieser Stelle Eintragungen enthält. Wer eine solche Abschrift in Händen hat, kann, falls es ihn interessiert und er gegenüber dem Grundbuchamt ein berechtigtes Interesse darlegt, den Inhalt der gelöschten Eintragung durch Einsichtnahme in das Grundbuch erfahren. So betrachtet ist der Vorteil einer Abschrift gegenüber einer Photokopie eher vordergründig. Gleichwohl empfahl ich dem Bürger für den Fall, daß ihm nach wie vor an einer Abschrift lag, es noch einmal beim Grundbuchamt zu versuchen. Schließlich weiß ich von anderen Grundbuchämtern, daß sie im Einzelfall sehr wohl noch maschinenschriftliche Abschriften ausstellen.

20. Besuch in der Strafanstalt

Ein Gefangener wandte sich wegen der Besuchsregelung „seiner" Vollzugsanstalt Mannheim vom 18. Januar 1985 an mich. Sie sah vor, daß Besuche nur noch nach vorheriger Terminvereinbarung stattfinden können und legte dazu im einzelnen fest: Der Gefangene, der Besuch begehrte, mußte diesen per Rapportzettel bei der Besuchsabteilung anmelden und seinen Terminwunsch und möglichst zwei Ausweichtermine angeben. Außerdem mußte er Namen und Anschrift des Besuchers mitteilen. Darüber hinaus sollten alle Gefangenen vorab der Vollzugsdienstleitung „zur schnelleren Besuchsabwicklung" all die Personen, die sie möglicherweise einmal besuchen — ihre „Bezugspersonen" — nennen, damit die Vollzugsanstalt diese in ihre Besuchskartei eintragen kann. Der Gefangene mutmaßte nun, die Pflicht zur vorherigen Angabe des konkreten und der möglichen Besucher diene allein dem Zweck, diese vor ihrem Besuch anhand polizeilicher Informationssysteme eingehend zu überprüfen, — ja womöglich gar, sie darin zu erfassen. Auf meine Nachfrage hin stellte die Vollzugsanstalt Mannheim dies entschieden in Abrede. Sie wollte mit der neuen Besuchsregelung den Gefangenen lediglich eine längere Besuchsdauer ermöglichen. Dazu müsse man wissen, daß ihr allein ein Besuchsraum mit beschränkter Aufnahmekapazität zur Verfügung stehe. Dieser sei in der Vergangenheit zu bestimmten Zeiten regelmäßig überbelegt gewesen, weshalb sie den Besuchern lange Wartezeiten hätten zumuten müssen. Zu anderen Zeiten hingegen sei der Besuchsraum nicht genutzt worden. Dies wolle sie mit der Neuregelung besser steuern und dadurch zugleich die Besuchsdauer pro Gefangenen von einer auf zwei Stunden erhöhen. Die vorherige Nennung der Besucher und Bezugspersonen ermögliche es, diese vor ihrem Besuch anhand einer von der Vollzugsanstalt geführten Besuchsausschlußliste zu überprüfen, in der — wie schon der Name sage — die Personen erfaßt seien, die von einem Besuch wegen einer früheren Störung der Sicherheit und Ordnung in der Anstalt ausgeschlossen seien. Diese Vorabprüfung habe den Vorteil, daß die künftigen Besucher in der Besuchskartei gegebenenfalls mit dem Vermerk „unbedenklich" eingetragen werden könnten, so daß im Falle ihres Besuches die Besuchsausschlußliste nicht mehr zur Hand genommen werden müsse. Trotz möglicher Vorteile mußte ich gegen diese Neuregelung datenschutzrechtliche Bedenken beim Justizministerium anmelden:

— Sie gründeten sich in erster Linie darauf, daß der Gefangene, so er Besuch erhalten wollte, gezwungen war, Namen und Anschrift des Besuchers anzugeben. Eine (quasi) zwangsweise Datenerhebung aber ist nach dem Volkszählungsurteil des Bundesverfassungsgerichts nur zulässig.

wenn es dafür eine präzise bereichsspezifische Rechtsgrundlage gibt. Eine solche aber enthält das Strafvollzugsgesetz nicht.

— Problematisch war auch, daß der Gefangene vorab seine Bezugsperson angeben soll. Gezwungen werden konnte er hierzu aus den vorgenannten Gründen nicht. Allerdings war zweifelhaft, ob die Anordnung des Anstaltsleiters so zu verstehen war oder ob dem Gefangenen eine solche Verfahrensweise freigestellt werden sollte.

— Bedenklich war schließlich, daß die Namen der Bezugspersonen der Gefangenen in der Besucherkartei gespeichert werden sollten, ohne daß feststand, daß sie den Gefangenen besuchen wollen. Da dies auf eine nach dem Volkszählungsurteil unzulässige, auch in der Vollzugsgeschäftsordnung nicht vorgesehene Datenvorratsspeicherung hinauslief, bat ich, hierauf zu verzichten.

Das Justizministerium trug meinen Bedenken Rechnung. Zwar soll der Gefangene auch in Zukunft den Besuchstermin mit der Vollzugsanstalt absprechen. Sofern er dazu jedoch nicht bereit oder in der Lage ist, soll er — und zwar ohne Darlegung von Gründen — auch unangemeldeten Besuch empfangen können. In diesem Fall wird die monatliche Besuchszeit allerdings von 2 auf 1½ Stunden verkürzt. Aus der Sicht des Datenschutzes wesentlicher ist, daß auf die vorzeitige Namensangabe der Bezugspersonen und Besucher sowie deren vorzeitige Erfassung in der Besucherkartei verzichtet wurde.

21. Der benachteiligte Gläubiger

Immer wieder wenden sich empörte Gläubiger an mich, weil ihnen Krankenkassen, Arbeitsämter, Landesversicherungsanstalten und andere Sozialleistungsträger nicht sagen, ob ihr Schuldner von ihnen Leistungen zu beanspruchen hat. Diese Empörung mag bis zu einem gewissen Grad verständlich sein; sie verkennt jedoch die konkrete Rechtslage. So war es auch bei einem Inkassobüro, das von der Landesversicherungsanstalt Württemberg wissen wollte, ob seinem Schuldner aus den bezahlten Sozialversicherungsbeiträgen Rückerstattungsansprüche zustehen. Die Landesversicherungsanstalt hielt sich an die Regeln des Sozialgesetzbuchs und antwortete nicht. Dies bedeutet freilich nicht, daß das Inkassobüro überhaupt keine Möglichkeit hätte, auf etwaige Leistungen der Landesversicherungsanstalt zuzugreifen. Notwendig dafür wäre, daß es den Weg zum Vollstreckungsgericht einschlägt, einen Vollstreckungstitel erwirkt und dann die Pfändung seiner rechtskräftig festgestellten Forderung bei der Landesversicherungsanstalt in die Wege leitet. Im Rahmen einer solchen Forderungspfändung ist die Landesversicherungsanstalt dann auch befugt zu sagen, ob der Schuldner tatsächlich eine pfändbare Sozialleistung erhält. Ich meine, diese Rechtslage bringt den angemessenen Ausgleich zwischen den unterschiedlichen Interessen von Gläubigern und Schuldnern. Den gleichen Weg müssen schon seit langem Gläubiger gehen, die wissen wollen, ob ihr Schuldner einen Erstattungsanspruch gegen die Steuerverwaltung hat. Was zum Schutze des Steuergeheimnisses recht ist, sollte auch für den Schutz des Sozialgeheimnisses billig sein.

22. Vertrauliches auf Farbbändern

Daß Bürger beim Datenschutz genau hinsehen und auch versteckte Risiken finden, zeigen mir ihre zahlreichen Zuschriften zur Vernichtung von Farbbändern. Wo ist hier der Dollpunkt? Bei vielen modernen Schreibmaschinen und elektronischen Druckern verwendet man spezielle Farbbänder mit einer Farbschicht auf Plastikfolie. Von der Plastikfolie dieser nur einmal zu beschreibenden Farbbänder läßt sich nachher noch leicht der geschriebene Text ablesen. Was also, wenn er Informationen über Personen enthält oder sonst Vertrauliches? Daß keine Lösung ist, die Bänder einfach in den Müll zu werfen, sah eine Stadträtin und erkundigte sich deshalb nach einer besseren Methode. Ich riet, den Transport zur Müllverbrennungsanlage nicht zu scheuen, und wies zugleich noch auf die Methode eines findigen und sparsamen Hausmeisters hin, mit seinem eigenen Handwerkszeug solche Bänder vollständig zu zerstören. Als die Stadträtin diese Antwort öffentlich bekanntgab, erschienen in mehreren Zeitungen humorvolle Kommentare, die den Sekretärinnen — quasi als Datenschutzausrüstung — Hammer und Säge nahelegten. Das wiederum rief die Bürofachgeschäfte auf den Plan: sie geißelten solch antiquierte Vernichtungsmethode und rieten statt dessen zum Kauf ihrer speziellen Geräte zur Farbbandvernichtung. Eines propagierte gar die Idee, für Schreibmaschinen und Drucker Zusatzgeräte einzusetzen, die in zufälliger Folge auf dem Farbband weitere Buchstaben zur Tarnung des geschriebenen Textes abdrucken.

Schlußbemerkung

Mein Rückblick auf das Jahr 1985 fällt zwiespältig aus. Zum einen gilt: die sorgfältige und konsequente Arbeit meines Amtes trug vielerorts ihre Früchte. Die Bürger schätzen sie seit eh und je und immer mehr auch die Behörden; in der Politik ist unser Rat je nach Einstellung zum Datenschutz gefragt oder eine Last. Zum andern gilt: 1985 zeichneten sich neue Bedrohungen des Datenschutzes ab. Die Verwaltung von Baden-Württemberg soll mit High Tech ein Wegbereiter der Informationsgesellschaft sein. Dabei lassen die Befürworter dieses Kurses bislang die notwendige Sensibilität für die damit einhergehenden Gefährdungen unseres persönlichen Freiraums vermissen. Ihnen sei nochmals gesagt: die Technik muß sich an der Verfassung orientieren und darf nicht dem Grundgesetz zuwiderlaufende autonome Ziele verfolgen. Nicht genug damit: auch sind Zweifel an der Bereitschaft der Verantwortlichen angebracht, ein wirksames Datenschutzrecht zu schaffen und eine effektive Datenschutzkontrolle sicherzustellen. Dies alles macht mir Sorge. Ich wünsche, daß mein Bericht zum Nachdenken anregt und beiträgt, festgefahrene Positionen zu überdenken. Wenn er zugleich hilft, die Risiken der modernen Informationstechnik in voller Tragweite zu sehen, und die Bereitschaft fördert, dagegen ernsthaft anzutreten, wäre auf dem Weg zu einem zeitgemäßen Datenschutz schon manches gewonnen.